The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

Jane Hyatt Thorpe, JD
Lara Cartwright-Smith, JD, MPH
Elizabeth Gray, JD, MHA
Marie Mongeon, MPH(c)

The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

September 28, 2017

TABLE OF CONTENTS

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

CHAPTER 1:

OVERVIEW OF LEGAL AND ETHICAL ARCHITECTURE FOR PCOR DATA

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Chapter 1

Overview of Legal and Ethical Architecture for PCOR Data

INTRODUCTION

The American healthcare system is experiencing an information revolution, rapidly approaching an age in which all patient records and related information will be maintained and accessed electronically. Volumes of data on a scale only recently imaginable are passing between individuals and institutions and are used in ways we could not predict. This "data revolution" is occurring as the U.S. healthcare delivery system undergoes a major transformation to become a more robust, evidence-based endeavor that is highly reliant on healthcare data for purposes ranging from real-time care delivery and coordination to research.

At the same time, access to, use of, and release of health information, particularly individually identifiable health information, is highly regulated at both the federal and state levels. Now more than ever, the law places real as well as perceived barriers and burdens on the collection and use of health information. Important privacy and security issues arise in relation to the use of health information for research, new payment and care delivery structures, and new expectations for patient safety, high-quality care, and patient engagement in their own healthcare.

These issues are particularly relevant to the expanding field of health-related research, which provides the evidence base necessary to transform the U.S. healthcare delivery system. In this dynamic environment of expanding data availability and greater technological capacity, patients and providers may access or have presented to them more health information than heretofore imagined. While the potential benefits of such information are significant, with more data come more complex legal and ethical issues. This is particularly true in the field of patient-centered outcomes research (PCOR) that requires patient-level data to improve health outcomes for individual patients as well as to provide evidence that will benefit other patients and providers. The Patient-Centered Outcomes Research Institute (PCORI) is leading efforts to identify research questions, fund patient-centered comparative effectiveness research (CER), and better disseminate findings to patients, providers, and other end users. PCORI's work is to determine through PCOR, a type of CER, which of the many healthcare options available to patients and those who care for them work best in particular circumstances.

Crucial to PCOR-related efforts is an infrastructure that ensures all parties understand the applicable legal requirements and ethical considerations when an individual's data is accessed or used for PCOR. The incorporation of patient-level data into PCOR requires balancing both the need for sufficient information granularity to allow for meaningful research protocols and conclusions with the heightened need to protect patient privacy. An architecture is necessary to ensure patient privacy is protected and health information is appropriately secured during collection, access, use, and disclosure as required by law, regulation, and/or policy. In addition, the architecture must support a culture of trust that promotes ongoing patient participation in all forms of research-related data collection, including clinical trials, survey data collection, and re-use of routinely collected data.

The PCOR Privacy and Security Research Scenario Initiative and Legal Analysis and Ethics Framework Development project, funded by the U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC), supported the development of a legal

and ethical architecture to enable robust PCOR while providing sufficient assurance to stakeholders that data used for PCOR and CER will be protected and secured as required by applicable laws and regulations. The final project product, this Legal and Ethical Architecture for PCOR Data ("Architecture"), is a collection of tools and resources designed to:

1. Provide a common structure and model of legal analysis of legal requirements and ethical considerations and responsibilities in research, particularly PCOR;
2. Support PCOR and CER through illustrative pathways for collecting and sharing data for research in compliance with relevant federal laws and regulations and in consideration of state law; and
3. Support a culture of trust between and among stakeholders through the application of meaningful and appropriate privacy and security parameters.

The creation of a legal and ethical architecture for PCOR and CER is a multifaceted task that must occur in a dynamic and evolving environment. Historically, health information was collected primarily during a patient/physician encounter and stored in a paper medical record at the physician's office. Administrative claims data were received and stored by relevant payers (e.g., health plans). Now, however, information is collected in a vast array of environments well beyond clinical and payment settings, including patient-generated health data captured in wearable technologies and personal health records. Furthermore, registries and health information exchanges also capture vast amounts of health information, whether required by law or through voluntary consumer participation. Finally, technology has advanced, enabling health information from different sources to be collected and aggregated virtually instantly and combined with other types of data as well. The legal framework has changed as well, largely in an attempt to better align the various legal requirements that apply to the use of patient data for research (discussed in further detail throughout the Architecture as well as in Appendix A: Summary of Statutes and Regulations Relevant to PCOR). For example, during the development of this Architecture, material changes were made to the Common Rule (governing human subjects research) and 42 C.F.R. Part 2 (confidentiality requirements governing federally supported substance use disorder programs). Researchers and other stakeholders should always monitor proposed and final changes in the legal framework as well as related guidance. The Architecture reflects the state of the legal framework as of September 2017.

The focus of this Architecture is enabling researchers to obtain data for PCOR while protecting the privacy of the individuals whose data are used. This Architecture and component parts are technology-neutral and do not address or recommend any particular technical standards for a health information technology (IT) system. Nor does the Architecture provide legal advice or a single path that can be followed to comply with all requirements. Rather, the Architecture gives an overview of the legal requirements that relate to data use, sharing, and disclosure for PCOR and provides tools to help researchers and others identify issues and navigate requirements. Each research project and specific data use is different and will require individualized analysis, of course, and the Architecture can guide and support that analysis. The goal of this project is to help researchers identify and overcome real and perceived barriers to obtaining data, combining data, and using data in a meaningful way that will yield better understanding of patient outcomes to support future policy decisions.

BACKGROUND

Concerns regarding health care quality, patient safety, and escalating healthcare costs have led to increasing demands to understand what works in healthcare and ensure that the right patient receives

the right care every time. There is thus a great need for PCOR to support better decision-making by patients and providers, as well as a more effective healthcare delivery system in general. Access to health information, particularly individually identifiable health information, is critical to PCOR and CER so that individuals can be followed over time and across settings to understand outcomes. This type of research is often hampered by real or perceived barriers that impede access to identifiable and other forms of health information. For example, health information needed for PCOR and CER is often held by different stakeholders across multiple sites, requiring researchers to interact with and align multiple sources of data. Researchers also often cite challenges associated with navigating the complex web of federal and state laws and regulations that govern health information.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules provide a federal floor related to the disclosure and protection of health information by and among specific stakeholders, including providers and payers. Because this is the most widely referenced legal framework related to health information, this project will use the HIPAA definition of "health information" as follows:

"Health information" is information (including demographic data) that relates to:

- the individual's past, present, or future physical or mental health or condition;
- the provision of health care to the individual; or
- the past, present, or future payment for the provision of health care to the individual.[1]

However, with the increasing availability and variety of data that relate to an individual's health and the different types of organizations and applications collecting information, that definition is becoming increasingly muddied. This has led to a challenging dynamic between HIPAA Regulated Entities and non-regulated entities that may create or collect the same types of data even if used for different purposes.

Furthermore, HIPAA is not the only legal framework that governs health information. For example, the Common Rule governs federally supported human subject research of all purposes (including health-related research). Health information also may be subject to a myriad of other federal and state laws that often overlap and may appear to be or even are contradictory. Furthermore, some types of health information as well as some types of individuals are subject to additional protections under federal and state law (e.g., substance abuse information, minors). This complex legal environment is challenging for stakeholders, including researchers, providers, consumers, payers, and health information organizations, to be certain of the legal requirements that govern the health information they hold or acquire and their use and/or disclosure of that information. The uncertainty may stifle innovation and/or inhibit perfectly legitimate uses of health information for PCOR.

In research, a single process may implicate many different obligations under different federal and state laws. A good example of this is patient consent for the disclosure of information (which is a separate issue from consent for treatment or for participation in research). Below is a table illustrating how the various elements of consent map to the different federal laws that impose requirements, depending on the context.

Table 1: Federal Requirements for Consent to Disclose Identifiable Health Information

	HIPAA[2]	Common Rule[3]	GINA[4]	Part 2[5]	Privacy Act[6] (HHS)
Required elements:					
Patient's name				X	
Specific description of information[7]	X	X	X	X	X
Identify person(s) or entity authorized to make the requested disclosure	X			X	
Identify person(s) or entity authorized to receive the requested information	X	X	X	X	X
Describe the intended use(s) of the requested information[8]	X	X	X	X	X
The expiration date or event	X	X		X	
Date signed	X	X		X	
Signature (and/or electronic signature where acceptable) of the individual or his/her personal representative	X	X		X	
Provide the following information:					
The individual's right to withdraw authorization (if any) and any applicable exceptions to that right.	X	X		X	
Whether any benefits may be conditioned on releasing the information and applicable consequences of refusal to consent. This includes stating that refusal will involve no penalty or loss of benefits where relevant.	X	X	X		
The potential for re-disclosure of the information (if any). This includes stating that information may not be re-disclosed without further authorization where applicable.	X	X		X	
Other requirements:					
The authorization must be written in plain language.	X	X			
Provide the individual with a copy of the form.	X	X			

Key Laws for PCOR Research

This Architecture is designed to help stakeholders navigate the legal and ethical landscape for PCOR. At the federal level, statutes and regulations may be organized by their primary focus. For example, some statutes and regulations are specific to the types of health information content they govern; others are specific to certain activities, such as research; and still others are specific to the settings of care where care is delivered.

Content-Specific Statutes and Regulations

These statutes and regulations govern certain specific types of health information that may be used to support PCOR and CER, assuming the relevant requirements are met. For example, the HIPAA regulations govern protected health information. Part 2 of Title 42 of the Code of Federal Regulations (Part 2) governs substance abuse information held by federally assisted programs and the Genetic Information Nondiscrimination Act of 2008 (GINA) governs genetic information used for various purposes. These

statutes and regulations are both permissive and prohibitive in nature, describing to whom and for what purposes these types of information may or may not be disclosed, as well as any other associated requirements. Other content-specific statutes and regulations include: the Patient Safety and Quality Improvement Act (PSQIA— patient safety work product); the Privacy Act of 1974 (individually identifiable information held by a federal agency); and the [federal] Freedom of Information Act (FOIA).

Research-Specific Statutes and Regulations

These statutes and regulations govern the health-related research enterprise, including PCOR and CER if certain requirements are met. For example, the Common Rule governs federally supported human subjects research. Similar to the Common Rule, FDA regulations govern experiments on human subjects involving products, drugs, or devices subject to FDA review and/or approval.

Setting-Specific Statutes and Regulations

These statutes and regulations govern health information that is collected, used, and/or disclosed by certain settings of care. For example, Title 38 of the U.S. Code governs health care delivered to veterans, Section 330 of the Public Health Services Act (PHSA) governs health care delivered in community health centers, and the Family and Education Rights and Privacy Act (FERPA) governs health information included in student education records.

Table 2: Federal Laws: Primary Focus

	Content-Specific	Research-Specific	Setting-Specific
Common Rule Subparts A–E		X	
FDA Research Regulations		X	
FERPA: Federal Educational Rights and Privacy Act			X
GINA: Genetic Information Nondiscrimination Act	X		
HIPAA Administrative Regulations	X		
42 C.F.R. Part 2	X		
Public Health Services Act § 330 Grantees (Community Health Centers)			X
PSQIA: Patient Safety and Quality Information Act	X		
Privacy Act of 1974/Freedom of Information Act (FOIA)	X		
Title X Providers (Family Planning Clinics)			X
Veteran's Administration Confidentiality Regulations (Title 38 USC § 7338)			X

At the state level, statutes and regulations that relate to health information vary greatly. For purposes of this project, the most relevant state statutes and regulations typically govern the privacy of health information for specific populations and specific types of information (e.g., individuals with HIV/AIDs, individuals with mental health conditions, and minors). For these populations, state laws may be more stringent than HIPAA requirements and thus must be followed as they relate to the collection, use, and disclosure of health information for these individuals.

Below are brief descriptions of the most relevant laws or areas of law that may apply to PCOR: HIPAA, the Common Rule (Subparts A-D), 42 C.F.R. Part 2, the Genetic Information Nondiscrimination Act of 2008 (GINA), and state law. For more detailed summaries of these and other relevant laws, see Appendix A.

HIPAA and its enabling regulations (the HIPAA Rules) establish a national framework for the management, transmission, and disclosure of health information. HHS has issued four sets of regulations implementing HIPAA's provisions. These regulations (the HIPAA Rules) govern Covered Entities (health plans, healthcare clearinghouses, and most healthcare providers) and their Business Associates (entities providing certain services or functions to or on behalf of the Covered Entity) and protect individually identifiable health information. The Privacy Rule governs the privacy and confidentiality of such information and lists numerous purposes for which information may be shared, including for treatment, payment, research, and certain public health activities. The Security Rule identifies baseline administrative, physical, and technical safeguards to protect electronic health information that Covered Entities and their Business Associates must implement. The Enforcement Rule sets forth the enforcement system for all the HIPAA Rules, and the Breach Notification Rule establishes a notification and reporting protocol in the event of an unauthorized disclosure.

The **Common Rule** sets forth a variety of requirements to ensure that research participants experience minimal risk to their health, safety, and privacy during and as a result of research. These regulations apply to all research protocols conducted, funded, or otherwise subject to regulation by any of 18 federal departments and agencies. There are four relevant sets of regulations governing research. Subpart A establishes general requirements for Institutional Review Board (IRB) structures, functions, and responsibilities and requirements governing the informed consent process. Subparts B–D add to and/or modify Subpart A requirements for certain types of research. Subpart B governs research involving pregnant women, human fetuses, neonates of uncertain viability, or nonviable neonates. Subpart C governs biomedical and behavioral research where the participants include prisoners. Subpart D governs research involving children as participants. Subpart E governs general administrative issues and has only been adopted by HHS.

42 C.F.R. Part 2 (Part 2) protects the confidentiality of substance use disorder patient records to ensure that such patients are not more vulnerable with respect to their privacy than those who do not seek treatment. This regulation applies to most substance use disorder programs receiving federal assistance, which is broadly defined, as well as recipients of Part 2 program patient records. The regulation prohibits disclosure of information that would identify a patient as having a substance use disorder without written patient consent, with limited exceptions for research, medical emergencies, and audits.

GINA protects individuals' and their family members' genetic information in order to enable individuals to take advantage of genetic testing, technologies, research, and new therapies without fear of discrimination in employment or health insurance. GINA is comprised of two titles. Title I governs most health plans and health insurance issuers and prohibits the use of genetic information to make decisions about covered individuals and, with some exceptions, prohibits requesting or requiring that beneficiaries undergo genetic testing or provide genetic information. Title II governs most private and public employers and prohibits the use of genetic information to discriminate against employees or applicants and from acquiring employee's or applicant's genetic information for most purposes. Both titles contain exceptions that enable disclosure of genetic information for research purposes in certain circumstances.

State laws may be more protective of patients' rights than their federal corollary and often govern data, patients, and/or entities not regulated under existing federal laws. Generally, researchers must comply with the state law provisions that are more protective of privacy or more expansive than federal statutes and regulations in addition to meeting relevant federal requirements. Most states provide enhanced or specific protections for sensitive information (e.g., HIV/AIDS status, mental health information) and vulnerable populations (e.g., minors, legally incompetent adults). States also generally have laws governing state-based registries, mandatory health information reporting (e.g., communicable diseases

or vital statistics), health insurance data collection requirements, data collection by public health entities, and healthcare provider licensure requirements—all of which may contain requirements related to data sharing, confidentiality, and patient consent.

Ethical Considerations

Many ethical principles apply in the field of research involving individuals and their personal information, including the three core principles in medical ethics: beneficence, justice, and respect for persons. These principles are codified in the Belmont Report of 1979. For the purpose of this Architecture, the most significant principle is respect for persons, which encompasses both the principle of individual autonomy and the principle of protection of those with diminished autonomy. This is the basis for the practice of informed consent. The consent process for any medical treatment or participation in research must include sufficient information for the patient or participant to understand the procedure, risks, benefits, alternative courses available, and the fact that they can revoke consent at any time. If the information given to a patient or participant was not understood in a meaningful way, the consent was not informed. Finally, participation in the treatment or research must be voluntary, meaning that the individual is not subject to coercion or undue influence. In some cases, informed consent may be omitted, but only where necessary to conduct the research and where the risk to participants is no more than minimal. In practice, IRBs review research proposals to determine whether informed consent is required and if the proposed practices for a particular research project meet ethical standards.

Ethical issues are likely to arise when considering consent for information sharing, the use of information without the consent of the subjects of the information, information about populations with sensitive conditions or special circumstances, and information thought to be de-identified but that can still be used to identify a particular person. Other relevant considerations include when, how, and whether to share information detailing the outcomes of the research to participants and issues related to disclosure of participant-specific data generated during the course of research to the participant or other parties (e.g., partner notification related to communicable diseases or familial notification related to a genetic anomaly). In many cases, ethical principles have been codified into law, as with the Common Rule's regulations for federally supported research and the HIPAA Privacy Rule's requirement for patient consent for the disclosure of protected health information (PHI) for activities other than those permitted in the Rule, such as treatment, payment, and healthcare operations.

Prior and Related Federal Efforts

In the research context, this complex web of statutes and regulations can create what may seem like insurmountable obstacles to access and use of health information in order to support public and population-based health research as well as PCOR or CER. HHS—specifically, ONC—has led efforts to ensure that privacy and security policies align with the dynamic health IT ecosystem. Since its inception, ONC has focused on developing policy, programs, and initiatives designed to advance the interoperable exchange of electronic health information. These efforts have consistently addressed the important role that privacy and security play in any efforts involving the use, release, and exchange of health information. The 2008 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information laid the groundwork for future efforts to promote transparency while protecting the privacy and security of individually identifiable health information. Efforts such as the Shared Nationwide Interoperability Roadmap[9] and HHS Open Data Initiatives[10] focused on encouraging data-sharing for research and other public benefit. The Federal Health IT Strategic Plan 2015–2020[11] includes several goals that relate to PCOR, including empowering individual,

family, and caregiver health management and engagement and improving healthcare quality, access, and experience through safe, timely, effective, efficient, equitable, and person-centered care. The Strategic Plan also calls for greater collaboration and highlights federal efforts to support PCOR.

Building on these earlier efforts, ONC has several parallel projects underway focusing on greater use of data for PCOR, including this Legal and Ethical Framework for PCOR Data and Architecture, a Legal and Ethical Framework for Public Health Research led by Centers for Disease Control and Prevention (CDC), and the Patient Choice Technical Project, which is focusing on developing technical standards to fulfill the technical capability for individual consent for sharing of health information for both health care and research. The process for the CDC project was similar to this project in that the project team developed scenarios with a multidisciplinary work group and applied legal and ethical analysis to develop a framework for research using public health data. That project's final document, the "Legal and Ethical Framework to Use Centers for Disease Control and Prevention Data for Patient-Centered Outcomes Research," sets forth three data use scenarios, which the CDC workgroup created to highlight unique legal and ethical implications for use of CDC data. CDC collects data for public health purposes, including surveillance of disease, injury, exposure to health threats, and research to address population needs. Secondary use of CDC's existing public health data for PCOR purposes can have a substantial impact on patient and public health through research in areas such as epidemiology, drug safety, outcomes research, vaccines, and health services research.

For more information about related federal offices, guidance, and projects, see Appendix C.

Development of the Architecture

Audience

This Architecture is designed for a broad audience of stakeholders who are engaged in or otherwise support PCOR and CER efforts. The primary audience for this Architecture is the community of researchers engaged in PCOR and CER and related professionals at their institutions, such as Institutional Review Boards, Contracting Officers, Research and Development Officers, Privacy Officers, Compliance Officers, and Internal and External Counsel. The Architecture is also designed to be useful for a wider audience, such as federal and state legislative and regulatory bodies considering legislation, rulemaking, and policy guidance; foundations and other organizations funding research; policy analysts; patient advocates; lawmakers; students; and scholars.

Process

This project was conceived in two phases. In Phase 1, the project team engaged a group of stakeholders in robust discussions of the opportunities and challenges related to research, specifically PCOR. This stakeholder engagement informed the development of a series of 17 research data use scenarios that address a variety of issues ranging from consent, to special populations, to merging clinical and claims data. The stakeholder discussions raised a number of issues and concerns related to the use of various types of data for PCOR and navigating the statutes and regulations that govern the use of this data for PCOR. In Phase 2, building on the lessons learned from the stakeholder discussions, the project team created tools for researchers and other stakeholders to navigate the health information law and policy landscape, culminating in this Architecture.

Phase 1 – Stakeholder Engagement and Research Data Use Scenarios and Use Cases

The project began with the development of a charter to establish a common understanding of the project goals, outcomes, timeline, and scope among the internal team and multidisciplinary stakeholder work group. The goals of the stakeholder discussions included: identifying research data use scenarios that are person-centric and encompass PCOR and CER; identifying necessary policies and requirements to enable data use in research; defining the gaps and needs in policies and ethical and legal requirements; and identifying instances where technical components intersect with policy requirements. The following areas were out of scope: data use scenarios focused on provider or payer operations or on educational records; data "ownership" issues; specific guidance related to IRBs; research and development activities undertaken at private companies; and development of solutions (technical or otherwise), which will be the work of other planned and future initiatives.

Next, the project team and subject matter experts developed research data use scenarios in order to illustrate the interactions between researchers attempting to collect and analyze data for PCOR and CER, and the various entities (e.g., data holders, IRBs), data systems, and requirements (e.g., state and federal laws, privacy policies), as well as highlight any legal and ethical areas of ambiguity or confusion that arise in planning or conducting research. Through an iterative process of group discussion of scenario topics and submission of ideas by stakeholders, internal development by the team, discussion during the multidisciplinary stakeholder work group, and meetings with individual stakeholders interested in the various scenario topics, the scenarios grew more detailed and robust. The scenarios eventually sorted into thematic areas: for example, based on the type of process being performed (e.g., combining data from multiple sources), data type (e.g., sensitive information, patient-generated health data), or research topic (e.g., precision medicine). The thematic areas further clustered under various use cases, which reflect the technical aspects of the scenarios, identifying specific actors, data system workflows, and requirements necessary for data movement (e.g., how the researcher obtains access to the data fueling her study).

While the scenarios and use cases do not represent an exhaustive list of issues that arise within the broad study of PCOR and CER, they represent a set of consensus issues raised as frequent and/or priority concerns by active members of the PCOR community (i.e., the multidisciplinary stakeholder work group). The data use scenarios and use cases that resulted from the stakeholder engagement process of Phase 1 were used by the project team for Phase 2 to identify questions that should be answered, inform the data flows that would be mapped, and guide development of decision tools that would be relevant to stakeholders.

Phase 2 – Legal and Ethical Framework for PCOR; Conceptual Enterprise Architecture

Considering the stakeholder discussions and the research data use scenarios developed in Phase 1, the Phase 2 project team turned to development of resources for stakeholders and analysis of laws that affect the accessibility of data for PCOR. The first step was to map the law and policy landscape by identifying key federal statutes and regulations, as well as relevant federal agencies and initiatives. Then, the team identified core legal and ethical questions and the types of data relevant to PCOR. The answers to certain key questions can help determine the legally relevant characteristics of the data, which in turn will help identify the legal and ethical significance of the different data types used for PCOR and CER. When using data for PCOR, it is critical to understand the data types and characteristics that trigger legal and ethical obligations.

Next, the project team organized the stakeholder concerns, issues, and challenges identified in Phase 1 by type of potential policy gap in order to clarify stakeholder needs and possible policy responses. The purpose of this gaps analysis was twofold: 1) identify areas of confusion for stakeholders that could benefit from treatment in the Architecture or other areas of this project, and 2) distinguish perceived or purely operational barriers to the use of data for PCOR from areas where laws and guidance are unclear or absent (and where ONC or other agencies could provide clarity).

The third activity in Phase 2 involved creating and analyzing representative data flows that may be found in PCOR research and mapping those data flows to legal requirements and key decision points. The scenarios for the data flow mapping were adapted from the research data use scenarios developed through the stakeholder engagement process in Phase 1. The project team also created a general scenario to illustrate where and how the relevant legal requirements arise when data flows through a typical research project.

Next, the project team created a Framework to help stakeholders identify the data characteristics and considerations in their research that will determine what laws apply and what decisions must be made. The Framework presents key questions related to data characteristics that a researcher must address, describes what the key questions mean, explains why they matter, and identifies legal and ethical considerations and activities for PCOR researchers related to each question, including implications for structuring research.

Finally, the team created this Architecture, incorporating the components described above into a comprehensive resource for PCOR researchers and related stakeholders to better understand legal and ethical requirements, identify issues and potential barriers to data use for PCOR, and navigate the legal and ethical considerations that will arise in the planning and execution of PCOR.

How to navigate and use the Architecture

The Architecture is designed as a resource for a variety of stakeholders, particularly researchers who are navigating legal requirements in the design and execution of research, but also individuals at organizations where research is conducted, such as IRB staff and privacy and compliance officers, legal counsel, health policy researchers, advocates, policymakers, research participants, and those who create or collect data that may be used in research. The project team recommends that users review the entire Architecture for a full understanding of the legal and ethical issues and considerations that may arise in the course of PCOR and how to navigate that landscape. For example, a researcher seeking substance use data may find the first data flow map that involves the use of data covered by Part 2 particularly interesting.

The structure of the Architecture consists of chapters serving different purposes that together serve as a comprehensive resource for a researcher or other stakeholder to better understand the legal and ethical issues that arise when accessing data for PCOR. This Chapter, Chapter 1, provides an overview of the key legal and ethical issues relevant to PCOR data, as well an overview of the Architecture and related efforts. Chapter 2 explores fundamental concepts to help stakeholders understand the features of their data. Chapter 2 can help users identify the types of data they are working with and the data issues that may arise in the course of PCOR. Chapter 3 links legal and ethical requirements to PCOR data. Chapter 4 is a visual decision tool that incorporates the fundamental concepts explored in Chapters 2 and 3. Researchers who are not sure what data-related issues may arise in their research should use the Framework in Chapter 4. The Framework serves to examine questions that may need to be asked and

considerations for conducting research in compliance with legal and ethical requirements. Chapter 5 provides example data use scenarios and maps the flow of data through those scenarios to legally significant decision points so that users can see how the laws may be implicated in realistic examples. A researcher could apply his or her specific research project to the Framework and create a data flow scenario similar to those in Chapter 5 to identify trigger points where decisions will have to be made in order to comply with legal and ethical requirements.

It is important to note that this Architecture does not constitute legal advice and is not a substitute for obtaining specific legal advice from those with health law and policy expertise, such as in-house counsel or compliance officers. Users also must take into account the laws of their individual states, which may vary from federal law. For purposes of the Architecture, the project team identified topic areas that are likely to vary from one state to the next, such as rules for consent and use of information about minors, but the specific state requirements must be identified for any given research project or proposed data use.

Users also should note that laws may change over time. The legal summaries and analyses in this Architecture are current as of September 2017. In the case of the Common Rule, the analysis reflects the Final Rule that was published in 2017 and due to take effect in 2018. As noted above, users should check for any changes or updates that may have occurred.

Architecture Structure

The Architecture consists of the following components, organized into chapters:

CHAPTER 1: Overview

This chapter provides an overview of legal and ethical considerations relevant to PCOR, background on the development of the Architecture, and guidance for navigating the Architecture.

CHAPTER 2: Legal and Ethical Significance of Data for PCOR

This chapter identifies legal and ethical questions to identify key characteristics of health information used for PCOR and describes the health information data types relevant to PCOR. In order to understand the legal and ethical significance of the different data types used for PCOR and CER, a number of key questions reflecting the legal and ethical principles that pertain to PCOR must be assessed. The answers to these questions help determine the legally relevant characteristics of the data. Together, the questions and associated answers provide the foundation for this Architecture and are woven throughout the various components of the Architecture. The common themes identified and summarized in this chapter address the key elements of health information and provide an outline of the core concepts that support this Architecture. This structure should serve as a tool for consistent application of the Architecture across research data use scenarios for PCOR and CER. The key characteristics include identifiability, content, subject, source, access, use/purpose, consent/authorization, security, and legal status. (These characteristics also appear in the Framework in Chapter 4). The data types include clinical data, administrative data, patient-generated health data (PGHD), patient reported outcomes (PROs), genetic information, biospecimens, surveillance data, and quality improvement data. Legal and ethical requirements will vary depending on the type of data sought or held by a researcher.

A stakeholder might use Chapter 2 to identify the characteristics of the data he or she intends to use and discover what laws apply to the use of that data. The process of considering the key questions and data

types in the context of a particular research project can help researchers understand not just what must be done to comply with relevant laws but also what issues with respect to privacy, security, consent, and ethics may arise in the course of their research, which could prompt improvement of the research design.

CHAPTER 3: Linking Legal and Ethical Requirements to PCOR Data

This chapter links specific legal requirements to the key questions raised in Chapter 2. There is not a single statute or set of statutes and regulations that provides a uniform and consistent framework for PCOR. Rather, many federal and state statutes and regulations (identified in Chapters 1 and 3 and summarized in Appendix A) govern and impose privacy and security requirements on health information that may be used for PCOR. These statutes and regulations stipulate different requirements and vary in their applicability (and perhaps even overlap or contradict) based on, for example: what type of data is being collected, accessed, used, or disclosed; the identity of the organization that collected the information; the purpose for which it was collected; the identity of the requesting organization; and the purpose for which the data was requested. This complex legal environment may make it difficult for stakeholders, including researchers, providers, consumers, payers, and health information organizations, to be certain of the legal requirements that govern the health information they hold or acquire and their use and/or disclosure of that information. This chapter organizes relevant legal provisions according to six key characteristics: identifiability and content; subject; source; access and use/purpose; consent/authorization; and security.

Issues related to identifiability, content, subject, and source help to identify whether a particular law and/or regulation apply. For example, HIPAA protects individually identifiable health information that meets certain requirements (which make the information PHI). If the health information in question is not individually identifiable, HIPAA does not apply no matter who holds the data, what kind of data it is, etc. Issues related to access, use/purpose, consent/authorization, and security help to identify what requirements must be met. For example, if individually identifiable health information is requested from a hospital by a researcher and HIPAA is triggered, the hospital must comply with the specific HIPAA requirements that govern disclosures for research. After identifying the features of the data in a given research project using Chapter 2, a stakeholder might use Chapter 3 to identify what laws may be triggered by the data issues unique to that research project.

CHAPTER 4: Framework for Navigating Legal and Ethical Requirements for PCOR

The Framework is intended to be a visual decision tool that highlights the key characteristics and considerations associated with the spectrum of data used for PCOR and the nature of the relationships between researchers and other stakeholders. It builds on the data characteristics and considerations addressed in Chapter 2 that are critical to navigating legal and ethical requirements that govern use and exchange of data for PCOR. The Framework takes a more guided approach, grouping and color-coding key characteristics to direct stakeholders to the factors that determine whether a statute or regulation applies to the data, how a researcher should navigate statutes and/or regulations that apply to the data in question, and whether there are case-specific determinations relating to data collection and use. Each characteristic is further explored individually in a decision-oriented structure that walks the decision-maker through a key question related to a data characteristic that a researcher must address, what it means, why it matters, and considerations for next steps.

Stakeholders who aren't sure what legal and ethical issues are presented by their research can apply the questions in the Framework to their own research scenario to identify the key characteristics of their specific research data set that determine what legal requirements and ethical principles apply.

CHAPTER 5: Mapping Research Data Flows to Legal Requirements

The project team identified, mapped, and analyzed representative data flows that reflect key concerns within each of the five use cases identified in Phase 1. The team started with an additional data flow map representing a general PCOR research process. The general data flow is intended to provide a foundational example of the mapping process, outlining general steps likely to be encountered in the course of PCOR research and the associated legal trigger/decision points. In addition to the general data flow, the project team mapped five data flows representing the following central areas of stakeholder concern: Combining Data for PCOR, Consent Management, Release and Use of Specially Protected Health Data, Identification and Re-Identification of PCOR Data, and Research Using Patient-Generated Health Data.

The data flow maps identify key steps associated with PCOR and link those steps directly to decision or trigger points that have legal significance. These decision or trigger points are linked to specific laws, with notes explaining why they are legally significant. A stakeholder might use the data flows to better understand how the laws apply to research scenarios and require certain decisions or actions. The data flows are designed to capture a variety of unique aspects of research data use (such as substance use data, de-identified data, data involving a minor, etc.) to allow different stakeholders to relate to the research activities mapped.

APPENDIX A: Summary of Statutes and Regulations Relevant to PCOR

This appendix summarizes the statutes and regulations that PCOR researchers are likely to encounter and highlights key ethical considerations. These summaries provide in-depth analysis of how the statutes and regulations apply to PCOR. Users of the Architecture should reference these summaries in addition to any visual overview or decision tool they may be using from another part of the Architecture.

APPENDIX B: Assessing Potential Barriers and Ambiguity in the Legal Landscape

This appendix organizes the stakeholder concerns, issues, and challenges identified in Phase 1 by type of potential policy gap. The gaps that were identified are organized into the following categories: Statutory, Regulatory and Policy Void; Ambiguous or Overlapping Federal Authority; Informal Guidance ("Soft Law"); Ineffective Regulation and Regulatory Bottleneck; Incompatible Stakeholder Implementation; State Law Variation; Ethical Issues; Legal/Compliance/Operational Issues; and Additional Areas of Stakeholder Concern and Suggestions.

APPENDIX C: Selected Federal Initiatives

This resources list includes the prior and current work of HHS and other federal agencies and initiatives related to privacy and security of health information that may be of interest to PCOR researchers and other stakeholders.

APPENDIX D: Selected Federal Resources

This resource list includes relevant federal agencies, initiatives, websites, and reports that will be of interest to a wide range of stakeholders.

APPENDIX E: Glossary

The glossary is a reference of commonly used terms related to health information and research law and policy.

REFERENCES

[1] 45 C.F.R. § 160.103 (2017).

[2] 45 C.F.R. § 164.508(c)(1) (2017).

[3] "Common Rule" Departments and Agencies. Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 at 7265-68 (2017) (to be codified at 45 C.F.R. Part 46 §§ 116, 117).

[4] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881, Title II, § 206(b) (codified at 42 U.S.C. 2000ff-5(b)).

[5] 42 C.F.R. § 2.31(a) (2017).

[6] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

[7] Note that for a consent under Part 2, the information to be disclosed must be limited to the minimum amount of information necessary to accomplish the stated purpose of the disclosure (42 C.F.R. § 2.31(a)(5) (2017)).

[8] Note that in the case of an authorization for use or disclosure of PHI for future research purposes, the authorization must adequately describe such purposes so that it would be reasonable for the individual to expect his or her PHI could be used for such future research (U.S. Department of Health and Human Services Office for Civil Rights (OCR). Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 82 Fed. Reg. 5566 at 5612 (January 25, 2013)).

[9] U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC). Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 9 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[10] HHS. Open Government Plan: Version 4.0 (2016), *available at* https://www.hhs.gov/sites/default/files/hhs-open-gov-plan-v4-2016.pdf; ONC. Health Data Initiative: Strategy and Execution Plan (2013), *available at* https://www.hhs.gov/idealab/wp-content/uploads/2016/06/HDI-strategy-and-execution-plan_v10-1.pdf; *see also* HHS. Healthdata.gov, *available at* https://www.healthdata.gov/ (*last visited* September 20, 2017).

[11] ONC. Federal Health IT Strategic Plan 2015-2020 (2015), *available at* https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf.

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

CHAPTER 2:

LEGAL AND ETHICAL SIGNIFICANCE OF DATA FOR PCOR

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Chapter 2

Legal and Ethical Significance of Data for PCOR

INTRODUCTION

The most basic definition of "health information" is any information concerning the health of at least one person. When considering law and policy, however, the regulated information must be specifically defined. For example, the physical medical record, the content of the record, biological samples taken from a person, and data aggregated from many different people can all be considered "health information," but they may be treated differently under the law. Not all health information is subject to regulation, and information that *is* regulated may be subject to laws that overlap or directly contradict each other.

In order to understand the legal and ethical significance of the different data types used for PCOR and CER, a number of key questions must be asked. There is no single legal framework governing "health information"; rather, information may be subject to one or more statutes and/or regulations depending on the information's specific characteristics. For purposes of applying legal protections and restrictions, health information can be defined based on a variety of characteristics, such as its content, its source, and its form. These characteristics are not mutually exclusive so that multiple overlapping rights and obligations may apply to a particular record or piece of information.

The answers to these questions help determine the legally relevant characteristics of the data. Together, the questions and associated answers provide the foundation for this Architecture and are woven throughout the various components of the Architecture. In practice, the law is applied to specific facts or scenarios. However, there are common themes that provide a more generalized legal analysis and that may be extrapolated to support a broader legal and ethical framework. The themes identified and summarized below address the key elements of health information and provide an outline of the core concepts that support this Architecture. This structure should serve as a tool for consistent application of the Architecture across research data use scenarios for PCOR and CER.

This chapter explains fundamental concepts for organizing data according to categories and types so that legal requirements can be applied. The first section presents questions to ask in order to identify the key characteristics of health information used for PCOR, and the second section gives an overview of the most significant health information data types relevant to PCOR. The key characteristics include identifiability, content, subject, source, access, use/purpose, consent/authorization, security, and legal status. (These characteristics also appear in the Framework in Chapter 4). The data types include clinical data, administrative data, patient-generated health data (PGHD), patient reported outcomes (PROs), genetic information, biospecimens, surveillance data, and quality improvement data. Legal and ethical requirements will vary depending on the type of data sought or held by a researcher. Together, the key characteristics and data types are the fundamental features of data that must be identified to discover the legal and ethical requirements that may apply to the data in question and map the various decisions and actions that must be taken to ensure that the research is conducted in compliance with applicable federal and state laws and ethical requirements.

KEY CHARACTERISTICS OF DATA TYPES FOR PCOR

Identifiability

Identifiability refers to the ability to link information to particular individuals. Health data that contains identifiable information will likely fall within the scope of federal and/or state privacy laws that govern the use and disclosure of health information (e.g., HIPAA, Family Educational Rights and Privacy Act (FERPA), 42 C.F.R. Part 2). Because these laws do not contain a consensus definition of "identifiable," determining whether particular data are identifiable will depend upon the circumstances of its collection and storage as well as its content and what laws apply to its collection and use. Common elements that render data identifiable include names, postal addresses, and social security numbers. Data that have been de-identified are generally afforded less privacy protection and consequently may be easier to access or share.[1]

Considerations for Identifiability

- What information does the data contain? Does this information directly identify individuals?
- Has the data been de-identified? If so, how?
- Can the data be re-identified when combined with data from another source?
- Where was the data collected? How was the data collected?

Content

Content refers to the subject matter or substance of the data. This may include contact, demographic, medical, insurance, web behavior, and/or employment information. Data that contain identifying information will be subject to federal and/or state privacy laws. Data that include information regarding mental health, substance abuse, genetics, and/or HIV status might be subject to additional regulation, depending upon the source of the data and the purpose for collecting or using the data.

Considerations for Content

- Does the data contain health information?
- Does the data contain identifying information?
- Does the data include information on mental health, substance abuse, genetics, HIV, and/or other conditions granted special legal protection?

Subject

Subject refers to the person or thing that is the focus of the data. Human subjects' protection and/or privacy laws may affect the collection/use of any individual's data by limiting the data that can be collected. In particular, these laws may impose stricter requirements for data belonging to members of certain classes, such as minors, prisoners, individuals with limited mental capacity, and pregnant women. Terms of service agreements may also affect data collection or use by limiting inclusion of certain types of information and/or information about certain classes of individuals.

Considerations for Subject

- Who or what is the focus of the data?
- Does the data contain identifying information about the subject and/or other individuals?
- Does the data pertain to a minor, a prisoner, a legally incompetent individual, or a member of another class that receives special consideration under the law?
- Does the user agreement or term of service agreement address subjects?

Source

Source refers to the person, entity, and/or setting in which the data originated or was collected. Persons that originate data may include: (1) patients (e.g., via a wearable device, patient-reported outcomes (PRO) survey); (2) providers (e.g., recording a measurement in a medical record, collecting biospecimens); (3) health plans (e.g., claims data); and (4) government agencies (e.g., Medicare payments, conducting public health surveillance tasks, collating encounter data into Medicaid data files). Settings in which data may originate include clinics, homes, laboratories, etc. Source may also refer to the persons or entity that shares data with another person or entity (e.g., a data repository, registry, or research network, or clearinghouse that provides data to researchers).

Considerations for Source

- Who generates or collects the data (e.g., a healthcare professional from an individual)?
- What is the setting in which data are collected?
- Is the data collection direct or indirect?
- Is the data generated or collected ancillary to another event (e.g., a clinic encounter), or does the data generation/collection occur as the primary event (e.g., an individual voluntarily submitting his or her data to a research network)?
- Is the data aggregated or combined with data from other sources, and if so, who aggregated/combined the data?

Access

Access (as used here) refers to the ability of a person or entity other than the individual subject(s) of the information to view, create, edit, or share data. Factors that impact a person's ability to access data (accompanied by a brief overview of the impact these factors may have on such ability) include:

- Content of the data (e.g., whether data contains identifying information subject to privacy laws, which will likely restrict access to the information, or includes information that is subject to special protections, such as substance abuse treatment information);
- Reason for accessing the data (i.e., access for certain purposes, such as for research, may require authorization/consent, whereas other purposes, such as treatment or administrative tasks, may not);
- Ownership interests (ownership issues are discussed in more detail below; ownership in general is relevant to access insofar as persons or entities may have the ability to limit access to data in which they have ownership interests); and
- Position or affiliation of the person(s) seeking to access data (privacy laws or data use agreements may limit data access to specified individuals).

Considerations for Access

- Does the data contain identifying information?
- What is the reason for accessing the data?
- What is the legal status of the data?
- What is the position/affiliation of the person seeking to access the data? Is there a legal relationship between the parties (e.g., employment)?
- Is there a contract governing access to the data? If so, what are the terms?
- Are there any reporting requirements associated with release and use of the data?

Use/Purpose

The intended use or purpose of the data collection will affect whether and how the data may be collected and used. Relevant uses/purposes for collecting/sharing data include patient care, research, claims processing, advertising/marketing, and personal uses.

Considerations for Use/Purpose

- What is the reason for collecting the data?
- What is the proposed use for the data?
- Who is collecting/using the data?
- Does the use/purpose involve sharing data with other individuals?
- What purpose was communicated to the subject(s) of the information?
- Who is requesting the data from the data source (e.g., patient, health plan, provider)?
- What disclosures and/or uses of the data are specified in the applicable notice(s) of privacy practices?

Consent/Authorization

Consent/authorization refers to the activities and documentation potentially required of researchers seeking permission to collect, use, or share data about an individual. Whether consent or authorization is necessary will depend upon the content of the data, the party collecting or sharing the data, the purposes for collecting or sharing the data, and relevant statutes and regulations. Consent/authorization procedures generally require notifying individuals of the intended uses and disclosures of their information and having individuals execute a document stating that they consent to or authorize the uses or disclosures of their information.

In general, the term “consent” is used to refer to informed consent to participate in research (a concept governed by the Common Rule). Authorization is used to refer to authorization given by an individual subject of information to an entity to disclose that information to a third party. Authorization is a term used in HIPAA, and here it is used to encompass all similar permissions (e.g., as they apply to Part 2, GINA, etc.).

Considerations for Consent/Authorization

- Is consent or authorization necessary prior to a researcher collecting, accessing, or releasing data?
- Is the data being collected/used for a study that is subject to Institutional Review Board (IRB) approval?
- Has an IRB waived the informed consent procedure applicable to participating in the research?

- Can persons withdraw their consent/authorization?
- Can persons opt-out of particular uses for their information (e.g., commercial use)?
- Did an agent (e.g., parent, person with medical power of attorney) give consent or authorization?
- Was consent/authorization a condition of receiving something else (such as medical treatment or payment)?
- Was consent/authorization combined with permission for something else (such as medical treatment)?

Security

Security refers to the means by which data is protected from unauthorized use or access. Security measures generally include technical, administrative, and physical safeguards. Technical safeguards include items such as encryption, firewalls, passwords, antivirus software, and SSL/TLS transmission. Physical safeguards include measures that limit an individual's access to facilities, workstations, and devices that house data or may be used to access data (e.g., policies that limit server room access to authorized personnel). Administrative safeguards include plans and policies for identifying security risks, preventing security breaches, monitoring security, remedying security breaches, and training employees on proper security procedures.

Considerations for Security

- What is the form or medium of the data?
- Where is the data held?
- Who can access the data?
- What technical, physical, and administrative safeguards are employed to secure the data?
- What are the researcher's data management obligations once the data has been obtained?

Legal Status

Legal Status refers to rights and responsibilities related to the data that may be triggered by ownership rights, agency principles, and/or contractual obligations. Legal status determines who may assert rights to that information. Individuals or entities with ownership interests may grant, restrict, or deny access to information. Contractual obligations, such as data use agreements, vendor contracts, or terms of service agreements, may apply. Principles of agency may give a researcher the rights and obligations of the healthcare organization that employs him or her. Finally, some state laws, such as consumer protection and patient privacy laws, may confer rights and responsibilities with respect to access to data or data held by researchers.

Considerations for Legal Status

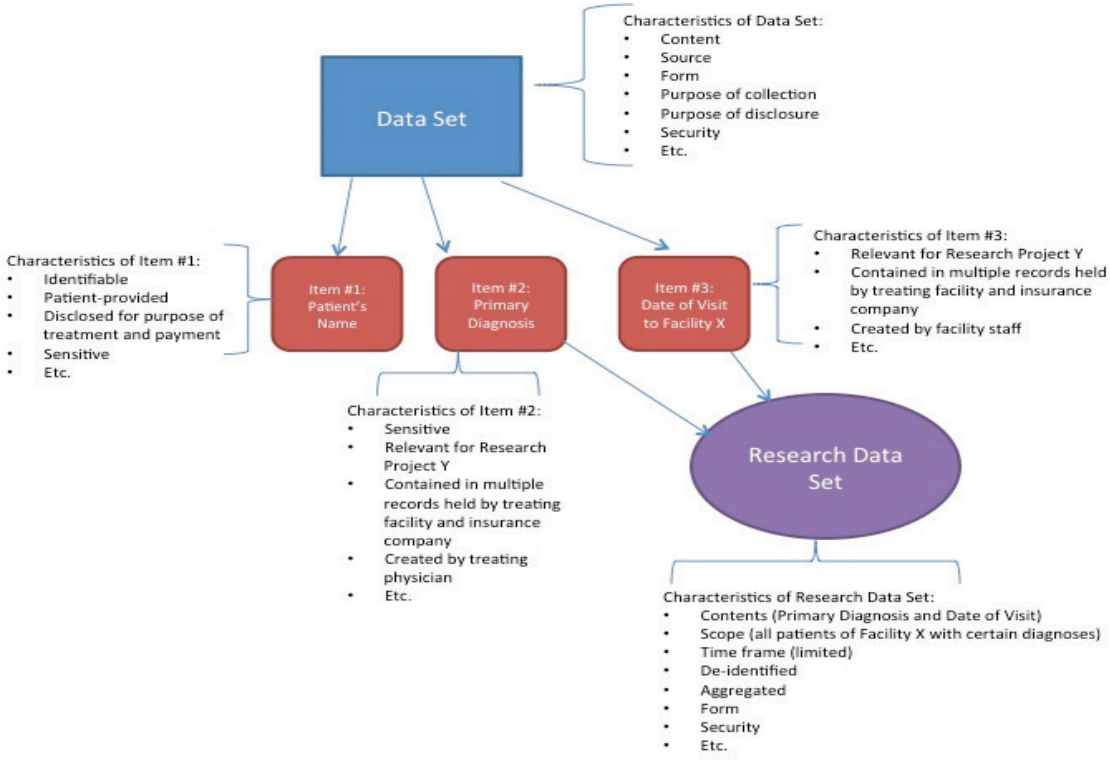
- Who owns the data?
- Are there contracts in place that govern how the parties to the contract or their agents may use the data?
- What is the position/affiliation of the person seeking access to the data? Is there a legal relationship between the parties (e.g., employment)?
- Does the state law grant ownership rights or rights to restrict access?

TYPES OF DATA RELEVANT TO PCOR

Given the scope and depth of PCOR, it necessarily involves the collection and use of a wide range of health data types often from multiple sources. When considering data "types" that are relevant to a legal and ethical analysis, note that any characteristic of a piece of data or set of data may be a common factor that will allow the information to be sorted by that factor as a particular type. The characteristic may be related to the data's content, source, form, or purpose, among other things.

Frequently, attempts to map data types will yield categories that only fit in the context of a particular transaction or reflect just one aspect of the data, such as "claims data" or "patient-generated data." These terms identify the source of the information but don't capture all of the characteristics necessary to map all data relevant to research to all of the legal requirements and ethical principles that may apply. This project maps the legally relevant characteristics of data in addition to defining common data types that reflect one or more common characteristics. The questions described above can be used to draw out the various characteristics of a given data set or individual data elements. As illustrated below, the characteristics may pertain to a collection of data, such as a research data set, or individual elements of the data, such as a particular patient's diagnosis. Individual components of a data set may have a characteristic, such as sensitivity or identifiability, which may not be shared by other components. If the data is collected into a different form, such as by aggregation, the new data set may have characteristics that are different from the characteristics of the source data. Even if the data is drawn from the same field in a database of multiple individuals' data, its characteristics may vary from one individual to the next. For example, the content of a field such as "primary diagnosis" may cause the information to be treated differently if the diagnosis is substance abuse-related.

Figure 1: Data Characteristics[2]



As noted above, a certain characteristic may be identified that pulls together many different pieces of data into a common data "type." This common characteristic is typically some significant aspect of the data, such as source or purpose. Defined below are the common data types that are identified in the health policy literature.

Clinical Data

Clinical data refers to data related to a patient's health, health status, and/or treatment that are collected orally or electronically via a patient-provider interaction in a clinical setting. Clinical data also may be collected as part of a clinical trial. A treating provider or research institution maintains clinical data (electronically or on paper), even though the data may initially be generated outside of the physical clinical setting (e.g., via a telehealth visit or a device such as a remote blood pressure monitor). Clinical data may be found in the following locations:

- Electronic Health Records
- Electronic Medical Records
- Paper-based Medical Records
- Biospecimens
- Clinical Trials
- FDA-Regulated Medical Devices and Technologies

Administrative Data

Administrative data refers to data collected and/or used primarily for administrative (e.g., record-keeping purposes, payment purposes). Administrative data typically includes patient demographic information, payment information (e.g., health plan information, claims), and other related information. Similar to clinical data, administrative data may be found in:

- Electronic Health Records
- Electronic Medical Records
- Paper-based Medical Records
- Practice Management Systems

Sources of administrative data include private and public payers (e.g., private health plans, Medicare, Medicaid) and providers.

Patient-Generated Health Data (PGHD)

PGHD is health-related data created, recorded, or gathered by or from patients (or patients' family members or other caregivers) in nonclinical settings.[3] PGHD may include a patient's health history (reported by the patient, family members, and/or caregivers), treatment history (including medications, biometric data, symptoms, and lifestyle choices), and/or other personal health-related information. This information is distinct from the clinical data discussed above (i.e., information created during or through provider encounters in clinical settings). While clinical data is generally protected by a variety of federal laws governing individually identifiable health information (e.g., HIPAA, Part 2—see discussion of these laws in Appendix A), PGHD is not subject to the same federal protections. PGHD is distinct from clinical data in that: 1) patients, not providers, are primarily responsible for capturing this information; and 2) patients are solely in control of how and with whom to share this information. Examples of PGHD include data collected or generated by these devices: blood glucose monitoring or blood pressure readings using

home health equipment (and which do not automatically transmit to an EHR) and exercise or diet tracking using a mobile app.[4] PGHD can be extremely helpful for both treatment and research purposes. For example, it can help providers track how patients are doing between medical visits, allow patients and providers to collect information on an ongoing basis rather than solely at clinical visits, and provide information useful to treat—as well as prevent—chronic diseases.

There is a rapidly evolving array of technologies designed to enable patients to collect their health information beyond the clinical setting and share that information with providers and researchers. Examples of these new technologies and applications include: Personal Health Records (PHRs), "wearables" such as Fitbit and Jawbone devices; and applications such as Apple Health, diabetes trackers, and the OneTouch Verio Sync Meter that uses Bluetooth to send data to a person's iPhone and then generates reports and data that can be shared with healthcare providers. In particular, Apple, Google, Nike, and Under Armour are investing in wearable technology that syncs with their health-tracking platforms. Devices used to test blood glucose levels, cholesterol, oxygen levels, etc., that can connect to networks have also been developed. Furthermore, the continued development of the Internet of Things[5] should lead to widespread use of fully networked devices. As such, the amount, variety, and quality of available data should increase in the future as more people use wearables, more devices join the Internet of Things, and technology continues to improve.

Patient Reported Outcomes (PROs)/Patient Reported Outcome Measures (PROMs)

According to the Food and Drug Administration (FDA), a PRO is "a report coming directly from the patient (i.e., study participant) about the status of a patient's health condition without amendment or interpretation of the patient's response by a clinician or anyone else."[6] PROs can be collected during clinic visits or at home through various web tools or mobile devices either for treatment or for clinical trial participation (e.g., PROMIS Assessment Center,[7] PatientViewpoint,[8] REDCap Research Electronic Data Capture[9]). PROs are distinguishable from PGHD (discussed above) because a researcher or clinician typically initiates collection using a scientifically validated survey or instrument, whereas collection of PGHD is generally patient-initiated and does not require a validated instrument or survey.

Genetic Information

Genetic information is information about an individual's genetic makeup and the genetic makeup of an individual's family members, as well as information about the manifestation of a disease or disorder in an individual's family members (e.g., family medical history).[10] Family medical history is included in the definition of genetic information because it is often used to determine whether someone has an increased risk of getting a disease, disorder, or condition in the future. Genetic information also includes an individual's request for, or receipt of, genetic services or participation in clinical research that includes genetic services by the individual or a family member of the individual, and the genetic information of a fetus carried by an individual or by a pregnant woman who is a family member of the individual and the genetic information of any embryo legally held by the individual or family member using an assisted reproductive technology.[11]

Personal Genomics/Direct-to-Consumer Genetic Testing is an emerging market that allows individuals to submit a DNA sample in order to determine their disease risk/carrier status, find relatives, determine paternity, etc. If direct-to-consumer genetic tests can avoid FDA scrutiny and gain widespread consumer interest, then personal genomics is another market that could generate significant amounts of relevant PCOR/CER data.

Biospecimens

Biospecimens, which are a type of genetic information, include tissue, blood, urine, or other human-derived material. A biospecimen can comprise subcellular structures, cells, tissue (e.g., bone, muscle, connective tissue, and skin), organs (e.g., liver, bladder, heart, and kidney), blood, gametes (sperm and ova), embryos, fetal tissue, and waste (urine, feces, sweat, hair and nail clippings, shed epithelial cells, and placenta). Biospecimens may be collected in a clinical setting, patient home, or other site. For example, some biospecimens (e.g., urine, saliva, hair follicles, sperm, etc.) may be safely collected and stored by an individual within the privacy of their own home. Many research studies allow at-home collection because it is more efficient than clinic visits. Individuals also may voluntarily donate samples to biobanks/biorepositories.

Surveillance Data

Surveillance data refers to the health information collected to facilitate the planning, implementation, or evaluation of public health activities. Government agencies/organizations (e.g., CDC, World Health Organization (WHO)) are often the party responsible for collecting and disseminating surveillance data. Examples of surveillance data sources include the CDC's Behavioral Risk Factor Surveillance System (BFRSS),[12] which continually monitors chronic health conditions, use of preventive services, and risk behaviors, and the FDA's Sentinel Initiative, which monitors the safety of FDA-regulated products.[13]

Quality Improvement Data

Quality data refers to information collected to assess the performance of healthcare providers and/or health plans and the results of these performance assessments to improve the quality of care delivery. Various government and non-government agencies/organizations (e.g., The Centers for Medicare & Medicaid Services, The National Committee for Quality Assurance, etc.) develop and maintain quality measures for use by private or public payers. Existing measures focus on a broad range of quality-related factors such as patient safety, patient-centered care, care coordination, and affordability.[14] Although there is no indication that quality improvement data is included in the scope of PCOR research, the increasing creation of quality improvement data could inform future research efforts.

REFERENCES

[1] *See also* U.S. Department of Commerce National Institute of Standards and Technology (NIST). Appendix A, HIPAA Information De-Identification Reference at p. 3. In De-Identification of Personal Information [Internal Report 8053] (2015). *Available at*: http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf; NIST. De-Identifying Government Datasets: Second Draft [Special Publication 800-188] (2016). *Available at*: http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf

[2] Graphic created by GW Team (2016).

[3] HealthIT.gov. "Patient-Generated Health Data" (*last updated* April 26, 2017). *Available at:* https://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data.

[4] HealthIT.gov. "Patient-Generated Health Data" (*last updated* April 26, 2017). *Available at:* https://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data.

[5] Jacob Morgan. "A Simple Explanation of 'The Internet of Things'" Forbes.com (May 13, 2014). *Available at:* http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#45f87ae56828.

[6] *See* U.S. Department of Health and Human Services Food And Drug Administration (FDA). Guidance For Industry, Patient-Reported Outcome Measures: Use In Medical Product Development To Support Labeling Claims, at p. 32 (2009). A*vailable at:* http://www.fda.gov/downloads/Drugs/.../Guidances/UCM193282.pdf.

[7] Assessment Center. "What is Assessment Center" (2013). A*vailable at:* https://www.assessmentcenter.net/.

[8] PatientViewpoint. "Welcome" [log-in credentials required]. A*vailable at:* https://www.patientviewpoint.org/Login.aspx (*last visited* March 16, 2016).

[9] Research electronic data capture (REDCap). "Homepage". *Available at:* http://project-redcap.org/ (*last visited* March 16, 2016).

[10] Adapted from definition of "genetic information" set forth in GINA Title I (2008).

[11] 29 U.S.C. § 1191b(d)(6) (2017).

[12] U.S. Department of Health and Human Services Centers for Disease Control and Prevention (CDC). "Behavioral Risk Factor Surveillance System" (*last updated* August 25, 2017). *Available at:* http://www.cdc.gov/brfss/.

[13] FDA. "FDA's Sentinel Initiative" (*last updated* December 14, 2016). *Available at:* http://www.fda.gov/Safety/FDAsSentinelInitiative/ucm2007250.htm.

[14] *See* National Quality Forum (NQF). National Priorities Partnership and the National Quality Strategy (2011). https://www.qualityforum.org/Setting_Priorities/NPP/Input_into_the_National_Quality_Strategy.aspx.

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

CHAPTER 3:

LINKING LEGAL AND ETHICAL REQUIREMENTS TO PCOR DATA

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Chapter 3

Linking Legal and Ethical Requirements to PCOR Data

INTRODUCTION

The legally relevant PCOR data characteristics identified in Chapter 2 are associated with specific legal requirements in the statutes and regulations that govern access and use of health information for PCOR. This chapter summarizes those specific legal requirements and links them directly to the key characteristics of PCOR data described in Chapter 2. More detailed summaries of the relevant statutes and regulations are provided in Appendix A.

LINKING LEGAL REQUIREMENTS TO RELEVANT PCOR CONSIDERATIONS

There is not a single statute or set of statutes and regulations that provides a uniform and consistent framework for PCOR. Rather, many federal and state statutes and regulations (summarized in detail in the Legal Appendix) govern and impose privacy and security requirements on health information that may be used for PCOR. These statutes and regulations stipulate different requirements, the applicability of which vary (and perhaps even overlap or contradict) based on, for example: what type of data is being collected, accessed, used, or disclosed; the identity of the organization that collected the information; the purpose for which it was collected; the identity of the requesting organization; and the purpose for which the data was requested. This complex legal environment may make it difficult for stakeholders, including researchers, providers, consumers, payers, and health information organizations, to be certain of the legal requirements that govern the health information they hold or acquire and their use and/or disclosure of that information.

Chapter 2 identified a series of issues that must be addressed or considered in order to determine: 1) whether a statute and/or regulation applies (i.e., what information it protects and who it applies to) and if so, 2) how it applies (i.e., how the information it protects may be used by the entities it governs and requirements related to this). This chapter organizes relevant legal provisions according to seven key data considerations:

- Identifiability and Content;
- Subject;
- Source;
- Access and Use/Purpose;
- Consent/Authorization;
- Security; and
- Legal Status

Issues related to identifiability, content, subject, and source help to identify whether a particular law and/or regulation apply. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] Rules[2] protect individually identifiable health information that meets certain requirements. If the health information in question is not individually identifiable, HIPAA does not apply no matter who holds the data, what kind of data it is, etc. Issues related to access, use/purpose, consent/authorization,

and security help to identify what requirements must be met. For example, if individually identifiable health information is requested from a hospital by a researcher and HIPAA is triggered, the hospital must comply with the specific HIPAA requirements that govern disclosures for research.

The following section links the relevant statutes and regulations that govern PCOR to these seven core issues.

Identifiability and Content

Identifiability is a legal concept that refers to the ability to link information to a particular individual. It is assessed based upon the presence of certain data elements and/or data characteristics. The federal and state privacy statutes and regulations that govern the use and disclosure of health information ONLY protect identifiable health information; all of these statutes and regulations define identifiability differently, but none are triggered by the use of de-identified information (i.e., no individually identifying elements remain in the data). Even if information has been de-identified, however, privacy statutes and regulations may still apply depending on the process of de-identification, the remaining data elements, and the potential for data re-identification.

Even if information meets a law or regulation's definition of "identifiable," each statute and regulation protects only certain types of identifiable information. In particular, the applicability of a particular statute or regulation will depend on the data's content. Content pertains to the subject matter or substance of the data, which may include contact, demographic, medical, insurance, and/or employment information. Data that includes sensitive information (e.g., mental health, substance abuse, genetics, and/or HIV status) might be subject to additional regulation. Other relevant data characteristics must also be present in order for a particular statute or regulation's protections to apply to the information (e.g., data source, purpose of collection)—these are discussed in other sections.

Key Statutes and Regulations Related to Identifiability and Content

Health Insurance Portability and Accountability Act (HIPAA): In general, the HIPAA Rules govern "protected health information" (PHI), which is **individually identifiable information** (including genetic information) maintained or transmitted in any form or medium (e.g., orally, electronically, or on paper) that:

1. Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and
2. Relates to:
    a. The provision of care to an individual;
    b. An individual's past, present, or future physical or mental health condition; or
    c. Payment for care provided to an individual, whether made in the past or present or expected in the future.[3]

Under HIPAA, information is individually identifiable if it directly identifies the individual or if there is a reasonable basis to believe the information could be used to identify the individual.[4] The HIPAA Rules do not govern employment records or education records subject to FERPA.[5] In general, all PHI is subject to the same requirements wherever HIPAA applies, though there are additional restrictions applicable to [identifiable] psychotherapy notes and genetic information. Other provisions apply depending on the subject of the information (e.g., minors, prisoners) and/or the purpose of disclosure (e.g., sale, research). These limitations are discussed in more detail in the relevant section below.

Note that **health information that has been de-identified is not considered to be PHI for purposes of HIPAA applicability**.[6] There are two methods by which information can be considered "de-identified" under HIPAA[7]—the Safe Harbor method and the Expert Determination method. The Safe Harbor method requires that the information be stripped of 18 specified identifiers (see Table 1 below).[8] Even where these 18 identifiers are removed, an individual's information is only considered de-identified under the Safe Harbor method if the Covered Entity does not have actual knowledge that the information could be used (on its own or in combination with other information) to identify the individual.[9] Note that a limited data set (LDS), which is information stripped of 16 specified identifiers, is still considered PHI (i.e., individually identifiable health information).[10] The Expert Determination method requires that a person appropriately qualified in de-identification methods determines that there is very small risk that an anticipated recipient of the information could use the information (on its own or in combination with other reasonably available information) to identify the individual.[11]

Table 1: Safe Harbor Method of De-Identification

The following elements must be removed as each relates to the individual subject of the information or to that individual's relatives, employers, or household members:
Names
All geographic subdivisions smaller than a **state**, including street address, **city**, **county**, precinct, **ZIP code**, and their equivalent geocodes, *except* for the initial three digits of the ZIP code if (according to the current publicly available data from the Bureau of the Census): • The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; OR • The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
All elements of dates (except year) for dates **that are directly related to an individual**, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
Telephone numbers
Fax numbers
Email addresses
Social security numbers
Medical record numbers
Health plan beneficiary numbers
Account numbers
Certificate/license numbers
Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers
URLs (Web Universal Resource Locators)
IP (Internet Protocol) address numbers
Biometric identifiers, including finger and voice prints
Full-face photographs and any comparable images
Any other unique identifying number, characteristic, or code

*Note: Items in bold may be included in a limited data set.

Common Rule:[12] NOTE: In September 2015, the federal departments and agencies that have adopted the Common Rule published a Notice of Proposed Rulemaking (NPRM) proposing significant changes to the regulations.[13] Changes were published in a Final Rule on January 19, 2017, with a January 19, 2018, effective date (and extended and/or suspended effective dates for certain provisions).[14] The Common Rule provisions referenced in this Chapter reflect the 2017 Final Rule provisions. Future changes may be made to the regulations, and researchers and other stakeholders should continue to monitor the status of the Common Rule.

The Common Rule Subpart A applies to all federally supported research involving human participants. Research (i.e., a systematic investigation designed to develop or contribute to generalizable knowledge)[15] involves human participants when an investigator:

- Obtains information or biospecimens about a living individual through intervention or interaction with the individual and uses, studies, or analyzes the information or biospecimens; or
- Obtains, uses, studies, analyzes, or generates ***identifiable*** private information or ***identifiable*** biospecimens about a living individual.[16]
    - Information and biospecimens are identifiable if the individual's identity is or may be readily ascertained by the investigator or associated with the information[17] or the biospecimen.[18]
    - Information is private when it is about behavior where an individual can reasonably expect that no observation or recording is taking place and information provided for specific purposes that the individual can reasonably expect will not be made public;[19]

The Common Rule also exempts several types of research from ALL of its requirements, including the following types related to data identifiability and content[20] (see section on Source below for discussion of additional exemptions):

1. Research that only involves interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[21] or that involves benign behavioral interventions[22] in conjunction with information collection from a participant[23] if:
    a. The researcher records information so that the participant's identity cannot be readily ascertained (directly or through linked identifiers); or
    b. Disclosure of a participant's responses outside the research setting would not reasonably place the participant at risk of criminal or civil liability or be damaging to the participant's financial standing, employability, educational advancement, or reputation;

2. Secondary research use of identifiable private information or identifiable biospecimens if:
    a. The researcher records such information so that the subject's identity cannot be readily ascertained (directly or through linked identifiers);[24] or
    b. Such use is limited to information collection and analysis regulated under the HIPAA Privacy Rule as a use or disclosure for the purposes of "health care operations" or "research" or for "public health activities and purposes";[25] and

3. Research and demonstration projects designed to study, evaluate, improve, or examine public benefit or service programs that are conducted, supported by, or subject to approval of a federal department or agency.[26]

The Common Rule also exempts some types of research from most, BUT NOT ALL, of its requirements based on identifiability and content (see section on Source below for discussion of additional partial exemptions):

1. Interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[27] or involving benign behavioral interventions[28] in conjunction with information collection[29] if an IRB conducts a limited review and determines that provisions to protect privacy and confidentiality are adequate;[30]
2. Storage or maintenance of identifiable private information or biospecimens for ***potential*** secondary research use if an IRB conducts a limited review and determines that broad consent will be appropriately obtained and documented;[31] and that, should there be a change in storage or maintenance of the information or biospecimens, the provisions in place to protect privacy and confidentiality are adequate;[32] or
3. Secondary research use of identifiable private information or biospecimens if:
    a. The investigator does not include "returning individual research results to [subjects]" as part of the study plan; and
    b. An IRB conducts a limited review and determines that the planned research is within the scope of broad consent;[33] and provisions in place to protect privacy and confidentiality are adequate.[34]

42 C.F.R. Part 2:[35] NOTE: In 2016, the Substance Abuse and Mental Health Services Administration (SAMHSA) proposed several major modifications to align the Part 2 regulations with the current U.S. healthcare system.[36] SAMHSA finalized changes to Part 2 in a Final Rulemaking issued on January 18, 2017.[37] The finalized changes to Part 2 went into effect on March 21, 2017; the Part 2 provisions referenced in this chapter reflect the 2017 Final Rule provisions. In conjunction with publishing the Final Rule, SAMHSA issued a Supplemental Notice of Proposed Rulemaking to propose additional clarifications to the amended Part 2 regulations and seek public comment on these proposals.[38] Future changes may be made to Part 2, and researchers and other stakeholders should continue to monitor the status of Part 2.

Part 2 restricts disclosure of all information, whether recorded or not, obtained by a Part 2 program (see section on Source below for more information) for purposes of providing substance use disorder services that would directly or indirectly[39] identify a patient as having or having had a substance use disorder.[40]

Under Part 2, information is identifying if it includes elements such as "name, address, social security number, fingerprints, photograph, or similar information by which a patient's identity can be determined with reasonable accuracy directly or by reference to other publicly available information."[41]

GINA: GINA protects genetic information from being collected or used for certain purposes. Genetic information is defined as information (other than information about sex or age) about:

1. An individual's genetic tests;[42]
2. The individual's family members' genetic tests; and
3. The manifestation of a disease or disorder in the individual's family members.

In addition to this definition, GINA required that the Secretary of the U.S. Department of Health and Human Services (HHS) modify the HIPAA Rules to explicitly include genetic information within the definition of PHI. In 2013, HHS issued a Final Rule that made multiple, significant changes to the HIPAA Rules, including adoption of the modification(s) required by GINA.[43]

Privacy Act of 1974:[44] The Privacy Act limits the disclosure of records about individuals that are maintained by a federal agency and contain the individual's "name or identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[45]

Family Educational Rights and Privacy Act (FERPA): FERPA protects education records and personally identifiable information contained within those records.[46] This includes health information collected at school-based clinics, for enrollment, or for other education-related purposes. Education records are records maintained by a federally funded educational agency, institution, or party acting for such an agency or institution that are directly related to a student. FERPA defines "personally identifiable information" as including the student's: name, address, personal identifiers (e.g., social security number, biometric record), indirect identifiers (e.g., date of birth, place of birth, mother's maiden name), family members' names, family members' addresses, information requested by a person who the educational agency or institution reasonably believes knows the identity of the individual to whom the record relates, and other information that (alone or in combination) is linked or linkable to the student that would allow a reasonable person in the school community (who does not have personal knowledge of the relevant circumstances) to identify the student with reasonable certainty.[47] The term "education records" does *not* include the following records:[48]

1. Those created by instructors, teachers, or administrators accessible only by the teacher or a substitute;
2. Those created for law enforcement purposes by a law enforcement unit of an education agency;
3. Those regarding educational agency or institution employees that are made in the normal course of business and only pertain to their employment; and
4. Those regarding a postsecondary student or student over the age of 18 created by a healthcare professional for treatment purposes *if* such records are only made, maintained, or used in connection with treatment of the student (e.g., "treatment records"). Treatment records may be disclosed for purposes other than treatment, but only if the disclosure meets an exceptions or with written consent.

State Law: States typically provide enhanced protection for sensitive information. This generally includes, but is not limited to: HIV/AIDS status, information related to sexually transmitted diseases (STD), mental health, domestic violence, women's reproductive health, alcohol and/or substance abuse, and health of the legally incompetent, including minors.

Subject

Subject refers to the person or thing that is the focus of the data. Human subjects protection and/or privacy laws apply to information depending not only on the content of the information but also on the subject of the information. Further, these laws may limit what data may be collected or used from certain classes of subjects and/or how such data can be used. Classes granted special protection may include minors, prisoners, incompetents, and pregnant women.

Key Statutes and Regulations Related to Subject

Health Insurance Portability and Accountability Act (HIPAA): HIPAA governs Regulated Entities' use and disclosure of **any** living individual or other entity's PHI[49] and any deceased individual's PHI for 50 years after the individual's death.[50] With respect to applying HIPAA's provisions, Covered Entities must treat an individual's personal representative as if the representative were the individual.[51] A personal representative is someone with authority to act on behalf of the individual in making decisions related to

health care under applicable state or other law.[52] Persons legally authorized to act as a personal representative on behalf of an unemancipated minor may include a parent, guardian, or other person acting *in loco parentis* on behalf of the minor, though in states that grant the minor capacity to consent to a particular healthcare service, the minor must request that the person be treated as his/her personal representative.[53]

The only other subject-specific provisions in HIPAA relate to inmates (i.e., a person incarcerated or otherwise confined to a correctional institution[54]). HIPAA permits Covered Entities to disclose PHI about inmates to law enforcement officials and correctional institutions without the inmate's authorization for limited health and safety-related purposes.[55] An individual is no longer an inmate when released on parole, probation, supervised release, or is otherwise no longer in lawful custody.[56]

Common Rule: Subpart A applies to federally supported research involving human participants (i.e., a living human being).[57]

Subparts B–D provide additional (or modified) protections for certain vulnerable populations involved in federally supported research:

1. Subpart B applies to research involving pregnant women, human fetuses, newborns of uncertain viability, and nonviable newborns;[58]
2. Subpart C applies to biomedical and behavioral research involving prisoners (i.e., individuals involuntarily confined or detained in a penal institution or alternative facilities);[59] and
3. Subpart D applies to research involving children (i.e., individuals under the legal age of consent for the treatment or procedures involved in the research).[60]

Part 2: Part 2 protects identifying information about patients, which includes any individual who has applied for or received diagnosis, treatment, or referral for treatment of a substance use disorder at a Part 2 program (see section on Source below for more information).[61] Part 2 does not treat minor patients' information differently where the relevant state's law grants the minor legal capacity to seek treatment without parental consent.[62] Where a state does not grant the minor such capacity,[63] or where a minor lacks capacity to make a rational choice (i.e., mental capacity),[64] Part 2 includes limitations on information disclosures (discussed below in the section on Consent/Authorization).

GINA: GINA protects genetic information[65] about individuals[66] and their family members. It also protects genetic information about any fetus carried by the individual (or their family member) and any embryo legally held by the individual (or their family member) utilizing assisted reproductive technology. A family member includes an individual's dependent(s) and an individual's first-, second-, third-, and fourth-degree relatives.

Privacy Act of 1974: The Privacy Act protects information about U.S. citizens and permanent legal residents held by a federal agency in a system of records.[67]

Family Educational Rights and Privacy Act (FERPA): FERPA protects education records directly related to students that are maintained by educational agencies and institutions. A student is any individual who is or has been in attendance at a federally funded public or private agency or institution that provides educational services and/or instruction to students.[68]

State Law: States often have their own laws and regulations governing health information pertaining to certain classes of individuals, which may mirror federal protections or provide additional protections. States also often govern information about classes of individuals not specifically protected by federal laws or regulations, including:

1. Adult individuals who lack [legal] capacity to make certain decisions;
2. Minors involved with the juvenile corrections system; and
3. Individuals who are on parole, probation, or other similar type of supervision.

Federal law defers to state law for specifics about certain subjects, such as the age to consent to certain health-related services and legal requirements related to personal representatives (e.g., documentation required).

Source

Source pertains to the person, entity, and/or setting in which the data originated or was collected. Persons that originate data may include patients, providers, health plans, and government agencies, and data may be collected in a variety of settings, including clinics, homes, laboratories, etc. Privacy laws and regulations only govern certain data sources' use and disclosure of the identifiable data types described above. A data source may be the original collector (e.g., a provider in a clinical setting) or may refer to a data holder that obtains data from an original or secondary source and then shares that data with another person or entity (e.g., a data repository, registry, or research network, or clearinghouse that provides data to researchers). Determining the source of data, and thus the applicability of laws and regulations, depends on other considerations, including: (1) the form or method of data collection; (2) whether data collection/generation is ancillary to another event (e.g., a clinic encounter) or occurs as the primary event (e.g., an individual voluntarily submitting their data to a research network); and (3) whether and how data are aggregated or combined with other sources.

Key Statutes and Regulations Related to Source

Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Rules apply to health plans, healthcare clearinghouses,[69] and any healthcare providers (regardless of size) that electronically transmit health information in connection with certain transactions.[70] These health-related entities are collectively known as "Covered Entities."[71] In addition, the rules apply to Covered Entities' "Business Associates," which are individuals or groups (other than members of the Covered Entity's workforce) that can or do access PHI when providing certain services or functions to or on behalf of a Covered Entity.[72] Covered Entities and their Business Associates together are referred to as "Regulated Entities."[73] The HIPAA Rules only protect the use and disclosure of PHI (see section on Identifiability above for more information) by Regulated Entities. The use or disclosure of PHI by other types of individuals or organizations that are not Regulated Entities is not governed by HIPAA.

Common Rule: Subpart A applies to federally supported research involving human participants. Research is federally supported if it is conducted, supported, or otherwise subject to regulation by a federal department or agency.[74]

The Common Rule specifically excludes some activities from its definition of research; these activities are not subject to any provisions of the Common Rule.[75] For example, public health surveillance activities, including the collection and testing of information or biospecimens, that are conducted, supported,

requested, ordered, required, or authorized by a public health authority are not considered "research" for purposes of Common Rule applicability.[76]

The Common Rule also exempts several types of research from ALL of its requirements, including the following types related to data source[77] (see section above on Identifiability and Content for discussion of additional exemptions):

1. Secondary research use of publicly available identifiable private information or identifiable biospecimens;[78] and

2. Secondary research use of identifiable private information or identifiable biospecimens where such research is conducted by or on behalf of a federal department or agency using government-generated or -collected information obtained for non-research activities[79] and maintained in systems of records (SORs) subject to the Privacy Act of 1974,[80] if certain other requirements are met.[81]

Part 2: The Part 2 regulations govern the disclosure and use of certain information maintained by "federally assisted" substance use disorder programs.[82] A program includes:

1. Individuals, entities, and identified units in general medical facilities that provide substance use disorder services (i.e., diagnosis, treatment, or referral for treatment) and hold themselves out as providing such services (e.g., advertises services, certified to provide addiction services—any activity that would lead one to conclude that the individual or entity provides substance use disorder services[83]); and
2. Medical personnel or other staff working within a general medical facility whose primary function is to provide substance use disorder services *and* who are identified as such providers.[84]

A program is "federally assisted" if it is conducted by any federal department or agency (directly or via contract), is carried out under any federal license, certification, registration, or authorization (e.g., Medicare/Medicaid certification, DEA registration to dispense a controlled substance used to treat substance use disorders), or receives any federal financial assistance (e.g., grants, federal tax-exempt status).[85]

Part 2 only protects substance abuse information that has been obtained by a federally assisted program. The restrictions on disclosure also apply to individuals and entities that have received patient records directly from Part 2 programs or from other lawful holders of patient identifying information and who have been properly notified of the prohibition on re-disclosure.[86]

GINA: GINA Title I governs collection and use of genetic information about individuals and their family members by health plans and health insurance issuers for certain purposes. GINA does not apply to life insurance plans, long-term care plan issuers, or disability insurers. GINA Title II governs employers' collection and use of genetic information about employees.

Privacy Act of 1974: The Privacy Act governs federal agency disclosure of records contained in a system of records, which is a group of any records under any agency's control from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Family Educational Rights and Privacy Act (FERPA): FERPA applies to all educational agencies and institutions that receive federal education funding (e.g., public schools and districts, private and public colleges, universities, and other postsecondary institutions) but typically exempts private and religious elementary and secondary schools.[87] Where a clinic is operating in a school (e.g., a community health

center offering satellite clinics in schools), FERPA would apply if the clinic is an agent of the school (i.e., if, under its agreement with a school, the clinic is carrying out the school's responsibilities and is subject to school direction). FERPA will also apply to health information collected directly by these schools, such as by school-based health professionals or for enrollment.

Food & Drug Administration (FDA) Law: There are several FDA-specific human subjects protection regulations scattered throughout Title 21 of the C.F.R.; these regulations are specific to the type of research being conducted. Parts 312 (clinical investigations of new drugs), 812 (clinical investigations of devices), and 814 (clinical investigations of Humanitarian Use Devices (HUD)[88]) all contain requirements that are in addition to or modify the requirements of Parts 50 and 56.

State Law: States generally have laws governing state-based disease registries, compulsory health information reporting (e.g., communicable diseases, vital statistics) by certain entities, health information exchanges (HIEs), and all-payer claims databases (APCDs). States also regulate health insurers, public health entities, and facility and provider licensure—requirements pertaining to these entities may relate to data sharing, confidentiality, and patient consent.

Access and Use/Purpose

The privacy laws and regulations govern access (i.e., who may, may not, or must be allowed to view, create, edit, or share protected data) and define the acceptable procedural parameters surrounding access. Factors that impact a person's ability to access data include: ownership interests (persons or entities may have the ability to limit access to data in which they have ownership interests), the data's content (access to information subject to heightened protections, such as psychotherapy notes, may be restricted), the position or affiliation of the persons seeking to access data, and the stated reason for accessing the data.

While access deals with **who** may use information, use/purpose deals with **how and why** they may use the information. Every privacy law and regulation sets forth parameters for collecting, using, and sharing data, which include the purpose and method of collecting and sharing information as well as uses that are prohibited or substantially limited. Common and generally relevant uses/purposes for collecting/sharing data include patient care, research, claims processing, advertising/marketing, and personal uses. In general, the laws and regulations allow the collection, use, or disclosure of an individual's information for any purpose with that individual's approval—this concept is discussed more fully in the section below on Consent. This section specifically addresses uses and disclosures that may occur without the individual subject's express approval.

Key Statutes and Regulations Related to Access and Use/Purpose

Health Insurance Portability and Accountability Act (HIPAA): The Privacy Rule governs when and how PHI can be disclosed, which can be grouped into four broad categories:

1. Required Disclosures: a Regulated Entity **must** disclose PHI to the individual subject of the PHI (or his/her personal representative) upon his/her request and to HHS for enforcement purposes and for HIPAA-related compliance investigations;[89]
2. Prohibited Disclosures: a Regulated Entity may not disclose PHI for certain purposes (e.g., most sales of PHI[90]) and may only disclose certain types of PHI (e.g., psychotherapy notes,[91] minors' PHI[92]) in limited circumstances, even with the individual's authorization;
3. Permissive Disclosures (see Table 2 below for a complete list): a Covered Entity **may** disclose PHI **without first obtaining the individual subject of the information's authorization** for a variety of

purposes (though some of these purposes require that, where practicable, the individual be given the opportunity to informally object to the disclosure);[93]

4. Authorized Disclosures: Any disclosures not required, permitted, or prohibited by the rule require written authorization from the individual who is the subject of the information.[94]

Table 2: List of HIPAA Permissive Exceptions Available to Covered Entities[95]

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose—and Relevant Limitations
For treatment purposes[96]	To any entity for its own or any healthcare provider's treatment activities
For payment purposes	To any entity for its own payment activities or to a Covered Entity or healthcare provider for the receiving entity's payment activities
For healthcare operations purposes	To any entity for its own healthcare operations purposes or to another Covered Entity for certain of the receiving CE's healthcare operations purposes, if both parties have/had a relationship with the patient and the PHI pertains to that relationship
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
As required by law	To a government authority about a patient who the entity reasonably believes to be a victim of abuse, neglect, or domestic violence
	In the course of any judicial or administrative proceeding, in response to an order, subpoena, discovery request, or other lawful process
	To a law enforcement official for limited purposes (e.g., suspect identification, reporting crime on premises, about suspected victims of crime)
For public health activities	To a public health authority that is legally authorized to collect the PHI to control or prevent disease, injury, or disability
	To an authorized government entity to report child abuse or neglect
	To an FDA-regulated entity about an FDA-regulated product or activity for quality, safety, or effectiveness activities
	To a person who may have been exposed to or be at risk of contracting or spreading a communicable disease
	To an employer about an employee if the entity is providing health care to the employee at the employer's request in order to conduct an evaluation relating to workplace medical surveillance or to evaluate whether an employee has a work-related illness or injury
	Proof of immunization information to a school about a student or prospective student
	To anyone the provider believes can lessen or prevent a serious and imminent threat to an individual or the public
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
For health oversight activities	To a health oversight agency[97] for legally authorized oversight activities
About decedents	To coroners and medical examiners to identify a deceased person, determine cause of death, or other legally authorized duties
	To a funeral director to carry out their legally authorized duties
	To organ procurement organizations for the purpose of facilitating donations and transplantations

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose—and Relevant Limitations
For research purposes	To researchers as authorized by an IRB or Privacy Board for limited, specific research purposes
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
For specialized government functions	About Armed Forces personnel where disclosure is deemed necessary by appropriate military authorities to execute military missions
	To authorized federal officials for national security and intelligence activities
	To authorized federal officials for the provision of protective services to the President
	To a correctional institution or law enforcement officer about an inmate or an individual in lawful custody
For worker's compensation	To entities legally authorized to receive such information for purposes of providing benefits for work-related injuries or illnesses
For directory purposes	To anyone identifying the patient by name,[98] if information disclosed is limited to location in the facility and general health status
For involvement in the patient's care	To any family member, close friend, or patient-designated representative to the extent that the information disclosed is directly relevant to the recipient's involvement with the patient's care or payment for care[99]
For notification, identification, or location of person responsible for patient's care	To any entity, if the information disclosed is limited to the patient's location and general health status or death.
Disclosures incident to any permitted or required disclosures	To any entity if the provider has in place reasonable safeguards to protect the privacy of patient information

The Privacy Rule requires that most permissive exception disclosures be limited to the "minimum [amount of PHI] necessary" to achieve the purpose for which the information was released or requested.[100] Determining what amount is the "minimum necessary" is at the discretion of the Covered Entity making the disclosure, using professional judgment under the circumstances.[101] Note, however, that the disclosing Covered Entity may rely on the intended recipient's request as the minimum necessary for the stated purpose when the requestor is: (1) another Covered Entity; (2) a member of the disclosing Covered Entity's workforce; (3) a public official for a purpose permitted under § 164.512; (4) a researcher acting in compliance with § 164.512(i); or (5) an entity providing professional services to the disclosing Covered Entity as its Business Associate.[102] The minimum necessary limitation does not apply to a disclosure made without authorization when required by law, to a provider for treatment purposes, or to the Secretary for compliance or enforcement purposes nor to disclosures made to the individual subject of the information or pursuant to an individual's authorization.[103]

Other than an individual's request for access, which is a required disclosure, it is important to underscore the permissive nature of the rest of these exceptions—the Covered Entity may, but is not required to, make disclosures without authorization for these specified purposes. If it is the Covered Entity's custom or common practice to first obtain written authorization for any disclosure (other than those required by the Rule), the Covered Entity may choose to maintain that custom or practice. However, such custom or practice is not mandated by the Privacy Rule, nor is there a HIPAA penalty for making use of these exceptions (or declining to do so). If a Covered Entity does or plans to make certain permissive

disclosures, it must specify the general types of disclosures in its Notice of Privacy Practices (NPP), which it must make available to all individuals. While the Privacy Rule gives providers the flexibility to utilize permissive exceptions in accordance with their own customs and preferences (so long as safeguards to protect such disclosures are followed), there are certain situations in which more restrictive standards apply:

1. A "more stringent"[104] state law prohibits certain disclosures without express authorization (e.g., information related to HIV/AIDS or mental illness);
2. The PHI is a substance abuse treatment record governed by 42 C.F.R. Part 2;
3. The Covered Entity is subject to more restrictive federal standards governing privacy and confidentiality (e.g., Title X grantees and Community Health Centers); or
4. The information is held in a record covered by FERPA.

Common Rule: In order for researchers to collect or use an individual's information for research, every entity involved in the research process must comply with requirements set forth in Subpart A.

1. Research Institutions. Every institution engaged in non-exempt research must submit a written assurance stating that it will comply with the Common Rule's requirements.[105] Federal departments and agencies also have authority to enforce Common Rule compliance directly against IRBs operated by institutions that do not hold a written assurance.[106] Where research takes place at an institution in which IRB oversight is conducted by an IRB not operated by that institution, the institution and the organization operating the IRB must document the institution's reliance on the IRB for research oversight and the responsibilities each entity will undertake to ensure compliance with the Common Rule's requirements.[107]

2. Institutional Review Boards (IRBs). An IRB must review and approve all non-exempt research protocols in accordance with Common Rule requirements,[108] such as determining that, where appropriate, there are adequate provisions to protect subjects' privacy and to maintain data confidentiality.[109] IRBs also must review research at least annually or—as determined by the IRB[110]—more frequently, depending on the degree of risk involved[111] (IRBs may use an expedited review process for eligible research activities,[112] including for exempt research protocols where limited review is required as a condition of exemption[113]).

Beginning on January 20, 2020,[114] all institutions engaged in cooperative research (with very limited exceptions) must rely on a single IRB for study approval.[115]

Part 2: Disclosure of Part 2 patient identifying information without written consent is permitted for limited purposes, including:

1. To medical personnel who need the information to treat a patient during a medical emergency in which the patient's prior informed consent could not be obtained;[116]
2. By the program or other lawful holder of Part 2 data for purposes of conducting scientific research, if the Part 2 program director determines that the information recipient meets one or both of the following requirements, as applicable:
    a. Is a HIPAA Regulated Entity and has obtained patient authorization or a HIPAA-compliant authorization waiver or alteration; and/or
    b. Is subject to the Common Rule and provides documentation that the recipient is in compliance with the Common Rule or is conducting research exempt from the Common Rule.[117]

3. By scientific researchers using data obtained from a Part 2 program in research reports, if the data is in aggregate form and all patient identifying information has been rendered non-identifiable.[118]
4. To certain specified entities for audit and evaluation activities of the program;[119]
5. To the parent, guardian, or authorized representative of a minor applicant for substance use disorder service of facts relevant to reducing a substantial threat to the life or physical well-being of any individual if the program director determines that the disclosure may reduce such a threat and that the minor lacks capacity to consent to the disclosure;[120] and
6. By the program director about a patient (other than a minor patient or those adjudicated incompetent) who has a medical condition that prevents knowing or effective action on their own behalf for purposes of obtaining payment for services from a third-party payer.[121]

Researchers using patient identifying information obtained from a Part 2 program may request linkages to data sets from a data repository holding patient identifying information if the request is reviewed and approved by an IRB registered with HHS.[122]

This includes disclosing whether an individual is or has been a patient with the program.[123] The restrictions on disclosure also apply to individuals and entities that have received patient records directly from Part 2 programs or from other lawful holders of patient identifying information and who have been properly notified of the prohibition on re-disclosure.[124]

GINA: Title I prohibits health plans and health insurance issuers from using genetic information to make eligibility, coverage, underwriting, or premium-setting decisions about covered individuals.[125] Generally, health plans and issuers may not request or require that beneficiaries undergo genetic testing or provide genetic information.[126] However, health plans may request that beneficiaries voluntarily provide genetic information for research, require genetic information for determining medical appropriateness of covered services, and obtain genetic information incidentally in the course of obtaining other information.[127]

Title II of GINA prohibits employers from using genetic information to discriminate against employees or applicants[128] and generally may not acquire employee or applicant genetic information,[129] subject to exceptions that are limited to legitimate business purposes. Title II also governs the confidentiality of acquired genetic information. Genetic information must be kept confidential and in a medical record separate from the employee's personnel file.[130] Genetic information may be disclosed to the employee at his or her written request and in several other circumstances, including:

1. To an occupational or health researcher; and
2. To a public health organization, if the information concerns a contagious disease that presents an imminent threat of serious harm or death and the employee is informed of the disclosure.[131]

Privacy Act of 1974: The Privacy Act allows a federal agency to release individually identifiable information to identified individuals (or to their designees with written consent) or pursuant to one of 12 exemptions for disclosure.[132] These exemptions include disclosure to federal agency employees, the Census Bureau, the National Archives and Records Administration, other government entities for civil and criminal law enforcement purposes, the Comptroller General, Congress or its committees, and a consumer reporting agency. Additional exemptions include disclosures for statistical research, disclosures required by FOIA, disclosures in response to emergency circumstances, and disclosures pursuant to a court order. In addition, research is commonly included as a permitted release under agency systems of records (SORs). FOIA requires federal executive agencies to disclose their records to individuals upon request, subject to nine exemptions. These exemptions prevent the disclosure of

information that is considered sensitive or of a personal nature, including information about a specific individual contained in personnel or medical files, the disclosure of which would be an "unwarranted invasion of personal privacy."[133]

Family Educational Rights and Privacy Act (FERPA): An educational agency or institution (or its agent) may disclose "education records" without written consent in several circumstances, which include:

1. When released to authorized representatives of the Comptroller General, the Attorney General, the Secretary of Education, or state and local educational authorities;
2. When a disclosure is required by law, judicial order, or subpoena;
3. When the disclosure is to accrediting organizations to perform accrediting functions;
4. When disclosed to organizations that conduct studies related to: predictive test development, validation, or administration; student aid program administration; and instructional improvements for or on behalf of educational agencies or institutions;
5. When disclosed to Department of Agriculture or Food and Nutrition Services representatives that need the information to monitor and evaluate the child nutrition programs; and
6. When disclosure is needed in an emergency to protect the health and safety of the student or others; and
7. To a parent about their postsecondary student's violation of any federal, state, or local law or institutional rule or policy governing the use or possession of alcohol or a controlled substance, if the student is under 21 at the time of disclosure (unless such disclosure is prohibited by state law).[134]

Consent/Authorization

Information may be accessed and used without the individual subject's approval for certain purposes and in certain circumstances. Beyond these situations, privacy and/or human subjects protection laws generally require entities like researchers and providers to obtain the individual's consent or authorization prior to collecting, using, or sharing data about that individual. Whether consent or authorization is necessary will depend upon the content of the data and the purposes for collecting or sharing the data. Consent/authorization procedures generally require notifying individuals of the intended uses and disclosures of their information and having individuals execute a document stating that they consent to or authorize the uses or disclosures of their information. Additional protections or considerations related to consent or authorization may apply where the subject is a special class (e.g., minor, pregnant woman, prisoner, etc.). In general, the term "consent" is used to refer to informed consent to participate in research (a concept governed by the Common Rule). Authorization is used to refer to authorization given by an individual subject of information to an entity to disclose that information to a third party. Authorization is a term used in HIPAA, and here it is used to encompass all similar permissions (e.g., as they apply to Part 2, GINA, etc.). Specific requirements that pertain to the content of an authorization to disclose information or an informed consent form are provided in Table 3 below.

Table 3: Federal Requirements for Consent to Disclose Identifiable Health Information

	HIPAA[135]	Common Rule[136]	GINA[137]	Part 2[138]	Privacy Act[139] (HHS)
Required elements:					
Patient's name				X	
Specific description of information[140]	X	X	X	X	X
Identify person(s) or entity authorized to make the requested disclosure	X			X	
Identify person(s) or entity authorized to receive the requested information	X	X	X	X	X
Describe the intended use(s) of the requested information[141]	X	X	X	X	X
The expiration date or event	X	X		X	
Date signed	X	X		X	
Signature (and/or electronic signature where acceptable) of the individual or his/her personal representative	X	X		X	
Provide the following information:					
The individual's right to withdraw authorization (if any) and any applicable exceptions to that right.	X	X		X	
Whether any benefits may be conditioned on releasing the information and applicable consequences of refusal to consent. This includes stating that refusal will involve no penalty or loss of benefits where relevant.	X	X	X		
The potential for re-disclosure of the information (if any). This includes stating that information may not be re-disclosed without further authorization, where applicable.	X	X		X	
Other requirements:					
The authorization must be written in plain language.	X	X			
Provide the individual with a copy of the form.	X	X			

Key Statutes and Regulations Related to Consent/Authorization

Health Insurance Portability and Accountability Act (HIPAA): As a threshold matter, the Privacy Rule requires written authorization for any disclosure except those required by the Rule. Where a personal representative is authorized to act on behalf of the individual (discussed above in section on Subjects), the personal representative may execute a valid authorization.

Common Rule: In general, an individual must give specific informed consent to participate in research before the research may begin.[142] The primary researcher must comply with several requirements related to obtaining and documenting informed consent, including providing specific information about the research protocol to potential participants.[143] IRBs may waive or alter some or all informed consent requirements under certain circumstances.[144] Note that there is a different set of waiver and alteration criteria and requirements for research involving public benefit or service programs conducted by or subject to the approval of state or local officials.[145]

An IRB may approve a research proposal in which an investigator will obtain identifiable private information without informed consent for the purpose of "screening, recruiting, or determining

eligibility" of prospective subjects, if the investigator will obtain the information through oral or written communication with the prospective subject or by accessing records or stored identifiable biospecimens.[146] In addition to including standard elements in the informed consent, investigators must also provide specific information where it is relevant to the research protocol.[147] This includes informing the participant about the following:

1. Biospecimens may be used for commercial profit and whether the participant will or will not share in such profit;[148]
2. Whether or not clinically relevant research results, including individual research results, will be disclosed to participants and, if so, under what conditions;[149] and
3. For research involving biospecimens, whether the research will or might include whole genome sequencing.[150]

Broad consent is a special kind of informed consent required for certain secondary use of identifiable biospecimens and identifiable private information (in addition to other requirements—see above sections discussing exemptions). Because a secondary use is a use other than that for which the biospecimen or private information was originally collected, researchers may seek a participant's consent to future unspecified research during the initial informed consent process. Where participants give such "broad consent," additional informed consent would not be required for the same or another researcher to use the information or biospecimens collected during the original research study. Researchers may rely on broad consent to conduct studies on stored information or biospecimens in lieu of seeking IRB waiver of the specific informed consent requirement. Broad consent incorporates some parts of the specific informed consent process, such as rules governing how consent can be obtained[151] and requirements for information that must be provided to the subject,[152] and includes requirements for provision of information specific to secondary use.[153]

Part 2: Part 2 bars most disclosures of that information without written consent by the patient and/or his/her personal representative.[154] This includes disclosing whether an individual is or has been a patient with the program.[155] Programs may disclose substance use disorder patient information with valid written consent from the patient.[156] There are certain other requirements for consent in special circumstances (e.g., minors, disclosures to central registries, etc.). A valid consent must include nine separate elements (see Table 3),[157] including identification of the intended recipient of the information. If the intended recipient is an individual, an entity with a treating relationship with the patient, or a third-party payer, the consent must specifically name the recipient.[158] If the recipient is an entity without a treating relationship with the patient (other than a third-party payer), the consent must give the entity's name *and:*

- The name(s) of an individual participant with the entity (e.g., Dr. Smith, Research Scientist at Jones Research Institution);
- The name of an entity participant(s) with a treating provider relationship with the patient (e.g., Southeastern Hospital, member of Eastern HIO); or
- A general designation of an individual or entity participant or class of participants, limited to those with a treating provider relationship with the patient (e.g., all current and future treating providers at Northern Academic Medical Center).[159]

Part 2 allows minors to consent to disclosure if their state grants minors the legal capacity to seek treatment without parental consent. In such states, only the minor can consent to information disclosure. If the state requires the minor to obtain parental consent before receiving substance abuse

treatment, then both the minor and the parent/guardian must give written consent to disclosure (special rules apply when a minor lacks the capacity to make a rational choice). Note that there is no payment exception to the consent rule. That is, a provider must obtain the written consent of the minor (and the parent/guardian if the state does not give the minor capacity to consent to treatment) before disclosing information to a third-party payer.

GINA: Genetic information may be disclosed to the employee at his or her written request.

Privacy Act of 1974: The Privacy Act allows a federal agency to release individually identifiable information to identified individuals (or to their designees with written consent).

Family Educational Rights and Privacy Act (FERPA): An educational agency or institution (or its agent) may only disclose "education records" with written parental consent or the consent of a student age 18 or older or enrolled in a postsecondary institution, unless an exception applies.

Security

Security refers to the means by which data are protected from unauthorized use or access. Various federal laws and regulations set forth requirements for security measures that must be in place to protect identifiable health information. Security measures generally include technical, administrative, and physical safeguards. Technical safeguards include items such as encryption, firewalls, passwords, antivirus software, and SSL/TLS transmission. Physical safeguards include measures that limit an individual's access to facilities, workstations, and devices that house data or may be used to access data (e.g., policies that limit server room access to authorized personnel). Administrative safeguards include plans and policies for identifying security risks, preventing security breaches, monitoring security, remedying security breaches, and training employees on proper security procedures.

Key Statutes and Regulations Related to Security

Health Insurance Portability and Accountability Act (HIPAA): The Security Rule requires Regulated Entities to establish and maintain reasonable and appropriate administrative, physical, technical, and organizational safeguards for protecting PHI that the Regulated Entity creates, receives, maintains, or transmits in electronic form (known as e-PHI).[160]

Regulated Entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted or required by the Privacy Rule; and
4. Ensure its workforce's compliance with the Security Rule.[161]

The Security Rule provides Regulated Entities considerable flexibility in meeting these requirements. Entities may use any security measure that allows them to reasonably and appropriately implement the Rule's standards and implementation specifications.[162] However, when deciding which security measures to use, an entity must always account for several factors, including: its size, complexity, and capabilities (including technical infrastructure, hardware, and software capabilities); the costs of security measures; and the probability and criticality of potential risks to e-PHI.[163]

Part 2: Part 2 programs and any other lawful holder of patient identifying information must have policies and procedures in place to protect against unauthorized uses and disclosures of information as well as any reasonably anticipated threats or hazards to the security of patient identifying information.[164] These policies must address transfer/transmission, removal, destruction, maintenance, use, and access with respect to paper and electronic records, as well as information de-identification and creation and receipt of electronic information.[165]

Legal Status

Legal Status refers to rights and responsibilities related to the data that may be triggered by ownership rights, agency principles, and/or contractual obligations. Legal status determines who may assert rights to that information. Individuals or entities with ownership interests may grant, restrict, or deny access to information. Contractual obligations, such as data use agreements, vendor contracts, or terms of service agreements, may apply. Principles of agency may give a researcher the rights and obligations of the healthcare organization that employs him or her. Finally, some state laws, such as consumer protection and patient privacy laws, may confer rights and responsibilities with respect to access to data or data held by researchers.

Key Statutes and Regulations Related to Legal Status

Health Insurance Portability and Accountability Act (HIPAA): HIPAA sets forth requirements for Covered Entities to enter into contractual arrangements in certain circumstances.

A Covered Entity may permit a Business Associate to create, receive, maintain, or transmit PHI on the Covered Entity's behalf but must first enter into a written contract or similar arrangement (i.e., a Business Associate Agreement) with the Business Associate that meets relevant requirements.[166] The contract provides assurances that the Business Associate will appropriately safeguard the PHI and must include several provisions relating to the obligations of both parties.[167]

When disclosing a limited data set (LDS) without first obtaining the individual subject's authorization, which is permissible for purposes of research, healthcare operations, and public health functions and activities, the Covered Entity must enter into a data use agreement (DUA) with the intended recipient of the LDS.[168] A DUA provides assurances to the disclosing Covered Entity that the intended recipient of the LDS will only use or disclose that PHI for limited purposes and must contain certain of information.[169] If a Covered Entity knows of a pattern of activity or practice of the LDS recipient that constitutes a material breach or violation of the DUA, the Covered Entity must take reasonable steps to cure the breach or end the violation, as applicable.[170] If such steps are unsuccessful, the Covered Entity must discontinue PHI disclosures to the recipient and report the problem to the HHS Secretary.

State Law: A number of areas of state law may apply to health care and research, including the areas of consumer protection, privacy, research practices, and health information exchange. Some states have laws addressing ownership of health information in particular. States generally have laws governing allowable terms and enforcement of contracts. States may also have laws that address the creation of an agency relationship or the scope of an agent's authority, but interpretation of agency is typically left to courts. Contracts may include terms related to an agency relationship and terms as well.

REFERENCES

[1] HIPAA, Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 45 U.S.C.).

[2] 45 C.F.R. Parts 160 and 164 (2017).

[3] 45 C.F.R § 160.103 (2017).

[4] 45 C.F.R § 160.103 (2017).

[5] Note that HIPAA also does not apply to what FERPA defines as "treatment records," which are excluded from FERPA's definition of "education records" (45 C.F.R. § 160.103, referencing 20 U.S.C. § 1232g(a)(4)(B)(iv)).

[6] 45 C.F.R §160.103 (2017); 45 C.F.R Part 164 §§ 302, 400, and 500(a) (2017).

[7] U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (2012), *available at*: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[8] 45 C.F.R. § 164.514(b)(2)(i) (2017).

[9] 45 C.F.R. § 164.514(b)(2)(ii) (2017).

[10] 45 C.F.R. § 164.514(e)(2) (2017).

[11] 45 C.F.R. § 164.514(b)(1) (2017).

[12] 45 C.F.R. Part 46, Subpart A (2017) (note: HHS version of the Common Rule).

[13] "Common Rule" Departments and Agencies, Notice of Proposed Rulemaking: Federal Policy for the Protection of Human Subjects, 80 Fed. Reg. 53933 (2017).

[14] "Common Rule" Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (2017).

[15] 82 Fed. Reg. 7149 at 7260-61 (to be codified at 45 C.F.R. § 46.102(l)).

[16] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)).

[17] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).

[18] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).

[19] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(4)).

[20] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104).

[21] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[22] Note: benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, and not likely to have a significant, adverse, lasting impact on the participants; further, the researcher must not have any reason to think the participants will find the interventions offensive or embarrassing (82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(ii)).

[23] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)). (Note that this exemption is only available to research with an adult participant, and the participant must prospectively agree to the intervention and information collection).

[24] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(ii)). (Note that for secondary research use in this context, the researcher may not contact and will not re-identify the subject).

[25] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(iii)). (Note: "research" and "health care operations" are defined at 45 C.F.R. § 164.501 (2017); "public health activities and purposes" are defined at 45 C.F.R. § 164.512(b) (2017)).

[26] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(5)). (Note: each federal department or agency must establish (on a publicly accessible federal website or in another manner determined by the department or agency head) a list of the research or demonstration projects it conducts or supports under this provision).

[27] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[28] Note: benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, and not likely to have a significant, adverse, lasting impact on the participants; further, the researcher must not have any reason to think the participants will find the interventions offensive or embarrassing (82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(ii)).

[29] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)). (Note that this exemption is only available to research with an adult participant, and the participant must prospectively agree to the intervention and information collection).

[30] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(7)). (Note: for this exemption, the information obtained by the researcher may be recorded in a way that allows the participant's identity to be readily ascertained, directly or through linked identifiers).

[31] 82 Fed. Reg. 7149 at 7262-63 (to be codified at 45 C.F.R. § 46.104(d)(7)).

[32] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)).

[33] 82 Fed. Reg. 7149 at 7262-63 (to be codified at 45 C.F.R. § 46.104(d)(7)). (Note that broad consent must be obtained in accordance with relevant requirements).

[34] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)).

[35] 42 C.F.R. Part 2 (2017).

[36] HHS Substance Abuse and Mental Health Services Administration (SAMHSA) Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 NPRM") 81 Fed. Reg. 6988 (2016).

[37] SAMHSA Supplemental Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Supplemental NPRM") 82 Fed. Reg. 6052 (2017).

[38] SAMHSA Final Rule: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Final Rule") 82 Fed. Reg. 5485 (2017).

[39] Indirect identification could occur by reference to other publicly available information or through verification of such an identification by another person.

[40] 42 C.F.R. § 2.12(a)(1) (2017).

[41] 42 C.F.R. § 2.11 at "Patient identifying information" (2017) (Note that this definition explicitly does not include a number assigned to [an individual] by a [Part 2] program if that number does not consist of or contain numbers (e.g., social security number or driver's license number) that could be used to identify [the individual] with reasonable accuracy and speed from sources external to the [Part 2] program).

[42] Note that a genetic test is defined as "analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes" (*see, e.g.,* GINA Title I, § 101(d) (2008)).

[43] Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 at 5689 (2013) (codified at 45 C.F.R. § 160.103 at "Health information" (2017)).

[44] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

[45] 5 U.S.C. § 552a(a)(4) (1974).

[46] 20 U.S.C. § 1232g(b)(1).

[47] 34 C.F.R. § 99.3 (2017).

[48] 34 C.F.R. § 99.3 (2017).

[49] 45 C.F.R. § 160.103 at "Person" (2017) (An entity can be a trust or estate, partnership, corporation, professional association or corporation, or other public or private entity).

[50] 45 C.F.R. § 160.103 at "Protected health information" ¶ (2)(iv) (2017).

[51] 45 C.F.R. § 164.502(g)(1) (2017).

[52] 45 C.F.R. § 164.512(g)(2)(2017).

[53] 45 C.F.R. § 164.512(g)(3)(i) (2017).

[54] 45 C.F.R. § 164.501 at "Inmate" (2017).

[55] 45 C.F.R. § 164.512(k)(5)(i) (2017).

[56] 45 C.F.R. § 164.512(k)(5)(iii) (2017).

[57] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)).

[58] 45 C.F.R. § 46.201(a) (2017).

[59] 45 C.F.R. § 46.301(a) (2017).

[60] 45 C.F.R. § 46.401(a) (2017).

[61] 42 C.F.R. § 2.11 at "Patient" (2017).

[62] 42 C.F.R. § 2.14(a) (2017).

[63] 42 C.F.R. § 2.14(b) (2017).

[64] 42 C.F.R. § 2.14(c) (2017).

[65] "Genetic information" is: (1) information about an individual's genetic tests (i.e., analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations or chromosomal changes); (2) information about the individual's family members' genetic tests; (3) information about the manifestation of a disease or disorder in the individual's family members; (4) requests for or receipt of genetic services (i.e., a genetic test, genetic counseling, or genetic education) by the individual, and (5) participation by the individual or any of the individual's family members in clinical research that includes genetic services (*see, e.g.,* GINA Title I, § 101(d) (2008)).

[66] GINA does not apply to individuals in the U.S. military, those receiving health benefits through the VA or Indian Health Service, or federal employees obtaining health care through the Federal Employees Health Benefits Plan (FEHBP).

[67] 5 U.S.C. § 552a(a)(2) (1974).

[68] 34 C.F.R. § 99.3 (2017).

[69] A healthcare clearinghouse is a business or agency that processes nonstandard health information it receives from another entity into a standard format, or vice versa (e.g., billing services, re-pricing companies) (45 C.F.R. § 160.103 (2017)).

[70] Covered transactions include, but are not limited to, benefit eligibility inquiries and claims (*see generally* 45 C.F.R. Part 162 (2017)).

[71] 45 C.F.R §160.103 (2017).

[72] 45 C.F.R §160.103 (2017) (Business Associate services are limited to legal, actuarial, accounting, consultation, data aggregation, management, administrative, accreditation, or financial services; relevant functions include claims processing, data analysis, utilization review, and billing).

[73] *See, e.g.* OCR Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (2013).

[74] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).

[75] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(l)).

[76] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.102(l)(2)).

[77] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104).

[78] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(i)).

[79] 5 U.S.C. § 552a (1974).

[80] 5 U.S.C. § 552a (1974).

[81] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(iv)) (Note: identifiable private information generated by the research must be maintained on information technology subject to and in compliance with the Privacy Impact Assessments requirements of the E-Government Act of 2002's Privacy Provisions (44 U.S.C. § 3501 note at § 208(b) (2002)) and, if applicable, the information used in the research must have been collected subject to the Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 *et seq.*)).

[82] 42 C.F.R. § 2.2(a) (2017).

[83] SAMHSA. "Applying the Substance Abuse Confidentiality Regulations: FAQs" at Question 10 (2011), *available at*: https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs.

[84] 42 C.F.R. § 2.11 at ¶ "Program" (2017).

[85] 42 C.F.R. § 2.12(b) (2017).

[86] 42 C.F.R. § 2.12(d)(2)(i) (2017).

[87] 34 C.F.R. § 99.1 (2017).

[88] HUD are devices intended to benefit patients in treating or diagnosing a disease that affects or is manifested in 4,000 or fewer individuals in the United States annually.

[89] 45 C.F.R. § 164.502(a)(2) (2017).

[90] 45 C.F.R. § 164.502(a)(5) (2017).

[91] 45 C.F.R. § 164.502(d)(2) (2017).

[92] 45 C.F.R. § 164.502(g) (2017).

[93] 45 C.F.R. Part 164, §§ 510 512 (2017).

[94] 45 C.F.R. § 164.502(a)(1) (2017).

[95] *See e.g.*, 45 C.F.R. Part 164, §§ 510 512 (2017); OCR."Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html; OCR Disclosures for Public Health Activities (2003), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf; OCR Research: 45 C.F.R. Part 164 §§ 501, 508, 512(i) (2003), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf; OCR Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care (2015), *available at* http://www.hhs.gov/sites/default/files/provider_ffg.pdf.

[96] Disclosures for these purposes are not subject to the minimum necessary limitation (45 C.F.R. § 164.502(b)(2)(i) (2017)).

[97] A health oversight agency is defined by HIPAA as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant" (45 C.F.R. § 164.501 (2017)).

[98] Providers must inform patients of directory disclosures and give them the opportunity to object to such disclosures or restrict them (may be accomplished via the provider's Notice of Privacy Practices or a verbal acknowledgement) (45 C.F.R. § 164.510(a)(2) (2017)). If patient is incapacitated, provider may make directory disclosures, but as soon as practicable, must inform patient of such disclosures and give patient the opportunity to object to or restrict further disclosures (45 C.F.R. § 164.510(a)(3) (2017)).

[99] Providers must give patients the opportunity to agree or object to such disclosures, by obtaining the patient's verbal or written approval, giving the patient the opportunity to object verbally or in writing, or inferring, based on professional judgment, that the patient does not object to such a disclosure and that disclosure is in the patient's best interest (45 C.F.R. § 164.510(b)(2) (2017)). If the patient is incapacitated, the provider may disclose if, using professional judgment, s/he determines that it is in the patient's best interest (45 C.F.R. § 164.510(b)(3) (2017)).

[100] 45 C.F.R. § 164.502(b) (2017).

[101] The Privacy Rule specifies limited circumstances in which a Covered Entity is permitted to rely on a requested disclosure as the minimum necessary (assuming such reliance is reasonable under the circumstances) (45 C.F.R. § 164.514(d)(3)(iii) (2017)). These circumstances include: (1) disclosures to public officials permitted under § 164.512; (2) information requested by another Covered Entity; (3) requests made by a professional who is member of its workforce for purposes of providing professional services to the Covered Entity; (4) requests made by its Business Associate for the purpose of providing professional services to the Covered Entity; (5) research disclosures under § 164.512, if appropriate documentation has been provided.

[102] 45 C.F.R. § 164.514(d)(3)(iii) (2017).

[103] 45 C.F.R. § 164.502(b)(2) (2017).

[104] 45 C.F.R. § 160.203(b) (2017).

[105] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.103).

[106] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).

[107] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.103(e)).

[108] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a)).

[109] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(7)).

[110] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.108(a)(3)(i)).

[111] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.109(e)).

[112] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(b)) (Note: expedited review is available for: (1) research appearing on the list of categories published by the HHS Secretary in the Federal Register and available through OHRP unless the reviewer determines that the study involves more than minimal risk; (2) minor changes in previously approved research during the period for which approval is authorized; and (3) research for which limited review is a condition of exemption).

[113] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110).

[114] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(2)).

[115] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(1)).

[116] 42 C.F.R. § 2.51(a)(1) (2017).

[117] 42 C.F.R. § 2.52(a) (2017).

[118] 42 C.F.R. § 2.52(b)(3) (2017).

[119] 42 C.F.R. § 2.53 (2017).

[120] 42 C.F.R. § 2.14(c) (2017).

[121] 42 C.F.R. § 2.15(a)(2) (2017).

[122] 42 C.F.R. § 2.52(c)(1)(i) (2017).

[123] 42 C.F.R. § 2.13(c)(1) (2017)

[124] 42 C.F.R. § 2.12(d)(2)(i) (2017).

[125] *See, e.g.* GINA Title I, § 102(a)(4) (2008) (Note: GINA does not apply to life insurance, casualty insurance, or long term care insurance).

[126] *See, e.g.* GINA Title I, § 101(b) (2008).

[127] *See, e.g.* GINA Title I, § 101(b) (2008).

[128] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. 2000ff-1(a) (2008).

[129] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. 2000ff-1(a) (2008).

[130] GINA Title II, § 206(a), codified at 42 U.S.C. 2000ff-5(a) (2008).

[131] GINA Title II, § 206(b), codified at 42 U.S.C. 2000ff-5(b) (2008).

[132] 5 U.S.C. § 552a(b) (1974).

[133] 5 U.S.C. § 552(b)(6) (1974).

[134] 34 C.F.R. § 99.31 (2017).

[135] 45 C.F.R. §164.508(c)(1) (2017).

[136] 45 C.F.R. Part 46 §§ 116(a),117(a) (2017).

[137] GINA Title II, § 206(b), 42 U.S.C. 2000ff-5(b) (2017).

[138] 42 C.F.R. § 2.31(a) (2017).

[139] 5 U.S.C. § 552a (as amended) (2017).

[140] Note that for a consent under Part 2, the information to be disclosed must be limited to the minimum amount of information necessary to accomplish the stated purpose of the disclosure (42 C.F.R. § 2.31(a)(5) (2017)).

[141] Note that in the case of an authorization for use or disclosure of PHI for future research purposes, the authorization must adequately describe such purposes so that it would be reasonable for the individual to expect his or her PHI could be used for such future research (OCR. Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 82 Fed. Reg. 5566 at 5612 (2013)).

[142] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(4)).

[143] 82 Fed. Reg. 7149 at 7265-67 (to be codified at 45 C.F.R. § 46.116).

[144] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(f)).

[145] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(e)) (Note: this is distinct from research and demonstrations projects conducted or supported by a federal department or agency that are designed to study, evaluate, improve, or examine public benefit or service programs, which are exempt from Common Rule requirements entirely (*see* 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(5)).

[146] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(g)).

[147] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)).

[148] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(7)).

[149] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(8)).

[150] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(9)).

[151] 82 Fed. Reg. 7149 at 7265-66 (to be codified at 45 C.F.R. § 46.116(a)(1)-(4), (6)).

[152] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(d)(1)).

[153] 82 Fed. Reg. 7149 at 7266-67 (to be codified at 45 C.F.R. § 46.116(d)(2)-(7)).

[154] 42 C.F.R. §§ 2.2(b)(1) and 2.13 (2017).

[155] 42 C.F.R. § 2.13(c)(1) (2017).

[156] 42 C.F.R. § 2.33 (2017).

[157] 42 C.F.R. § 2.31(a) (2017).

[158] 42 C.F.R. § 2.31(a)(4)(i), (ii), and (iii)(A) (2017).

[159] 42 C.F.R. § 2.31(a)(4)(iii)(B) (2017).

[160] 45 C.F.R. § 164.306 (2017).

[161] 45 C.F.R. § 164.306(a) (2017).

[162] 45 C.F.R. § 164.306(b)(1) (2017).

[163] 45 C.F.R. § 164.306(b)(2) (2017).

[164] 42 C.F.R. § 2.16(a) (2017).

[165] 42 C.F.R. § 2.16(a)(1)-(2) (2017).

[166] 45 C.F.R. Part 164 §§ 314(a) and 504(e) (2017).

[167] 45 C.F.R. § 164.504(e)(2) (2017).

[168] 45 C.F.R. § 164.514(e)(4)(i) (2017).

[169] 45 C.F.R. § 164.514(e)(4)(ii) (2017).

[170] 45 C.F.R. § 164.514(e)(4)(iii) (2017).

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

CHAPTER 4:

FRAMEWORK FOR NAVIGATING LEGAL AND ETHICAL REQUIREMENTS FOR PCOR

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Chapter 4

Framework for Navigating Legal and Ethical Requirements for PCOR

INTRODUCTION

Building on Chapters 2 and 3, this chapter presents a visual decision tool that highlights the key considerations associated with the spectrum of data used for PCOR and the nature of the relationships between researchers and other stakeholders. This Framework is built on the data characteristics and types (discussed in the previous chapters) that are critical to navigating legal and ethical requirements that govern use and exchange of data for PCOR.

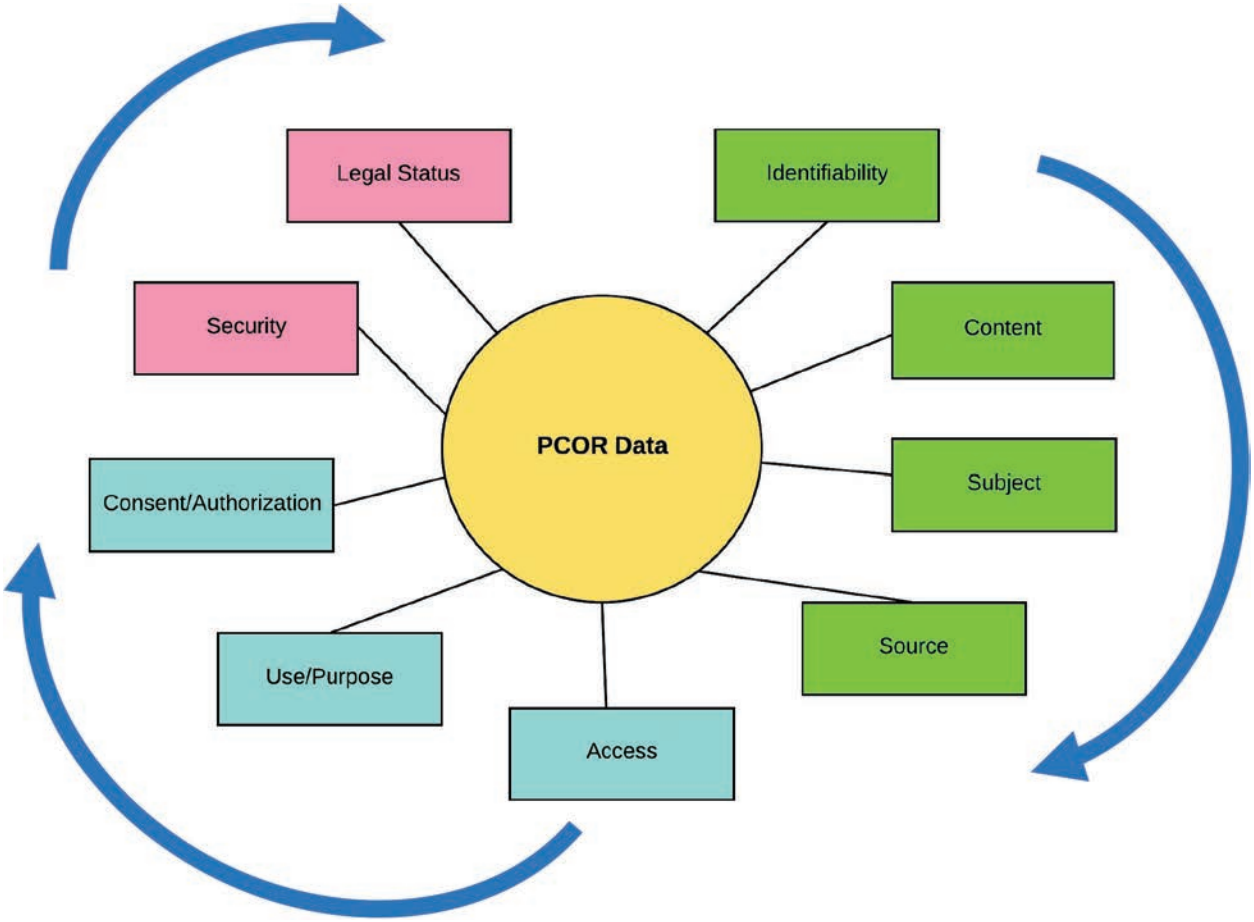
PCOR FRAMEWORK

This Framework is designed to serve as a decision tool for PCOR researchers that addresses the key data characteristics and considerations (previously discussed in Chapter 2) both individually and collectively. While the characteristics presented here are by no means exclusive, they represent the key characteristics of data that determine what legal requirements and ethical principles apply for research use of that data.

- Identifiability: Refers to the ability to link information to particular individuals.
- Content: Refers to the subject matter or substance of the data.
- Subject: Refers to the person or thing that is the focus of the data.
- Source: Refers to the person, entity, and/or setting in which the data originated or was collected.
- Access: Refers to the ability of a person or entity other than the individual subject(s) of the information to view, create, edit, or share data.
- Use/Purpose: The intended use or purpose of the data collection will affect whether and how the data may be collected and used.
- Consent/Authorization: Refers to the activities and documentation potentially required of researchers seeking permission to collect, use, or share data about an individual.
- Security: Refers to the means by which data is protected from unauthorized use or access.
- Legal Status: Refers to rights and responsibilities related to data that may be triggered by ownership rights, agency principles, and/or contractual obligations.

These characteristics are not mutually exclusive, and the considerations that surround them are interconnected and frequently overlapping. For example, ownership of a certain data set under the terms of a contract (which is an aspect of "legal status") also determines who may access the data; the content and subject characteristics of data affect how it may be used; and identifiability may determine what consent or authorization must be obtained in order to use the data for research. Users are encouraged to review all of the characteristics thoroughly to determine if/how they apply to their research.

As discussed in Chapter 2, answers to key questions related to these characteristics can help researchers understand the legal and ethical significance of different aspects of data used for PCOR. These data characteristics are displayed as the spokes around a wheel, with the center of the wheel representing PCOR data.



For this chapter, the key characteristics are organized into three color-coded groups according to their priority for decision-making by researchers and are organized around the wheel in the order in which a researcher should consider them, starting with "Identifiability" in the top right position and moving clockwise around to "Legal Status."

Step One: The lime-colored characteristics (Identifiability, Content, Subject, and Source) are the factors that determine whether a statute or regulation applies to the data. A researcher should consider these characteristics first because determinations associated with these characteristics will inform a researcher whether and what statutes and regulations potentially apply and also inform the researcher of the need to move on to the second step for consideration. For example, if a researcher determines that the data in question is identifiable, several statutes and regulations potentially apply, and their requirements will depend on secondary considerations such as Access and Use/Purpose. If a researcher determines that the data is de-identified, then no statute or regulation applies to the data, and the researcher will not need to consider the secondary considerations.

Step Two: The aqua-colored characteristics (Access, Use/Purpose, and Consent/Authorization) are issues that address how a researcher should navigate statutes and/or regulations that apply to the data in question. If a statute and/or regulation applies, the collection or use of the data may be limited or restricted by requirements related to these characteristics.

Step Three: The pink-colored characteristics (Security and Legal Status) involve case-specific determinations relating to data collection and use by a PCOR researcher. For each research protocol, a researcher should consider these characteristics separate and apart from the considerations discussed in steps one and two to the extent they apply. In all cases (as noted at the bottom of each diagram), a researcher should consult with legal counsel (in-house or external), IRB policies and practices, and organizational policies and procedures.

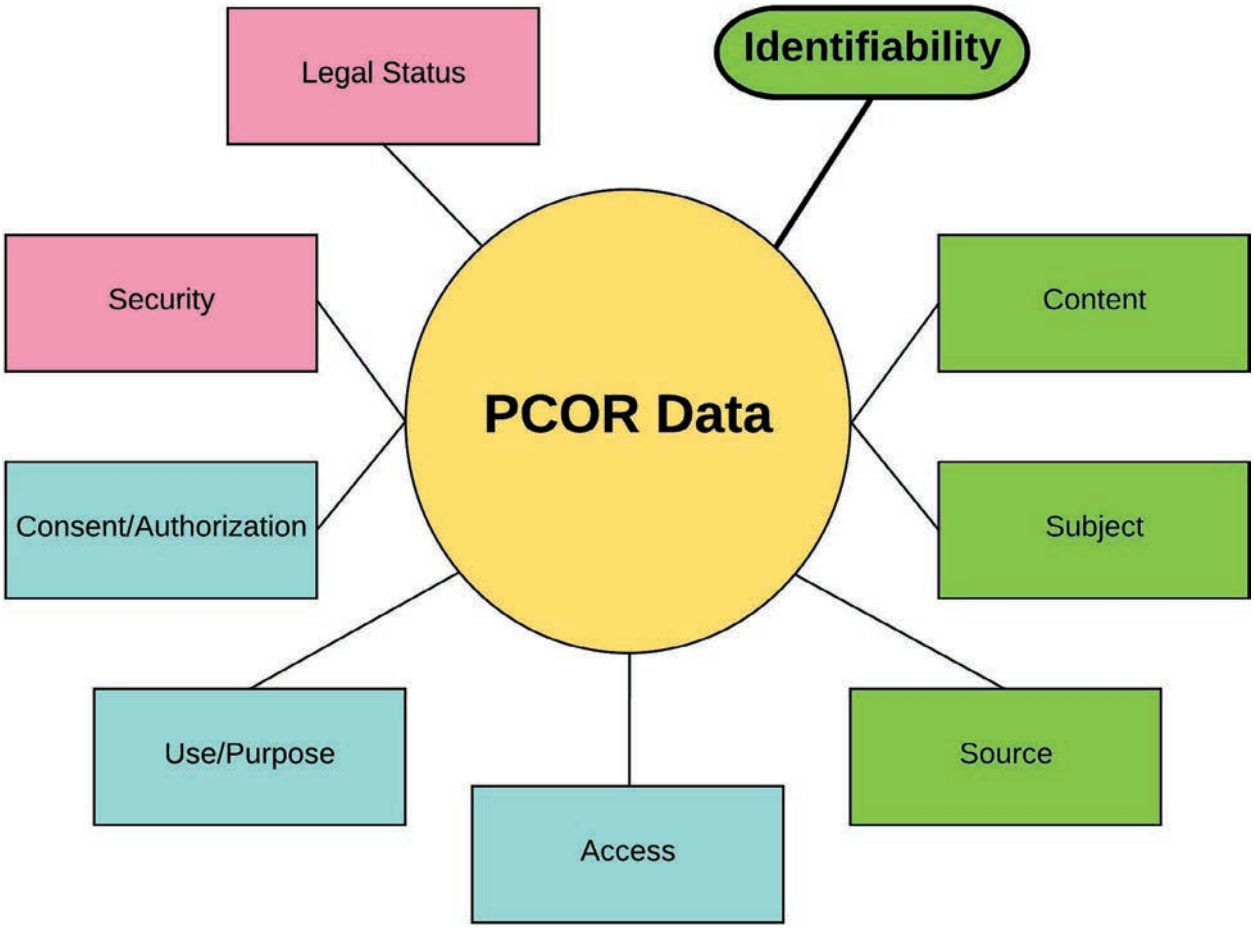
Each characteristic is further explored individually in a decision-oriented structure that illustrates key questions and considerations related to each data characteristic:

- *Key Question:* The content in this column identifies the key questions related to a data characteristic that a researcher must address.
- *What It Means:* The content in this column identifies the meaning and/or interpretation of the key questions related to PCOR.
- *Why It Matters:* The content in this column identifies the legally significant aspects of the issue raised by the question, including identification of any relevant statutes and regulations that are potentially implicated by the issue.
- *Considerations for Next Steps:* The content in this column identifies legal and ethical considerations and activities for PCOR researchers related to each question, including implications for structuring research.
- *General Note:* At the end of each data characteristic's structure are reminders to ensure that research complies with relevant legal and ethical requirements and to identify the parties to consult for further guidance.

This chapter is designed to be a decision tool for PCOR researchers guiding them through a series of considerations specific to the key characteristics that determine whether laws apply to particular data and if so, what requirements attach to collection and use of the data. Potentially applicable laws are referenced throughout the Framework, and complete summaries of key laws are included in Appendix A.

It is important to note that, by design, this chapter does not delve into the complex legal requirements as do Chapters 1, 2, and 3. Rather, as noted above, this chapter provides a decision guide for PCOR researchers to help them understand both the independence and interconnectedness of the characteristics associated with relevant data and a suggested model for assessing and understanding those issues, their relationship to relevant statutes and regulations, and next steps.

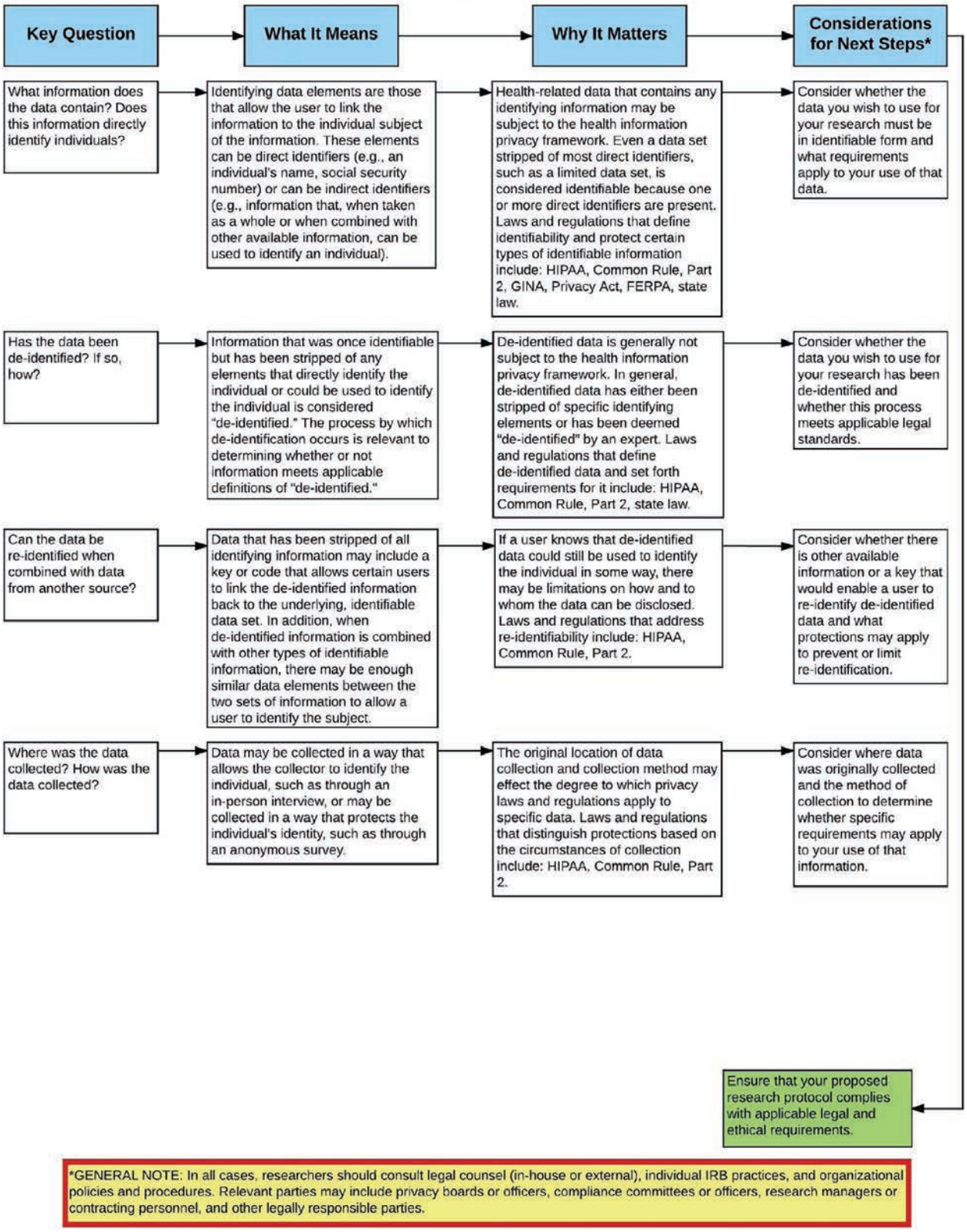
Data Characteristic 1: Identifiability



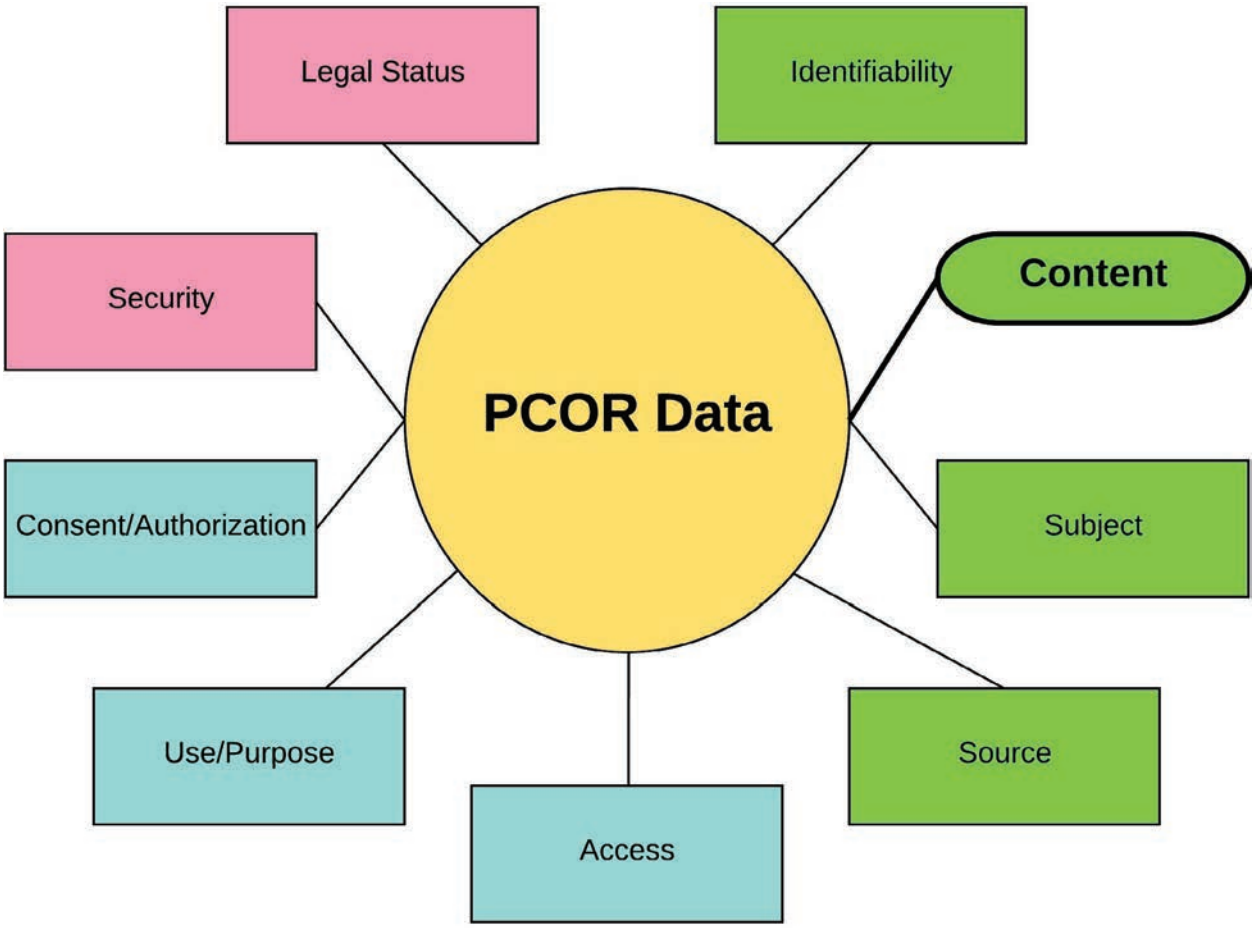
Identifiability

Identifiability refers to the ability to link information to particular individuals.

Identifiability pg. 2



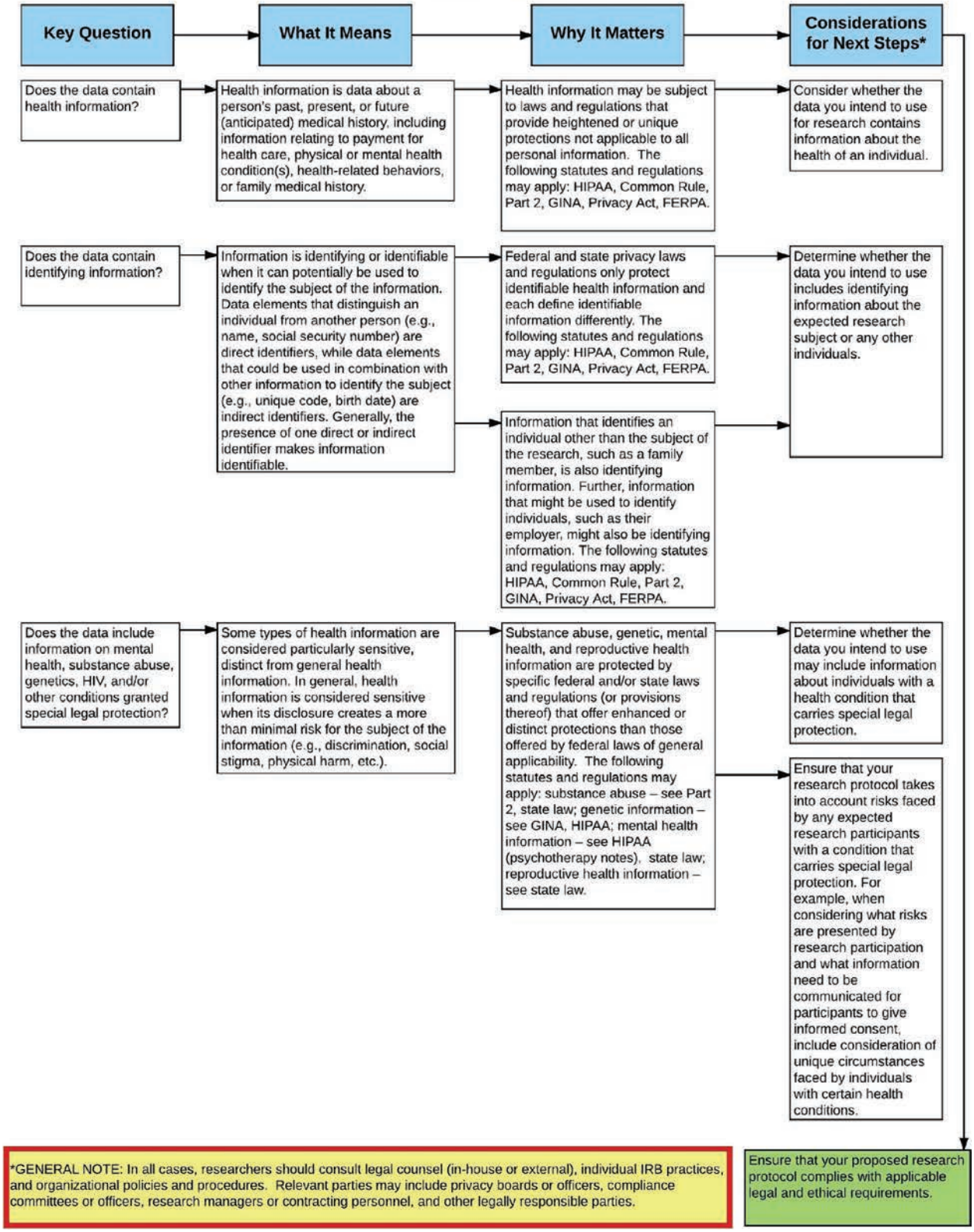
Data Characteristic 2: Content



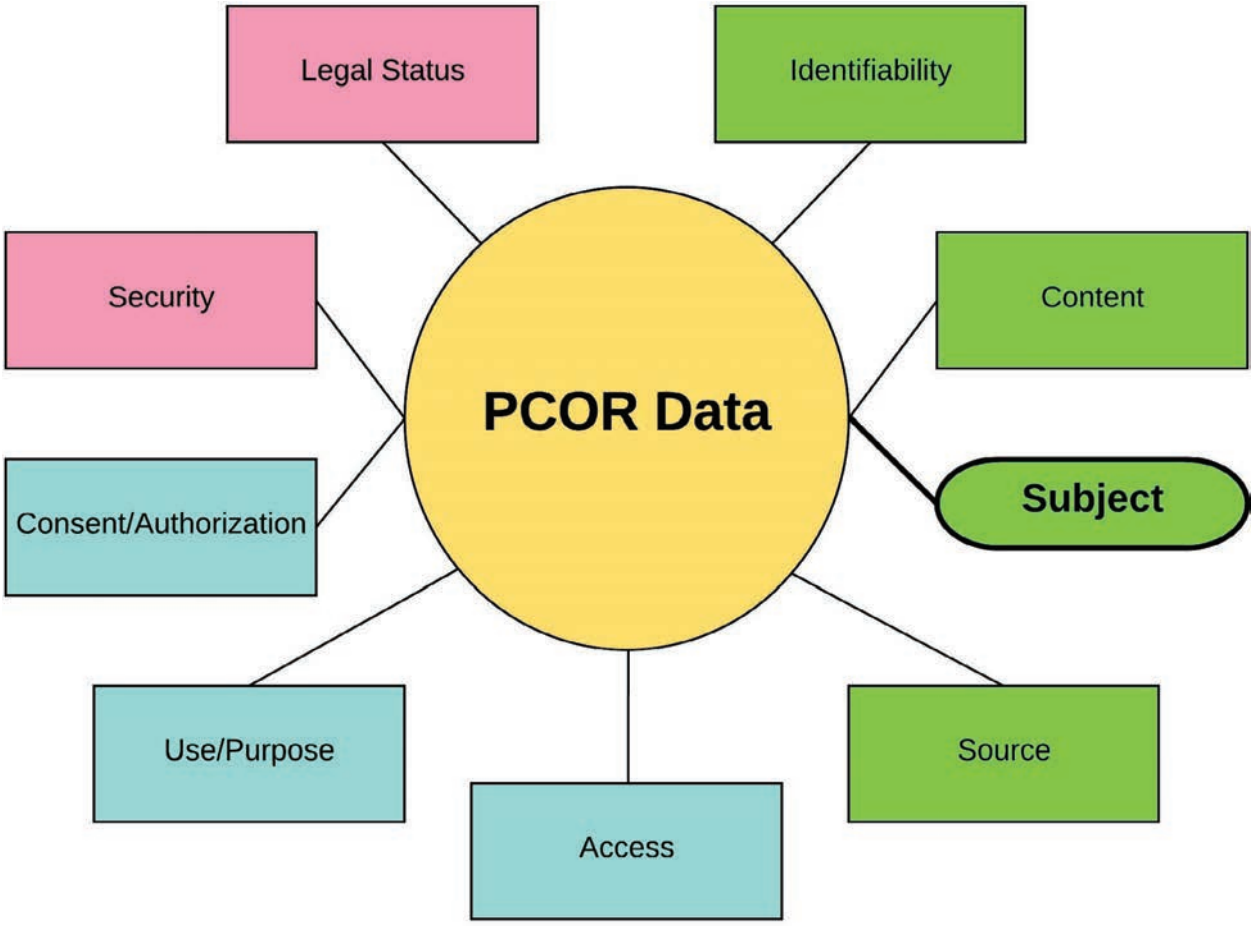
Content

Content refers to the subject matter or substance of the data.

Content pg. 2


Key Question
What It Means
Why It Matters
Considerations for Next Steps*
Does the data contain health information?
Health information is data about a person's past, present, or future (anticipated) medical history, including information relating to payment for health care, physical or mental health condition(s), health-related behaviors, or family medical history.
Health information may be subject to laws and regulations that provide heightened or unique protections not applicable to all personal information. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.
Consider whether the data you intend to use for research contains information about the health of an individual.
Does the data contain identifying information?
Information is identifying or identifiable when it can potentially be used to identify the subject of the information. Data elements that distinguish an individual from another person (e.g., name, social security number) are direct identifiers, while data elements that could be used in combination with other information to identify the subject (e.g., unique code, birth date) are indirect identifiers. Generally, the presence of one direct or indirect identifier makes information identifiable.
Federal and state privacy laws and regulations only protect identifiable health information and each define identifiable information differently. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.
Information that identifies an individual other than the subject of the research, such as a family member, is also identifying information. Further, information that might be used to identify individuals, such as their employer, might also be identifying information. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA.
Determine whether the data you intend to use includes identifying information about the expected research subject or any other individuals.
Does the data include information on mental health, substance abuse, genetics, HIV, and/or other conditions granted special legal protection?
Some types of health information are considered particularly sensitive, distinct from general health information. In general, health information is considered sensitive when its disclosure creates a more than minimal risk for the subject of the information (e.g., discrimination, social stigma, physical harm, etc.).
Substance abuse, genetic, mental health, and reproductive health information are protected by specific federal and/or state laws and regulations (or provisions thereof) that offer enhanced or distinct protections than those offered by federal laws of general applicability. The following statutes and regulations may apply: substance abuse – see Part 2, state law; genetic information – see GINA, HIPAA; mental health information – see HIPAA (psychotherapy notes), state law; reproductive health information – see state law.
Determine whether the data you intend to use may include information about individuals with a health condition that carries special legal protection.
Ensure that your research protocol takes into account risks faced by any expected research participants with a condition that carries special legal protection. For example, when considering what risks are presented by research participation and what information need to be communicated for participants to give informed consent, include consideration of unique circumstances faced by individuals with certain health conditions.
*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

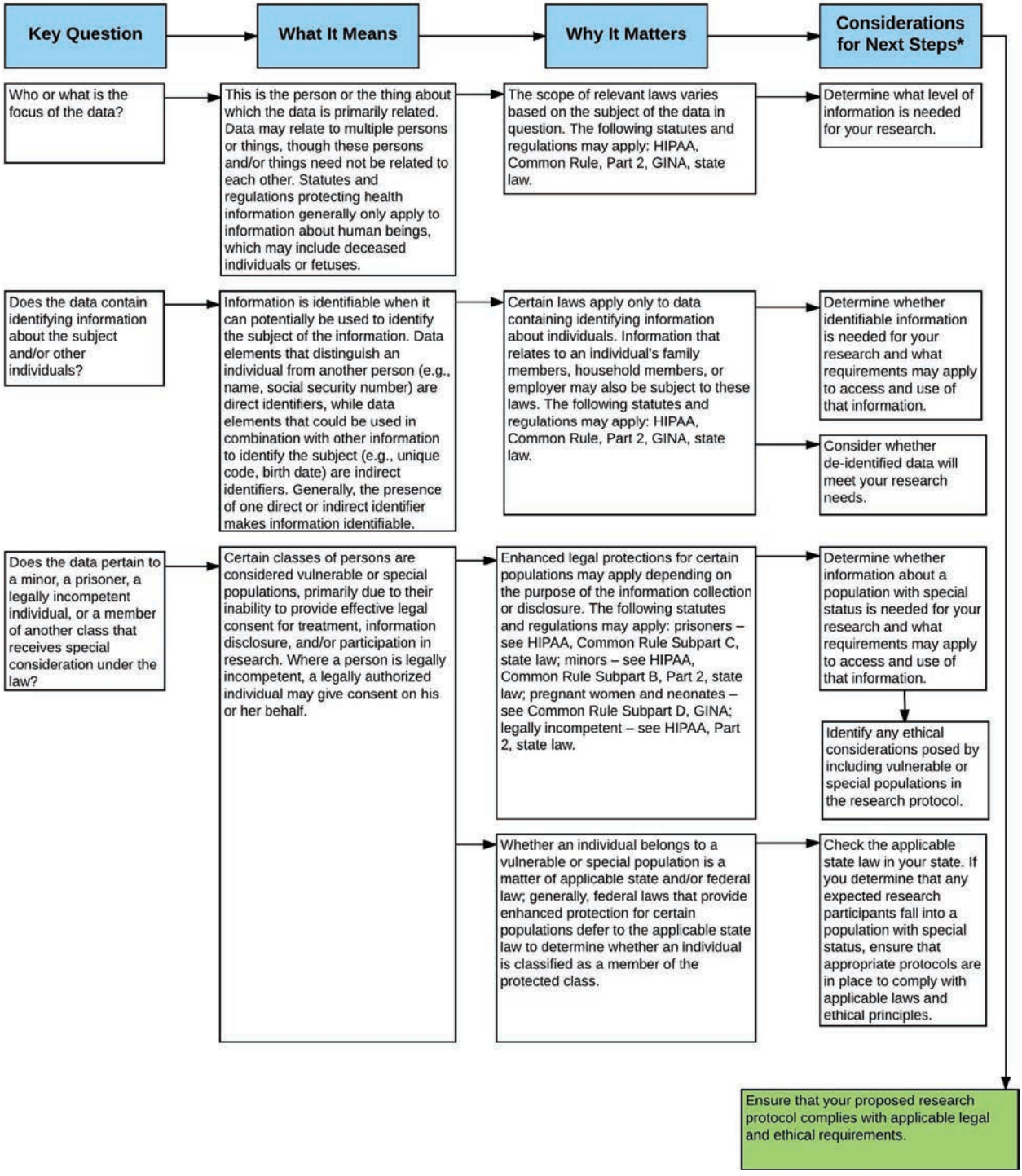
Data Characteristic 3: Subject

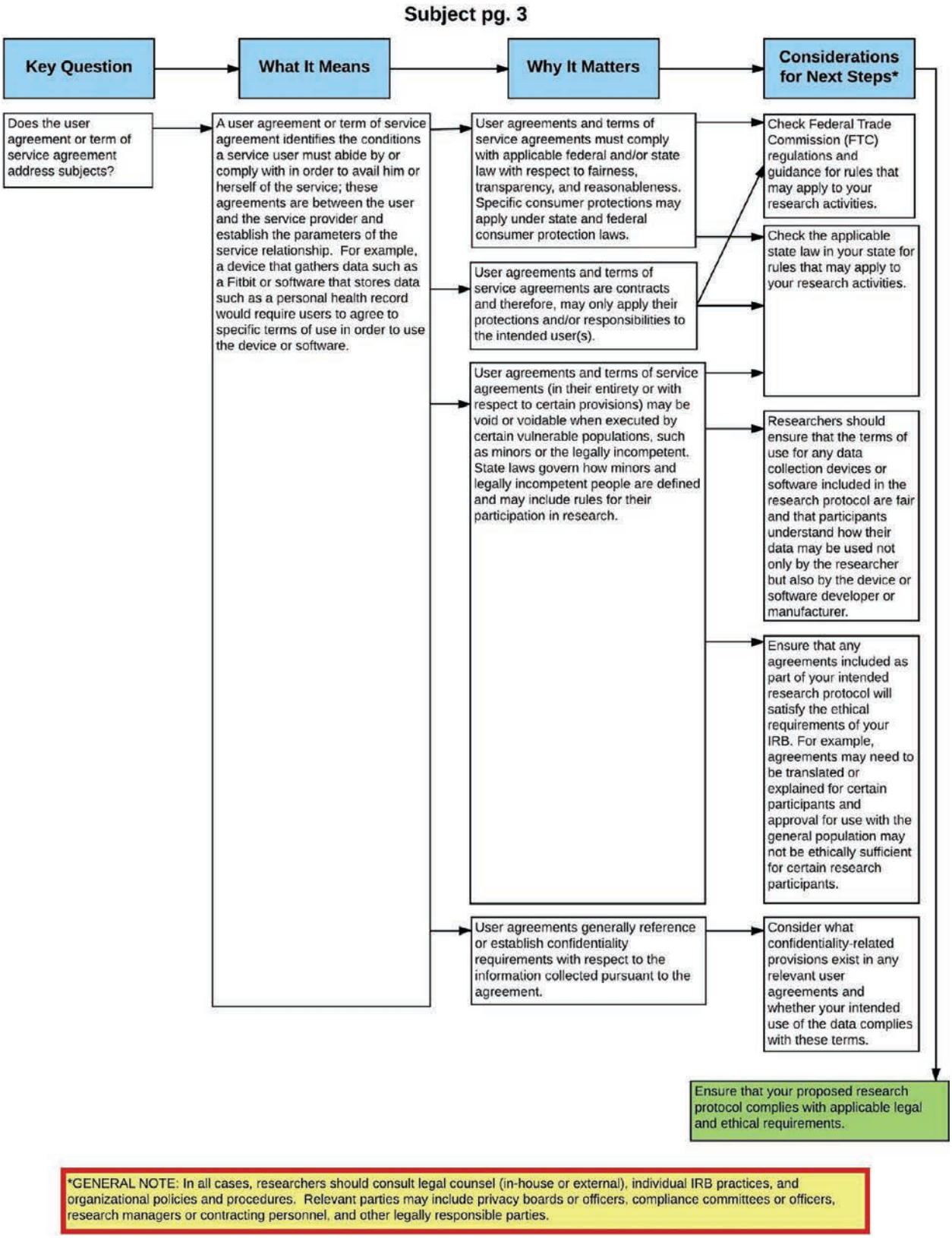


Subject

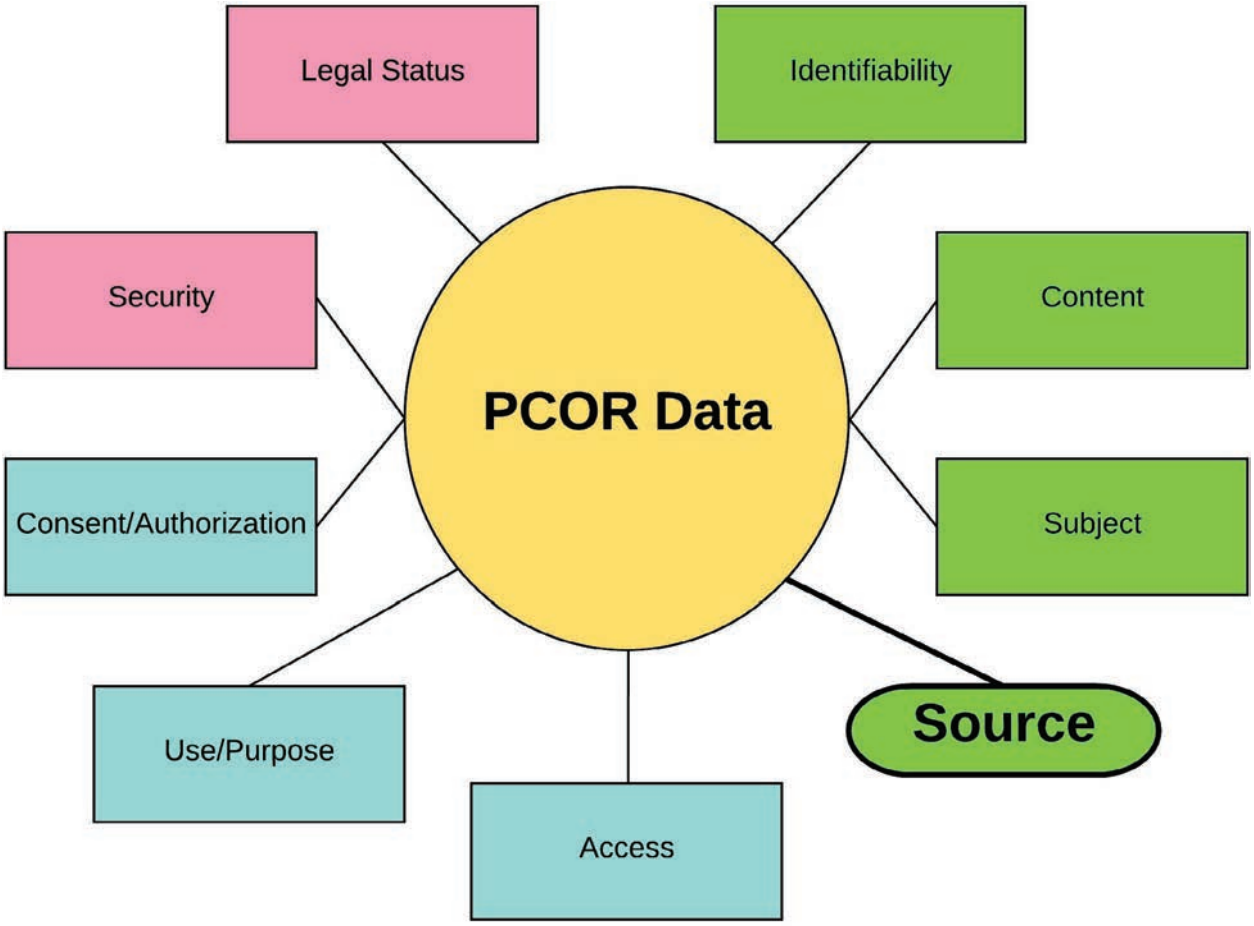
Subject refers to the person or thing that is the focus of the data.

Subject pg. 2


Key Question
What It Means
Why It Matters
Considerations for Next Steps*
Who or what is the focus of the data?
This is the person or the thing about which the data is primarily related. Data may relate to multiple persons or things, though these persons and/or things need not be related to each other. Statutes and regulations protecting health information generally only apply to information about human beings, which may include deceased individuals or fetuses.
The scope of relevant laws varies based on the subject of the data in question. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, state law.
Determine what level of information is needed for your research.
Does the data contain identifying information about the subject and/or other individuals?
Information is identifiable when it can potentially be used to identify the subject of the information. Data elements that distinguish an individual from another person (e.g., name, social security number) are direct identifiers, while data elements that could be used in combination with other information to identify the subject (e.g., unique code, birth date) are indirect identifiers. Generally, the presence of one direct or indirect identifier makes information identifiable.
Certain laws apply only to data containing identifying information about individuals. Information that relates to an individual's family members, household members, or employer may also be subject to these laws. The following statutes and regulations may apply: HIPAA, Common Rule, Part 2, GINA, state law.
Determine whether identifiable information is needed for your research and what requirements may apply to access and use of that information.
Consider whether de-identified data will meet your research needs.
Does the data pertain to a minor, a prisoner, a legally incompetent individual, or a member of another class that receives special consideration under the law?
Certain classes of persons are considered vulnerable or special populations, primarily due to their inability to provide effective legal consent for treatment, information disclosure, and/or participation in research. Where a person is legally incompetent, a legally authorized individual may give consent on his or her behalf.
Enhanced legal protections for certain populations may apply depending on the purpose of the information collection or disclosure. The following statutes and regulations may apply: prisoners – see HIPAA, Common Rule Subpart C, state law; minors – see HIPAA, Common Rule Subpart B, Part 2, state law; pregnant women and neonates – see Common Rule Subpart D, GINA; legally incompetent – see HIPAA, Part 2, state law.
Determine whether information about a population with special status is needed for your research and what requirements may apply to access and use of that information.
Identify any ethical considerations posed by including vulnerable or special populations in the research protocol.
Whether an individual belongs to a vulnerable or special population is a matter of applicable state and/or federal law; generally, federal laws that provide enhanced protection for certain populations defer to the applicable state law to determine whether an individual is classified as a member of the protected class.
Check the applicable state law in your state. If you determine that any expected research participants fall into a population with special status, ensure that appropriate protocols are in place to comply with applicable laws and ethical principles.
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.


Subject pg. 3
Key Question
What It Means
Why It Matters
Considerations for Next Steps*
Does the user agreement or term of service agreement address subjects?
A user agreement or term of service agreement identifies the conditions a service user must abide by or comply with in order to avail him or herself of the service; these agreements are between the user and the service provider and establish the parameters of the service relationship. For example, a device that gathers data such as a Fitbit or software that stores data such as a personal health record would require users to agree to specific terms of use in order to use the device or software.
User agreements and terms of service agreements must comply with applicable federal and/or state law with respect to fairness, transparency, and reasonableness. Specific consumer protections may apply under state and federal consumer protection laws.
User agreements and terms of service agreements are contracts and therefore, may only apply their protections and/or responsibilities to the intended user(s).
User agreements and terms of service agreements (in their entirety or with respect to certain provisions) may be void or voidable when executed by certain vulnerable populations, such as minors or the legally incompetent. State laws govern how minors and legally incompetent people are defined and may include rules for their participation in research.
User agreements generally reference or establish confidentiality requirements with respect to the information collected pursuant to the agreement.
Check Federal Trade Commission (FTC) regulations and guidance for rules that may apply to your research activities.
Check the applicable state law in your state for rules that may apply to your research activities.
Researchers should ensure that the terms of use for any data collection devices or software included in the research protocol are fair and that participants understand how their data may be used not only by the researcher but also by the device or software developer or manufacturer.
Ensure that any agreements included as part of your intended research protocol will satisfy the ethical requirements of your IRB. For example, agreements may need to be translated or explained for certain participants and approval for use with the general population may not be ethically sufficient for certain research participants.
Consider what confidentiality-related provisions exist in any relevant user agreements and whether your intended use of the data complies with these terms.
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.
*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

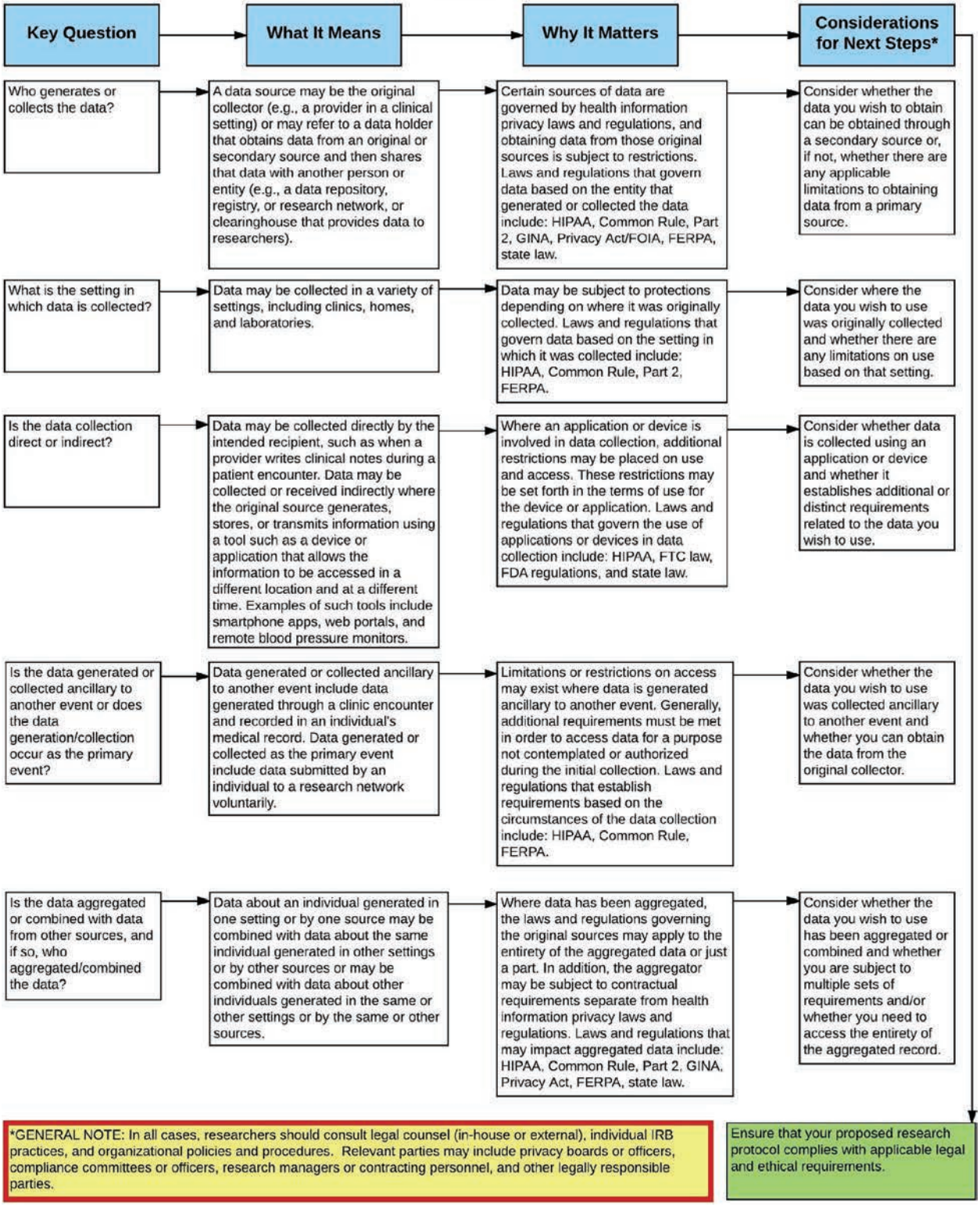
Data Characteristic 4: Source



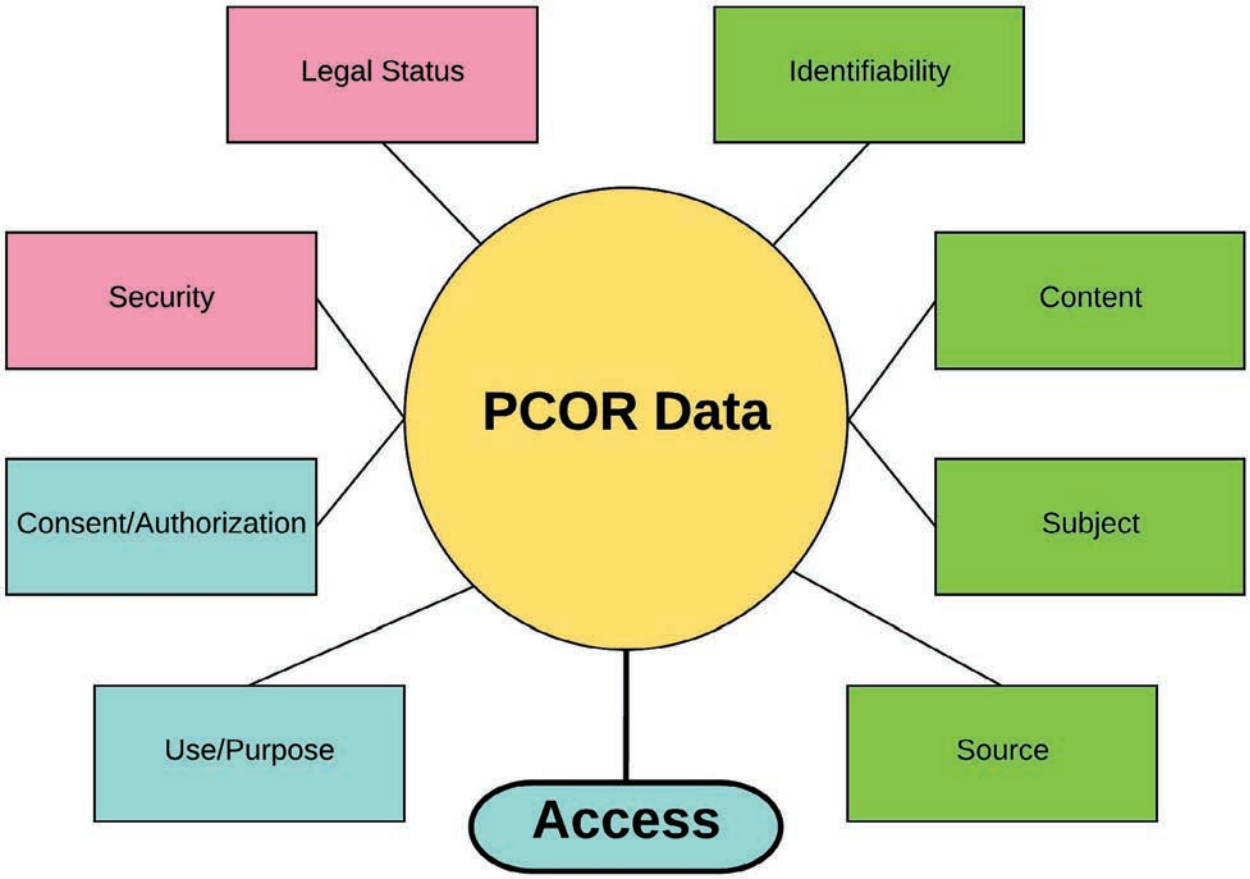
Source

Source refers to the person, entity, and/or setting in which the data originated or was collected.

Source pg. 2


Key Question
What It Means
Why It Matters
Considerations for Next Steps*
Who generates or collects the data?
A data source may be the original collector (e.g., a provider in a clinical setting) or may refer to a data holder that obtains data from an original or secondary source and then shares that data with another person or entity (e.g., a data repository, registry, or research network, or clearinghouse that provides data to researchers).
Certain sources of data are governed by health information privacy laws and regulations, and obtaining data from those original sources is subject to restrictions. Laws and regulations that govern data based on the entity that generated or collected the data include: HIPAA, Common Rule, Part 2, GINA, Privacy Act/FOIA, FERPA, state law.
Consider whether the data you wish to obtain can be obtained through a secondary source or, if not, whether there are any applicable limitations to obtaining data from a primary source.
What is the setting in which data is collected?
Data may be collected in a variety of settings, including clinics, homes, and laboratories.
Data may be subject to protections depending on where it was originally collected. Laws and regulations that govern data based on the setting in which it was collected include: HIPAA, Common Rule, Part 2, FERPA.
Consider where the data you wish to use was originally collected and whether there are any limitations on use based on that setting.
Is the data collection direct or indirect?
Data may be collected directly by the intended recipient, such as when a provider writes clinical notes during a patient encounter. Data may be collected or received indirectly where the original source generates, stores, or transmits information using a tool such as a device or application that allows the information to be accessed in a different location and at a different time. Examples of such tools include smartphone apps, web portals, and remote blood pressure monitors.
Where an application or device is involved in data collection, additional restrictions may be placed on use and access. These restrictions may be set forth in the terms of use for the device or application. Laws and regulations that govern the use of applications or devices in data collection include: HIPAA, FTC law, FDA regulations, and state law.
Consider whether data is collected using an application or device and whether it establishes additional or distinct requirements related to the data you wish to use.
Is the data generated or collected ancillary to another event or does the data generation/collection occur as the primary event?
Data generated or collected ancillary to another event include data generated through a clinic encounter and recorded in an individual's medical record. Data generated or collected as the primary event include data submitted by an individual to a research network voluntarily.
Limitations or restrictions on access may exist where data is generated ancillary to another event. Generally, additional requirements must be met in order to access data for a purpose not contemplated or authorized during the initial collection. Laws and regulations that establish requirements based on the circumstances of the data collection include: HIPAA, Common Rule, FERPA.
Consider whether the data you wish to use was collected ancillary to another event and whether you can obtain the data from the original collector.
Is the data aggregated or combined with data from other sources, and if so, who aggregated/combined the data?
Data about an individual generated in one setting or by one source may be combined with data about the same individual generated in other settings or by other sources or may be combined with data about other individuals generated in the same or other settings or by the same or other sources.
Where data has been aggregated, the laws and regulations governing the original sources may apply to the entirety of the aggregated data or just a part. In addition, the aggregator may be subject to contractual requirements separate from health information privacy laws and regulations. Laws and regulations that may impact aggregated data include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA, state law.
Consider whether the data you wish to use has been aggregated or combined and whether you are subject to multiple sets of requirements and/or whether you need to access the entirety of the aggregated record.
*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

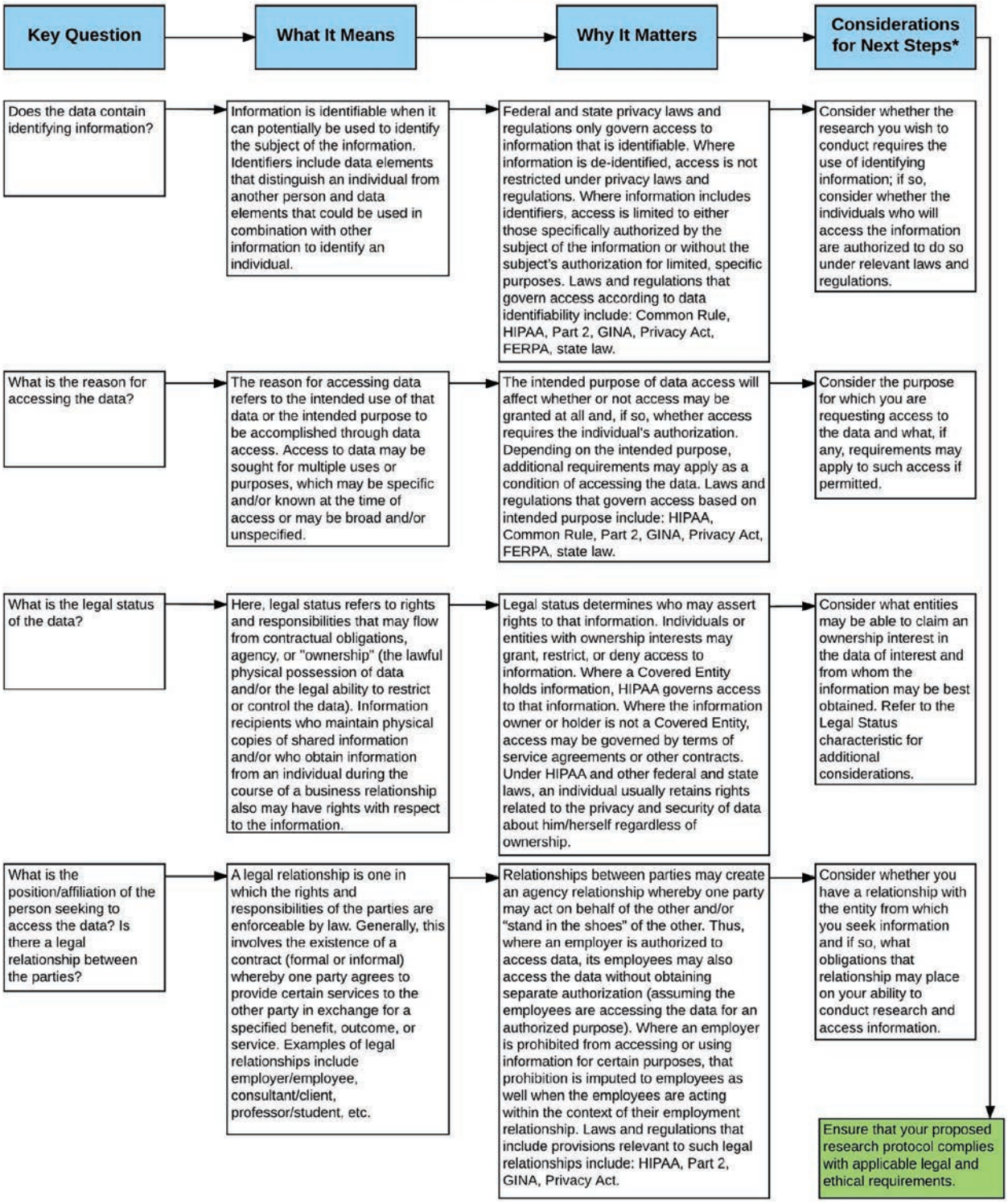
Data Characteristic 5: Access



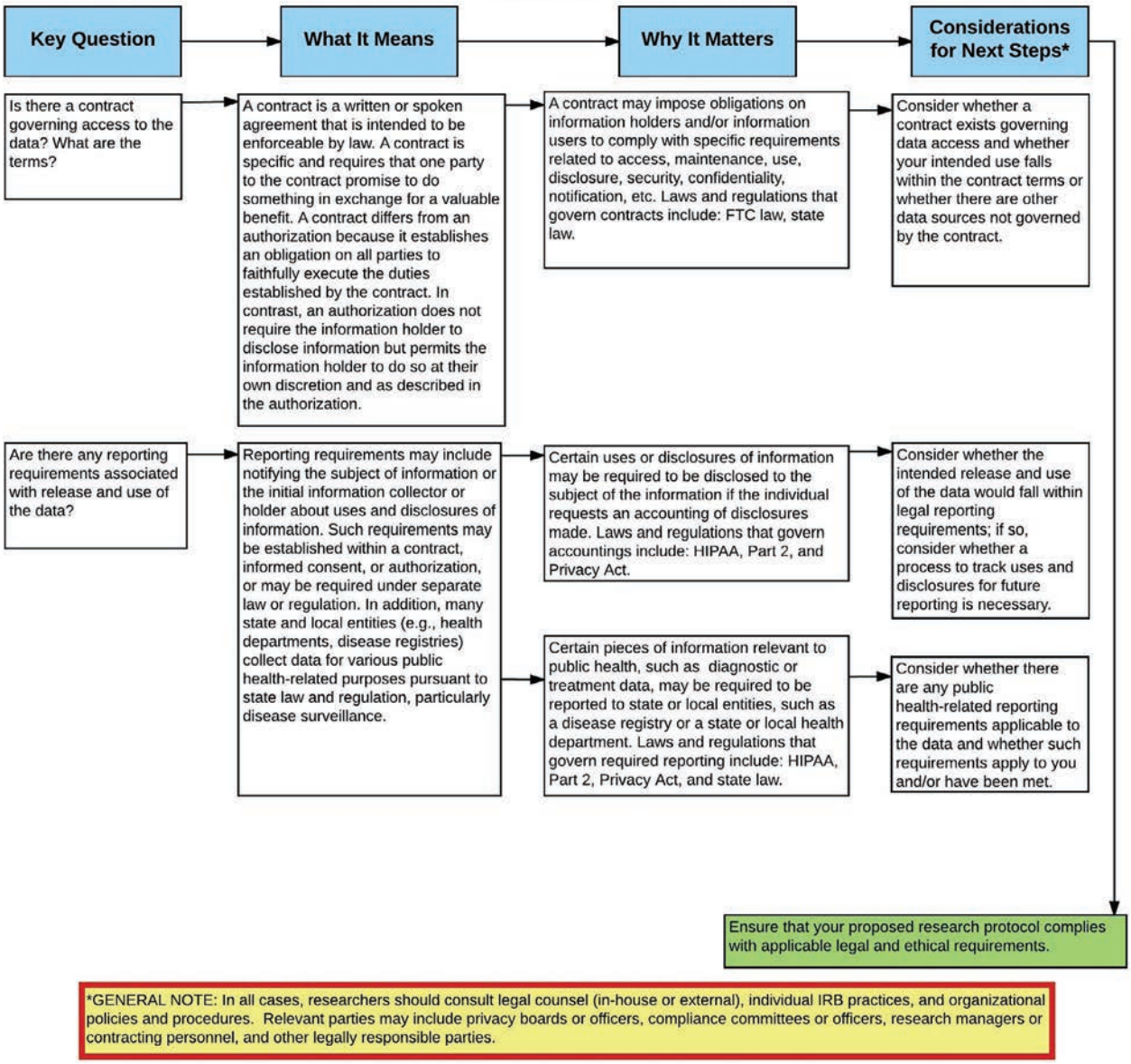
Access

Access refers to the ability of a person or entity other than the individual subject(s) of the information to view, create, edit, or share data.

Access pg. 2

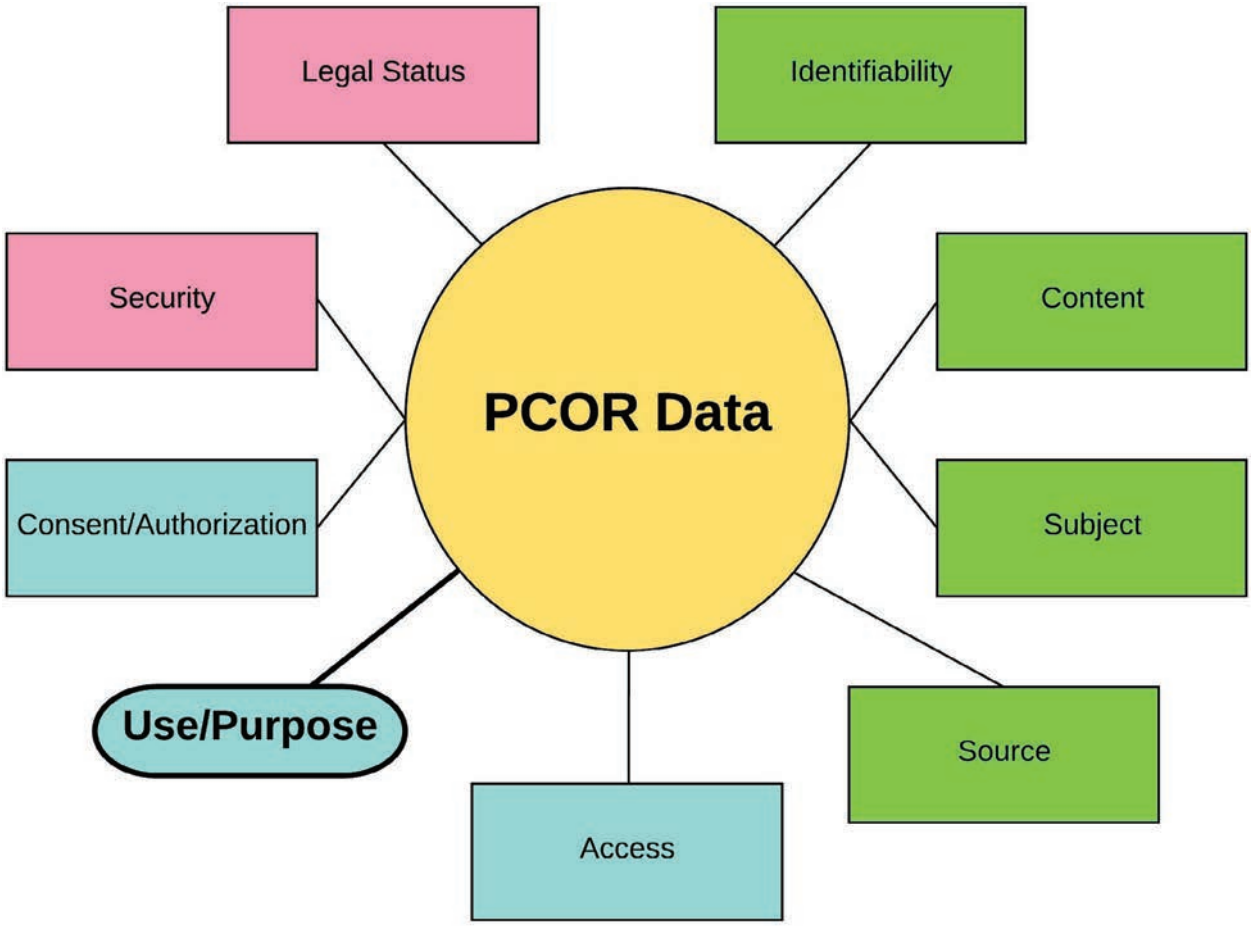

Key Question
What It Means
Why It Matters
Considerations for Next Steps*
Does the data contain identifying information?
Information is identifiable when it can potentially be used to identify the subject of the information. Identifiers include data elements that distinguish an individual from another person and data elements that could be used in combination with other information to identify an individual.
Federal and state privacy laws and regulations only govern access to information that is identifiable. Where information is de-identified, access is not restricted under privacy laws and regulations. Where information includes identifiers, access is limited to either those specifically authorized by the subject of the information or without the subject's authorization for limited, specific purposes. Laws and regulations that govern access according to data identifiability include: Common Rule, HIPAA, Part 2, GINA, Privacy Act, FERPA, state law.
Consider whether the research you wish to conduct requires the use of identifying information; if so, consider whether the individuals who will access the information are authorized to do so under relevant laws and regulations.
What is the reason for accessing the data?
The reason for accessing data refers to the intended use of that data or the intended purpose to be accomplished through data access. Access to data may be sought for multiple uses or purposes, which may be specific and/or known at the time of access or may be broad and/or unspecified.
The intended purpose of data access will affect whether or not access may be granted at all and, if so, whether access requires the individual's authorization. Depending on the intended purpose, additional requirements may apply as a condition of accessing the data. Laws and regulations that govern access based on intended purpose include: HIPAA, Common Rule, Part 2, GINA, Privacy Act, FERPA, state law.
Consider the purpose for which you are requesting access to the data and what, if any, requirements may apply to such access if permitted.
What is the legal status of the data?
Here, legal status refers to rights and responsibilities that may flow from contractual obligations, agency, or "ownership" (the lawful physical possession of data and/or the legal ability to restrict or control the data). Information recipients who maintain physical copies of shared information and/or who obtain information from an individual during the course of a business relationship also may have rights with respect to the information.
Legal status determines who may assert rights to that information. Individuals or entities with ownership interests may grant, restrict, or deny access to information. Where a Covered Entity holds information, HIPAA governs access to that information. Where the information owner or holder is not a Covered Entity, access may be governed by terms of service agreements or other contracts. Under HIPAA and other federal and state laws, an individual usually retains rights related to the privacy and security of data about him/herself regardless of ownership.
Consider what entities may be able to claim an ownership interest in the data of interest and from whom the information may be best obtained. Refer to the Legal Status characteristic for additional considerations.
What is the position/affiliation of the person seeking to access the data? Is there a legal relationship between the parties?
A legal relationship is one in which the rights and responsibilities of the parties are enforceable by law. Generally, this involves the existence of a contract (formal or informal) whereby one party agrees to provide certain services to the other party in exchange for a specified benefit, outcome, or service. Examples of legal relationships include employer/employee, consultant/client, professor/student, etc.
Relationships between parties may create an agency relationship whereby one party may act on behalf of the other and/or "stand in the shoes" of the other. Thus, where an employer is authorized to access data, its employees may also access the data without obtaining separate authorization (assuming the employees are accessing the data for an authorized purpose). Where an employer is prohibited from accessing or using information for certain purposes, that prohibition is imputed to employees as well when the employees are acting within the context of their employment relationship. Laws and regulations that include provisions relevant to such legal relationships include: HIPAA, Part 2, GINA, Privacy Act.
Consider whether you have a relationship with the entity from which you seek information and if so, what obligations that relationship may place on your ability to conduct research and access information.
Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

Access pg. 3



*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

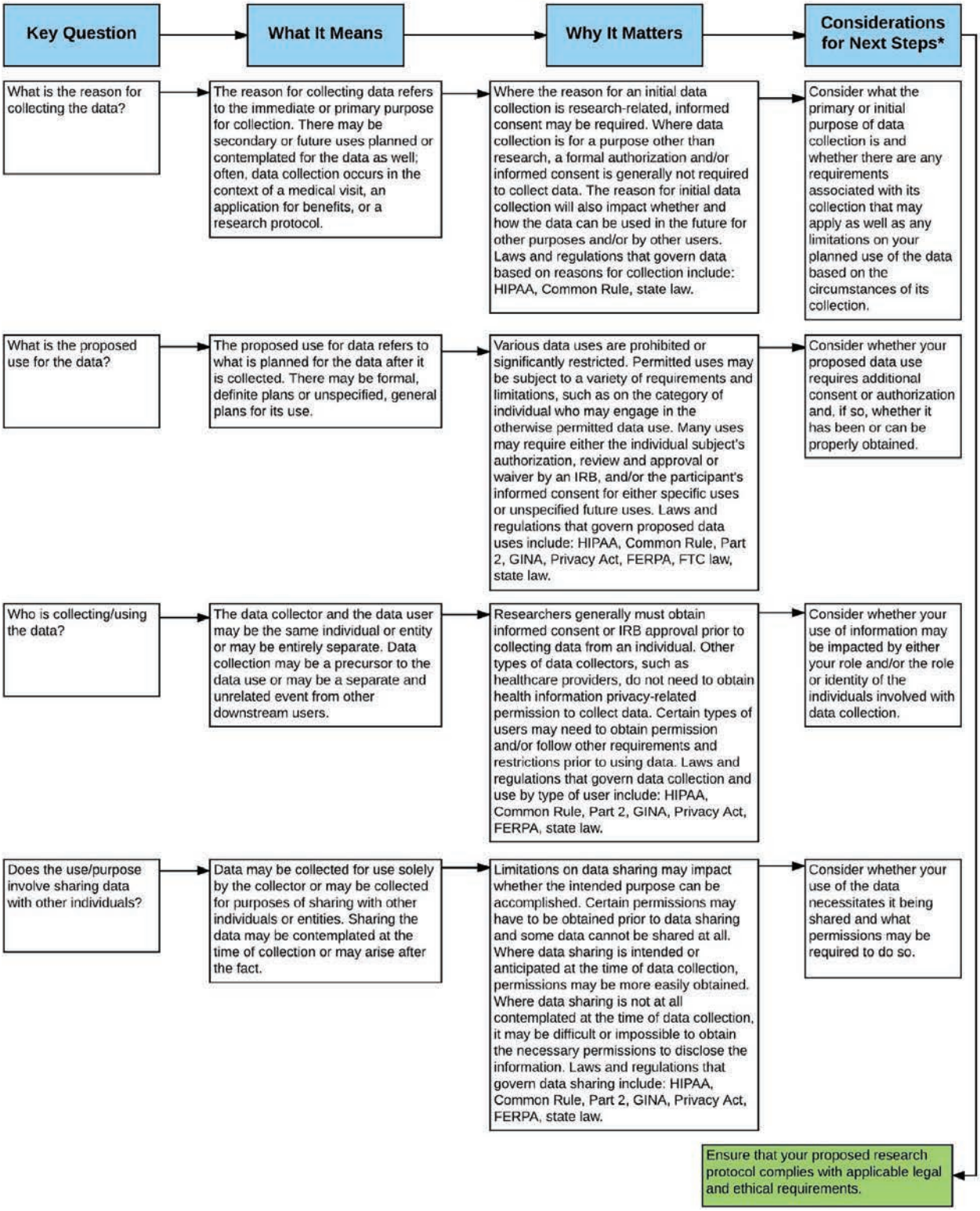
Data Characteristic 6: Use/Purpose



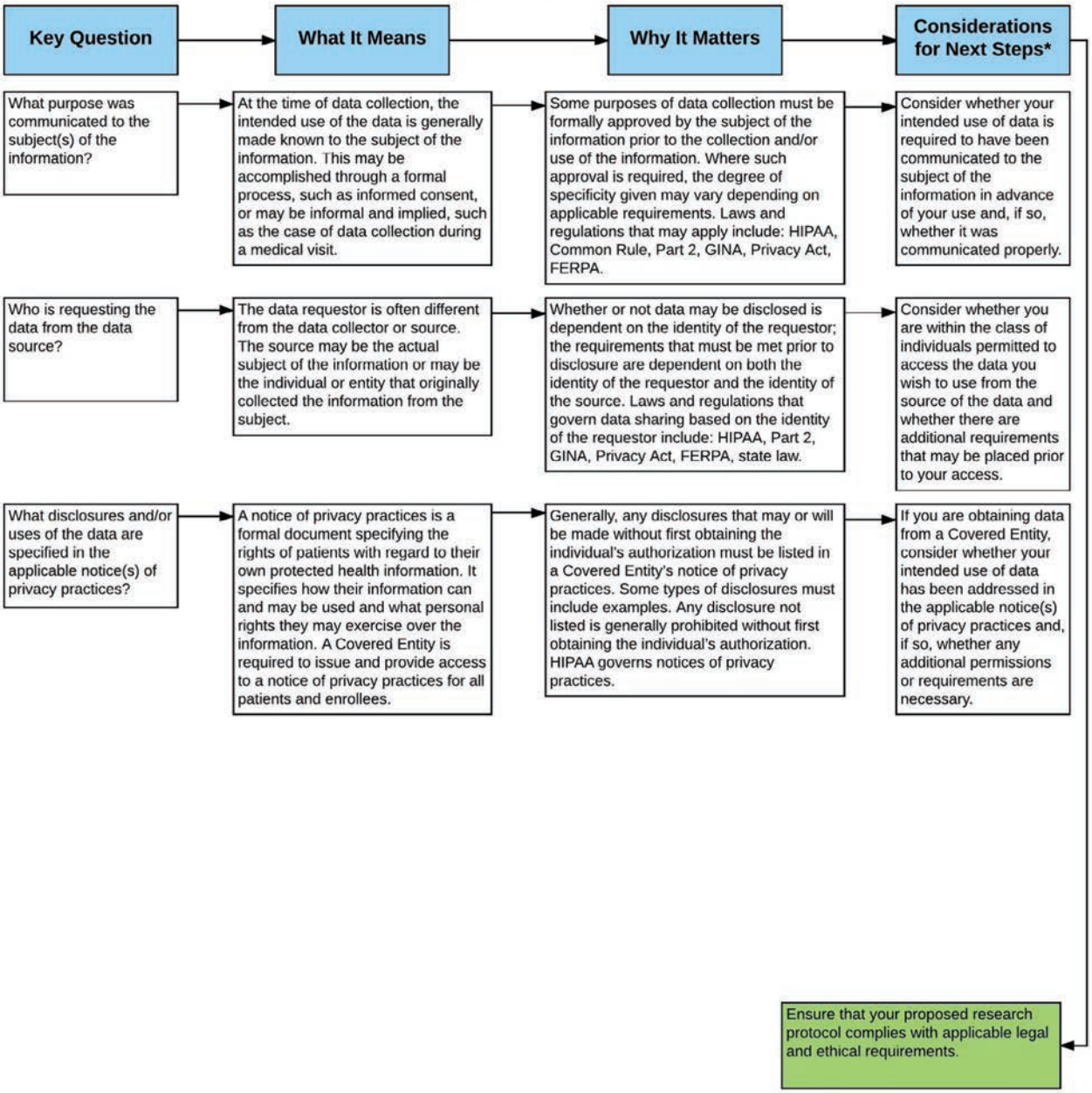
Use/Purpose

The intended use or purpose of the data collection will affect whether and how the data may be collected and used.

Use/Purpose pg. 2

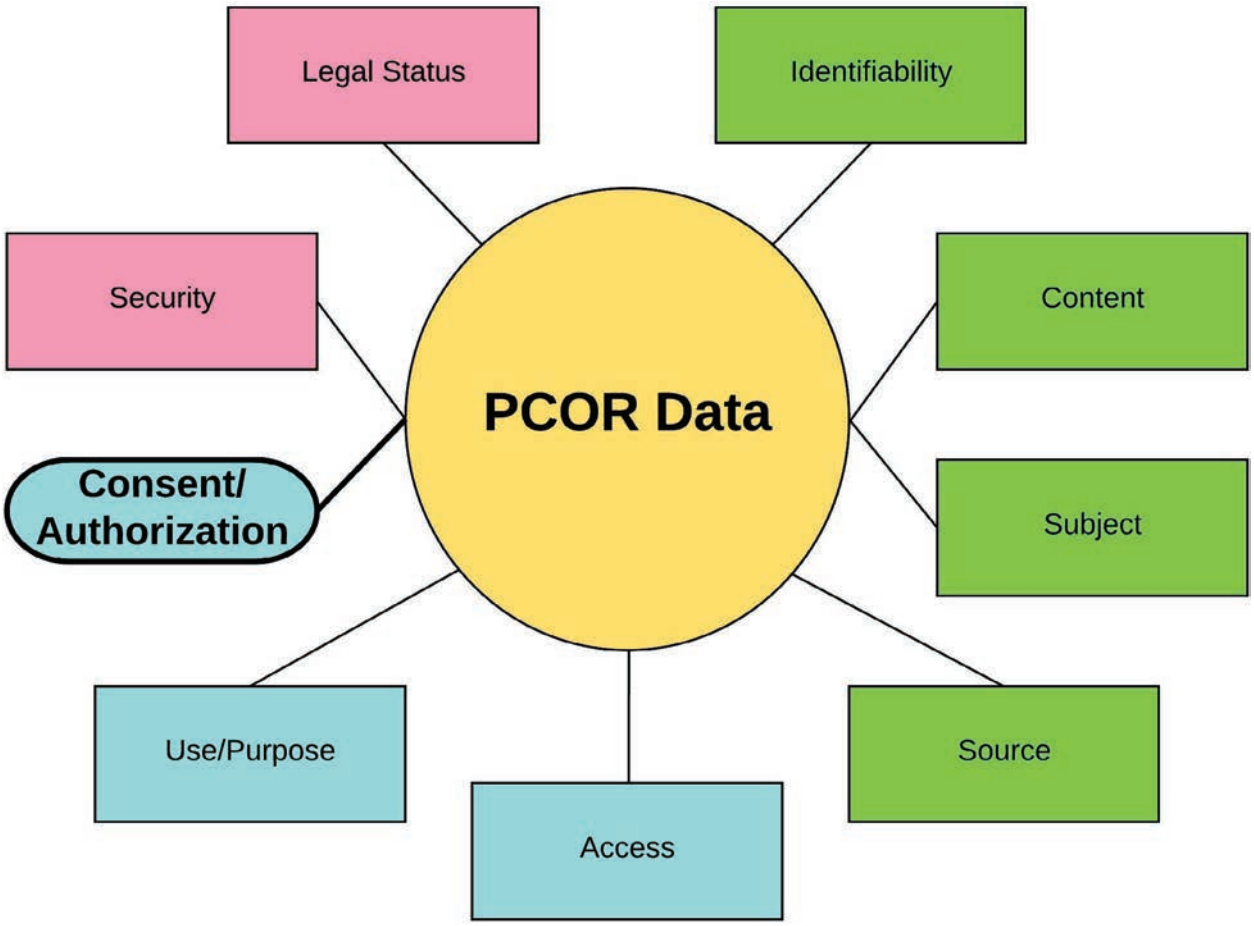


Use/Purpose pg. 3



*GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

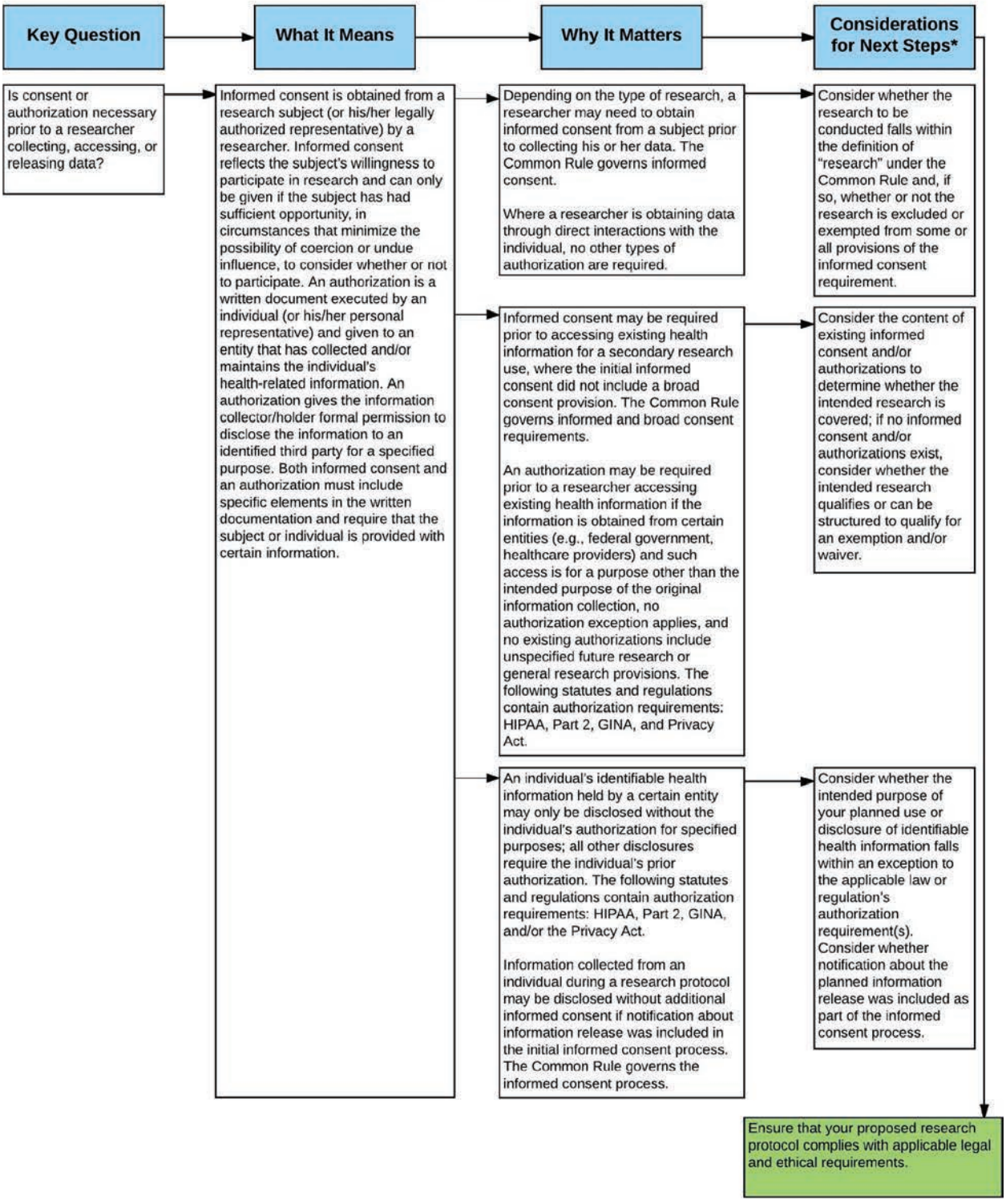
Data Characteristic 7: Consent/Authorization



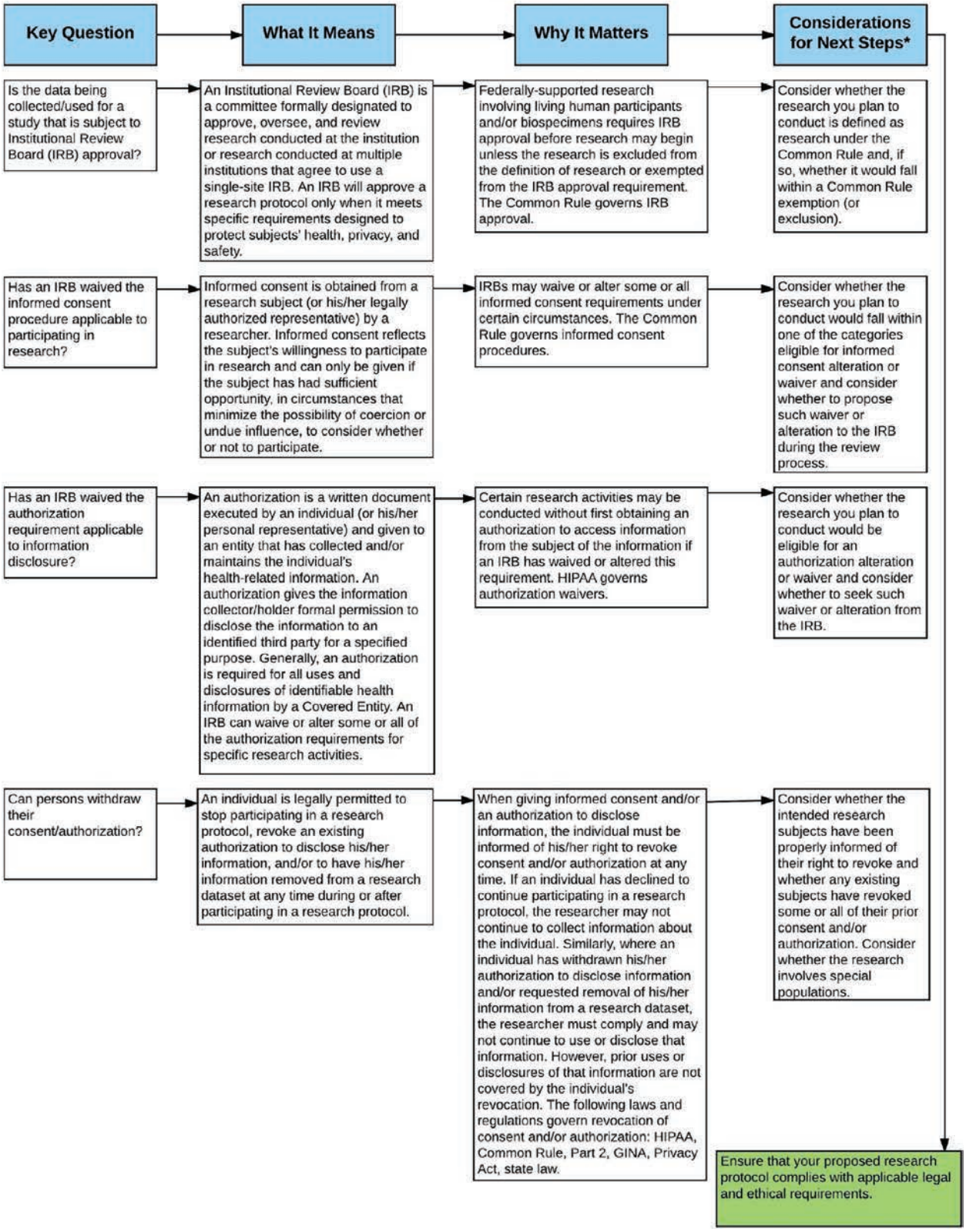
Consent/Authorization

Consent/Authorization refers to the activities and documentation potentially required of researchers seeking permission to collect, use, or share data about an individual.

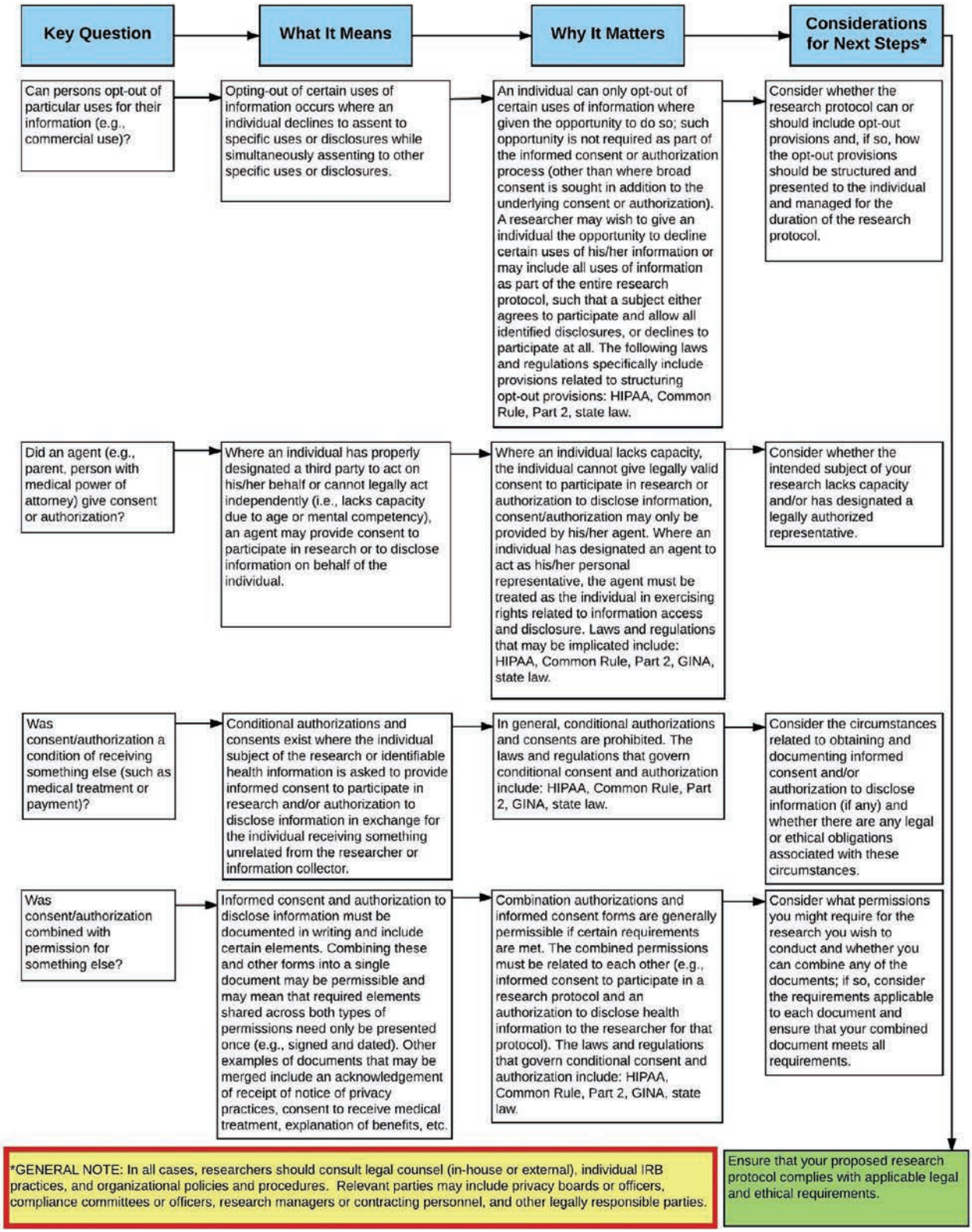
Consent/Authorization pg. 2



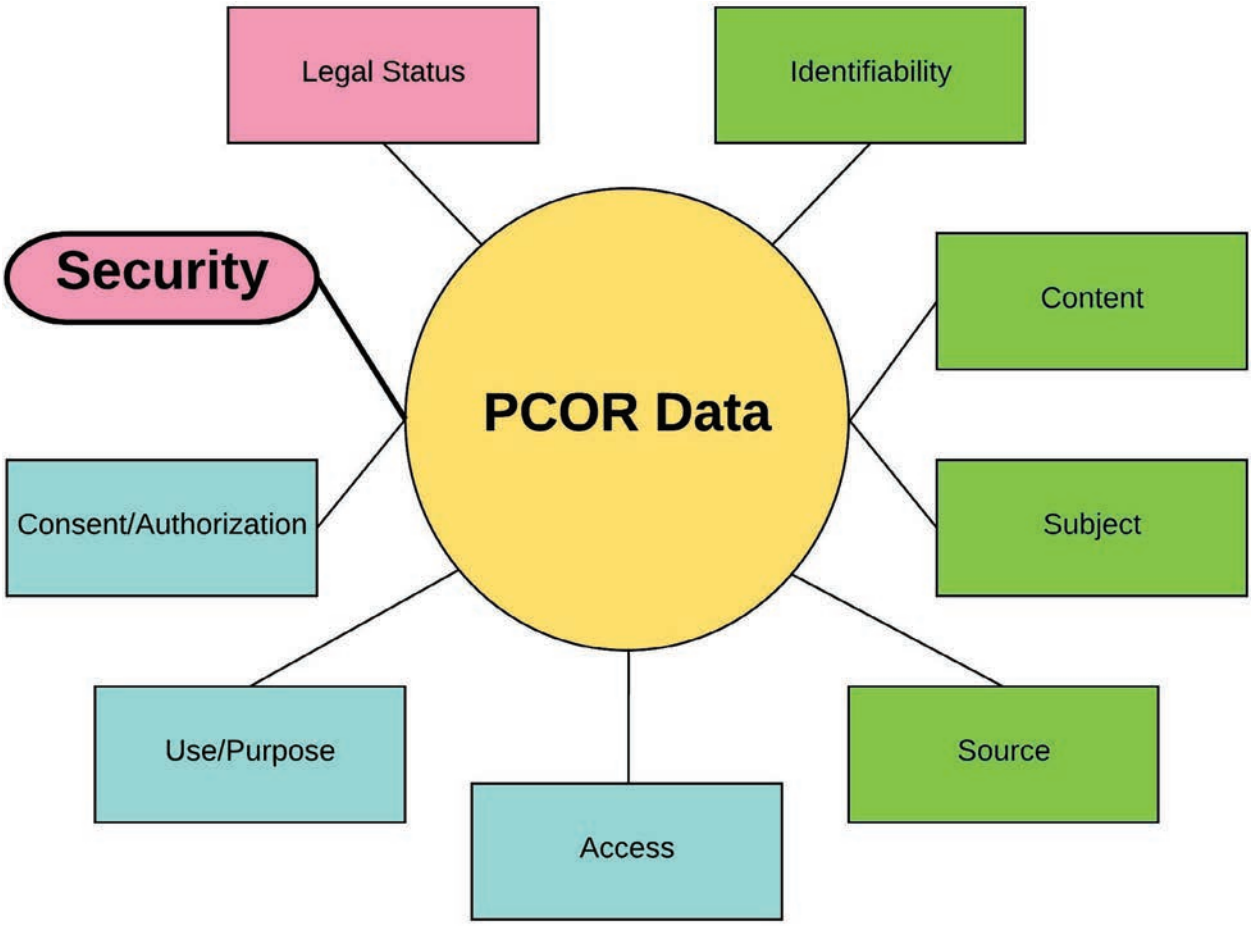
Consent/Authorization pg. 3



Consent/Authorization pg. 4



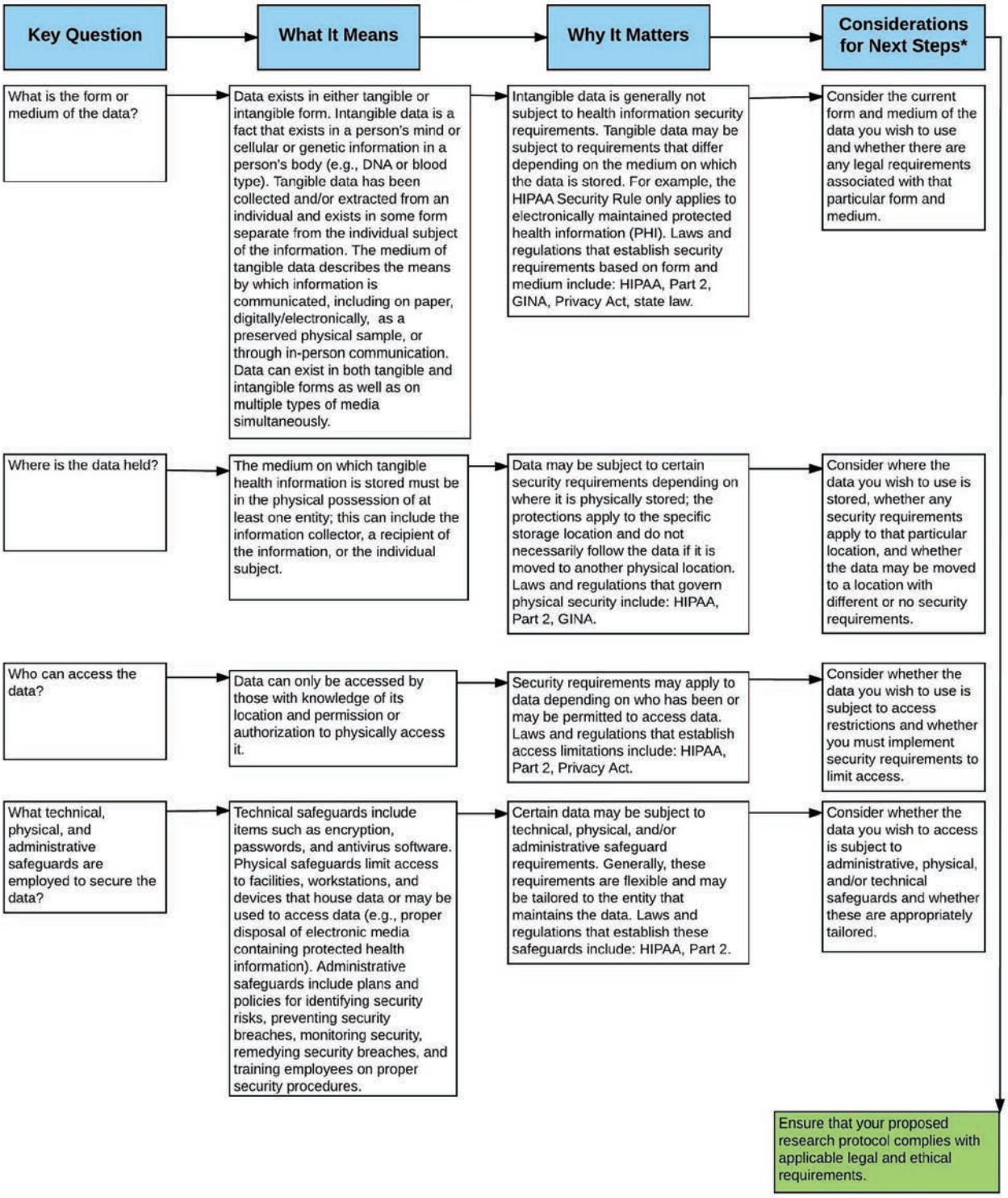
Data Characteristic 8: Security



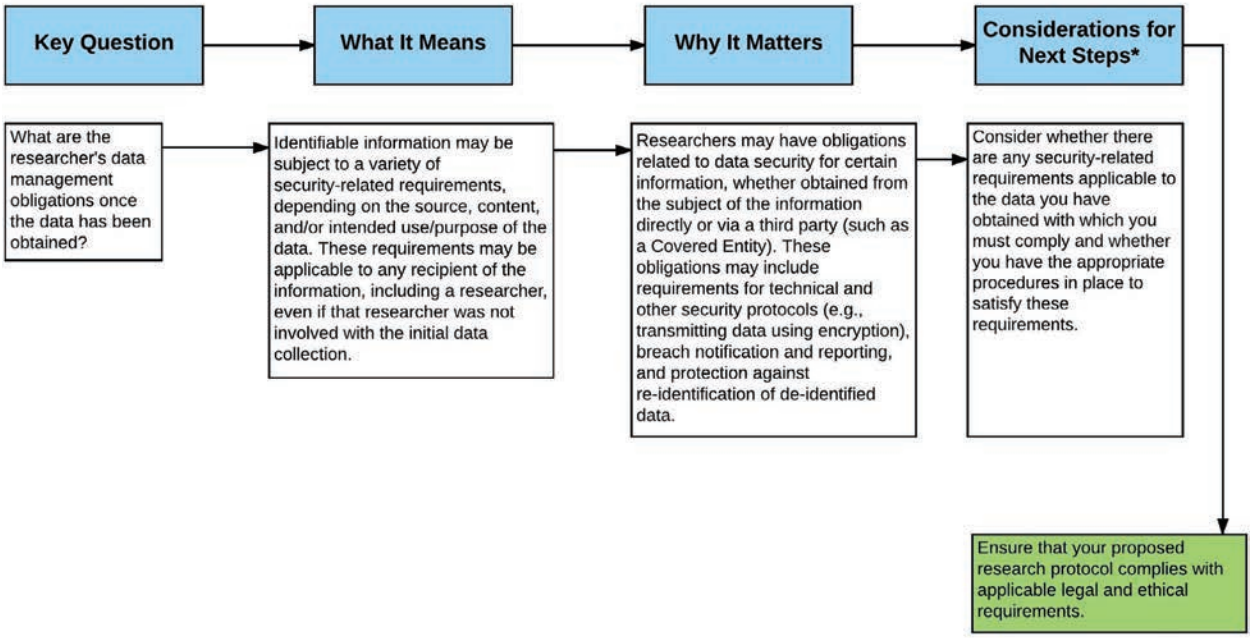
Security

Security refers to the means by which data is protected from unauthorized use or access.

Security pg. 2

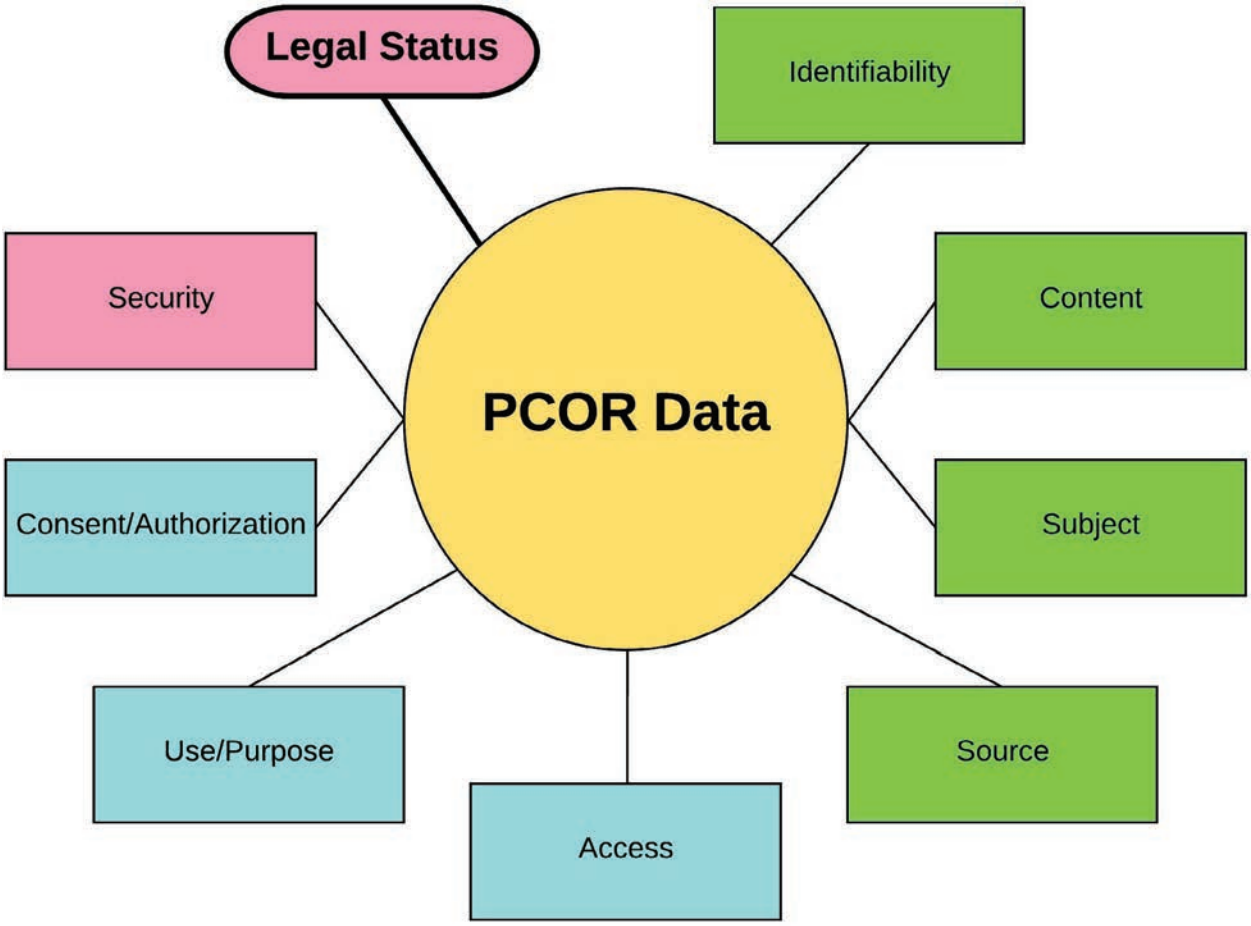


Security pg. 3



GENERAL NOTE: In all cases, researchers should consult legal counsel (in-house or external), individual IRB practices, and organizational policies and procedures. Relevant parties may include privacy boards or officers, compliance committees or officers, research managers or contracting personnel, and other legally responsible parties.

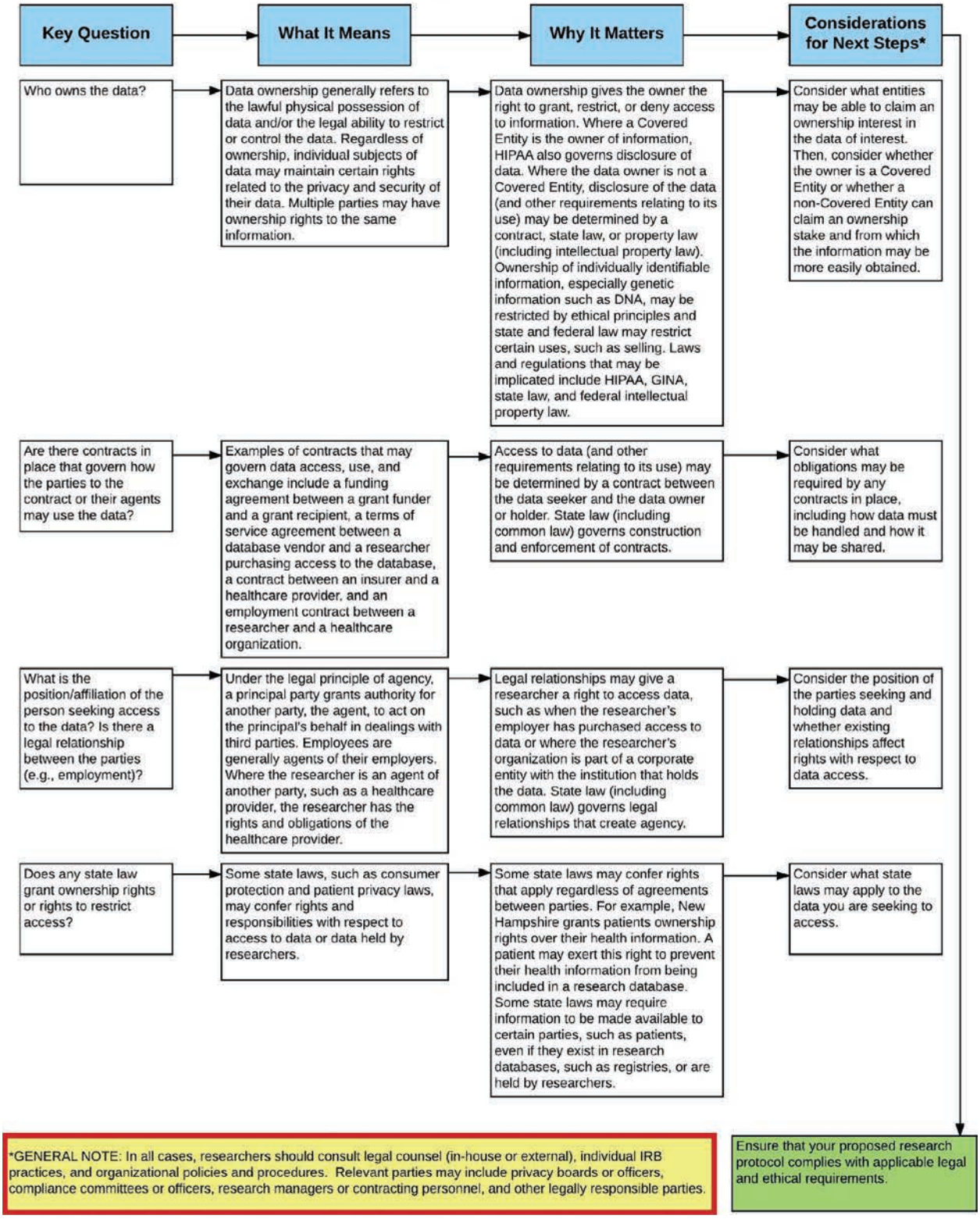
Data Characteristic 9: Legal Status



Legal Status

Legal Status refers to rights and responsibilities related to the data that may be triggered by ownership rights, agency principles, and/or contractual obligations.

Legal Status pg. 2



The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

CHAPTER 5:

MAPPING RESEARCH DATA FLOWS TO LEGAL REQUIREMENTS

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Chapter 5

Mapping Research Data Flows to Legal Requirements

INTRODUCTION

Stakeholder discussions organized during the early part of the development of the Architecture (described in further detail in Chapter 1) raised a number of issues and concerns related to the use of various types of data for PCOR (discussed in Chapter 2) and navigation of the statutes and regulations that govern the use of this data for PCOR (discussed in Chapters 3, 4, and Appendix A). The stakeholders further identified topics of particular concern ranging from consent to special populations to merging clinical and claims data that were incorporated into a series of research data use scenarios.

This chapter builds on these research data use scenarios that reflect stakeholder comments and concerns related to the use of health information for PCOR. Specifically, this chapter identifies, maps, and analyzes representative data flows that reflect key concerns within each of the five use cases identified by the project team as well as a sixth data flow map representing a general PCOR research process. The general data flow is intended to provide a foundational example of the mapping process, outlining general steps likely to be encountered in the course of PCOR research and the associated legal trigger/decision points. Collectively, the data flow maps are designed to identify key steps associated with PCOR and link those steps directly to decision or trigger points that have legal significance.

REPRESENTATIVE DATA FLOWS

There are five use cases of most relevance to PCOR and CER:

- Use Case 1: Combine Data for PCOR
- Use Case 2: Consent Management
- Use Case 3: Release and Use of Specially Protected Health Data
- Use Case 4: Identification and Re-Identification of PCOR Data
- Use Case 5: Patient-Generated Health Data

Under each of these broad use cases, there are two or more related scenarios illustrating a particular research scenario, including a description of issues and areas of potential confusion identified by stakeholders. These scenarios were based on conversations with a multidisciplinary stakeholder work group as well as research about the issues of concern to the broader research community.

This chapter includes representative data flows that are related to one or more scenarios within each of the five use cases. The research data use scenarios discussed above represent fact patterns representative of researcher experience and potential policy gaps or challenges, rather than legal questions, so it was necessary to synthesize the key points from the scenarios and incorporate additional details to create a data flow that captured legally significant points. The data flow maps below include one representative data flow for each use case, and each data flow is related to one or more scenarios that were presented under the use cases described above. (For ease of reference, the data flow maps are numbered the same as the use cases they reflect.) In addition, there is a general research data flow (Data Flow 0) designed to illustrate a data flow that might be typically encountered in

PCOR. Again, this general data flow is intended to provide a foundational example of the mapping process, making the connections between activities in the data flow and key legal requirements.

For each data flow, the key legal points are mapped under the most relevant statutes or regulations that may apply to PCOR: HIPAA, the Common Rule, Part 2, GINA, and state law. Each map indicates which statutes and/or regulations apply to that data flow. The legal notes under each statute or regulation in the map reflect legally significant trigger or decision points. Examples of legally significant trigger points include when a statute or regulation becomes applicable, information acquires a certain status, a particular action must be taken under the law, or a limitation applies to an activity under the law. When a point in the data flow triggers a particular legal issue, the map includes a brief explanation of that issue in the color-coded column that apples to the statute or regulation in question. Because most legal issues require more explanation than the space allowed on each data flow map, the "Explanatory Notes" section provides more explanation of each issue. The brief legal notes in the map refer to the relevant explanatory note by number. For more in-depth analysis of the statutes, regulations, and their relevant requirements, including summaries of the five statutes and regulations that are implicated in the data flow maps, see Appendix A.

In the maps below, the first blue column shows the flow of information through a representative research scenario, including a description of a legally significant action or event associated with the use or disclosure of information for PCOR. The blue column shows an arrow continuing until the data flow ends, with individual steps separated in boxes and identified by a number to the left of the column. Moving left to right, the green column addresses HIPAA provisions that are relevant to the action or event. The yellow column addresses Common Rule provisions that are relevant to the action or event. The purple column addresses state law provisions that are relevant to the action or event. The red column addresses 42 CFR Part 2 provisions that are relevant to the action or event. And finally, the pink column addresses GINA provisions that are relevant to the action or event. The color columns begin when the relevant statute or regulation is triggered and continue until the law no longer applies, illustrating that a statute or regulation may apply to numerous actions or events within a data flow map. The end of a colored bar indicates the end of the relevant application of that particular statute or regulation to the data flow. Where there is no colored column for a particular statute or regulation, that law does not apply. Within each arrow, the data flow maps highlight the legal issue raised by the action or event specific to the law or regulation with a brief explanation of the legal issue inside a box placed in line with the relevant action in the data flow at left. Further explanation is included in the explanatory notes referenced in the text of the legal notes within each column (e.g., "*See HIPAA Note 1*"), which are organized by law and included in the "Explanatory Notes" section following the maps section. Alongside the data flow is a legend that defines the acronyms used in that particular data flow map. (Note that these are research-oriented use cases and the data flows only apply to PCOR; these should not be taken out of context.)

Data Flow 0—General Research Scenario

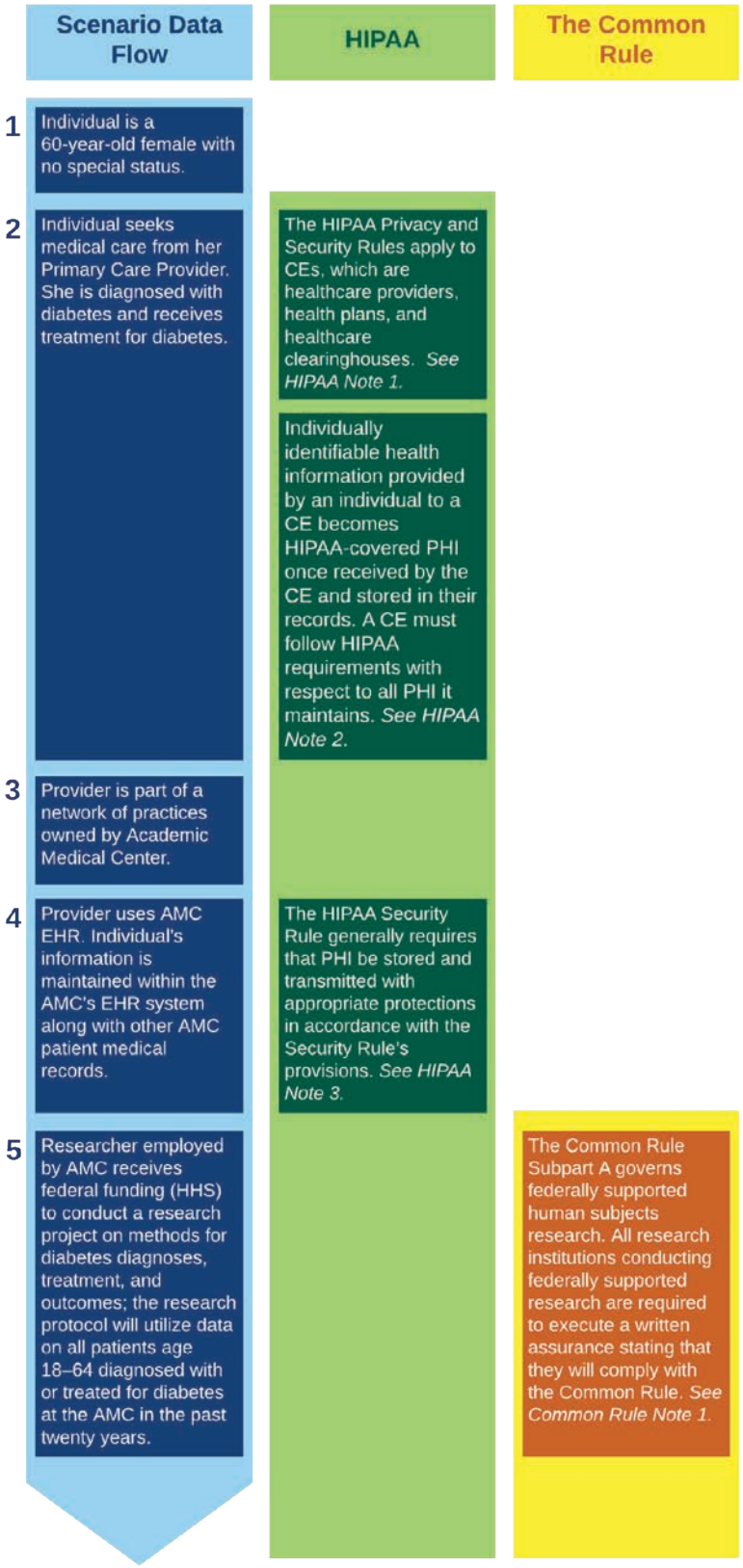
Scenario Narrative:

Individual is a 60-year-old female with no special status. She seeks medical care from her primary care provider. She is diagnosed with diabetes and receives treatment for diabetes. The provider is part of a network of practices owned by an Academic Medical Center (AMC). The provider uses the AMC's Electronic Health Record (EHR). Individual's information is maintained within the AMC's EHR system along with other AMC patient medical records. A researcher employed by the AMC receives HHS funding to conduct a research project comparing methods for diabetes diagnoses, treatment, and outcomes among current and former patients. The researcher seeks data on all patients ages 18–64 diagnosed with or treated for diabetes at the AMC in the past 20 years. The researcher submits the research plan to the AMC's Institutional Review Board (IRB) for review and requests both a waiver of authorization and an exemption determination. The IRB determines that the research is exempt because the planned study will be limited to collection and analysis of existing information, which is governed by HIPAA's research provisions. The IRB also grants the authorization waiver because obtaining authorization from former patients would not be practicable, the PHI is necessary to complete the planned research study, and the research plan includes appropriate protections for patient privacy. The researcher submits documentation of the waiver to the AMC and requests the following information on patients ages 18–64 with a diagnosis of diabetes: Age, All Diagnoses, Race, Ethnicity, Dates of Service, Insulin Pump Serial Number, and Services Provided. The researcher conducts the analysis and publishes aggregated, de-identified results in a peer-reviewed journal.

Statutes/Regulations implicated: HIPAA, Common Rule

Acronyms for Data Flow 0	
AMC	Academic Medical Center
CE	Covered Entity
DUA	Data Use Agreement
EHR	Electronic Health Record
LDS	Limited Data Set
PHI	Protected Health Information

Data Flow 0—General Research Scenario



Data Flow 0—General Research Scenario (continued)

	Scenario Data Flow	HIPAA	The Common Rule
6	Researcher plans to request the following information on patients ages 18–64 diagnosed with or treated for diabetes in the past twenty years at the AMC: Age, All Diagnoses, Race, Ethnicity, Dates of Service, Insulin Pump Serial Number, and Services Provided.	Information is PHI when it includes any data elements that directly identify or could be used to identify the individual subject of the information. *See HIPAA Note 2.*	
7	Researcher requests and receives waiver of authorization and an exemption determination for the research protocol from the AMC's IRB.	A researcher may obtain PHI for research without the subject's authorization when an IRB waives or alters the authorization requirement. *See HIPAA Note 10.*	An IRB must review all proposed research. *See Common Rule Note 2.* Certain types of research are exempt from the Common Rule's requirements, including secondary use of information for research governed by HIPAA. *See Common Rule Note 4.* Informed consent is not required because the research is exempt. *See Common Rule Note 6.*
8	Researcher submits documentation of IRB waiver authorization and requests and receives electronic data file from AMC.	A CE must obtain documentation of an IRB's waiver of authorization prior to disclosing PHI. *See HIPAA Note 10.* The HIPAA Security Rule generally requires that PHI be stored and transmitted with appropriate protections in accordance with the Security Rule. *See HIPAA Note 3.*	
9	Researcher conducts analysis and publishes aggregated, de-identified results in peer-reviewed journal.	Once information is de-identified, it is no longer PHI and no longer protected by HIPAA. *See HIPAA Note 2.*	Use of information that is not identifiable is not considered "research" under the Common Rule. *See Common Rule Note 1.*
		HIPAA no longer applies to de-identified results of study.	**Common Rule no longer applies to non-research activities.**

Data Flow 1—Use Case 1: Combining Data for PCOR

Scenario Narrative:

Individual is a 60-year-old female with no special status. She seeks treatment for opioid dependence at a federally assisted substance abuse (Part 2) program. Individual's information is maintained within the Part 2 Program's Electronic Health Record (EHR) system. With written patient consent, the Part 2 Program submits an insurance claim to Individual's Health Plan for substance use disorder treatment services provided to Individual. A researcher employed by an independent Research Institution wants to assess the cost-effectiveness and comparative effectiveness of several treatments, comparing pharmaceuticals and psychosocial treatment for opioid dependence in a federally funded research project. She plans to use identifiable clinical and claims data for this research protocol. The Health Plan has a Business Associate Agreement (BAA) with a Coordinating Center to perform data aggregation and other initiatives on its behalf. The Part 2 program has a Qualified Service Organization Agreement (QSOA) with the Coordinating Center to provide it with data processing, data aggregation, and other professional services. The researcher plans to seek a limited data set (LDS), compiled by the Coordinating Center, to include the following elements drawn from Part 2 Program clinical data and Health Plan claims data: Age, All Diagnoses, Dates of Service, Treatments Received, and Cost of Services Provided. Researcher seeks an exemption determination from the Research Institution's Institutional Review Board (IRB) as well as an approval of the planned data linkage request. The IRB approves the data linkage request and determines that the research is exempt from the Common Rule because the researcher is using existing information, will not record the information in a way that identifies the subjects, and will not contact the subjects or re-identify the information. The researcher provides documentation of this exemption determination to the Part 2 Program Director, who determines that identifiable Part 2 information can be disclosed without obtaining patient consent because the research qualifies for an exemption under the Common Rule. The researcher executes a data use agreement (DUA) with the Health Plan and the Part 2 Program and requests that the Coordinating Center create an LDS linking all relevant data from the Health Plan and the Part 2 Program. Individual's Part 2 clinical information from the Part 2 Program and claims data from the Health Plan are transferred to the Coordinating Center for inclusion in the LDS. In compliance with the DUAs and the terms of its BAA with the Health Plan and QSOA with the Part 2 Program, the Coordinating Center combines all the data and produces an LDS with research unique identifiers. The Coordinating Center provides the LDS to the researcher. The researcher conducts the analysis and publishes aggregated, de-identified results in a peer-reviewed journal.

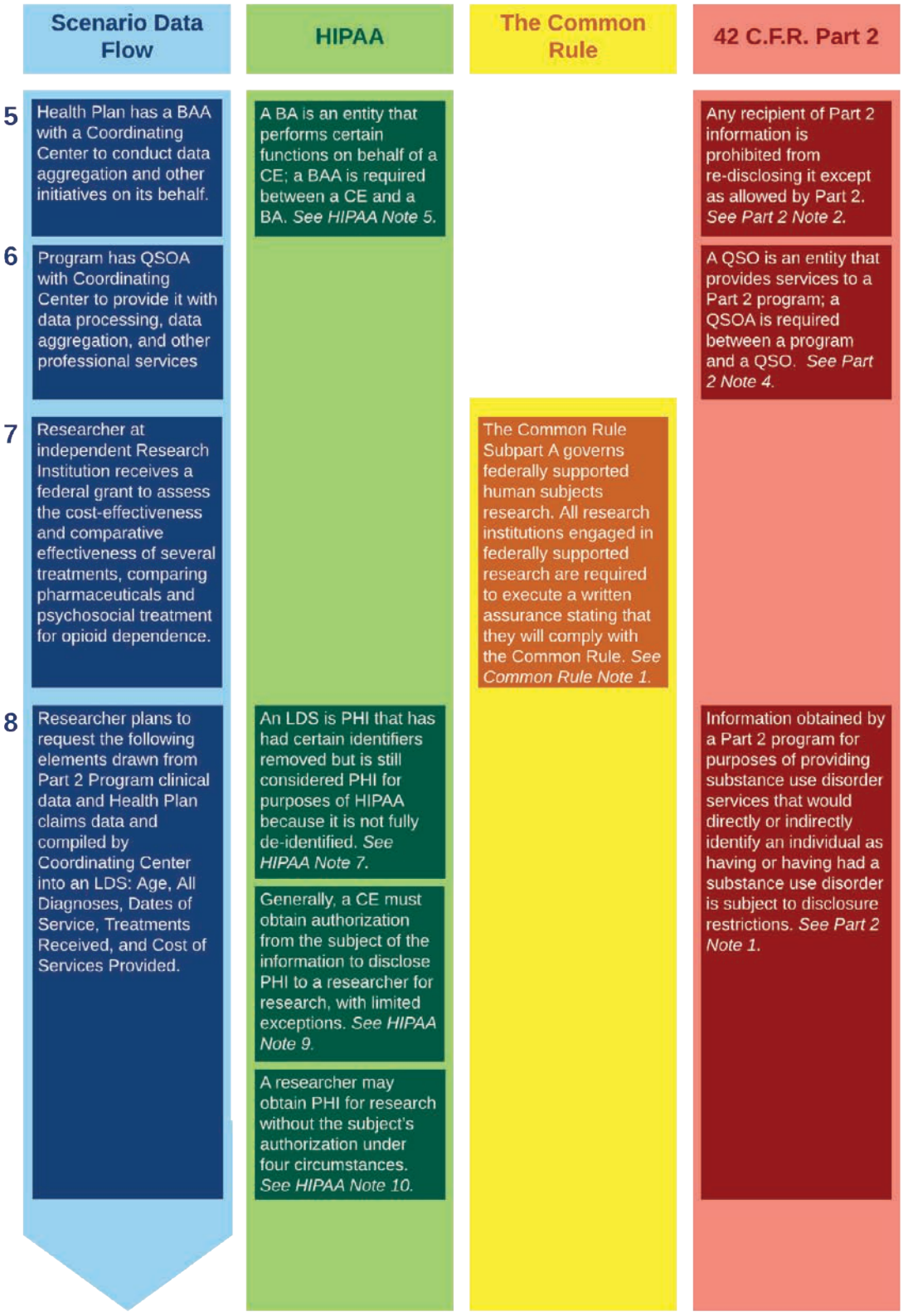
Statutes/Regulations implicated: HIPAA, Common Rule, Part 2

Acronyms for Data Flow 1	
BA	Business Associate
BAA	Business Associate Agreement
CE	Covered Entity
DUA	Data Use Agreement
EHR	Electronic Health Record
IRB	Institutional Review Board
LDS	Limited Data Set
PHI	Protected Health Information
QSO	Qualified Service Organization
QSOA	Qualified Service Organization Agreement

Data Flow 1—Use Case 1: Combining Data for PCOR

	Scenario Data Flow	HIPAA	The Common Rule	42 C.F.R. Part 2
1	Individual is 60-year-old female with no special status.			
2	Individual seeks treatment for opioid dependence at a federally assisted substance abuse (Part 2) Program.	The HIPAA Privacy and Security Rules apply to CEs, which are healthcare providers, health plans, and healthcare clearinghouses. *See HIPAA Note 1.*		42 C.F.R. Part 2 (Part 2) applies to all federally assisted substance use disorder programs (i.e., Part 2 programs). *See Part 2 Note 1.*
		Individually identifiable health information provided by an individual to a CE becomes HIPAA-covered PHI once received by the CE and stored in their records. *See HIPAA Note 2.*		Part 2 protects information obtained by a Part 2 program for purposes of providing substance use disorder services that would directly or indirectly identify an individual as having or having had a substance use disorder. *See Part 2 Note 1.*
3	Individual's information is maintained within the Program's EHR system.	The HIPAA Security Rule generally requires that PHI be stored and transmitted with appropriate protections in accordance with the Security Rule's provisions. *See HIPAA Note 3.*		Records maintained by Part 2 programs must comply with certain security requirements. *See Part 2 Note 5.*
4	The Program submits an insurance claim to Individual's Health Plan for substance abuse treatment services provided to Individual.			Although HIPAA would allow disclosure of PHI to Health Plan for payment purposes without patient authorization, Part 2 requires patient consent to disclose substance use disorder patient identifying information to Health Plan for such purpose. *See Part 2 Note 4.*

Data Flow 1—Use Case 1: Combining Data for PCOR (continued)



Data Flow 1—Use Case 1: Combining Data for PCOR (continued)

	Scenario Data Flow	HIPAA	The Common Rule	42 C.F.R. Part 2
9	Researcher seeks an exemption determination and review of the data linkage request from Research Institution's IRB		An IRB must review all proposed research at organizations subject to the Common Rule. *See Common Rule Note 2.*	An IRB must review all data linkage requests from researchers using Part 2 information. *See Part 2 Note 6.*
10	IRB approves data linkage request and determines that research is exempt because it uses preexisting (stored) private identifiable information and the researcher will not record the information in a manner that identifies subjects and will not re-identify or contact subjects.		Certain research is exempt from all Common Rule requirements, including requirements related to informed consent and IRB review and approval. *See Common Rule Note 4.*	An IRB must approve all data linkage requests from researchers using Part 2 information; researchers are required to produce evidence of such approval upon request. *See Part 2 Note 6.*
11	The researcher submits documentation of the IRB's exemption determination to the Part 2 Program Director, who determines that Part 2 information may be disclosed without patient consent because the research qualifies as exempt under the Common Rule.		**Common Rule no longer applies once research is determined to be fully exempt.**	Part 2 patient identifying information may be disclosed without patient consent by the Part 2 program director or any other lawful holder of the data for scientific research in certain circumstances. *See Part 2 Note 3.*
12	Researcher executes DUAs with Health Plan and with the Part 2 Program through which Health Plan and Program may share an LDS with researcher.	A DUA is a contract between a CE and a recipient of an LDS from the CE. A DUA is required when a CE discloses an LDS to a researcher for research. *See HIPAA Note 6.*		A DUA is not required under Part 2; however, because Part 2 programs are often also HIPAA CEs, relevant HIPAA requirements may apply where there is no conflicting Part 2 requirement. *See Part 2 Note 7.*

Data Flow 1—Use Case 1: Combining Data for PCOR (continued)

	Scenario Data Flow	HIPAA	The Common Rule	42 C.F.R. Part 2
13	In compliance with DUAs and in accordance with the terms of its BAA with Health Plan and its QSOA with Part 2 Program, Coordinating Center combines the requested clinical and claims data and produces an LDS that contains the requested data elements, linked with unique research identifiers.	A DUA is a contract between a CE and a recipient of an LDS from the CE. *See HIPAA Note 6.* A DUA is required when a CE discloses an LDS to a researcher for research. A BA is an entity that performs certain functions on behalf of a CE; a BAA is required between a CE and a BA. *See HIPAA Note 5.*		A Part 2 program may disclose patient identifying information to a QSO for certain purposes pursuant to the terms of a QSOA (Coordinating Center may access patient identifying information to create an LDS and/or data linkages as a QSO). *See Part 2 Note 4.* Any entity creating data linkages at the request of a researcher accessing Part 2 patient identifying information under the research exception must follow specific requirements related to the data after the linkages are complete. *See Part 2 Note 6.*
14	Researcher conducts analysis and publishes aggregated, de-identified results in peer-reviewed journal.	De-identified information contains no individually identifiable information either by removal of specified elements or because certified as de-identified by an expert. *See HIPAA Note 8.* Once information is de-identified, it is no longer PHI and no longer protected by HIPAA. *See HIPAA Note 2.*		Part 2 does not protect information that does not identify individuals as having or having had a substance use disorder. *See Part 2 Note 1.*
		HIPAA no longer applies to de-identified results of study.		**Part 2 no longer applies to information that is not patient identifying.**

Data Flow 2—Use Case 2: Consent Management

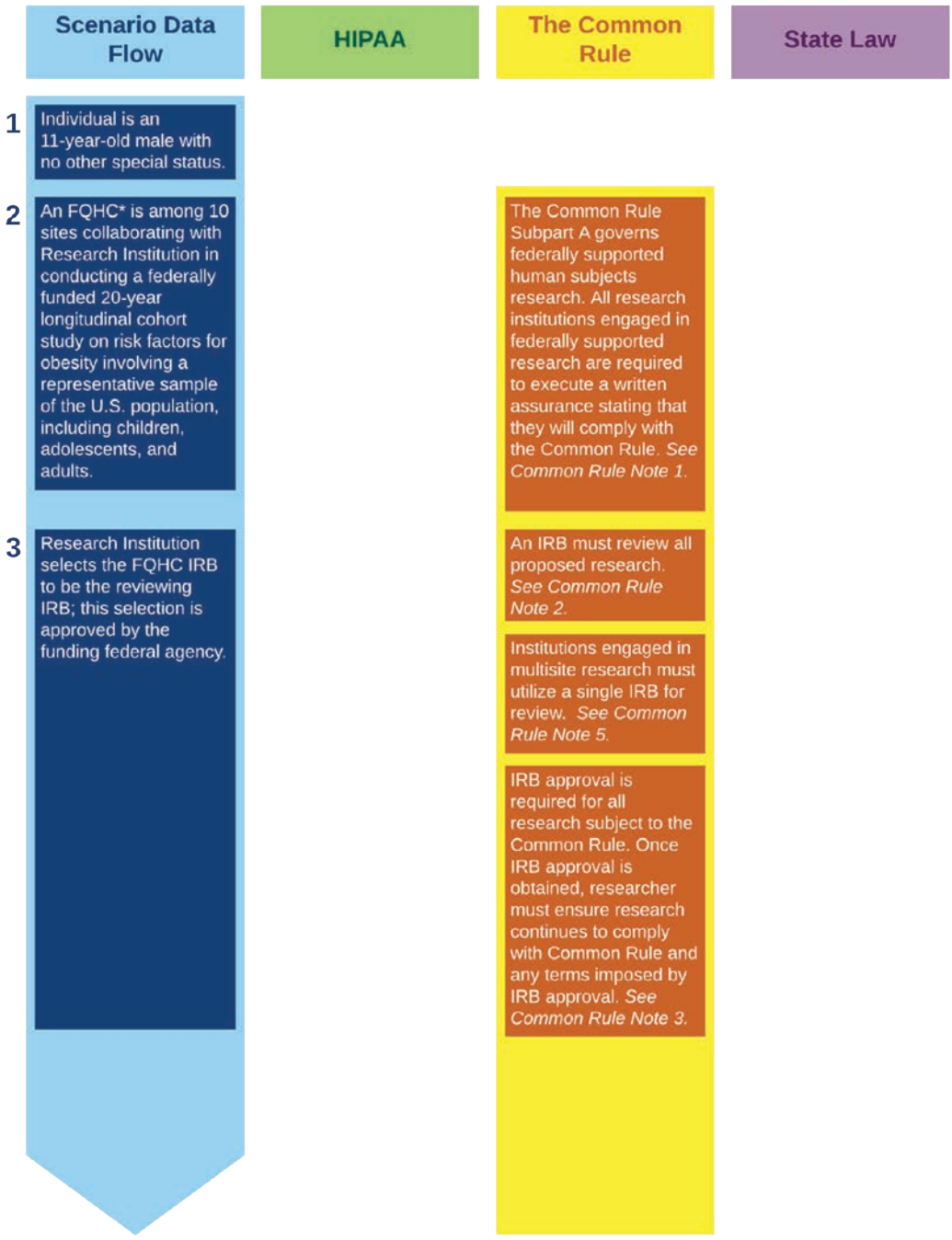
Scenario Narrative:

Individual is an 11-year-old male with no other special status. A Federally Qualified Health Center (FQHC) is among 10 sites collaborating with a Research Institution in conducting a federally funded 20-year longitudinal cohort study on risk factors for obesity involving a representative sample of the U.S. population, including children, adolescents, and adults. All entities participating in the research agree to use a common Institutional Review Board (IRB), which approves the research protocol. Individual seeks treatment at the FQHC for asthma. Individual's mother consents to his treatment. Individual's BMI is recorded in the obese range. Individual's information is maintained within the FQHC's Electronic Health Record (EHR) system along with other patient medical records. At the time of his asthma treatment, the FQHC recruits Individual to participate in a research study in which Individual's health data collected in the course of treatment will be reported to the Research Institution at quarterly intervals. Individual's mother consents to Individual's participation in the research study and for Individual's information to be given to the Research Institution. Per the approved research protocol, the FQHC also obtains Individual's assent to participate in the research. Individual's mother also consents to unspecified future research at the Research Institution using Individual's information. Data is collected by the FQHC and reported quarterly to the researcher. The researcher conducts her analysis, combining clinical information from research participants with public economic and housing data. The researcher publishes an analysis of five years of data in de-identified, aggregated form (planning to publish updates every five years and then at end of study). Individual turns 18 and withdraws from research protocol, revoking authorization for his information to be used in further research, but continues receiving asthma treatment at the FQHC.

Statutes/Regulations implicated: HIPAA, Common Rule, State Law

Acronyms for Data Flow 2	
CE	Covered Entity
EHR	Electronic Health Record
FQHC	Federally Qualified Health Center
IRB	Institutional Review Board
PHI	Protected Health Information

Data Flow 2—Use Case 2: Consent Management



* Note that community health centers receiving funding under Section 330 of the Public Health Service Act are subject to separate confidentiality requirements under federal law (42 C.F.R. § 51c.110).

Data Flow 2—Use Case 2: Consent Management (continued)

	Scenario Data Flow	HIPAA	The Common Rule	State Law
4	Individual seeks treatment at the FQHC for asthma. Individual's mother consents to his treatment. Individual's BMI is recorded in the obese range. Individual's information is maintained within the FQHC's EHR system along with other patient medical records.	The HIPAA Privacy and Security Rules apply to CEs, which are healthcare providers, health plans, and healthcare clearing-houses. *See HIPAA Note 1.* Individually identifiable health information provided by an individual to a CE becomes HIPAA-covered PHI once received by the CE and stored in their records. *See HIPAA Note 2.* The HIPAA Security Rule generally requires that PHI be stored and transmitted with appropriate protections in accordance with the Security Rule's provisions. *See HIPAA Note 3.*		State law defines the age of majority and also defines the ages at which minors may consent to medical treatment or research (which may vary based on type of treatment or research). *See State Law Note 3.* For a minor or legally incompetent patient or research participant, state law determines who is empowered to provide consent as the individual's parent or legal guardian. *See State Law Note 3.*
5	At time of treatment, FQHC recruits Individual to participate in research study in which Individual's health data collected in the course of treatment will be reported to Research Institution at quarterly intervals. Individual's mother consents to Individual's participation in the research study and for Individual's information to be given to Research Institution.	Generally, a CE must obtain authorization from the subject of the information to disclose PHI to a researcher for research, with limited exceptions. *See HIPAA Note 9.* HIPAA Authorization to disclose PHI may be combined with consent to participate in research (compound authorization). *See HIPAA Note 11.*	Informed consent is required unless the IRB waives it in full or in part. *See Common Rule Note 6.* For minors participating in research, the consent of a single parent may be sufficient for certain studies. *See Common Rule Note 7.*	For a minor or legally incompetent patient or research participant, state law determines who is empowered to provide consent as the individual's parent or legal guardian. *See State Law Note 3.*
6	Per the approved research protocol, FQHC also obtains Individual's assent to participate in the research.		Assent to participate in research is required for children capable of providing consent, as determined by an IRB. *See Common Rule Note 8.*	

Data Flow 2—Use Case 2: Consent Management (continued)

	Scenario Data Flow	HIPAA	The Common Rule	State Law
7	Individual's mother also consents to unspecified future research at the Research Institution using Individual's information.	A researcher is permitted to obtain authorization for unspecified future research. *See HIPAA Note 13.*	Broad consent may be obtained to store private identifiable information and identifiable biospecimens for potential future research use, provided certain requirements are met. *See Common Rule Note 6.*	
8	Data is collected by FQHC and reported quarterly to Researcher.	The HIPAA Security Rule generally requires that PHI be stored and transmitted with appropriate protections in accordance with the Security Rule's provisions. *See HIPAA Note 3.*		
9	Researcher conducts analysis, combining clinical information from research participants with public economic and housing data. Researcher publishes analysis of five years of data in de-identified, aggregate form (planning to publish updates every five years and then at end of study).	Once information is de-identified, it is no longer PHI and no longer protected by HIPAA. *See HIPAA Note 2.*	Use of de-identified information would not be subject to the Common Rule. *See Common Rule Note 10.*	
10	Individual turns 18 and withdraws from research protocol, revoking authorization for his information to be used in further research, but continues receiving asthma treatment at the FQHC.	Under HIPAA, when a research participant revokes authorization, PHI may continue to be used and disclosed only to the extent necessary to protect the integrity of the research study. Information that was previously published or de-identified may continue to be used because it is no longer PHI. *See HIPAA Note 20.*	If a research participant withdraws consent to participate, the Common Rule allows continued use of the individual's already-collected and identifiable information and biospecimens by the researcher with some exceptions. *See Common Rule Note 9.*	Age of majority is 18 in almost all states. Some states give individuals the ability to consent to certain medical treatments at younger ages (and thus the right to direct and control related information to the extent such rights are granted to adults). *See State Law Note 3.*
		HIPAA no longer applies to de-identified results of study.		**State Law governing minors no longer applies once individual reaches age of majority.**

Data Flow 3—Use Case 3: Release and Use of Specially Protected Health Data

Scenario Narrative:

Individual is a 30-year-old male with no special status who is employed in the IT department at an Academic Medical Center (AMC). Individual has a family history of Huntington's Disease. His employer-sponsored Health Plan covers genetic testing, so at his next check-up Individual goes to on-site lab for genetic tests and general blood work. One test comes back indicating genetic markers for Huntington's. Tests also show Individual is HIV-positive. After receiving these results, Individual contacts his Employee Assistance Program (EAP) for intake, assessment, and referral to a psychologist specializing in treating depression related to fatal diseases. Individual subsequently seeks treatment for depression at the AMC from a psychologist employed by the AMC. Information about Individual's mental health treatment is maintained within the AMC's Electronic Health Record (EHR) system along with other AMC patient medical records. The psychologist treating Individual is involved with a research protocol housed within the AMC, serving as a recruiter. The psychologist recruits Individual to participate in the research study. The research study is federally funded and involves tracking patients with a genetic marker for Huntington's over a five-year period and monitoring relationship of psychological factors to the onset and progression of physical factors. Researchers monitor participants directly, administer surveys on a regular basis, and conduct ongoing physical monitoring. The researcher also accesses treatment records from providers, including psychologist. The researcher collects detailed information about Individual's family history known to Individual. Individual passes away unexpectedly two months after the conclusion of the research protocol. Researchers wish to publish Individual's information as part of a featured case study and contact Individual's sister to seek consent for such disclosures. His sister declines to allow information to be published in an identifiable manner, so the proposed case study cannot be published. Information about Individual can be published in a de-identified, aggregated manner only.

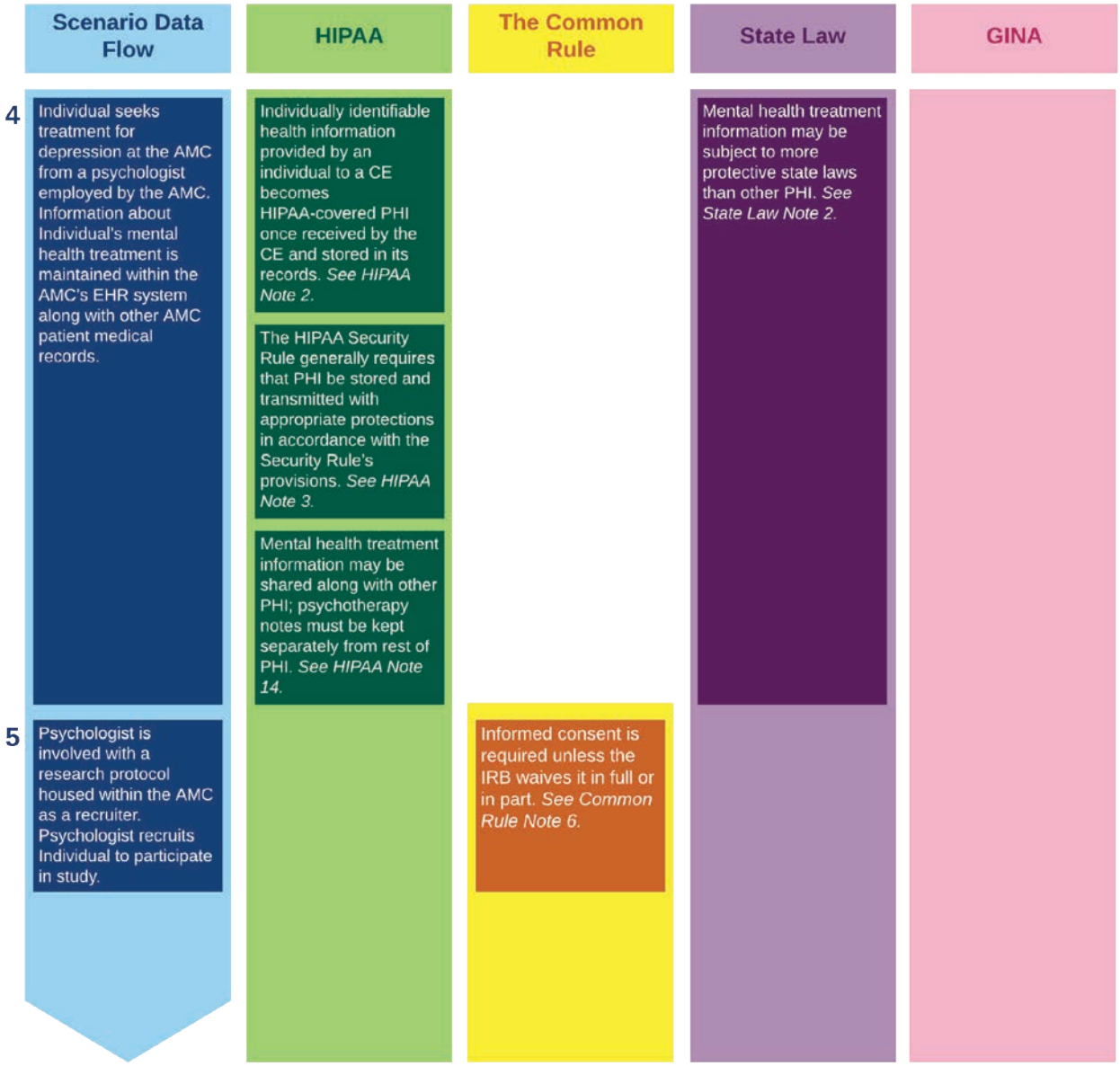
Statutes/Regulations implicated: HIPAA, Common Rule, State Law, GINA

Acronyms for Data Flow 3	
AMC	Academic Medical Center
CE	Covered Entity
EAP	Employee Assistance Program
EHR	Electronic Health Record
HD	Huntington's Disease
IRB	Institutional Review Board
PHI	Protected Health Information

Data Flow 3—Use Case 3: Release and Use of Specially Protected Health Data

	Scenario Data Flow	HIPAA	The Common Rule	State Law	GINA
1	The individual is a 30-year-old male with no special status who is employed in an Academic Medical Center's IT department. Individual has a family history of Huntington's Disease. His employer-sponsored health plan covers genetic testing so at his next check-up, he goes to on-site lab for genetic tests and general bloodwork.	The HIPAA Privacy and Security Rules apply to CEs, which are healthcare providers, health plans, and healthcare clearinghouses. *See HIPAA Note 1.*			GINA restricts how employers and insurers can collect and use genetic information about individuals. *See GINA Note 1.* Employers and insurers cannot request, acquire, or use genetic information to discriminate in employment or insurance-related decisions. *See GINA Note 2.*
2	Test comes back indicating genetic markers for HD. Tests also show Individual is HIV positive.	A CE is permitted to disclose PHI to the state without authorization if required by state law or if permitted or required by public health authority under state law. *See HIPAA Note 12.*		State laws may impose requirements for CEs and laboratories to report certain PHI to the state; CEs are permitted under HIPAA to disclose where required or authorized by state law. *See State Law Note 1.*	
3	After receiving these results, Individual contacts his EAP for intake, assessment, and referral to a psychologist specializing in treating depression related to fatal diseases.	Employee information held by an employer in employment records (such as information obtained by an EAP) is not considered PHI and thus is not governed by HIPAA, even where the employer is a CE or the information is otherwise health-related. *See HIPAA Note 4.*			

Data Flow 3—Use Case 3: Release and Use of Specially Protected Health Data (continued)



Data Flow 3—Use Case 3: Release and Use of Specially Protected Health Data (continued)

	Scenario Data Flow	HIPAA	The Common Rule	State Law	GINA
6	Research study is federally funded and involves tracking over a five-year period patients with a genetic marker for Huntington's and monitoring relationship of psychological factors to onset and progression of physical factors.		The Common Rule Subpart A governs federally supported human subjects research. All research institutions engaged in federally supported research are required to execute a written assurance stating that they will comply with the Common Rule. *See Common Rule Note 1.* An IRB must review all proposed research at organizations subject to the Common Rule. *See Common Rule Note 2.* IRB approval is required for all research activities that are subject to the Common Rule. Once IRB approval is obtained, researcher must ensure research continues to comply with Common Rule and any terms imposed by IRB approval. *See Common Rule Note 3.*		
7	Researchers monitor participants directly, administer surveys on a regular basis, and conduct ongoing physical monitoring; researchers also access treatment records from providers, including psychologist.	HIPAA Authorization to disclose PHI may be combined with consent to participate in research (compound authorization). *See HIPAA Note 11.* Mental health treatment information may be shared along with other PHI; psychotherapy notes must be kept separately from rest of PHI. *See HIPAA Note 14.* HIPAA authorization to disclose psychotherapy notes must be made separately from other authorizations and specifically for psychotherapy notes. *See HIPAA Note 15.*			

Data Flow 3—Use Case 3: Release and Use of Specially Protected Health Data (continued)

	Scenario Data Flow	HIPAA	The Common Rule	State Law	GINA
8	AMC-employed researcher collects detailed information about AMC-employed Individual's family history known to Individual.	Family history information given to a CE by an individual is part of the individual's PHI. *See HIPAA Note 16.*			An individual's genetic information protected by GINA includes genetic information about family members. *See GINA Note 1.* GINA restricts how employers and insurers can collect and use genetic information about individuals. *See GINA Note 1.* Employers and insurers generally cannot request or acquire genetic information nor use genetic information to discriminate in employment or insurance-related decisions. *See GINA Note 2.*
9	Individual passes away unexpectedly two months after the conclusion of the research protocol. Researchers wish to publish the Individual's information as part of a featured case study and contact Individual's sister to seek consent for such disclosures.	PHI of deceased patients may be accessed and disclosed as authorized by a personal representative of the deceased. *See HIPAA Note 17.*	The Common Rule governs human subject research, defined as research involving living human beings. *See Common Rule Note 1.*	For a deceased person, state law defines who may serve as the personal representative for purposes of control over their PHI. *See State Law Note 4.*	
10	Sister declines to allow information to be published in an identifiable manner; case study cannot be published. Information can be published in a de-identified, aggregate manner only.	Information about a deceased individual remains PHI until fifty years after date of his/her death. Authorization to disclose PHI must be obtained from the deceased's personal representative. *See HIPAA Note 21.*	**Common Rule no longer applies to deceased individual's information.**		
		HIPAA no longer applies to de-identified results of study or to PHI 50 years after death.			

Data Flow 4—Use Case 4: Identification and Re-Identification of PCOR Data

Scenario Narrative:

Individual is a 60-year-old Alaska Native female living in a small town in Arkansas with no special status. A National Institutes of Health (NIH) research team plans to do research including a large national survey on chronic disease. The researchers plan to link survey data to other data sets, including claims data from participants' health plans. The researchers plan to maintain the confidentiality of all information collected and publish only de-identified data, although the information will be maintained in identifiable form within NIH for research purposes. The Institutional Review Board (IRB) at NIH approves the research protocol. Seeking a random sample, NIH researchers contact individuals of all ages in designated areas using published phone numbers. Individual is contacted by the research team and consents to provide data to the research team in response to their survey, including information about past and current diagnoses, treatments, and lifestyle. Individual also consents to the researchers gathering claims data from her Health Plan about her health care in the past year. As part of the consent process, Individual is told that her data will be kept confidential and only de-identified information will be published. In order for researchers to get the Health Plan data, Individual must provide an authorization under HIPAA specifically directing the Health Plan to provide specific information to researchers. Researchers provide a generic HIPAA Authorization form, but Individual's Health Plan may require the use of its own form. Researchers collect survey data and receive specified claims data from Individual's Health Plan. Researchers combine both data sets into a single research record. Researchers conduct their analysis and de-identify data using the Safe Harbor approach under HIPAA. Researchers publish results, including de-identified information about participants. An information reseller (data miner) finds the published research on the Internet. The reseller combines the de-identified information in the published research with data from public sources and succeeds in re-identifying certain individuals who had participated in the research. Individuals from smaller racial and ethnic groups in their respective geographic areas are more likely to be re-identified. The reseller puts together a list of people with names and contact information also identifying a variety of characteristics, including health information gleaned from the de-identified research data. Reseller sells that list to a marketer who targets Individual with advertising for certain health products.

Statutes/Regulations implicated: HIPAA, Common Rule

Acronyms for Data Flow 4	
CE	Covered Entity
EHR	Electronic Health Record
IRB	Institutional Review Board
NIH	National Institutes of Health
PHI	Protected Health Information

Data Flow 4—Use Case 4: Identification and Re-Identification of PCOR Data

Scenario Data Flow	HIPAA	The Common Rule
1 Individual is a 60-year-old Alaska Native female living in a small town in Arkansas with no special status.		
2 An NIH research team plans to do research, including a large national survey on chronic disease. Researchers plan to link survey data to other data sets, including claims data from participants' health plans. Researchers plan to maintain the confidentiality of all information collected and publish only de-identified data, although the information will be maintained in identifiable form within NIH for research purposes. The IRB at NIH reviews and approves the research protocol.		The Common Rule Subpart A governs federally supported human subjects research. All research institutions engaged in federally supported research are required to execute a written assurance stating that they will comply with the Common Rule. *See Common Rule Note 1.* An IRB must review all proposed research at organizations subject to the Common Rule. *See Common Rule Note 2.* IRB approval is required for all research activities that are subject to the Common Rule. Once IRB approval is obtained, researcher must ensure research continues to comply with Common Rule and any terms imposed by IRB approval. *See Common Rule Note 3.*

Data Flow 4—Use Case 4: Identification and Re-Identification of PCOR Data (continued)

	Scenario Data Flow	HIPAA	The Common Rule
3	NIH researchers contact individuals of all ages in designated areas using published phone numbers. Individual is contacted and consents to provide data in response to the survey and to the researchers gathering claims data from her health plan about her health care in the past year. As part of the consent process, Individual is told that her data will be kept confidential and only de-identified information will be published. Individual provides a HIPAA authorization permitting her health plan to provide PHI to researchers.	Generally, a CE must obtain authorization from the subject of the information to disclose PHI to a researcher for research, with limited exceptions. *See HIPAA Note 9.* HIPAA Authorization to disclose PHI may be combined with consent to participate in research (compound authorization). *See HIPAA Note 11.* HIPAA requires CEs to disclose PHI where directed by the individual who is the subject of the information. *See HIPAA Note 19.*	Informed consent is required unless the IRB waives it in full or in part. *See Common Rule Note 6.*
4	Researchers collect survey data, including information about Individual's past and current diagnoses, treatments, and lifestyle, and receive specified claims data from Individual's health plan. Researchers combine both data sets into a single research record.	The HIPAA Security Rule generally requires that PHI be stored and transmitted with appropriate protections in accordance with the Security Rule's provisions. *See HIPAA Note 3.*	

Data Flow 4—Use Case 4: Identification and Re-Identification of PCOR Data (continued)

	Scenario Data Flow	HIPAA	The Common Rule
5	Researchers conduct their analysis and de-identify data using the Safe Harbor approach under HIPAA. Researchers publish results including de-identified information about participants.	Once information is de-identified, it is no longer PHI and no longer protected by HIPAA. *See HIPAA Note 2.* De-identified information contains no individually identifiable information either by removal of specified elements (i.e., Safe Harbor method) or because certified by an expert. *See HIPAA Note 8.*	Research use of non-identifiable information is not subject to the Common Rule. *See Common Rule Note 1.*
6	An information reseller (data miner) finds the published research on the Internet. Reseller combines the de-identified information in the published research with data from public sources and succeeds in re-identifying certain individuals who had participated in the research. Individuals from smaller racial and ethnic groups in their respective geographic areas are more likely to be re-identified.	Information is not de-identified under the Safe Harbor method if the CE has actual knowledge that the data could be re-identified. Once a CE has actual knowledge that de-identified data has been or could be re-identified, the information is no longer considered de-identified and is instead considered PHI. The CE *See HIPAA Note 8.*	**Common Rule does not govern use of non-identifiable information.**
7	Reseller puts together a list of people with names and contact information also identifying a variety of characteristics, including health information gleaned from the de-identified research data. Reseller sells that list to a marketer who targets Individual with advertising for certain health products.	**HIPAA does not govern use or disclosure of PHI by non-Regulated Entities.**	

Data Flow 5—Use Case 5: Research Using Patient-Generated Health Data

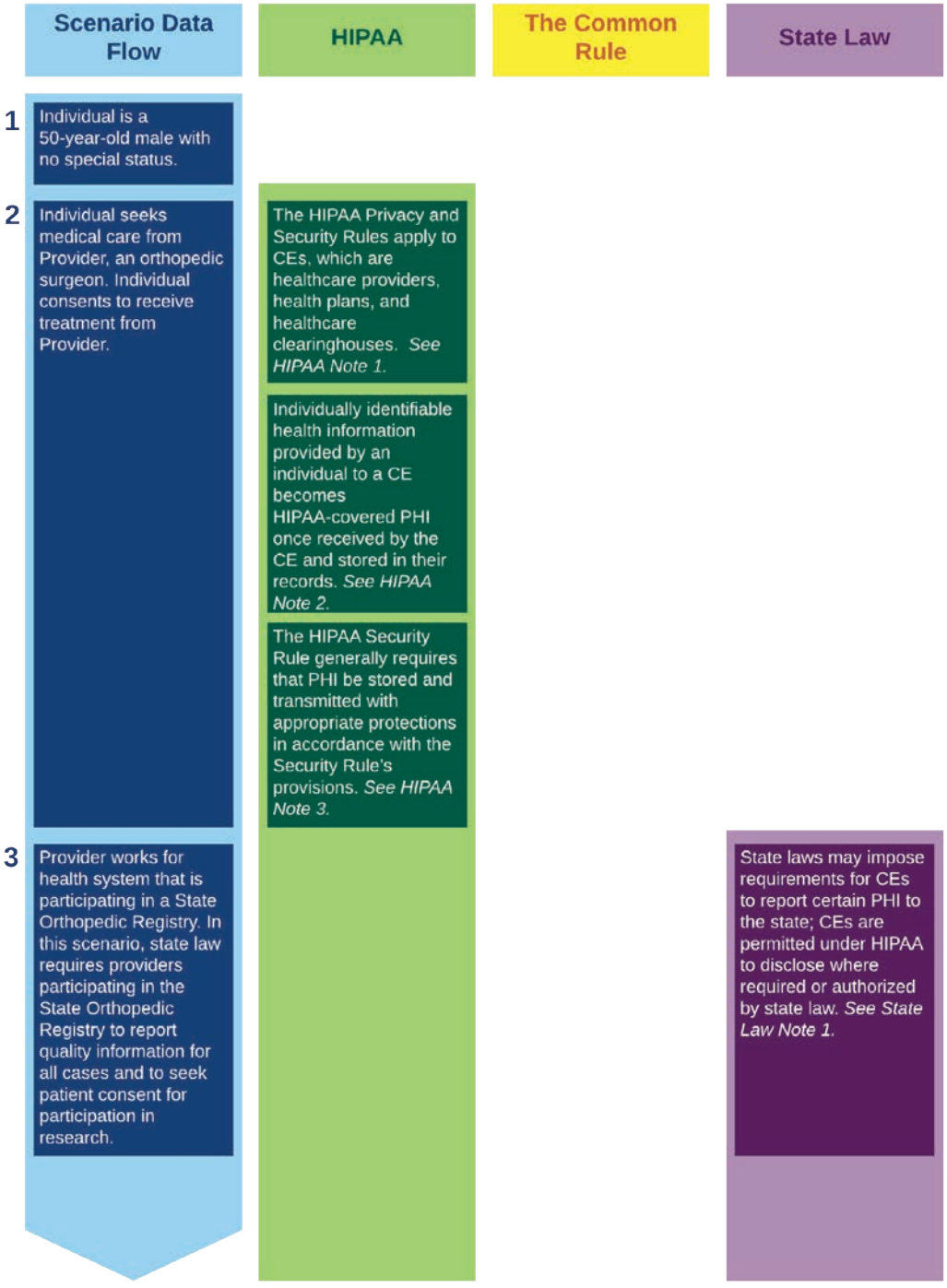
Scenario Narrative:

Individual is a 50-year-old male with no special status. Individual seeks medical care from a healthcare provider, specifically an orthopedic surgeon. Individual consents to receive treatment from the provider. The provider works for a health system that is participating in a State Orthopedic Registry. In this scenario, state law requires providers participating in the State Orthopedic Registry to report quality information for all cases and to seek patient consent for participation in research. The registry is used for federally funded research, in addition to quality reporting. The provider informs Individual of the registry and its use for research and quality reporting. Information reported to the registry includes demographic data as well as health information excerpted from the provider's Electronic Health Record (EHR). Individual is also asked to consent to be contacted in the future for information about the outcome of his treatment; the information reported is considered Patient-Reported Outcome (PRO) data. Individual receives medical treatment (orthopedic surgery) from the provider. The provider reports identifiable information about Individual and medical treatment provided to the registry. At specified intervals in the future, Individual is contacted by a researcher from the registry. The researcher administers an IRB-approved survey over the telephone asking for details about Individual's health, lifestyle, and mental state after the surgery. The researcher combines information from Individual and others who received orthopedic surgery in the state during the specified timeline and identifies factors that are associated with good outcomes and poor outcomes. The researcher de-identifies the information that will be included in a public report about orthopedic surgery outcomes and quality of orthopedic surgery providers in the state. The published report will include the names of individual providers but no Protected Health Information (PHI).

Statutes/Regulations: HIPAA, Common Rule, State Law

Acronyms for Data Flow 5	
CE	Covered Entity
EHR	Electronic Health Record
IRB	Institutional Review Board
PHI	Protected Health Information
PRO	Patient Reported Outcome

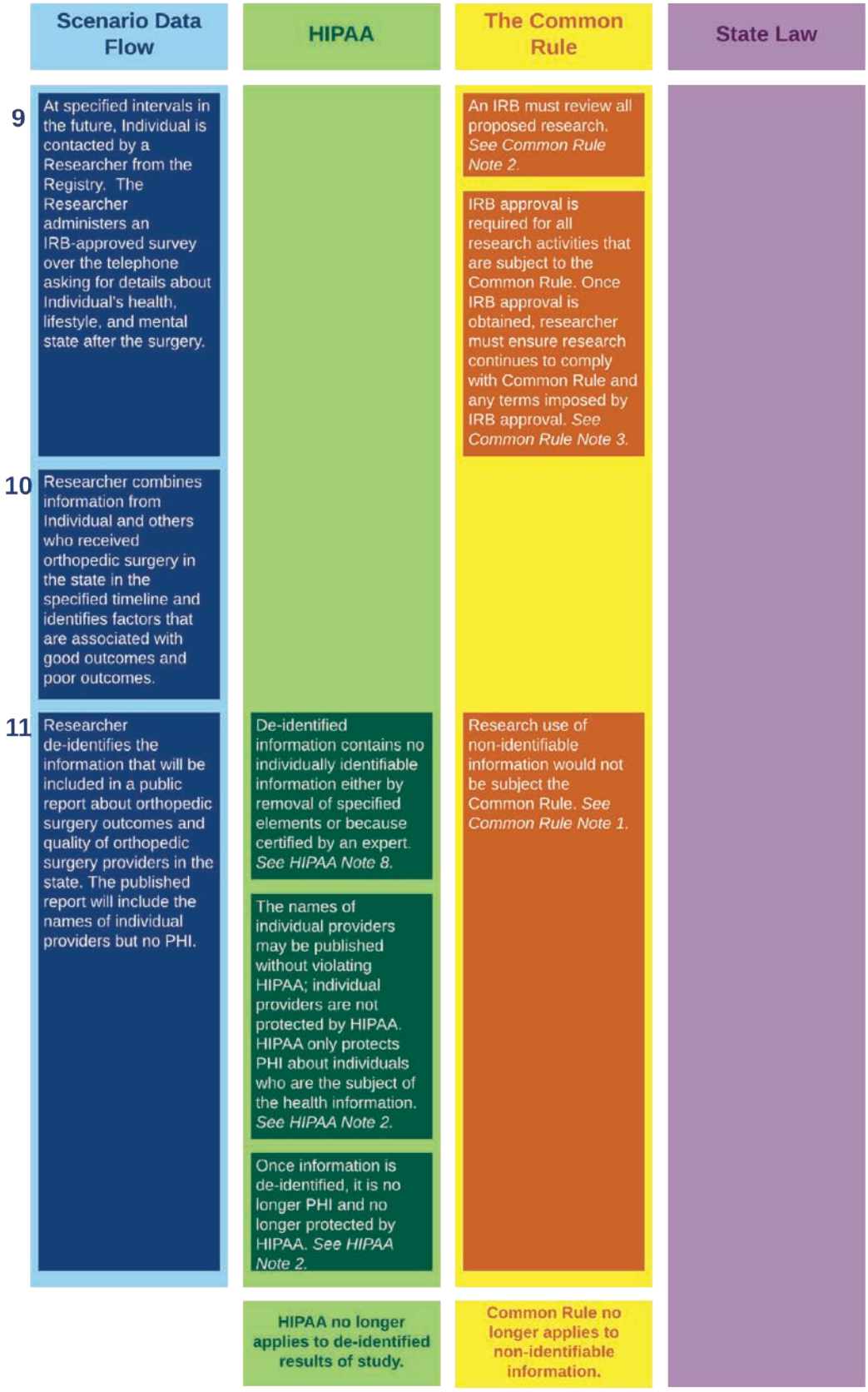
Data Flow 5—Use Case 5: Research Using Patient-Generated Health Data



Data Flow 5—Use Case 5: Research Using Patient-Generated Health Data (continued)

	Scenario Data Flow	HIPAA	The Common Rule	State Law
4	Registry is used for federally funded research, in addition to quality reporting.		The Common Rule Subpart A governs federally supported human subjects research. All research institutions engaged in federally supported research are required to execute a written assurance stating that they will comply with the Common Rule. *See Common Rule Note 1.*	
5	Provider informs Individual of Registry and its use for research, in addition to quality reporting.	Generally, a CE must obtain authorization from the subject of the information to disclose PHI to a researcher for research, with limited exceptions. *See HIPAA Note 9.*		
6	Provider asks Individual for his consent to include identifiable information in the Registry. Information includes demographic data as well as health information excerpted from Provider's EHR. Individual is also asked to consent to be contacted in the future for information about the outcome of his treatment (PRO).	HIPAA Authorization to disclose PHI may be combined with consent to participate in research (compound authorization). *See HIPAA Note 11.* A researcher is permitted to obtain authorization for unspecified future research. *See HIPAA Note 13.*	Informed consent is required unless the IRB waives it in full or in part. *See Common Rule Note 6.*	
7	Individual receives medical treatment (orthopedic surgery) from Provider.			
8	Provider reports identifiable information about Individual and medical treatment provided to Registry.	A CE is permitted to disclose PHI to the state without authorization if required by state law or permitted or required by public health authority under state law. *See HIPAA Note 12.*		State laws may impose requirements for CEs to report certain PHI to the state; CEs are permitted under HIPAA to disclose where required or authorized by state law. *See State Law Note 1.*

Data Flow 5—Use Case 5: Research Using Patient-Generated Health Data (continued)



EXPLANATORY NOTES

General Note: See Appendix A for more detailed summaries of the statutes and regulations addressed below.

HIPAA Notes

1. The HIPAA Rules apply to health plans, healthcare clearinghouses, and all healthcare providers, regardless of size, that electronically transmit health information in connection with certain transactions—collectively, these are known as "Covered Entities" (CE). The HIPAA Rules do not apply to researchers directly; however, researchers may seek data from CEs that must comply with HIPAA Rules when using or disclosing Protected Health Information (PHI) for research purposes. Researchers also may be employed by a CE and subject to HIPAA requirements as a member of its workforce.

2. Protected Health Information (referred to as PHI) is individually identifiable information in any form or medium (electronic, paper, or oral) that is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that relates to:

   a. The provision of care to an individual;

   b. An individual's past, present, or future physical or mental health condition; or

   c. An individual's payment for care, whether made in the past or present or expected in the future.[1]

   Information is individually identifiable when it directly references an individual or could be used to identify the individual.[2] PHI does not include education records or employment records held by a CE in its role as an employer.[3] **Information that is neither identifiable nor stored or maintained by a CE is not protected by HIPAA.** While there is not an exhaustive list of identifiable data elements, the list of data elements that must be removed from a data set in order for the data set to be considered de-identified under the Safe Harbor method is instructive. *See HIPAA Note 8.*

3. The HIPAA Security Rule allows great flexibility for CEs to protect electronic PHI. Note that the HIPAA Security Rule only applies to electronic PHI. A CE may use any security measures that enable the CE to ensure the confidentiality, integrity, and availability of electronic PHI, protect against reasonably anticipated threats, and protect again reasonably anticipated disclosures that are not permitted. Selected security measures must include administrative, technical, and physical safeguards.[4]

4. The definition of PHI excludes individually identifiable health information held in employment records by a CE in its role as an employer.[5] Where a workplace wellness or employee assistance program (EAP) is offered to an employee directly by his/her employer and not in connection with a group health plan, information collected from or created about program participants (i.e., employees) is not considered PHI and not protected by the HIPAA Rules.[6]

   Note also that CEs can be hybrid entities. A hybrid entity means "a single legal entity" that is a CE "whose business activities include both covered and non-covered functions and that designates healthcare components" accordingly.[7] For example, a large health center may function as both a

healthcare provider (a CE) and an employer (not a CE). The healthcare component of the hybrid entity (e.g., the healthcare provider component) must comply with the relevant provisions of HIPAA; other than organizational requirements associated with a hybrid designation, the part of the organization that does not perform HIPAA-covered functions, does not have to comply with HIPAA (e.g., the employer component).[8] Where an individual is employed by the non-CE portion of a hybrid entity, the employee does not act as a CE in the execution of his/her job duties. Note that an employer-sponsored workplace wellness program or an EAP would not, by itself, make the overall organization a hybrid entity. Rather, the organization would have to engage in business activities that include both covered and non-covered functions (as opposed to offering benefits to employees such as an EAP or workplace wellness program).

5. The HIPAA Privacy and Security Rules apply to Covered Entities' "Business Associates," which are individuals or organizations (other than members of the Covered Entity's workforce) that have access to PHI when providing certain services or functions to or on behalf of a CE. Business Associate services are limited to legal, actuarial, accounting, consultation, data aggregation, management, administrative, accreditation, or financial services; relevant functions include claims processing, data analysis, utilization review, and billing.[9] A Business Associate Agreement (BAA) is required between the CE and a BA that includes certain provisions, including that the BA will comply with applicable parts of the HIPAA Rules, the BA will only use and disclose PHI as permitted by HIPAA and the terms of the BAA, and the BA will use appropriate safeguards for electronic PHI in compliance with the HIPAA Security Rule.[10] Further, BAs are directly liable under HIPAA for compliance with applicable provisions of the HIPAA Privacy and Security Rules.[11]

6. A data use agreement (DUA) between a CE and a data recipient must establish the permitted uses and disclosures of PHI by the limited data set (LDS) recipient, who is permitted to use or receive the LDS, and contain other specifications related to what the LDS recipient may and may not do with the data.[12]

7. In order to be considered a limited data set (LDS), the following identifying information must be removed from a data set about the individual or of relatives, employers, or household members of the individual: names, postal address information, telephone numbers, fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers, Biometric identifiers, including finger and voice prints, and full face photographic images and any comparable images.[13] Even with these identifiers removed, an LDS is still considered to be PHI.

8. Health information that has been de-identified is not considered to be PHI for purposes of HIPAA applicability.[14] Information can be de-identified under HIPAA in either of two ways:

    a. Safe Harbor Method:[15] Information is de-identified under this method when all of 18 specific identifiers are removed from the PHI that relate to the individual or his/her relatives, household members, or employers. Information is not de-identified under this method if the CE has actual knowledge that the information could be used (alone or in combination with other information) to identify the individual. Once the CE has actually obtained such knowledge, the information is no longer considered de-identified and must be treated as PHI (even if the 18 identifiers are removed).

b. Statistical/Expert Method:[16] This method relies on analysis by an individual with sufficient knowledge and experience regarding statistical and scientific methods and principles for de-identifying information. Information is considered de-identified under this method when the expert individual, after applying these methods and principles, determines that there is very small risk that an anticipated recipient could identify an individual either from the information alone or in combination with other available information.

9. CEs are permitted to use and disclose PHI for research with individual authorization or without individual authorization if certain requirements are met. *See HIPAA Note 10*. Research is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[17]

   To use or disclose PHI with individual authorization, the CE must obtain an authorization that meets certain requirements.[18] There is a general set of authorization requirements that apply to all uses and disclosures; however, research authorizations may include certain provisions unique to research purposes. HIPAA allows an individual to authorize disclosures for "future, unspecified research." *See HIPAA Note 13*. Further, an authorization for research need not include a specific expiration date or event for the authorization (e.g., does not expire, no expiration date or event, or continues until the end of the research study). Finally, authorizations for research (unlike any other type of authorization under HIPAA) may be combined with a consent to participate in the same or other research study or with other legal permissions related to research.[19] *See HIPAA Note 11*. Disclosure of PHI pursuant to an individual's authorization is not subject to the minimum necessary standard.[20]

   Note that a CE may always use or disclose health information that has been de-identified without obtaining authorization or waiver of authorization by an IRB or Privacy Board.[21]

10. A CE may use or disclose PHI without individual authorization for research under the following four circumstances described in further detail below.

    a. Alteration or waiver of authorization approved by an Institutional Review Board (IRB) or Privacy Board.[22] The following documentation must be obtained by the CE related to the alteration waiver of authorization: a) IRB or Privacy Board identification and date of approval; b) IRB or Privacy Board statement that three criteria referenced below are met; c) description of the PHI requested; d) IRB or Privacy Board statement of review or approval; and e) signature of the chair or other designated member.[23] In order for an IRB or Privacy Board to approve a waiver of authorization, the IRB or Privacy Board must determine the following: a) the use or disclosure of PHI does not present more than minimal risk to the privacy of the individuals [e.g., adequate plan to protect identifiers from improper use or disclosure; adequate plan to destroy the identifiers in most circumstances; and adequate written assurances that the PHI will not be reused or re-disclosed]; b) the research could not be conducted without the waiver or alteration; and c) the research could not be conducted without access to and use of the PHI.[24]

    b. Representations from the researcher that the PHI will be used solely to prepare a research protocol.[25] The CE must also obtain representations (written or oral) that the researcher will not remove any PHI from the CE and that the PHI requested is necessary for the research.[26]

    c. Representations from the researcher that the PHI is solely used for research using the PHI of decedents.[27] The CE must also obtain representations (written or oral) from a researcher that

the PHI requested is necessary for the research and, if specifically requested by the CE, documentation of the death of the decedent whose PHI is requested.[28]

d. Use of a Limited Data Set (LDS) [for research], after the CE and the researcher enter into a Data Use Agreement (DUA).[29] An LDS may not include any direct identifiers of the individual, relatives, employers, or household members and must meet certain requirements.[30] *See HIPAA Notes 6 and 7*.

11. HIPAA allows a valid authorization for use or disclosure of PHI to be combined with any other written permissions for the same or another research study, including:

- Another authorization for research (e.g., authorization to disclose PHI to another entity involved in the research);
- A consent to participate in research (i.e., informed consent required by the Common Rule or the FDA regulations);
- An authorization to create or maintain a research database or repository.[31]

Authorization to use or disclose psychotherapy notes for research may not be combined with other authorizations.[32] A CE that has made signing an authorization a condition of receiving research-related treatment may combine such a conditional authorization with an unconditioned authorization, but must clearly differentiate between the conditioned and unconditioned research components and provide an opportunity for individuals to opt-in to the unconditioned component.

12. A CE may use or disclose PHI without authorization if the use or disclosure is required by state law.[33] A CE may also use or disclose PHI without authorization for public health activities, including disclosure to a public health authority that is authorized by law to collect or receive the PHI for the purpose of preventing or controlling disease, injury, or disability. Public health activities may include: reporting birth or death; public health surveillance; investigations and interventions; or activities at the direction of a public health authority.[34] Note that the minimum necessary standard does not apply to permissive disclosures of PHI by a CE that are required by law.[35] A CE also may disclose certain PHI to an employer about an employee in very limited circumstances related to workplace health and safety, to individuals who may have been exposed to a communicable disease, and to the FDA about product safety, effectiveness, and quality under the permitted disclosures for public health activities.[36]

13. A HIPAA authorization may permit future research[37] if the authorization adequately describes the future research such that it would be reasonable for the individual to expect that his/her PHI could be used or disclosed for that purpose.[38] Note that the 21st Century Cures Act directed the Secretary of HHS to issue guidance on future research authorizations clarifying the circumstances under which such an authorization contains a sufficient description of the intended purpose of the use or disclosure.[39] The Act proposes that such guidance require that authorizations: (1) describe the purpose of the disclosure such that it would be reasonable for the individual to expect that the PHI could be used or disclosed for future research, (2) include a specific expiration date or event or disclaimer that it will remain valid unless revoked, and (3) provide instructions on how to revoke such authorization at any time. [40]

14. HIPAA defines psychotherapy notes as "notes recorded (in any medium) by a healthcare provider who is a mental health professional documenting or analyzing the contents conversations during a

private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record."[41]

15. With limited exceptions, such as use by the originator of the psychotherapy notes for treatment, HIPAA requires an authorization for the use and disclosure of psychotherapy notes. Authorizations for the use and disclosure of psychotherapy notes may not be combined with any other authorization.[42]

16. When a CE, such as a healthcare provider, takes an individual's medical history, including family medical history, and includes the information in the patient's medical record, this information becomes PHI protected by HIPAA.[43] *See also HIPAA Note 2.*

17. The HIPAA Privacy Rule protects the individually identifiable health information about a decedent for 50 years following the date of death of the individual. During this 50-year period, the authorized personal representative of the decedent may exercise the individual's rights under the HIPAA Privacy Rule in the decedent's place. (See relevant state law for guidance on who is considered a "personal representative.") HIPAA also permits a CE to disclose an individual's PHI to a family member or other persons involved in the individual's care or payment for care that is relevant to the person's involvement unless inconsistent with prior preferences expressed by the individual.[44]

18. The HIPAA Privacy Rule protects the individually identifiable health information about a decedent for 50 years following the date of death of the individual. After that time, the information is no longer considered PHI and HIPAA no longer applies regardless of who holds or maintains the information.[45]

19. HIPAA only requires CEs to disclose PHI in two instances: 1) to the individual and 2) to the HHS Secretary to investigate compliance with HIPAA.[46] HIPAA also requires CEs to treat a personal representative as the individual if under applicable law that person has the authority to act on behalf of an individual.[47] A CE must disclose PHI to another person designated by the individual if the individual's request for access directs the CE to transmit the PHI directly to another person. The request must be in writing, signed by the individual, and clearly identify the designated person.[48] This does not apply to psychotherapy notes; such disclosure to a designated person must be done via a valid authorization, not a request for access.[49]

20. An individual may revoke authorization of the use of the individual's PHI at any time, except to the extent a CE has taken action in reliance on the authorization. The revocation must be in writing.[50] In the context of research, the reliance exception permits the continued use and disclosure of PHI already obtained pursuant to a valid authorization to the extent necessary to protect the integrity of the research study.[51]

21. An individual's personal representative is to be treated as if the representative is the individual for purposes of the Privacy Rule, with some exceptions related to the treatment of minors under state law. The personal representative may authorize disclosures, request and receive PHI, and exercise all other rights under HIPAA with respect to the PHI of the individual. HIPAA protects PHI for 50 years after an individual's death, and the personal representative would be permitted to exercise HIPAA rights during those 50 years. *See HIPAA Note 18*. State law generally governs who may serve as a personal representative and related requirements. *See State Law Note 4*.

Common Rule Notes

1. The Common Rule Subpart A governs federally supported human subjects research. Research is "federally supported" when it is conducted, funded, or otherwise subject to specific research regulation by a federal department or agency that has adopted the Common Rule's provisions.[52] Fifteen federal departments and agencies have adopted the Common Rule provisions.[53]

   Research is a systematic investigation designed to develop or contribute to generalizable knowledge.[54] Certain activities are not considered "research" under the Common Rule and excluded from its provisions.

   A human subject is a living individual about whom a researcher conducting research: (1) obtains information or biospecimens through intervention or interaction with the individual and uses, studies, or analyzes the information or biospecimens; or (2) obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.[55] Intervention includes both physical procedures by which information or biospecimens are gathered and manipulations of the participant or the participant's environment performed for research purposes.[56] Interaction includes communication or interpersonal contact between the researcher and participant.[57] Private information includes: (1) information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place; and (2) information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public.[58] Private information and/or a biospecimen is identifiable if the participant's identity is or may be readily ascertained by the researcher or associated with the information and/or biospecimen.[59]

   Each institution engaged in non-exempt research that is conducted or supported by a federal department or agency must provide a written assurance satisfactory to that department or agency head that it will comply with Common Rule requirements.[60] HHS requires that institutions submit a Federalwide Assurance (FWA), which is approved for use by all other federal departments and agencies.[61]

   Note that the requirement for institutions to provide a written assurance technically only applies to those institutions engaged in research supported by an HHS agency that is not exempt from the Common Rule's requirements.[62]

2. An IRB that meets the Common Rule's membership requirements must review all non-exempt research activities as well as exempt research activities for which limited IRB review is a condition of exemption.[63]

   <u>Standard Review Process</u>

   As part of the review process for non-exempt research, the IRB must require that information given to research participants (or their legally authorized representative, when appropriate) as part of informed consent complies with Common Rule requirements and may require that additional information be provided where the IRB determines that it would meaningfully add to the protection of participants' rights and welfare.[64] *See Common Rule Note 6* for additional discussion of informed consent. The IRB must either require documentation of informed consent or waive documentation where permitted.[65]

Expedited Review Process

Certain types of research may be reviewed by an IRB through an expedited review procedure; a list of research categories eligible for expedited review is established by the Secretary of HHS and published as a Notice in the Federal Register.[66] An IRB may use the expedited procedure to review research on this list (if the reviewer determines that it does not involve more than minimal risk),[67] minor changes in previously approved research during the period for which the initial research approval is authorized,[68] and exempt research for which limited IRB review is a condition of exemption.[69]

Certain types of exempt research require limited IRB review as a condition of exemption. This includes storage or maintenance of identifiable private information or identifiable biospecimens for ***potential*** secondary research use and secondary research use of identifiable private information and identifiable biospecimens if the IRB determines after limited review that certain requirements to protect confidentiality and ensure subject's broad consent are in place. *See Common Rule Note 4.*

3. After reviewing proposed research, an IRB has authority to approve, require modifications to, or disapprove any research activity covered by the Common Rule.[70] An IRB may only approve non-exempt research after it determines that the research meets all of the following requirements:

   - Risks to participants are minimized by using procedures consistent with sound research design that do not unnecessarily expose subjects to risk and, whenever appropriate, by using procedures already being performed on the participants for diagnostic or treatment purposes;
   - Risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects and the importance of the knowledge that may reasonably be expected to result;
   - Selection of subjects is equitable;
   - Informed consent will be sought to the extent required and appropriately documented or waived;
   - When appropriate, the research plan makes adequate provisions to monitor data collected to ensure participants' safety; and
   - When appropriate, the research plan makes adequate provisions to protect participants' privacy and to maintain data confidentiality.[71]

   All research requiring approval (whether after standard IRB review or limited IRB review) that includes some or all participants likely to be vulnerable to coercion or undue influence (e.g., children, prisoners, individuals with impaired decision-making capacity, economically or educationally disadvantaged persons) must also include additional safeguards to protect the rights and welfare of these participants.[72]

   Continuing Review

   An IRB must conduct continuing review of the research (at least annually or more frequently as appropriate to the degree of risk).[73] Unless an IRB determines otherwise, continuing review is not required for research eligible for expedited review and research that has reached the data analysis stage and/or has progressed to accessing standard follow-up clinical data. [74]

4. Certain types of human subjects research are exempt from some or all Common Rule requirements unless otherwise subjected to such requirements by a department or agency head.[75] Institutions may choose to have an IRB review all research even if the research is exempt from all Common Rule

requirements.[76] Note, however, that this latitude applies only to research exempt from all Common Rule requirements—research exempt from only some Common Rule requirements must undergo "limited" IRB review (see below). The HHS Office for Human Research Protections (OHRP) has issued guidance instructing institutions to have a "clear policy" that sets forth who shall determine whether research falls within an exempt category and noting that investigators "should not" have the authority to make an independent determination that research is exempt.[77] The 2017 Final Rule does not formalize this requirement, and the OHRP guidance has not been updated since the rulemaking process began; as such, OHRP's position may change in light of the Final Rule's provisions.

There are two categories of exempt research—the first includes types of research that are not subject to any Common Rule requirements whereas the second includes types of research that are subject to only some Common Rule requirements.

Research not subject to any Common Rule requirements includes secondary research use of identifiable private information or identifiable biospecimens when certain privacy protections are in place, including when HIPAA or the Privacy Act of 1974 protect use of the information against improper disclosure. *For additional discussion, see HIPAA Note 9.* Note that information that is linked with a code derived from identifying information or related to information about the individual is not considered to be individually identifiable under the Common Rule.[78] *See also Common Rule Note 1.* Such information would still be considered individually identifiable under HIPAA and may be subject to HIPAA requirements, depending on the source of the information.

Research subject to some Common Rule requirements includes storage of identifiable private information or identifiable biospecimens for ***potential*** secondary research use as well as secondary use of identifiable private information or identifiable biospecimens where broad consent has been obtained from the subject and the IRB conducts limited review to determine that relevant requirements are met.

5. Beginning on January 20, 2020,[79] all institutions engaged in cooperative research must rely on a single IRB for study approval, with limited exceptions; the relevant federal department or agency will identify the reviewing IRB or approve it after its proposal by the lead institution.[80] Where a cooperative research project is not subject to the cooperative IRB requirement, participating institutions may enter into a joint review arrangement, rely on the review of another IRB, or make similar arrangements to avoid effort duplication.[81]

   The NIH released a Final Policy on the use of a single IRB for multisite research in June 2016.[82] For all competing grant applications with receipt dates on or after May 25, 2017, all domestic sites of NIH-funded multisite studies where each site will conduct the same protocol involving non-exempt human subjects research are expected to rely on a single IRB of record that has been selected to carry out the Common Rule's IRB review requirements.[83] Participating sites are responsible for meeting all other regulatory obligations (e.g., obtaining informed consent, reporting study problems, etc.).[84]

6. As a condition of approving non-exempt research protocols, IRBs must determine that informed consent will be sought from each prospective participant or his/her legally authorized representative in accordance with relevant requirements.[85] There are six general requirements governing the process by which informed consent may be obtained (e.g., information given to the

participant must be in language he/she can understand[86]).[87] As part of the informed consent process, the potential research participant must be provided with nine specific pieces of information about the research;[88] where appropriate and relevant, up to nine additional specific pieces of information about the research must also be included.[89] An IRB may approve a consent procedure that does not include (or that alters) some or all of these elements or may waive the informed consent requirement entirely.[90] In order to waive or alter this requirement, the IRB must determine that the research:

- Is to be conducted by or subject to the approval of state or local government officials; is designed to study, evaluate, or otherwise examine public benefit or service programs and/or related inquires; and could not be practicably carried out without the waiver or alteration,[91] or
- Involves no more than minimal risk to the subjects; could not practicably be carried out without the requested waiver or alteration; and, where applicable, could not be practicably carried out without using identifiable private information or identifiable biospecimens.[92] In addition, the IRB must determine that the waiver or alteration would not adversely affect the subjects' rights and welfare, and, wherever appropriate, the participants will be provided with additional pertinent information after participation.

Informed consent must be documented on a written form approved by the IRB and signed by the participant (or his/her legally authorized representative)[93] and a copy of the form must be provided to the signatory.[94] The IRB may waive the requirement to obtain a signed consent form for some or all participants in certain circumstances.[95]

Most exempt research is not required to meet the informed consent requirements. *See Common Rule Note 4.* Certain secondary use of identifiable biospecimens and identifiable private information must meet broad consent requirements. Because a secondary use is a use other than that for which the biospecimen or private information was originally collected, researchers may seek a participant's consent to future unspecified research during the initial informed-consent process. Where participants give such "broad consent," additional informed consent would not be required for the same or another researcher to use the information or biospecimens collected during the original research study. Broad consent incorporates some parts of the specific informed consent process, such as rules governing how consent can be obtained[96] and requirements for information that must be provided to the subject,[97] and includes requirements for provision of information specific to secondary use.[98]

These provisions align with existing HIPAA provisions permitting authorizations for future unspecified research use. *For additional discussion, see HIPAA Note 13*.

7. To the extent that consent is required under Common Rule Subpart A, an IRB may only approve research involving children where adequate provisions are made to solicit the permission of each child subject's parent or guardian.[99] Where the research involves no greater than minimal risk[100] or presents the prospect of direct benefit to the individual subject,[101] the IRB may determine that the permission of only one parent is sufficient for research to be conducted.[102]

   Note that Common Rule Subpart D governs research involving children as subjects that is being conducted or supported by the Department of Health and Human Services.[103] A child is any person who has not attained legal age to consent to the treatments or procedures involved in the

research—legal age for these purposes is determined under the applicable law of the jurisdiction in which the research will be conducted.[104] *For additional discussion, see State Law Note 3*.

8. Where the IRB has determined that the children involved in the research are capable of providing assent, the IRB may only approve research where adequate provisions are made for soliciting the children's assent.[105] This determination may be made for all children to be involved in research under a particular protocol, or for each child, as deemed appropriate by the IRB.[106] The IRB may waive the assent requirement under the same circumstances in which consent may be waived under Subpart A.[107]

9. The Common Rule requires that, as part of the informed consent process, a researcher informs the potential participant of the consequences of a decision to withdraw from the research and procedures for orderly termination of participation.[108] With respect to broad consent (*see Common Rule Note 6*), researchers should inform subjects that information stripped of its identifiers may not be traceable and thus consent for its future use or distribution would not be possible.[109] However, to the extent the researcher commits to permitting a subject to discontinue use of the subject's identifiable private information or identifiable biospecimens, HHS expects that the investigator will honor that commitment by not removing identifiers.[110] Note that these are not formal requirements but originate from the preamble to the 2017 Final Rule—these are thus not enforceable requirements but are dispositive of the issue (*see Appendix B for discussion of ambiguity related to "soft law"*). Note that OHRP guidance released prior to the 2017 Final Rule interpreted the Common Rule to allow investigators to retain and analyze already-collected data relating to any subject who has chosen to withdraw or whose participation has been terminated by the researcher, if the analysis of this data falls within the scope of the analysis described in the IRB-approved protocol.[111] This guidance is still publicly available but may be revised in the future to harmonize with and formalize the discussion in the 2017 preamble.

10. Any federally supported research involving identifiable private information about a human subject is subject to the Common Rule unless specifically exempted. *See also Common Rule Note 1*. Information that is not identifiable private information or identifiable biospecimens or is not information or biospecimens obtained directly by the researcher from the individual is not subject to the Common Rule (i.e., it is not considered part of human subject research).

Part 2 Notes

1. Part 2 protects drug and/or alcohol abuse information, whether or not recorded, that is obtained by a federally assisted drug and/or alcohol abuse program for purposes of treating, diagnosing, or referring for treatment of a substance use disorder and that would identify a patient directly, by reference to other publicly available information, or through verification of identity by another person as having or having had a substance use disorder.[112]

   A patient is any individual who has applied for or been given diagnosis, treatment, or referral for treatment for a substance use disorder at a Part 2 program.[113] Substance use disorder is defined as a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems.[114]

2. Part 2 protects any information, whether or not recorded, obtained by a Part 2 program for the purpose of treating a substance use disorder that would directly or indirectly identify a patient as having or having had a substance use disorder.[115] Part 2 restrictions on disclosure apply to third-

party payers with regard to records disclosed to them by Part 2 programs, to entities with direct administrative control over Part 2 programs with regard to information communicated to them by the program, and to persons or entities that receive patient records directly from a Part 2 program or other lawful holder of patient identifying information that are notified of the restriction on re-disclosure of information in accordance with Part 2 requirements.[116]

3. A consent form may authorize disclosure of Part 2 patient information to different recipients for different purposes (i.e., a multi-party consent form), though must specify the kind and amount of information that can be disclosed to each of the named recipients.[117] Disclosure of Part 2 patient identifying information without written consent is permitted for limited purposes, including by the program or other lawful holder of Part 2 data for purposes of conducting scientific research or if the Part 2 program director determines that the information recipient meets one or both of the following requirements, as applicable:

   a. Is a HIPAA Regulated Entity and has obtained patient authorization or a HIPAA-compliant authorization waiver or alteration; and/or

   b. Is subject to the Common Rule and provides documentation that the recipient is in compliance with the Common Rule or is conducting research exempt from the Common Rule.[118]

   Further, scientific researchers using data obtained from a Part 2 program may use the data in research reports, if the data is in aggregate form and all patient identifying information has been rendered non-identifiable.[119]

4. Most disclosures of Part 2 patient identifying information require the patient's written consent—this includes disclosures for most treatment, payment, and healthcare operations activities. Part 2 programs may disclose patient identifying information with patient consent, which requires a validly executed consent form.[120]

   Part 2 does not apply to certain disclosures of substance abuse information, including communications of information between a Part 2 program and a qualified service organization (QSO) where the information is needed by the QSO to provide services to the program.[121] A QSO is a person who provides services to a Part 2 program (e.g., data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting, or other professional services) and who has entered into a Qualified Service Organization Agreement (QSOA) with the program.[122] A QSOA is a written agreement under which the QSO acknowledges that in receiving, storing, processing, or otherwise dealing with any patient records from the program, it is fully bound by Part 2 regulations and, if necessary, it will resist any efforts in judicial proceedings to obtain access to patient records except as permitted by Part 2.[123]

5. Part 2 programs and any other lawful holder of patient identifying information must have policies and procedures in place to protect against unauthorized uses and disclosures of information as well as any reasonably anticipated threats or hazards to the security of patient identifying information.[124] These policies must address transfer/transmission, removal, destruction, maintenance, use, and access with respect to paper and electronic records, as well as information de-identification and creation and receipt of electronic information.[125]

6. Researchers using patient identifying information obtained from a Part 2 program may request linkages to data sets from a data repository holding patient identifying information if the request is

reviewed and approved by an IRB registered with HHS.[126] After providing a researcher with linked data, the data repository must destroy or delete the linked data from its records to render the information non-retrievable.[127]

7. A Part 2 program is subject to the Part 2 regulations; however, a Part 2 program is generally also a Covered Entity under HIPAA. A Part 2 program is a health care provider but is not a CE if it does not conduct any HIPAA-covered transaction electronically (e.g., billing). When a Part 2 program is a CE, it must comply with HIPAA as well as Part 2 requirements. To the extent that a provision of the Part 2 regulations conflicts with the provisions of HIPAA, Part 2 (as the more protective regulation) would apply. However, where provisions in Part 2 and HIPAA are complementary or do not conflict, a Part 2 program that is also a CE must follow both sets of requirements.

GINA Notes

1. Genetic information is defined as information (other than information about sex or age) about:

   - An individual's genetic tests;[128]
   - The individual's family members' genetic tests; and
   - The manifestation of a disease or disorder in the individual's family members.[129]

   GINA Title I governs health plans and health insurance issuers but does not apply to life insurance plans, long-term care plan issuers, or disability insurers. Title I prohibits health plans and health insurance issuers from using genetic information to make eligibility, coverage, underwriting, or premium-setting decisions about covered individuals.[130] Generally, health plans and issuers may not request or require that beneficiaries undergo genetic testing or provide genetic information, with limited exceptions.[131]

   GINA Title II prohibits public and private employers[132] from using genetic information to discriminate against employees or applicants and generally prohibits employers from acquiring employee or applicant genetic information, subject to exceptions that are limited to legitimate business purposes.[133]

2. GINA Title I prohibits covered health plans and insurers from requesting or requiring that beneficiaries undergo genetic testing or provide genetic information, except:

   - For purposes of determining the medical appropriateness of covered items and services;
   - To request that an individual voluntarily provide genetic information for research purposes, if certain requirements are met; and
   - When the plan obtains genetic information ancillary to the requesting, requiring, or purchasing of other information.[134]

   GINA Title II prohibits employers from acquiring genetic information except in six limited circumstances, which are:

   - Inadvertent acquisition;
   - Obtained as part of health or genetic services offered by the employer on a voluntary basis (if certain specific requirements are met);

- Acquired as part of the certification process for Family and Medical Leave Act (FMLA) leave where an employee is asking for leave to take care of a family member with a serious health condition;
- Acquired through commercially and publicly available documents if the employer is not searching those sources with the intent of finding genetic information or accessing sources from which they are likely to acquire genetic information;
- From a genetic monitoring program that monitors biological effects of toxic substances in the workplace where the monitoring is required by law or, in very specific situations, where the program is voluntary; and
- Where employers engage in DNA testing for law enforcement purposes as with a forensic lab or for purposes of human remains identification, acquisition of genetic information is permitted for use in analyzing DNA markers for quality control to detect sample contamination.[135]
- Where employers have legally acquired an employee's genetic information, the information must be kept confidential and in a medical record separate from the employee's personnel file.[136]

State Law Notes

1. HIPAA sets a federal floor for patient privacy and security but does not preempt more protective state laws.[137] This means that in addition to complying with applicable federal law, providers, plans, and researchers must comply with any state laws that are more protective of patients' rights, as well as any state laws governing data, patients, or entities not regulated by existing federal law. States typically provide enhanced protection for sensitive information (e.g., HIV/AIDS status, mental health information) and vulnerable populations (e.g., minors, legally incompetent adults). States also generally have laws governing state-based registries, compulsory health information reporting (e.g., communicable diseases, vital statistics), health insurers, public health entities, and provider licensure—all of which may contain requirements related to data sharing, confidentiality, and patient consent.

2. States may have laws that provide greater protection for mental health information by preventing its disclosure unless consent is given, even where the disclosure would be allowed for physical health information. State laws may also require certain disclosures that federal law does not require, such as disclosures for state oversight of the mental health system or disclosure of patient information to state authorities to prevent harm to the individual or others.

3. States define the age of majority under state law, meaning the age at which one is no longer a minor. HIPAA defers to the state definition, so that when a person is a minor under state law, that person is also a minor for purposes of HIPAA.[138] In almost all states and the District of Columbia, the age of majority for consenting to medical treatment is 18 (the exception is Alabama, where the age of majority is 19).[139] However, states may also have other relevant laws that affect consent for treatment or research, including those addressing when a minor may consent to treatment or information disclosure and those defining parental and/or guardianship relationships and rights.

4. States generally govern who may serve as an individual's personal representative for various purposes (e.g., medical decision-making). States also set forth requirements for the process by which an individual may appoint (or have appointed on his/her behalf) a personal representative. This applies in the context of minors (*see State Law Note 3*), those declared legally incompetent, the deceased, and (in some states) other circumstances.

REFERENCES

[1] 45 C.F.R. § 160.103 (2017).

[2] 45 C.F.R. § 160.103 (2017).

[3] 45 C.F.R. § 160.103 (2017).

[4] 45 C.F.R. Part 164, §§ 302-318 (2017).

[5] 45 C.F.R. § 160.103 at "Protected health information" at ¶ (2)(iii) (2017).

[6] See, e.g., U.S. Department of Health and Human Services Office for Civil Rights (OCR). HIPAA Privacy and Security and Workplace Wellness Programs – QI: Do the HIPAA Rules apply to workplace wellness programs? (*last reviewed* April 20, 2015). *Available at*: https://www.hhs.gov/hipaa/for-professionals/privacy/workplace-wellness/index.html

[7] 45 C.F.R. § 164.103 (2017).

[8] 45 C.F.R. Part 164, §§ 103, 105 (2017).

[9] 45 C.F.R. § 160.103 (2017).

[10] 45 C.F.R. § 164.504(e) (2017). For example BAA language, see OCR. Business Associate Contracts: Sample Business Associate Agreement Provisions (2013). *Available at:* http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

[11] *See, e.g.*, 45 C.F.R. Part 164, §§ 502(a)(3) (2017) and 302 (2017).

[12] 45 C.F.R. § 164.514(e)(4) (2017).

[13] 45 C.F.R. § 164.514(e)(2) (2017).

[14] 45 C.F.R Part 160, § 103 (2017) and Part 164, §§ 302,.400, and 500(a) (2017).

[15] 45 C.F.R. § 164.514(b)(2)(i) (2017).

[16] 45 C.F.R. § 164.514(b)(1) (2017).

[17] 45 C.F.R. § 164.501 (2017).

[18] 45 C.F.R. § 164.508(b) (2017).

[19] 45 C.F.R. § 164.508(b), (c) (2017).

[20] 45 C.F.R. § 164.502(b)(ii), (iii). (2017).

[21] 45 C.F.R. Part 164 §§ 502(d) and 514(a) – (c) (2017).

[22] 45 C.F.R. § 164.512(i)(1)(i) (2017).

[23] 45 C.F.R. § 164.512(i)(2) (2017).

[24] 45 C.F.R. § 164.512(i)(2) (2017).

[25] 45 C.F.R. § 164.512(i)(1)(ii) (2017).

[26] 45 C.F.R. § 164.512(i)(1)(ii) (2017).

[27] 45 C.F.R. § 164.512(i)(1)(iii) (2017).

[28] 45 C.F.R. § 164.512(i)(1)(iii) (2017).

[29] 45 C.F.R. § 164.514(e) (2017).

[30] 45 C.F.R. § 164.514(e) (2017).

[31] 45 C.F.R. § 164.508(b)(3) (2017).

[32] 45 C.F.R. § 164.508(b)(3) (2017).

[33] 45 C.F.R. § 164.512(a) (2017).

[34] 45 C.F.R. § 164.512(b)(i), (ii) (2017).

[35] 45 C.F.R. § 164.502(b)(v) (2017).

[36] 45 C.F.R. § 164.512(b) (2017).

[37] 45 C.F.R. § 164.508(c)(1)(v) (2017).

[38] OCR. Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 at 5612 (2013).

[39] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, 1080-81, § 2063(b) (*codified at* 42 U.S.C. 1320d-2) (2016).

[40] 21st Century Cures Act, § 2063(b)(1) (*codified at* 42 U.S.C. 1320d-2) (2016).

[41] 45 C.F.R. § 164.501 (2017).

[42] 45 C.F.R. § 164.508(a)(3)(i,ii) (2017).

[43] *See also*, OCR. Frequently Asked Questions about Family Medical History Information (January 12, 2009). *Available at*: http://www.hhs.gov/sites/default/files/familyhealthhistoryfaqs.pdf

[44] 45 C.F.R. § 164.510(b)(5) (2017) .

[45] 45 C.F.R. § 160.103 at "Protected health information" ¶ (2)(iv) (2017).

[46] 45 C.F.R. § 164.502(a)(2) (2017).

[47] 45 C.F.R. § 164.502(g)(1), (2) (2017).

[48] 45 C.F.R. § 164.524(c)(3)(ii) (2017).

[49] 45 C.F.R. § 164.524(a)(1)(i) (2017).

[50] 45 C.F.R. § 164.508(b)(5) (2017).

[51] *See* U.S. Department of Health and Human Services Office for Human Research Protections (OHRP). Withdrawal of Subjects from Research Guidance (2010). *Available at:* https://www.hhs.gov/ohrp/regulations-and-policy/guidance/guidance-on-withdrawal-of-subject/index.html

[52] Common Rule Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (January 19, 2017) (to be codified in multiple titles of the C.F.R.), at 7259 (to be codified at 45 C.F.R. § 46.101(a))

[53] These are: the Departments of Agriculture, Energy, Commerce, Housing and Urban Development, Justice, Defense, Education, Veterans Affairs, Health and Human Services, and Transportation; and the National Aeronautics and Space Administration, Consumer Product Safety Commission, Agency for International

Development, Environmental Protection Agency, and National Science Foundation (*see, e.g.* OHRP. Federal Policy for the Protection of Human Subjects ("Common Rule") (*last reviewed* March 18, 2016). *Available at*: http://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html)). Note that three other departments and agencies comply with the Common Rule's provisions but have not issued the Common Rule in regulation—these are: the Central Intelligence Agency, the Department of Homeland Security, and the Social Security Administration.

[54] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(l)).

[55] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)(i)).

[56] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(2)).

[57] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(3)).

[58] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(4)).

[59] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).

[60] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.103(a)).

[61] OHRP. Assurance Process FAQs: What Assurance of Compliance Process for Human Subject Protection Is Accepted by the Office for Human Research Protections (OHRP) and Other Federal agencies? *Available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/assurance-process/index.html (last visited September 19, 2017).

[62] *See generally*, OHRP. Federalwide Assurance (FWA) for the Protection of Human Subjects: Applicability (*last updated* July 31, 2017). *Available at*: https://www.hhs.gov/ohrp/register-irbs-and-obtain-fwas/fwas/fwa-protection-of-human-subjecct/index.html

[63] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a))

[64] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a)).

[65] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(c)).

[66] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(a)).

[67] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(b)(1)(i))

[68] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(b)(1)(ii))

[69] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(b)(1)(iii))

[70] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a)).

[71] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(1)-(7)).

[72] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(b)).

[73] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.109(e)).

[74] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(f)(1)).

[75] 45 C.F.R. § 46.101(b) (2017).

[76] OHRP. Exempt Research and Research That May Undergo Expedited Review, [Number 95-02], (1995) *Available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/exempt-research-and-research-expedited-review/index.html

[77] OHRP. Exempt Research and Research That May Undergo Expedited Review, [Number 95-02], (1995) *Available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/exempt-research-and-research-expedited-review/index.html

[78] *See, e.g.* OHRP. Guidance: Coded Private Information or Specimens Use in Research (2008). *Available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html

[79] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(2)).

[80] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(1)).

[81] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(c)).

[82] U.S. Department of Health and Human Services National Institutes of Health (NIH). Final Policy on the Use of a Single Institutional Review Board for Multi-Site Research [Notice Number NOT-OD-16-094] (2016). *Available at*: https://grants.nih.gov/grants/guide/notice-files/NOT-OD-16-094.html

[83] NIH. Final Policy on the Use of a Single Institutional Review Board for Multi-Site Research at pp. 8–10 (2016).

[84] NIH. Final Policy on the Use of a Single Institutional Review Board for Multi-Site Research at p. 9 (2016).

[85] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(4)).

[86] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.116(a)(3)).

[87] 82 Fed. Reg. 7149 at 7265-66 (to be codified at 45 C.F.R. § 46.116(a)(2)-(6)).

[88] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(b))

[89] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)).

[90] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(e)(1)-(2), (f)(1)-(2)).

[91] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(e)(3)).

[92] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(f)(3)).

[93] Note that the provisions of the Common Rule apply to the research participant's legally authorized representative (LAR) to the same extent they would apply directly to the research participant.

[94] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.117(a)).

[95] 82 Fed. Reg. 7149 at 7268 (to be codified at 45 C.F.R. § 46.117(c)(1)).

[96] 82 Fed. Reg. 7149 at 7265-66 (to be codified at 45 C.F.R. § 46.116(a)(1)-(4), (6)).

[97] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(d)(1)).

[98] 82 Fed. Reg. 7149 at 7266-67 (to be codified at 45 C.F.R. § 46.116(d)(2)-(7)).

[99] 45 C.F.R. § 46.408(b) (2017).

[100] *See* 45 C.F.R. § 46.404 (2017).

[101] *See* 45 C.F.R. § 46.405 (2017).

[102] 45 C.F.R. § 46.408(b) (2017).

[103] 45 C.F.R. § 46.401(a) (2017).

[104] 45 C.F.R. § 46.402(a) (2017).

[105] 45 C.F.R. § 46.408(a) (2017).

[106] 45 C.F.R. § 46.408(a) (2017).

[107] 45 C.F.R. § 46.408(a) (2017).

[108] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(4)).

[109] 82 Fed. Reg. 7149 at 7221.

[110] 82 Fed. Reg. 7149 at 7221.

[111] OHRP. Withdrawal of Subjects from Research Guidance (2010). *Available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/guidance-on-withdrawal-of-subject/index.html; *see also* 82 Fed. Reg. at 7264 (to be codified at 45 C.F.R. § 46.109(f)(1)(iii)(A)).

[112] 42 C.F.R. § 2.12(a)(1) (2017).

[113] 42 C.F.R. § 2.11 at "Patient" (2017).

[114] 42 C.F.R. § 2.11at "Substance use disorder" (2017).

[115] 42 C.F.R. § 2.12(a)(1) (2017).

[116] 42 C.F.R. § 2.12(d)(2)(i) (2017).

[117] U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration (SAMHSA). Substance Abuse Confidentiality Regulations: Applying the Substance Abuse Confidentiality Regulations Question 4 (2011). *Available at*: https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs

[118] 42 C.F.R. § 2.52(a) (2017).

[119] 42 C.F.R. § 2.52(b)(3) (2017).

[120] 42 C.F.R. § 2.33 (2017).

[121] 42 C.F.R. § 2.12(c)(4) (2017).

[122] 42 C.F.R. § 2.11 at "Qualified service organization" (2017).

[123] 42 C.F.R. § 2.11 at "Qualified service organization" ¶ (2)(2017).

[124] 42 C.F.R. § 2.16(a) (2017).

[125] 42 C.F.R. § 2.16(a)(1)-(2) (2017).

[126] 42 C.F.R. § 2.52(c)(1)(i) (2017).

[127] 42 C.F.R. § 2.52(c)(2)(i) (2017).

[128] Note that a genetic test is defined as "analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes" (*see, e.g.* GINA Title I, § 101(d) (2008)).

[129] GINA Title I, § 101(d) (2008).

[130] *See, e.g.* GINA Title I, § 102(a)(4) (2008).

[131] *See, e.g.* GINA Title I, § 101(b) (2008).

[132] GINA Title II, § 207 (2008).

[133] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. 2000ff-1(a) (2008).

[134] *See, e.g.* GINA Title I, § 101(b) (2008).

[135] *See, e.g.* GINA Title II, § 202(b), codified at 42 U.S.C. 2000ff-1(b) (2008).

[136] GINA Title II, § 206(a), 42 U.S.C. 2000ff-5(a).

[137] *See* 45 C.F.R. 160.201, *et seq*. (2017).

[138] *See* 45 C.F.R. 164.502(g) (2017).

[139] Campbell, AT. Appendix B, State Regulation of Medical Research with Children and Adolescents: An Overview and Analysis at Table B.2: Age of Majority. In Field MJ, Behrman RE (eds.), Ethical Conduct of Clinical Research Involving Children. Institute of Medicine Committee on Clinical Research Involving Children. Washington (DC): National Academies Press (2004). *Available at*: http://www.ncbi.nlm.nih.gov/books/NBK25556/.

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX A:

STATUTES AND REGULATIONS RELEVANT TO PCOR

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Appendix A

Statutes and Regulations Relevant to PCOR

This appendix includes summaries of the statutes and regulations discussed throughout the Architecture relevant to PCOR.

INTRODUCTION

Health care is one of the most highly regulated industries. The foundation of the U.S. healthcare system is patient and public health information that primarily supports patient and provider decision-making, payment, and research. Health information, even more so than financial information, is considered to be highly sensitive and protected by a vast array of federal and state statutes and regulations, organizational policies and procedures, and ethical considerations.

At the federal level, statutes and regulations may be organized by their primary focus. For example, some statutes and regulations are specific to the types of health information content they govern; others are specific to certain activities, such as research; and still others are specific to the settings of care where care is delivered.

Content-Specific Statutes and Regulations: These statutes and regulations govern certain specific types of health information that may be used to support PCOR and CER, assuming the relevant requirements are met. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations govern protected health information. Part 2 of Title 42 of the Code of Federal Regulations (Part 2) governs substance abuse information held by federally assisted programs, and the Genetic Information Nondiscrimination Act of 2008 (GINA) governs genetic information used for various purposes. These statutes and regulations are both permissive and prohibitive in nature, describing to whom and for what purposes these types of information may or may not be disclosed as well as any other associated requirements. Other content-specific statutes and regulations include: the Patient Safety and Quality Improvement Act (PSQIA—patient safety work product); the Privacy Act of 1974 (individually identifiable information held by a federal agency); and the [federal] Freedom of Information Act (FOIA).

Research-Specific Statutes and Regulations: These statutes and regulations govern the health-related research enterprise, including PCOR and CER if certain requirements are met. For example, the Common Rule governs federally supported human subjects research. Similar to the Common Rule, FDA regulations govern experiments on human subjects involving products, drugs, or devices subject to FDA review and/or approval.

Setting-Specific Statutes and Regulations: These statutes and regulations govern health information that is collected, used, and/or disclosed by certain settings of care. For example, Title 38 of the U.S. Code governs health care delivered to Veterans, Section 330 of the Public Health Services Act (PHSA) governs health care delivered in community health centers, and the Family Educational Rights and Privacy Act (FERPA) governs health information included in student education records.

Table 1: Federal Laws—Primary Focus

	Content-Specific	Research-Specific	Setting-Specific
Common Rule Subparts A–E		X	
FDA Research Regulations		X	
Family Educational Rights and Privacy Act (FERPA)			X
Genetic Information Nondiscrimination Act (GINA)	X		
HIPAA Administrative Regulations	X		
42 C.F.R. Part 2	X		
Public Health Services Act § 330 Grantees (Community Health Centers)			X
Patient Safety and Quality Information Act (PSQIA)	X		
Privacy Act of 1974/Freedom of Information Act (FOIA)	X		
Title X Providers (Family Planning Clinics)			X
Veteran's Administration Confidentiality Regulations (Title 38 USC § 7338)			X

At the state level, statutes and regulations that relate to health information vary greatly. For purposes of this project, the most relevant state statutes and regulations typically govern the privacy of health information for specific populations and specific types of information (e.g., individuals with HIV/AIDs, individuals with mental health conditions, and minors). For these populations, state laws are typically more stringent than HIPAA requirements and thus must be followed as they relate to the collection, use, and disclosure of health information for these individuals.

OVERVIEW OF FEDERAL LAWS: CONTENT-SPECIFIC

Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1]

Purpose. HIPAA and its enabling regulations (the HIPAA Rules) set a national framework for the management, transmission, and disclosure of health information. At HIPAA's core lies an effort to balance individuals' right to control access by third parties to information about their health and health care against providers' and payers' need to exchange and manage this information for treatment, payment, and healthcare operations. As a result, HIPAA gives healthcare providers, payers, and clearinghouses considerable flexibility over information management and exchange, if done prudently, while at the same time giving individuals some ability to control information flow.

The U. S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for implementing and enforcing four separate sets of HIPAA regulations:[2]

1. The Privacy Rule, which governs the privacy and confidentiality of individually identifiable health information;[3]
2. The Security Rule, which identifies baseline administrative, physical, and technical safeguards to protect electronic health information;[4]
3. The Enforcement Rule, which sets forth the enforcement system for all the HIPAA Rules;[5] and
4. The Breach Notification Rule, which establishes a notification and reporting protocol in the event of an unauthorized disclosure.[6]

Scope. The HIPAA Rules regulate "protected health information" (PHI). PHI is individually identifiable information that is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that relates to:

1. The provision of care to an individual;
2. An individual's past, present, or future physical or mental health condition; or
3. An individual's payment for care, whether made in the past or present or expected in the future.[7]

Information is individually identifiable when it directly references an individual or could be used to identify the individual.[8] The HIPAA Rules do not govern Covered Entities' employment records or education records subject to FERPA[9]—even if those records contain health information.[10]

The HIPAA Rules apply to health plans, healthcare clearinghouses,[11] and all healthcare providers, regardless of size, that electronically transmit health information in connection with certain transactions[12]—collectively, these are known as "Covered Entities."[13] In addition, the HIPAA Rules apply to Covered Entities' "Business Associates," which are individuals or groups (other than members of the Covered Entity's workforce) that have access to PHI when providing certain services or functions to or on behalf of a Covered Entity.[14] Covered Entities and their Business Associates together are referred to as "Regulated Entities."[15] The HIPAA Rules do not apply to any other types of individuals or organizations.[16]

Information De-Identification

Health information that has been de-identified is not considered to be PHI for purposes of HIPAA applicability.[17] Information can be de-identified under HIPAA in either of two ways:

1. Safe Harbor Method:[18] Information is de-identified under this method when all of 18 direct identifiers are removed (*see* Table 2: Federal Requirements for Consent to Disclose Identifiable Health Information). However, information is not de-identified under this method if the Covered Entity knows that the information (stripped of these 18 identifiers) could still be used, alone or in combination with other information, to identify the individual.
2. Statistical/Expert Method:[19] Under this method, an individual with sufficient knowledge in and experience with statistical and scientific methods and principles for de-identifying information must analyze the information. Information is considered de-identified when the expert individual, after applying these methods and principles, determines that there is very small risk that an anticipated recipient could identify an individual either from the information alone or in combination with other available information.

When information has been de-identified, regardless of the method employed, a Regulated Entity may assign a code or use another means of record identification that allows the information to be re-identified, if certain criteria are met:

1. The code may not be derived from or related to information about the individual;
2. It must be impossible for the code to be translated so as to identify the individual;
3. The Regulated Entity may not use or disclose the code for any purpose; and
4. The Regulated Entity may not disclose the mechanism for re-identification.[20]

Although HIPAA's methods are the only federal standards available for de-identifying information, concerns regarding the potential to re-identify "de-identified" data have arisen due to the increase in data collection from all facets of life, the aggregation and sale of such data, and advances in computer science and machine learning.[21] The subjective nature of the expert determination method and the

susceptibility of information de-identified via the Safe Harbor method to the "mosaic effect" (whereby data from multiple sources can be pieced together to obtain private information) raise concerns about the efficacy of both HIPAA methods for de-identification.

Recognizing these concerns, the Health Information Technology Policy Committee (HITPC) Privacy and Security Workgroup's August 2015 Health Big Data Recommendations included the following recommendations for addressing the risk of re-identification:

1. Enable the Office for Civil Rights (OCR—the HHS office that enforces the HIPAA Rules) to take an active role in managing the HIPAA de-identification standards, including methodology review, recommending updates to methodologies and policies, and obtaining the assistance of third-party experts (e.g., the National Institute of Standards and Technology);
2. Develop programs to evaluate the ability of statistical methodologies to reduce re-identification risks to "very low;" and
3. Encourage the use of proven de-identification methods by having OCR assign Safe Harbor status to methods that prove effective within specific contexts.[22]

The Privacy Rule

Purpose. The HIPAA Privacy Rule's dual purpose is to regulate the use and disclosure of PHI by Regulated Entities and to establish an individual's rights with respect to their own PHI held by a Covered Entity. Although the Privacy Rule establishes important safeguards for health information privacy, the Rule is fundamentally and intentionally designed to create a privacy "operating system" for the core of the American healthcare system. This approach to health information management protects information while still enabling stakeholders to engage in the types of information exchange vital to health care and the overall operation of the healthcare system. In particular, the Privacy Rule gives significant latitude to exchange information among providers of clinical care and between providers and insurers for essential health care functions. The Privacy Rule was initially published in 2000 and then later updated in 2002 and 2013.

Scope. The Privacy Rule regulates all PHI held or transmitted by a Covered Entity or its Business Associate, in any form or medium (electronic, paper, or oral).[23] The Rule governs when and how PHI can be disclosed, which can be grouped into four broad categories:

1. Required Disclosures: a Regulated Entity **must** disclose PHI to the individual subject of the PHI (or a designated representative) upon his/her request for access and to HHS for enforcement purposes and for HIPAA-related compliance investigations;[24]
2. Prohibited Disclosures: a Regulated Entity may not disclose PHI for certain purposes (e.g., most sales of PHI[25]) and may only disclose certain types of PHI (e.g., psychotherapy notes,[26] minors' PHI[27]) in limited circumstances;
3. Permissive Disclosures (*see* Table 4: List of Permissive Exceptions Available to Covered Entities): a Covered Entity **may** disclose PHI **without first obtaining the individual subject of the information's authorization** for a variety of purposes (though some of these purposes require that, where practicable, the individual be given an informal opportunity to object to the disclosure[28]);[29]
4. Authorized Disclosures: Any disclosures not required, permitted, or prohibited by the Rule require written authorization from the individual who is the subject of the information.[30]

The Privacy Rule requires written authorization for any disclosure except those required or permitted by the Rule. The permissive disclosure exceptions to the authorization requirement are critical to enable proper functioning of the healthcare system. For example, the exception permitting disclosure without

authorization for treatment purposes allows a health center to provide a specialist with a patient's entire medical record upon request, enabling the specialist to fully understand the patient's medical condition and provide the most appropriate treatment. To balance Regulated Entities' legitimate needs to exchange PHI with patients' interest in the privacy of their information, the Privacy Rule requires that most disclosures be limited to the "minimum [amount of PHI] necessary" to achieve the purpose for which the information was released or requested.[31] Determining what amount is the "minimum necessary" is at the discretion of the Covered Entity making the disclosure, using professional judgment under the circumstances.[32] The requirement to limit disclosures to the minimum amount necessary does not apply to disclosures without authorization that are required by [state or other] law, made to a provider for treatment purposes, or made to the Secretary for compliance or enforcement purposes nor to disclosures made to the individual subject of the PHI or made pursuant to an individual's authorization.[33]

It is important to underscore the permissive nature of these exceptions—the Covered Entity may, but is not required to, make disclosures without authorization for these specified purposes. If it is the Covered Entity's custom or common practice to first obtain written authorization for some or all otherwise-permitted disclosures, the Covered Entity may choose to maintain that custom or practice. However, such custom or practice is not mandated by the Privacy Rule, nor is there a HIPAA penalty for making use of the permissive exceptions (or declining to do so). While the Privacy Rule gives providers the flexibility to utilize permissive exceptions in accordance with their own customs and preferences (when certain safeguards are employed, such as the minimum necessary standard), there are specific situations in which more restrictive standards apply:

1. A "more stringent"[34] state law prohibits certain disclosures without express authorization (e.g., information related to HIV/AIDS or mental illness);
2. The PHI is a substance abuse treatment record governed by 42 C.F.R. Part 2;
3. The Covered Entity is subject to more restrictive federal standards governing privacy and confidentiality (e.g., Title X grantees and Community Health Centers); or
4. The information is held in a record covered by FERPA.

The Security Rule

Purpose. The Security Rule requires Regulated Entities to establish and maintain reasonable and appropriate administrative, physical, technical, and organizational safeguards for protecting PHI that the Regulated Entity creates, receives, maintains, or transmits in electronic form (known as e-PHI).[35]

Scope. Regulated Entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
3. Protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted or required by the Privacy Rule; and
4. Ensure its workforce complies with the Security Rule.[36]

The Security Rule provides Regulated Entities considerable flexibility in meeting these requirements. Entities may use any security measure that allows them to reasonably and appropriately implement the Rule's standards and implementation specifications.[37] However, when deciding which security measures to use, an entity must always account for several factors, including: its size, complexity, and capabilities

(including technical infrastructure, hardware, and software capabilities); the costs of security measures; and the probability and criticality of potential risks to e-PHI.[38]

The Enforcement Rule

Purpose. The Enforcement Rule governs the HIPAA enforcement process, establishing protocols for compliance investigations, hearings, and penalties for violations.

Scope. The Enforcement Rule does not give individuals the right to sue Regulated Entities whom they believe have violated the provisions of the HIPAA Rules.[39] Instead, the Rule allows aggrieved individuals to file a complaint with OCR.[40] OCR may investigate complaints, and an investigation is required when a preliminary review of the facts indicates a possible violation due to willful neglect.[41] The Enforcement Rule utilizes a four-tiered penalty structure to correspond to the levels of culpability associated with a HIPAA violation.[42] Regulated Entities that violate the HIPAA Privacy, Security, and Breach Notification Rules may be liable for penalties up to $1.65 million[43] per violation category, per year (subject to annual increase for inflation), depending on their level of culpability.[44]

The Breach Notification Rule

Purpose. The Breach Notification Rule requires Regulated Entities to disclose breaches of unsecured PHI (PHI in any form or medium that has not been rendered "unusable, unreadable, or indecipherable to unauthorized individuals"[45]) to the individuals affected, the HHS Secretary, and, in certain circumstances, the media.

Scope. A breach of unsecured PHI is a use or disclosure that is impermissible under the Privacy Rule and that "compromises the security or privacy of the [PHI]." Any disclosure that is impermissible under the Privacy Rule is presumed to be a breach unless the Regulated Entity conducts a risk assessment that demonstrates a low probability that the PHI was compromised.[46] In the event of a breach, the Regulated Entity must provide notification to the affected individuals that includes a description of the breach and the type of PHI involved and what the Covered Entity is doing to investigate the breach, mitigate losses, and protect against further breaches.[47] The Regulated Entity must also concurrently notify the HHS Secretary of the breach,[48] and in some cases must notify relevant media outlets.[49] The notification requirements are not applicable in certain situations, such as where a disclosure was made in good faith to an otherwise-authorized member of the Regulated Entity's workforce.[50]

42 C.F.R. Part 2 (Substance Abuse Information)[51]

Purpose. Part Two of Title 42 of the Code of Federal Regulations (C.F.R.) governs the confidentiality of substance use disorder patient records obtained by federally assisted programs. These protections exist to ensure that individuals in a substance abuse treatment program are not more vulnerable with respect to their privacy than those who do not seek treatment.[52]

The Part 2 regulations were issued in 1970 and updated in 1987. In 2016, the Substance Abuse and Mental Health Services Administration (SAMHSA) proposed several major modifications to better align the regulations with the current U.S. healthcare system.[53] SAMHSA finalized changes to Part 2 in a Final Rulemaking issued on January 18, 2017.[54] The finalized changes to Part 2 went into effect on March 21, 2017; these changes are reflected in the summary below. In conjunction with publishing the Final Rule, SAMHSA issued a Supplemental Notice of Proposed Rulemaking to propose additional clarifications to the amended Part 2 regulations and seek public comment on these proposals.[55] Future changes may be made to Part 2, and researchers and other stakeholders should continue to monitor the status of Part 2.

Scope. The Part 2 regulations govern the disclosure and use of certain information maintained by "federally assisted" substance use disorder programs.[56] A program includes:

1. Individuals, entities, and identified units in general medical facilities that provide substance use disorder services (i.e., diagnosis, treatment, or referral for treatment) and hold themselves out as providing such services (e.g., advertises services, is certified to provide addiction services—any activity that would lead one to conclude that the individual or entity provides substance use disorder services[57]); and
2. Medical personnel or other staff working within a general medical facility whose primary function is to provide substance use disorder services *and* who are identified as such providers.[58]

A program is "federally assisted" if it is conducted by any federal department or agency (directly or via contract), is carried out under any federal license, certification, registration, or authorization (e.g., Medicare/Medicaid certification, DEA registration to dispense a controlled substance used to treat substance use disorders), or receives any federal financial assistance (e.g., grants, federal tax-exempt status).[59]

There are several situations in which the Part 2 regulations do not apply. Relevant exemptions include:

1. Veteran's Administration (VA): substance use disorder patient information maintained in connection with the VA's provision of services to a veteran with a service-related disability (this information is covered by VA-specific regulations, discussed below);
2. Program Communications: communication of information within a Part 2 program or between a Part 2 program and an entity with direct administrative control over that program,[60] to the extent the information is needed by personnel in connection with providing substance use disorder services;
3. Qualified Service Organizations (QSOs)[61]: communication of information between a Part 2 program and a QSO where the QSO needs the information to provide services to the program; [62] and
4. Vital Statistics: disclosures of information relating to a patient's cause of death in accordance with laws that require death or other vital statistics collection or that permit cause of death inquiries.[63]

Part 2 restricts disclosure of all information, whether recorded or not, obtained by a Part 2 program for purposes of providing substance use disorder services that would identify a patient as having or having had a substance use disorder, either through direct or indirect identification (i.e., by reference to other publicly available information or through verification of such an identification by another person).[64] Part 2 bars most disclosures of that information without written consent by the patient and/or his/her personal representative.[65] This includes disclosing whether an individual is or has been a patient with the program.[66] The restrictions on disclosure also apply to individuals and entities that have received patient records directly from Part 2 programs or from other lawful holders of patient identifying information and who have been properly notified of the prohibition on re-disclosure.[67]

Disclosure of Part 2 patient identifying information without written consent is permitted for limited purposes, including:

1. To medical personnel who need the information to treat a patient during a medical emergency in which the patient's prior informed consent could not be obtained;[68]
2. By the program or other lawful holder of Part 2 data for purposes of conducting scientific research, if the Part 2 program director determines that the information recipient meets one or both of the following requirements, as applicable:

a. Is a HIPAA Regulated Entity and has obtained patient authorization or a HIPAA-compliant authorization waiver or alteration; and/or
b. Is subject to the Common Rule and provides documentation that the recipient is in compliance with the Common Rule or is conducting research exempt from the Common Rule.[69]

3. By scientific researchers using data obtained from a Part 2 program in research reports, if the data is in aggregate form and all patient identifying information has been rendered non-identifiable.[70]
4. To certain specified entities for audit and evaluation activities of the program;[71]
5. To the parent, guardian, or authorized representative of a minor applicant for substance use disorder service of facts relevant to reducing a substantial threat to the life or physical well-being of any individual if the program director determines that the disclosure may reduce such a threat and that the minor lacks capacity to consent to the disclosure;[72] and
6. By the program director about a patient (other than a minor patient or those adjudicated incompetent) who has a medical condition that prevents knowing or effective action on their own behalf for purposes of obtaining payment for services from a third-party payer.[73]

Researchers using patient identifying information obtained from a Part 2 program may request linkages to data sets from a data repository holding patient identifying information if the request is reviewed and approved by an Institutional Review Board (IRB) registered with HHS.[74] After providing a researcher with linked data, the data repository must destroy or delete the linked data from its records to render the information non-retrievable.[75]

Programs may disclose substance use disorder patient information with valid written consent from the patient.[76] There are certain other requirements for consent in special circumstances (e.g., minors, disclosures to central registries, etc.). A valid consent must include nine separate elements (*see* Table 2: Federal Requirements for Consent to Disclose Identifiable Health Information),[77] including identification of the intended recipient of the information. If the intended recipient is an individual, an entity with a treating relationship with the patient, or a third-party payer, the consent must specifically name the recipient.[78] If the recipient is an entity without a treating relationship with the patient (other than a third-party payer), the consent must give the entity's name *and:*

- The name(s) of an individual participant with the entity (e.g., Dr. Smith, Research Scientist at Jones Research Institution);
- The name of an entity participant(s) with a treating provider relationship with the patient (e.g., Southeastern Hospital, member of Eastern HIO); or
- A general designation of an individual or entity participant or class of participants, limited to those with a treating provider relationship with the patient (e.g., all current and future treating providers at Northern Academic Medical Center).[79]

Part 2 programs and any other lawful holder of patient identifying information must have policies and procedures in place to protect against unauthorized uses and disclosures of information as well as any reasonably anticipated threats or hazards to the security of patient identifying information.[80] These policies must address transfer/transmission, removal, destruction, maintenance, use, and access with respect to paper and electronic records, as well as information de-identification and creation and receipt of electronic information.[81]

Genetic Information Nondiscrimination Act of 2008 (GINA)[82]

Purpose. GINA protects individuals'[83] genetic information[84] from being used by employers, health plans, and health insurance issuers in a discriminatory manner. GINA does not apply to life insurance plans, long-term care plan issuers, or disability insurers.

Scope. GINA is comprised of two titles. Title I prohibits health plans and health insurance issuers from using genetic information to make eligibility, coverage, underwriting, or premium-setting decisions about covered individuals.[85] Generally, health plans and issuers may not request or require that beneficiaries undergo genetic testing or provide genetic information.[86] However, health plans may request that beneficiaries voluntarily provide genetic information for research, require genetic information for determining medical appropriateness of covered services, and obtain genetic information incidentally in the course of obtaining other information.[87]

Title II prohibits most employers[88] from using genetic information to discriminate against employees or applicants[89] and generally prohibits employers from acquiring employee's or applicant's genetic information,[90] subject to exceptions that are limited to legitimate business purposes. Title II also governs the confidentiality of lawfully acquired genetic information. Genetic information must be kept confidential and stored in a medical record separate from the employee's personnel file.[91] Genetic information may be disclosed to the employee at his or her written request and without the employee's consent in several other circumstances, including:

1. To an occupational or health researcher; and
2. To a public health organization, if the information concerns a contagious disease that presents an imminent threat of serious harm or death and the employee is informed of the disclosure.[92]

Patient Safety and Quality Improvement Act of 2005 (PSQIA)[93]

Purpose. PSQIA was enacted in response to concerns about patient safety and *To Err is Human: Building a Safer Health System* (a 1999 Institute of Medicine Report) and aims to encourage reporting of adverse events in order to improve patient safety.[94]

Scope. PSQIA protects patient safety work product (PSWP), which includes data, reports, records, memoranda, analyses, or statements that could result in improved patient safety, healthcare quality, or healthcare outcomes.[95] PSQIA established a voluntary reporting program where providers share PSWP with Patient Safety Organizations (PSOs), which aggregate and analyze the information.[96] Identifiable PSWP is subject to privilege and confidentiality requirements, each of which have specific exceptions that permit disclosure under certain circumstances, including:

1. To carry out patient safety activities;
2. If the PSWP is non-identifiable, whether voluntarily disclosed or not;
3. By a provider to the FDA with respect to a product or activity regulated by the FDA;
4. To entities carrying out research, evaluation, or demonstration projects authorized, funded, certified, or otherwise sanctioned by HHS; and
5. For business operations if disclosure is consistent with the goals of patient safety improvement.[97]

Privacy Act of 1974[98] and Freedom of Information Act (FOIA)[99]

Purpose. The Privacy Act protects information about individuals (e.g., patients and practitioners) held or collected by the federal government that can be retrieved by a personal identifier (e.g., name, Social

Security number). FOIA permits disclosure of information contained within a federal agency record, unless the information is exempted from disclosure.

Scope. The Privacy Act allows a federal agency to release individually identifiable information to identified individuals (or to their designees with written consent) or pursuant to one of 12 exemptions for disclosure.[100] These exemptions include disclosure to federal agency employees, the Census Bureau, the National Archives and Records Administration, other government entities for civil and criminal law enforcement purposes, the Comptroller General, Congress or its committees, and a consumer reporting agency. Additional exemptions include disclosures for statistical research, disclosures required by FOIA, disclosures in response to emergency circumstances, and disclosures pursuant to a court order. In addition, research is commonly included as a permitted release under agency systems of records (SORs) that each collecting agency establishes (see Common Rule exemption categories below for further discussion of information in SORs used for research). FOIA requires federal executive agencies to disclose their records to individuals upon request, subject to nine exemptions. These exemptions prevent the disclosure of information that is considered sensitive or of a personal nature, including information about a specific individual contained in personnel or medical files, the disclosure of which would be an "unwarranted invasion of personal privacy."[101] The 21st Century Cures Act explicitly prohibits the use of FOIA to gain access to an individual's biomedical information—if there is even a very small risk that individual biomedical research data could be used to identify an individual, HHS may prevent such data from being publicly disclosed under a FOIA request.

OVERVIEW OF FEDERAL LAWS: RESEARCH-SPECIFIC

Common Rule[102]

Purpose. The Protection of Human Subjects regulations set forth a variety of requirements to ensure that human subjects (i.e., research participants) experience minimal risk to their health, safety, and privacy during and as a result of federally supported research. There are four separate regulations (Subparts A–D), created and adopted by HHS in 1991. Subpart A is known as "the Common Rule" because it has been codified by 15 federal departments/agencies and informally adopted by three federal agencies.

In an effort to modernize the Common Rule and harmonize its provisions with other federal privacy regulations, the Common Rule departments and agencies proposed significant changes to the regulations in a 2015 NPRM.[103] Changes were published in a Final Rule on January 19, 2017, with a January 19, 2018, effective date (and extended and/or suspended effective dates for certain provisions).[104] The summary below reflects the 2017 Final Rule provisions. Future changes may be made to the regulations, and researchers and other stakeholders should continue to monitor the status of the Common Rule.

Scope. **Subpart A** applies to federally supported research involving human participants. Research is federally supported if it is conducted, supported, or otherwise subject to regulation by a federal department or agency.[105] Research (i.e., a systematic investigation designed to develop or contribute to generalizable knowledge)[106] involves human participants when an investigator:

- Obtains information or biospecimens about a living individual through intervention or interaction with the individual and uses, studies, or analyzes the information or biospecimens; or
- Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens about a living individual.[107] Information about behavior where an individual can

reasonably expect that no observation or recording is taking place as well as information provided for specific purposes that the individual can reasonably expect will not be made public is private information.[108] Information and biospecimens are identifiable if the individual's identity is or may be readily ascertained by the investigator or associated with the information or biospecimen.[109] Note that unlike the HIPAA Privacy Rule, the Common Rule does not specify identifiable elements of information, though does require that federal departments and agencies regularly consult with experts to reexamine and, as appropriate, alter the interpretation of identifiability.[110]

The Common Rule specifically excludes some activities from its definition of research; these activities are not subject to any provisions of the Common Rule.[111] For example, public health surveillance activities, including the collection and testing of information or biospecimens, which are conducted, supported, requested, ordered, required, or authorized by a public health authority are not considered "research" for purposes of Common Rule applicability.[112]

The Common Rule also exempts some types of research from its requirements;[113] the Office for Human Research Protections (OHRP, an office within HHS) strongly recommends that an Institutional Review Board (IRB) or administrative review process be utilized to determine whether proposed research is considered exempt.[114] Research meeting any of the following definitions is not subject to any Common Rule requirements:

1. Research that only involves interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[115] or that involves benign behavioral interventions[116] in conjunction with information collection from an adult participant (if the participant prospectively agrees to the intervention and information collection)[117] if:

    a. The researcher records information so that the participant's identity cannot be readily ascertained (directly or through linked identifiers); and/or
    b. Disclosure of a participant's responses outside the research would not reasonably place the participant at risk of criminal or civil liability or be damaging to the participant's financial standing, employability, educational advancement, or reputation.

2. Secondary research use of publicly available identifiable private information or identifiable biospecimens;[118]
3. Secondary research use of identifiable private information or identifiable biospecimens if the researcher records the information so that the subject's identity cannot be readily ascertained (directly or through linked identifiers), does not contact the subject, and will not re-identify the subject;[119]
4. Secondary research use of identifiable private information or identifiable biospecimens (limited to information collection and analysis) if such use is regulated under the HIPAA Privacy Rule for the purposes of "health care operations" or "research," or for "public health activities and purposes";[120]
5. Secondary research use of identifiable private information or identifiable biospecimens conducted by or on behalf of a federal department or agency using government-generated or -collected information obtained for non-research activities and maintained in systems of records (SORs) subject to the Privacy Act of 1974,[121] if certain other requirements are met;[122] and
6. Research and demonstration projects designed to study, evaluate, improve, or examine public benefit or service programs that are conducted, supported by, or subject to approval of a federal department or agency.[123]

The Common Rule also exempts some types of research from most, but not all, of its requirements. Research meeting the following definitions need only meet the requirements specified below:

1. Research that only involves interactions using educational tests, survey procedures, interview procedures, or observation of public behavior[124] or that involves benign behavioral interventions[125] in conjunction with information collection from an adult participant (if the participant prospectively agrees to the intervention and information collection)[126] if an IRB conducts a limited review of the research to determine that, when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data;[127]
2. Storage or maintenance of identifiable private information or identifiable biospecimens for ***potential*** secondary research use if an IRB conducts a limited review and determines that:[128]

    a. Broad consent for such storage, maintenance, and secondary research use is obtained in accordance with relevant requirements;[129]
    b. Broad consent is appropriately documented or waiver of documentation is appropriate;[130] and
    c. If there is a change made in the way the information or biospecimens are stored or maintained for research purposes, there are adequate provisions to protect the privacy of participants and maintain the confidentiality of data;[131] and

3. Secondary research use of identifiable private information and identifiable biospecimens if:[132]

    a. Broad consent for the storage, maintenance, and secondary research use of the identifiable private information or identifiable biospecimens was obtained in accordance with relevant requirements;
    b. Documentation of informed consent or waiver of documentation of consent was obtained in accordance with relevant requirements;
    c. An IRB conducts a limited review and determines that the research to be conducted is within the scope of broad consent and that, when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data; and
    d. The investigator does not include "returning individual research results to participants" as part of the study plan.

Note that research initially approved by an IRB prior to January 19, 2018, that was determined exempt or for which review was waived by a department or agency head[133] must comply with the regulations as published in the 2016 edition of the Code of Federal Regulations.[134] After the 2017 Final Rule goes into effect, institutions still engaged in such research may comply with the updated regulations if appropriate.

Subpart A specifies requirements for every entity involved in the research process, including:

1. Research Institutions. Every institution engaged in non-exempt research must submit a written assurance stating that it will comply with the Common Rule's requirements regulations; the relevant federal department or agency will only conduct or support non-exempt research if it receives such an assurance and if the institution has properly certified that an IRB has reviewed and approved the research (unless the relevant department or agency has waived the certification requirement).[135] Federal departments and agencies also have authority to enforce Common Rule compliance directly against IRBs operated by institutions that do not hold a written assurance.[136]

a. Where research takes place at an institution in which IRB oversight is conducted by an IRB not operated by that institution, the institution and the organization operating the IRB must document the institution's reliance on the IRB for research oversight and the responsibilities each entity will undertake to ensure compliance with the Common Rule's requirements.[137]

2. Institutional Review Boards (IRBs). IRBs must comply with several specifications governing their membership,[138] operations,[139] recordkeeping,[140] and responsibilities.[141] An IRB must review and approve all non-exempt research protocols in accordance with Common Rule requirements,[142] including requirements related to subject selection, data monitoring, and informed consent.[143] IRBs may use an expedited review process for eligible research activities,[144] including for exempt research protocols where limited review is required as a condition of exemption.[145] IRBs must also conduct continuing review of most research at intervals appropriate to the degree of risk and no less than once a year.[146] Continuing review is not required for:[147]

   a. Research eligible for expedited review (including exempt research protocols subject to limited review as a condition of exemption);
   b. Research that has reached the data analysis stage and/or has progressed to accessing standard follow-up clinical data (to the extent that either or both activities were part of the IRB-approved study).

Beginning on January 20, 2020,[148] all institutions engaged in cooperative research must rely on a single IRB for study approval; the relevant federal department or agency will identify the reviewing IRB or approve it after its proposal by the lead institution.[149] Certain research is not subject to the cooperative IRB requirement, including research for which more than single IRB review is required by law (including tribal law) or for which any relevant federal department or agency determines a single IRB is not appropriate.[150] Where a cooperative research project is not subject to the cooperative IRB requirement, participating institutions may enter into a joint review arrangement, rely on the review of another IRB, or make similar arrangements to avoid effort duplication.[151]

Informed Consent

In general, an individual must give specific informed consent to participate in research before the research may begin.[152] The primary researcher must comply with several requirements related to obtaining and documenting informed consent, including providing specific information about the research protocol to potential participants.[153] IRBs may waive or alter some or all informed consent requirements under certain circumstances.[154] Note that there is a different set of waiver and alteration criteria and requirements for research involving public benefit or service programs conducted by or subject to the approval of state or local officials.[155] An IRB may approve a research proposal in which an investigator will obtain identifiable private information without informed consent for the purpose of "screening, recruiting, or determining eligibility" of prospective subjects, if the investigator will obtain the information through oral or written communication with the prospective subject or by accessing records or stored identifiable biospecimens.[156] In addition to including standard elements in the informed consent, investigators must also provide specific information where it is relevant to the research protocol.[157] This includes informing the participant about the following:

1. Biospecimens may be used for commercial profit and whether the participant will or will not share in such profit;[158]
2. Whether or not clinically relevant research results, including individual research results, will be disclosed to participants and, if so, under what conditions;[159] and

3. For research involving biospecimens, whether the research will or might include whole genome sequencing.[160]

Broad Consent

Broad consent is a special kind of informed consent required for certain secondary use of identifiable biospecimens and identifiable private information (in addition to other requirements—see above section discussing exemptions). Because a secondary use is a use other than that for which the biospecimen or private information was originally collected, researchers may seek a participant's consent to future unspecified research during the initial informed consent process. Where participants give such "broad consent," additional informed consent would not be required for the same or another researcher to use the information or biospecimens collected during the original research study. Researchers may rely on broad consent to conduct studies on stored information or biospecimens in lieu of seeking IRB waiver of the specific informed consent requirement. Broad consent incorporates some parts of the specific informed consent process, such as rules governing how consent can be obtained[161] and requirements for information that must be provided to the subject,[162] and includes requirements for provision of information specific to secondary use.[163]

Subparts B–D add to (or modify) Subpart A requirements for federally supported research that involves certain vulnerable populations.

1. Subpart B applies to all research that involves pregnant women, human fetuses, neonates of uncertain viability, or nonviable neonates.[164] Note that all the exemptions available under Subpart A are available to research subject to Subpart B;[165]
2. Subpart C applies to all biomedical and behavioral research where the participants include prisoners.[166] Note that none of the exemptions available under Subpart A are available to research subject to Subpart C (except for research aimed at a broad population that only incidentally includes prisoners);[167] and
3. Subpart D applies to all research involving children as participants.[168] Note that some of the exemptions available under Subpart A are available to research subject to Subpart C.[169]

Note that there is a **Subpart E**, which governs IRB registration with the federal government and is not technically part of the "Common Rule," as it applies government-wide. Note also that Subparts B–E were not amended in conjunction with the 2017 Final Rule that changed Subpart A. However, HHS has expressed its intent to eventually amend Subparts B-E to the extent appropriate to modernize those provisions.[170]

U.S. Food and Drug Administration (FDA) Regulations[171]

Purpose. The FDA has not adopted the Common Rule's regulations protecting human participants. Instead, the FDA has implemented multiple regulations that generally mirror the Common Rule's provisions, with some notable differences. The FDA regulations govern experiments on human participants involving products, drugs, or devices subject to FDA review and/or approval.

Note that the FDA research regulations were not amended in conjunction with the 2017 Final Rule that modified the Common Rule Subpart A. However, HHS has expressed its intent to eventually update FDA regulations to the extent appropriate to modernize its provisions and align it with changes made to the Common Rule.[172] Further, the 21st Century Cures Act requires the Secretary to harmonize the differences between Subpart A of the Common Rule and the FDA's human subject regulations.[173]

Scope. There are several FDA-specific human subjects protection regulations scattered throughout Title 21 of the C.F.R.; these regulations are specific to the type of research being conducted. Parts 50 and 56 govern all experiments involving a human participant(s) that require prior FDA approval or the results of which require FDA investigation—these, like Subpart A, are broad and generally apply to most types of research under FDA's purview. Like the Common Rule, the FDA regulations establish requirements and responsibilities for IRBs and requirements for obtaining and documenting informed consent, including requirements for children (i.e., Subpart D). Some key differences between these regulations and Subpart A include:

1. The FDA has singular authority to waive any requirements in its regulations (e.g., IRBs do not have the authority to waive or modify the review or consent process).[174]
2. Waiver of consent is permitted in emergency circumstances without prior approval;[175]
3. Waiver of consent for investigational drug or device trials is permitted if the proposed clinical tests pose no more than minimal risk to [human] participants and includes appropriate safeguards to protect participants' rights, safety, and welfare;[176]
4. The FDA does not use the FWA mechanism;[177] and
5. The FDA defines "human subject" as a participant in research, whether as a recipient of the "test article" or the control (i.e., FDA does not govern information about an individual obtained from a secondary source).[178]

The 21st Century Cures Act directed the FDA to allow multisite and cooperative research projects to use single IRB review, in line with the 2017 Final Rule changes made to the Common Rule Subpart A.

Part 54 governs researchers' financial disclosures to the research sponsor; Parts 312 (clinical investigations of new drugs), 812 (clinical investigations of devices), and 814 (clinical investigations of Humanitarian Use Devices (HUD)[179]) all contain requirements that are in addition to or modify the requirements of Parts 50 and 56.

HIPAA, Common Rule, and Research

Purpose. The HIPAA Rules apply only to Regulated Entities (defined and discussed above) and thus are primarily relevant in relation to healthcare treatment, payment, and operations. However, because a Covered Entity may itself conduct research or be a resource for research (such as by supplying data for researchers to use), the HIPAA Privacy Rule establishes requirements for research involving a Covered Entity.

Scope. HIPAA does not mandate informed consent for research participation, leaving those requirements to the Common Rule. In general, as with any disclosure not required, permitted, or prohibited by the Privacy Rule, most disclosures of PHI for research purposes require written authorization from the individual subject of the PHI. However, PHI disclosure without authorization is permitted for research purposes (regardless of funding, unlike the Common Rule and FDA human participants protections)[180] in the following four circumstances:

1. The researcher needs the PHI only to prepare for research (e.g., develop a research protocol) and the PHI will not be physically removed from the Covered Entity;[181]
2. The only PHI sought is decedents' PHI, the researcher can provide documentation of those individuals' death (upon request), and the PHI is necessary for the research;[182] and
3. The disclosure is of a limited data set (LDS),[183] which is information with 16 identifiers removed but that is still considered PHI.[184] The Covered Entity and the intended recipient of the LDS (the

researcher) must first enter into a data use agreement (DUA) that meets multiple criteria regarding safeguards the researcher will employ to protect the PHI.[185] Note that an LDS may also be used or disclosed without authorization for healthcare operations purposes or public health activities and purposes.

4. An IRB or Privacy Board approves a partial or full waiver or alteration of the authorization requirement.[186] Note that a waiver or alteration can only be approved if the use of the PHI presents a minimal risk to individuals' privacy and the research could not be practicably conducted without the waiver/alteration or access to the PHI. The Privacy Rule explicitly requires IRBs to follow relevant Common Rule regulations[187] and sets forth requirements for Privacy Boards related to the review process and board structure.[188]

Non-exempt research subject to the Common Rule would still require informed consent even if HIPAA would not require the researcher to obtain an authorization to use or disclose the participant's PHI. Changes made to the Common Rule in the 2017 Final Rule created an exemption for research covered by the HIPAA Privacy Rule. Researchers may, without obtaining a subject's informed or broad consent, conduct secondary research involving the collection and analysis of the subject's private identifiable information or identifiable biospecimens when such use is regulated under the Privacy Rule for purposes of research, healthcare operations, or public health activities and purposes.[189] This exemption category is scheduled to take effect on January 18, 2018. The HIPAA Privacy Rule governs entities using information and protects an individual's information only if the information holder or user (in this case, a researcher) is a Regulated Entity. A researcher that is not affiliated with a Regulated Entity (e.g., employed by a private research institution or the non-covered component of a hybrid Covered Entity) is not subject to HIPAA, even when using information obtained from a Regulated Entity (including, but not limited to, use of a limited data set). Thus, this Common Rule provision likely only exempts secondary research use of identifiable information and biospecimens when the researcher is a Regulated Entity. However, the updated regulations are not explicit that this is the case, and institutions may interpret the provision differently. Note that there are other Common Rule exemptions for secondary research uses of identifiable information and biospecimens, which are associated with other requirements and limitations.

Where the Common Rule requires a researcher to have obtained broad consent for secondary use of identifiable private information or identifiable biospecimens, HIPAA would also require the researcher to obtain an authorization to disclose the information (if HIPAA applies to that researcher) unless such requirement is waived or altered by an IRB or Privacy Board. However, the Privacy Rule allows researchers to obtain an authorization for future research purposes "so long as the authorization adequately describes [as the purpose of the requested use or disclosure] the future research such that it would be reasonable for the individual to expect that his or her [PHI] could be used or disclosed for such future research."[190] Thus, when a researcher is obtaining a participant's broad consent for secondary use of information or biospecimens, the researcher may simultaneously seek the participant's authorization to disclose that information for such future research. Note that a valid authorization for research-related disclosures need not include an expiration date or event (as is required for all other authorizations under the Privacy Rule).[191] However, the 21st Century Cures Act directed the Secretary of HHS to issue guidance on future research authorizations stating that such an authorization must either include a specific expiration date or event or provide instructions on how to revoke the authorization.

Another relevant provision in the Privacy Rule permits the creation of compound authorizations in research contexts; that is, an authorization for use or disclosure of PHI for a research study (where the

authorization requirement has not been waived or altered) may be combined with any other written permissions for the same or another research study, including:

1. Another authorization for the same research study (e.g., authorization to disclose PHI to another entity involved in the research);
2. A consent to participate in research (i.e., informed consent required by the Common Rule or the FDA regulations);
3. An authorization to create or maintain a research database or repository.[192]

OVERVIEW OF FEDERAL LAWS: SETTING-SPECIFIC

Confidentiality of Veterans Affairs Medical Records[193]

Purpose. All medical records pertaining to treatments or services for drug abuse, alcoholism/alcohol abuse, HIV, and/or sickle cell anemia that were provided by or performed on behalf of the U.S. Department of Veteran Affairs (VA) must be kept confidential.

Scope. These regulations apply to records that contain information regarding the identity, diagnosis, prognosis, or treatment of a patient or research participant and are maintained in relation to a program or activity pertaining to drug abuse, alcohol abuse, HIV, and/or sickle cell anemia.[194] Programs or activities can include education, training, treatment, rehabilitation, and research but must be administered by or performed on behalf of the VA in order for the records to fall within the scope of the confidentiality regulations.

In general, these records remain confidential even if the patient/participant is no longer a VA patient. The regulations require patients to issue written consent to release their records, though there are exceptions to this requirement, including:

1. Disclosure to medical personnel to respond to a medical emergency;[195]
2. Disclosure to qualified personnel to conduct scientific research,[196] perform management or financial audits, or evaluate programs (if results do not directly or indirectly identify individuals);[197]
3. Disclosure to federal, state, and/or local public health authorities to comply with HIV reporting laws;[198]
4. Where a patient lacks decision-making capacity, disclosure to a personal representative to make an informed treatment decision;[199] or
5. Disclosure to state controlled substance monitoring programs in order to prevent misuse of prescription medication.[200]

42 C.F.R. Part 2 expressly exempts from its regulations services provided by or performed on behalf of the U.S. Department of Veteran's Affairs. As a result, the VA's regulations, while covering more types of patients than Part 2 (i.e., those with HIV/AIDS and/or sickle cell anemia in addition to substance abuse patients), substantially mirrors Part 2's confidentiality protections, limiting disclosure without patient consent in similar manner.

Family Educational Rights and Privacy Act (FERPA)[201]

Purpose. The purpose of FERPA is to protect the privacy of student education records.

Scope. FERPA applies to all educational agencies and institutions that receive federal education funding (e.g., public schools and districts, private and public colleges, universities, and other postsecondary institutions) but typically exempts private and religious elementary and secondary schools.[202] FERPA governs education records, which are "records, files documents, and other materials" that "contain information directly related to a student" and that "are maintained by an education agency or institution" or an entity acting as the agent of an institution.[203] Defining an "agent" of an institution is a matter of federal law but generally includes employees, contractors, and others working on behalf of or at the direction of the institution. FERPA treats elementary and secondary student health records, including immunization records, as education records. Where a clinic is operating in a school (e.g., a community health center offering satellite clinics in schools), FERPA would apply if the clinic is an agent of the school (i.e., if, under its agreement with a school, the clinic is carrying out the school's responsibilities and is subject to school direction). The term "education records" does *not* include the following records:[204]

1. Created by instructors, teachers, or administrators accessible only by the teacher or a substitute;
2. Created for law enforcement purposes by a law enforcement unit of an education agency;
3. Regarding educational agency or institution employees that are made in the normal course of business and only pertain to their employment; and
4. Regarding a postsecondary student or student over the age of 18 created by a healthcare professional for treatment purposes *if* such records are only made, maintained, or used in connection with treatment of the student (e.g., treatment records"). Treatment records may be disclosed for purposes other than treatment, but only if the disclosure meets an exception or with written consent.

An educational agency or institution (or its agent) may only disclose "education records" with written parental consent or the consent of a student age 18 or older or enrolled in a postsecondary institution, unless an exception applies. The main and most common exception to the FERPA written consent requirement is disclosure to a dependent child's parents. Other relevant exceptions include:

1. When released to authorized representatives of the Comptroller General, the Attorney General, the Secretary of Education, or state and local educational authorities.
2. When a disclosure is required by law, judicial order, or subpoena;
3. When the disclosure is to accrediting organizations to perform accrediting functions;
4. When the disclosure is to organizations that conduct studies related to: predictive test development, validation, or administration; student aid program administration; and instructional improvements for or on behalf of educational agencies or institutions;
5. When the disclosure is to the Department of Agriculture or Food and Nutrition Services representatives that need the information to monitor and evaluate the child nutrition programs; and
6. When disclosure is needed in an emergency to protect the health and safety of the student or others; and
7. To a parent about their postsecondary student's violation of any federal, state, or local law or institutional rule or policy governing the use or possession of alcohol or a controlled substance, if the student is under 21 at the time of disclosure (unless such disclosure is prohibited by state law).[205]

HIPAA Covered Entities Subject to More Stringent Requirements

There are several types of information that may be collected or used by a HIPAA Covered Entity but which are subject to more restrictive disclosure requirements than general PHI. For example, virtually all

substance abuse treatment providers subject to Part 2 would be considered HIPAA Covered Entities; however, disclosure of substance abuse patient treatment records without patient consent is much more limited as compared to HIPAA's permissive disclosure exceptions. Because Part 2 is more protective of information, its requirements supersede HIPAA's where those requirements conflict.

Another example are providers funded under certain sections of the Public Health Services Act (PHSA), including family planning projects (awarded grants under Title X of the PHSA) and Community Health Centers (CHCs) (awarded grants under § 330 of PHSA). While both Title X grantees and CHCs are HIPAA Covered Entities, the enabling regulations for each type of entity limit disclosure of patient information further than would otherwise be required under HIPAA. For Title X grantees, all information as to personal facts and circumstances about individuals receiving services must be held confidential and may not be disclosed without authorization except as is necessary to provide services or as is required by law.[206] CHCs may only disclose patient information without authorization as is required by law, for HHS audits, or as is necessary to provide services.[207] Note, however, that the definition of "services" under the CHC regulations is significantly broader in scope than the definition of treatment under HIPAA.

State Laws in General and Relationship to Federal Laws

Purpose. Providers and researchers must comply with any relevant federal requirements related to information disclosure and consent. In general, they also must comply with any state laws that are more protective of patients' rights, as well as any state laws governing data, patients, or entities not regulated by existing federal law. In some cases, there is a relationship between federal requirements and state laws such that they complement, rather than preempt, the other.

Scope. States typically provide enhanced protection for sensitive information (e.g., HIV/AIDS status, mental health information) and vulnerable populations (e.g., minors, legally incompetent adults). States also generally have laws governing state-based registries, compulsory health information reporting (e.g., communicable diseases, vital statistics), health insurers, public health entities, and provider licensure—all of which may contain requirements related to data sharing, confidentiality, and patient consent. Further, states often enact laws or regulations that offer more stringent protections than federal law, or that provide specific requirements implementing federal laws. For example, HIPAA provides individuals with the right to request and receive access to (most) of their PHI held by a Regulated Entity within 30 days at a reasonable cost-based fee.[208] States will often reduce the time frame in which Regulated Entities may provide access and/or will specify a fee structure for PHI access.[209]

One example of the relationship between federal and state laws exists in their treatment of minors. Federal laws often specifically reference minors' rights to privacy but defer to states for specifics, such as defining the age or circumstances of majority, setting the circumstances that trigger a minor's ability to consent to treatment or information disclosure, or defining parental and/or guardianship relationships and rights. Primary examples of the relationship between federal and state laws include:

HIPAA and Minors

The HIPAA Privacy Rule treats an unemancipated minor's parent, guardian, or other person acting *in loco parentis* as the minor's personal representative if state law gives such person authority to act on the minor's behalf in making health care decisions.[210] A personal representative stands in the shoes of the individual, meaning that the representative may request and obtain access to PHI, provide authorization for disclosures, and exercise any and all of the rights identified in the Privacy Rule. There are three circumstances in which a minor has the authority to act on his/her behalf: (1) when the minor consents

to the health care service and no other consent is required by law; (2) in cases in which a minor may lawfully obtain the health care service without parental consent (e.g., contraceptive services); and (3) in situations in which the parent agrees that the health care provider and the minor may keep the information confidential.[211]

Part 2 and Minors

Part 2 allows minors to consent to disclosure if their state grants minors the legal capacity to seek treatment without parental consent. In such states, only the minor can consent to information disclosure. If the state requires the minor to obtain parental consent before receiving substance abuse treatment, then both the minor and the parent/guardian must give written consent to disclosure (special rules apply when a minor lacks the capacity to make a rational choice). Note that there is no payment exception to the consent rule. That is, a provider must obtain the written consent of the minor (and the parent/guardian if the state does not give the minor capacity to consent to treatment) before disclosing information to a third-party payer.

Table 2: Federal Requirements for Consent to Disclose Identifiable Health Information

	HIPAA[212]	Common Rule[213]	GINA[214]	Part 2[215]	Privacy Act[216] (HHS)
Required elements:					
Patient's name				X	
Specific description of information[217]	X	X	X	X	X
Identify person(s) or entity authorized to make the requested disclosure	X			X	
Identify person(s) or entity authorized to receive the requested information	X	X	X	X	X
Describe the intended use(s) of the requested information[218]	X	X	X	X	X
The expiration date or event	X	X		X	
Date signed	X	X		X	
Signature (and/or electronic signature where acceptable) of the individual or his/her personal representative	X	X		X	
Provide the following information:					
The individual's right to withdraw authorization (if any) and any applicable exceptions to that right.	X	X		X	
Whether any benefits may be conditioned on releasing the information and applicable consequences of refusal to consent. This includes stating that refusal will involve no penalty or loss of benefits where relevant.	X	X	X		
The potential for re-disclosure of the information (if any). This includes stating that information may not be re-disclosed without further authorization, where applicable.	X	X		X	
Other requirements:					
The authorization must be written in plain language.	X	X			
Must provide the individual with a copy of the form.	X	X			

Table 3: Safe Harbor Method of De-Identification

In order for PHI to be considered de-identified, the following 18 elements must be removed from the information as it relates to the individual subject of the information or to the individual's relatives, employers, or household member

Names
All geographic subdivisions smaller than a **state**, including street address, **city**, **county**, precinct, **ZIP code**, and their equivalent geocodes, *except* for the initial three digits of the ZIP code if (according to the current publicly available data from the Bureau of the Census): • The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; OR • The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
All elements of dates (except year) for dates **that are directly related to an individual**, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
Telephone numbers
Fax numbers
Email addresses
Social security numbers
Medical record numbers
Health plan beneficiary numbers
Account numbers
Certificate/license numbers
Vehicle identifiers and serial numbers, including license plate numbers
Device identifiers and serial numbers
URLs (Web Universal Resource Locators)
IP (Internet Protocol) address numbers
Biometric identifiers, including finger and voice prints
Full-face photographs and any comparable images
Any other unique identifying number, characteristic, or code

*Note: Items in bold may be included in a limited data set.

Table 4: List of HIPAA Permissive Exceptions Available to Covered Entities[219]

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose and Relevant Limitations
For treatment purposes[220]	To any entity for its own or any healthcare provider's treatment activities
For payment purposes	To any entity for its own payment activities or to a Covered Entity or healthcare provider for the receiving entity's payment activities
For healthcare operations purposes	To any entity for its own healthcare operations purposes or to another Covered Entity for certain of the receiving CE's healthcare operations purposes, if both parties have/had a relationship with the patient and the PHI pertains to that relationship
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
As required by law[220]	To a government authority about a patient who the entity reasonably believes to be a victim of abuse, neglect, or domestic violence
	In the course of any judicial or administrative proceeding, in response to an order, subpoena, discovery request, or other lawful process
	To a law enforcement official for limited purposes (e.g., suspect identification, reporting crime on premises, about suspected victims of crime)
For public health activities	To a public health authority that is legally authorized to collect the PHI to control or prevent disease, injury, or disability
	To an authorized government entity to report child abuse or neglect
	To an FDA-regulated entity about an FDA-regulated product or activity for quality, safety, or effectiveness activities
	To a person who may have been exposed to or be at risk of contracting or spreading a communicable disease
	To an employer about an employee if the entity is providing health care to the employee at the employer's request in order to conduct an evaluation relating to workplace medical surveillance or to evaluate whether an employee has a work-related illness or injury
	Proof of immunization information to a school about a student or prospective student
	To anyone the provider believes can lessen or prevent a serious and imminent threat to an individual or the public
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement
For health oversight activities	To a health oversight agency[221] for legally authorized oversight activities
About decedents	To coroners and medical examiners to identify a deceased person, determine cause of death, or other legally authorized duties
	To a funeral director to carry out their legally authorized duties
	To organ procurement organizations for the purpose of facilitating donations and transplantations
For research purposes	To researchers as authorized by an IRB or Privacy Board for limited, specific research purposes
	To any entity in the form of a limited data set, if the Covered Entity and the intended recipient first execute a valid Data Use Agreement

General Purpose of Covered Entity Disclosure	To Whom a Covered Entity May Disclose and Relevant Limitations
For specialized government functions	About Armed Forces personnel where disclosure is deemed necessary by appropriate military authorities to execute military missions
	To authorized federal officials for national security and intelligence activities
	To authorized federal officials for the provision of protective services to the President
	To a correctional institution or law enforcement officer about an inmate or an individual in lawful custody
For worker's compensation	To entities legally authorized to receive such information for purposes of providing benefits for work-related injuries or illnesses
For directory purposes	To anyone identifying the patient by name,[222] if information disclosed is limited to location in the facility and general health status
For involvement in the patient's care	To any family member, close friend, or patient-designated representative to the extent that the information disclosed is directly relevant to the recipient's involvement with the patient's care or payment for care[223]
For notification, identification, or location of person responsible for patient's care	To any entity, if the information disclosed is limited to the patient's location and general health status or death[223]
Disclosures incident to any permitted or required disclosures	To any entity if the provider has in place reasonable safeguards to protect the privacy of patient information

Table 5: Disclosures for Purposes of Treatment, Payment, and Healthcare Operations[224]

Activity		To Whom Covered Entity May Disclose	
Treatment	Providing, coordinating, or managing health care and related services by a provider(s)	To any entity, for the disclosing Covered Entity's own activities	To any entity for a healthcare provider's (need not be a Covered Entity) own activities
	Coordinating or managing health care by a provider with a third party		
	Consultation between providers relating to a patient		
	Referring a patient for health care from one provider to another		
Payment	Activities undertaken by a health plan[225] to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan, if the activities relate to the individual to whom health care is provided.[226]	To any entity, for the disclosing Covered Entity's own activities	To a healthcare provider (need not be a Covered Entity), for the receiving provider's own activities To any Covered Entity, for the receiving entity's own activities
	Activities undertaken by a healthcare provider or health plan[225] to obtain or provide reimbursement for the provision of health care, if the activities relate to the individual to whom health care is provided. [226]		
Healthcare Operations	Conducting quality assessment and improvement activities (e.g., outcomes evaluation and development of clinical guidelines) and related functions that do not include treatment, if the primary purpose of any studies resulting from such activities is **not** to obtain generalizable knowledge.	To any entity, for the disclosing Covered Entity's own activities	To any Covered Entity, for that entity's own activities IF: (1) The disclosing entity has or had a relationship with the subject of the PHI; (2) The recipient has or had a relationship with the subject of the PHI; and (3) the PHI pertains to these relationships.
	Patient safety activities[227] and related functions that do not include treatment		
	Population-based activities relating to improving health or reducing health care costs and related functions that do not include treatment.		
	Protocol development and related functions that do not include treatment.		
	Case management and care coordination and related functions that do not include treatment.		
	Contacting healthcare providers and patients with information about treatment alternatives and related functions that do not include treatment.		
	Reviewing the competence or qualifications of healthcare professionals		
	Evaluating practitioner and provider performance		
	Health plan performance		
	Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as healthcare providers[228]		
	Training of non-healthcare professionals		
	Accreditation, certification, licensing, or credentialing activities		
Healthcare Operations (continued)	Conducting quality assessment and improvement activities (e.g., outcomes evaluation and development of clinical guidelines) and related functions that do not include treatment, if the primary purpose of any studies resulting from such activities is **not** to obtain generalizable knowledge.		To any Covered Entity, for the receiving entity's own activities IF: (1) The discloser has or had a relationship with the subject of the PHI; (2) The recipient has or had a relationship with the subject of the PHI; (3) the PHI pertains to these relationships; and (4) the intended use of the PHI is for fraud and abuse detection and/or compliance
	Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.[229]		
	Ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance). [229]		
	Business planning and development[230]		
	Business management and general administrative activities[231]		

REFERENCES

[1] HIPAA, Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 45 U.S.C.).

[2] There are also general regulations that contain definitions and relevant technical specifications applicable to all four rules (45 C.F.R. Part 160, Subparts A and B) as well as general provisions applicable to the Privacy, Security, and Breach Notification Rules (45 C.F.R. Part 164, Subpart A).

[3] 45 C.F.R. Part 164, Subpart E (2017).

[4] 45 C.F.R. Part 164, Subpart C (2017).

[5] 45 C.F.R. Part 160, Subparts C, D, and E (2017).

[6] 45 C.F.R. Part 164, Subpart D (2017).

[7] 45 C.F.R. § 160.103 at ¶ "Health information" (2017).

[8] 45 C.F.R. § 160.103 at ¶ "Individually identifiable health information" (2017).

[9] Note that HIPAA also does not apply to what FERPA defines as "treatment records" (see FERPA section for more information), which are excluded from FERPA's definition of "education records" (45 C.F.R. § 160.103 (2017), referencing 20 U.S.C. 1232g(a)(4)(B)(iv)).

[10] 45 C.F.R. § 160.103, at ¶ (2) of "Protected health information" (2017).

[11] A healthcare clearinghouse is a business or agency that processes nonstandard health information it receives from another entity into a standard format, or vice versa (e.g., billing services, re-pricing companies) (45 C.F.R. § 160.103 at "Healthcare clearinghouse" (2017)).

[12] Covered transactions include, but are not limited to, benefit eligibility inquiries and claims (45 C.F.R. Part 162 (2017)).

[13] 45 C.F.R. § 160.103 at ¶ "Covered Entity" (2017).

[14] 45 C.F.R. § 160.103 at ¶ "Business Associate" (2017). Note that Business Associate services are limited to legal, actuarial, accounting, consultation, data aggregation, management, administrative, accreditation, or financial services; relevant functions include claims processing, data analysis, utilization review, and billing.

[15] *See, e.g.* U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules 78 Fed. Reg. 5566 (2013).

[16] The healthcare component of a hybrid entity (defined by HIPAA as: "a single legal entity that is a covered entity whose business associate activities include both covered and non-covered functions and that designates healthcare components in accordance with [relevant HIPAA provisions]" (45 C.F.R. § 164.103 (2017))) is subject to all HIPAA requirements applicable to Covered Entities to the extent that it performs covered functions.

[17] 45 C.F.R. § 160.103 at ¶ "Covered Entity" (2017); 45 C.F.R. Part 164 §§ 302, 400, 500(a) (2017).

[18] 45 C.F.R. § 164.514(b)(2)(i) (2017).

[19] 45 C.F.R. § 164.514(b)(1) (2017).

[20] 45 C.F.R. § 164.514(c) (2017).

[21] *See* Paul Ohm Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Rev. 1701 (2010).

[22] Health Information Technology Policy Committee (HITPC) Privacy and Security Workgroup Health Big Data Recommendations at 14 (2015), *available at*: https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

[23] 45 C.F.R. § 164.502(d)(2) (2017).

[24] 45 C.F.R. § 164.502(a)(2) (2017).

[25] 45 C.F.R. § 164.502(a)(5) (2017). Note: a Covered Entity may sell PHI after obtaining the individual subject's valid written authorization for such sale, if the authorization states the disclosure of PHI will result in remuneration to the Covered Entity (45 C.F.R. § 164.508(a)(4) (2017)).

[26] 45 C.F.R. § 164.508(a)(2) (2017).

[27] 45 C.F.R. § 164.502(g) (2017).

[28] 45 C.F.R. § 164.510 (2017).

[29] 45 C.F.R. § 164.512 (2017); *see also* HHS Office for the National Coordinator for Health Information Technology (ONC) and OCR Permitted Uses and Disclosures: Exchange for Treatment (2016), *available at* http://www.hhs.gov/sites/default/files/exchange_treatment.pdf; ONC and OCR Permitted Uses and Disclosures: Exchange for Health Care Operations (2016), *available at* http://www.hhs.gov/sites/default/files/exchange_health_care_ops.pdf.

[30] 45 C.F.R. § 164.502(a)(1) (2017).

[31] 45 C.F.R. § 164.502(b) (2017).

[32] The Privacy Rule specifies limited circumstances in which a Covered Entity is permitted to rely on a requested disclosure as the minimum necessary (assuming such reliance is reasonable under the circumstances) (45 C.F.R. § 164.514(d)(3)(iii) (2017)). These circumstances include: (1) disclosures to public officials permitted under § 164.512; (2) information requested by another Covered Entity; (3) requests made by a professional who is member of its workforce for purposes of providing professional services to the Covered Entity; (4) requests made by its Business Associate for the purpose of providing professional services to the Covered Entity; (5) research disclosures under 164.512, if appropriate documentation has been provided.

[33] 45 C.F.R. § 164.502(b)(2) (2017).

[34] 45 C.F.R. § 160.203(b) (2017).

[35] 45 C.F.R. § 164.306 (2017).

[36] 45 C.F.R. § 164.306(a) (2017).

[37] 45 C.F.R. § 164.306(b)(1) (2017).

[38] 45 C.F.R. § 164.306(b)(2) (2017).

[39] Note that § 13410(e) of the Health Information Technology for Clinical Health (HITECH) Act, a part of the American Recovery and Reinvestment Act of 2009 (ARRA), gave State Attorneys General authority to bring civil actions on behalf of their state's residents for violations of the HIPAA Privacy and Security Rules (ARRA, Pub. L. No. 111-5, 115 Stat. 123 at Div. A, Title XIII, 123 Stat. 271-76 (2009)).

[40] 45 C.F.R. § 160.306(a) (2017).

[41] 45 C.F.R. § 160.306(c) (2017).

[42] 45 C.F.R. § 160.404 (2017).

[43] The violation amount is adjusted on an annual basis in accordance with inflation (45 C.F.R. § 160.404(a) (2017)).

[44] 45 C.F.R. § 160.404 (2017).

[45] 45 C.F.R. § 164.402 (2017).

[46] 45 C.F.R. § 164.402 (2017).

[47] 45 C.F.R. § 164.404(a)(1) (2017).

[48] 45 C.F.R. § 164.408(a) (2017). Notice to the HHS Secretary must be in the manner specified on HHS's website.

[49] 45 C.F.R. § 164.406(a) (2017).

[50] 45 C.F.R. § 164.402 (2017).

[51] 42 C.F.R. Part 2 (2017).

[52] 42 C.F.R. § 2.2(b)(2) (2017).

[53] U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration (SAMHSA) Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 NPRM") 81 Fed. Reg. 6988 (2016).

[54] SAMHSA Supplemental Notice of Proposed Rulemaking: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Supplemental NPRM") 82 Fed. Reg. 6052 (2017).

[55] SAMHSA Final Rule: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Final Rule") 82 Fed. Reg. 5485 (2017).

[56] 42 C.F.R. § 2.2(a) (2017).

[57] SAMHSA. "Applying the Substance Abuse Confidentiality Regulations: FAQs" at Question 10 (2011), *available at*: https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs.

[58] 42 C.F.R. § 2.11 at "Program" (2017).

[59] 42 C.F.R. § 2.12(b) (2017).

[60] Note that entities with direct administrative control over Part 2 programs are subject to the Part 2 disclosure restrictions with respect to the information communicated to them by the Part 2 program (42 C.F.R. § 2.12(d)(2)(i)(B) (2017)).

[61] A QSO is an individual or entity that provides professional services (e.g., data processing, dosage preparation, population health management, legal services, etc.) or services to prevent or treat child abuse or neglect to a Part 2 program (42 C.F.R. § 2.11 at "Qualified service organization" ¶ (1) (2017)). A QSO must have a written agreement with the program in which the QSO acknowledges that it is bound by the Part 2 regulations and agrees to resist any efforts to obtain access to patient records in judicial proceedings except as permitted by Part 2. (42 C.F.R. § 2.11 "Qualified service organization" (2) (2017)).

[62] 42 C.F.R. § 2.12(c) (2017).

[63] 42 C.F.R. § 2.15(b)(1) (2017).

[64] 42 C.F.R. § 2.12(a)(1) (2017).

[65] 42 C.F.R. Part 2 §§ 2(b)(1) and 13 (2017).

[66] 42 C.F.R. § 2.13(c)(1) (2017).

[67] 42 C.F.R. § 2.12(d)(2)(i) (2017).

[68] 42 C.F.R. § 2.51(a)(1) (2017).

[69] 42 C.F.R. § 2.52(a) (2017).

[70] 42 C.F.R. § 2.52(b)(3) (2017).

[71] 42 C.F.R. § 2.53 (2017).

[72] 42 C.F.R. § 2.14(c) (2017).

[73] 42 C.F.R. § 2.15(a)(2) (2017).

[74] 42 C.F.R. § 2.52(c)(1)(i) (2017).

[75] 42 C.F.R. § 2.52(c)(2)(i) (2017).

[76] 42 C.F.R. § 2.33 (2017).

[77] 42 C.F.R. § 2.31(a) (2017).

[78] 42 C.F.R. § 2.31(a)(4)(i),(ii), and (iii)(A) (2017).

[79] 42 C.F.R. § 2.31(a)(4)(iii)(B) (2017).

[80] 42 C.F.R. § 2.16(a) (2017).

[81] 42 C.F.R. § 2.16(a)(1), (2) (2017).

[82] Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (Title I amended scattered provisions of 29 U.S.C. §§ 1182 *et seq.*, 42 U.S.C. §§ 300gg-1 *et seq.*, 42 U.S.C. § 1395ss, 42 U.S.C. § 1320d-9, and 26 U.S.C. §§ 9802 *et seq*; Title II is codified at 42 U.S.C. §§ 2000f *et seq*.); implementing regulations found throughout multiple titles of the C.F.R.

[83] GINA does not apply to individuals in the U.S. military, those receiving health benefits through the VA or Indian Health Service, or federal employees obtaining health care through the Federal Employees Health Benefits Plan (FEHBP).

[84] "Genetic information" is: (1) information about an individual's genetic tests (i.e., analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations or chromosomal changes); (2) information about the individual's family members' genetic tests; (3) information about the manifestation of a disease or disorder in the individual's family members; (4) requests for or receipt of genetic services (i.e., a genetic test, genetic counseling, or genetic education) by the individual, and (5) participation by the individual or any of the individual's family members in clinical research that includes genetic services (*see, e.g.* GINA Title I, § 101(d) (2008)).

[85] *See, e.g.* GINA Title I, § 102(a)(4) (2008).

[86] *See, e.g.* GINA Title I, § 101(b) (2008).

[87] *See, e.g.* GINA Title I, § 101(b) (2008).

[88] Title II does not apply to employers with fewer than 15 employees.

[89] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. § 2000ff-1(a) (2008).

[90] *See, e.g.* GINA Title II, § 202(a), codified at 42 U.S.C. § 2000ff-1(a) (2008).

[91] GINA Title II, § 206(a), 42 U.S.C. § 2000ff-5(a).

[92] GINA Title II, § 206(b), 42 U.S.C. § 2000ff-5(b).

[93] PSQIA, Pub. L. No. 109-41, 119 Stat. 424 (2005) (amending scattered sections of the Public Health Services Act (PHSA), 42 U.S.C. §§ 299 *et seq*.).

[94] HHS Agency for Healthcare Research and Quality (AHRQ) "Patient Safety and Quality Improvement Act of 2005" (2008), *available at*: http://archive.ahrq.gov/news/newsroom/press-releases/2008/psoact.html

[95] PSQIA, 42 U.S.C. § 299b-21(7)(A) (2005).

[96] PSQIA, 42 U.S.C. § 299b-21(6) (2005).

[97] PSQIA, 42 U.S.C. § 299b-22(c)(2) (2005).

[98] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

[99] The Freedom of Information Act (FOIA), Pub. L. No. 89-487, 80 Stat. 250 (updated as amended by Pub. l. No. 114-185, 130 Stat. 538) (amending 5 U.S.C. § 552) (2016).

[100] 5 U.S.C. § 552a(b) (1974).

[101] 5 U.S.C. § 552(b)(6) (2016).

[102] 45 C.F.R. Part 46, Subparts A-E (2017).

[103] "Common Rule" Departments and Agencies, Notice of Proposed Rulemaking: Federal Policy for the Protection of Human Subjects, 80 Fed. Reg. 53933 (2015).

[104] "Common Rule" Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (2017).

[105] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).

[106] 82 Fed. Reg. 7149 at 7260-61 (to be codified at 45 C.F.R. § 46.102(l)).

[107] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(1)).

[108] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(4)).

[109] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(5), (6)).

[110] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(e)(7)(i)).

[111] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(l)).

[112] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.102(l)(2)).

[113] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104).

[114] HHS Office for Human Research Protections (OHRP), Exempt Research and Research That May Undergo Expedited Review [Number 95-02] (1995), *available at*: http://www.hhs.gov/ohrp/regulations-and-policy/guidance/exempt-research-and-research-expedited-review/index.html.

[115] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[116] Note: benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, and not likely to have a significant, adverse, lasting impact on the participants; further, the researcher must not have any reason to think the participants will find the interventions offensive or embarrassing (82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(ii)).

[117] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)).

[118] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(i)).

[119] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(ii)).

[120] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(iii)) (Note: "research" and "health care operations" are defined at 45 C.F.R. § 164.501 (2017); "public health activities and purposes" are defined at 45 C.F.R. § 164.512(b) (2017)).

[121] 5 U.S.C. § 552a (1974).

[122] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(4)(iv)) (Note: identifiable private information generated by the research must be maintained on information technology subject to and in compliance with the Privacy Impact Assessments requirements of the E-Government Act of 2002's Privacy Provisions (44 U.S.C. § 3501 note at § 208(b) (2002)) and, if applicable, the information used in the research must have been collected subject to the Paperwork Reduction Act of 1995 (44 U.S.C. §§ 3501 *et seq*).

[123] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(5)) (Note: each federal department or agency must establish (on a publicly accessible federal website or in another manner determined by the department or agency head) a list of the research or demonstration projects it conducts or supports under this provision).

[124] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(2)).

[125] Note: benign behavioral interventions are brief in duration, harmless, painless, not physically invasive, and not likely to have a significant, adverse, lasting impact on the participants; further, the researcher must not have any reason to think the participants will find the interventions offensive or embarrassing (82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(ii)).

[126] 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(3)(i)).

[127] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(7)) (Note: for this exemption, the information obtained by the researcher may be recorded in a way that allows the participant's identity to be readily ascertained, directly or through linked identifiers).

[128] 82 Fed. Reg. 7149 at 7262-63 (to be codified at 45 C.F.R. § 46.104(d)(7)).

[129] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)(i)).

[130] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)(ii)).

[131] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(8)(iii)).

[132] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.104(d)(8)).

[133] *See* 45 C.F.R. § 46.101(i) (2016).

[134] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(3)).

[135] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.103).

[136] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(a)).

[137] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.103(e)).

[138] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.107).

[139] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.108).

[140] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.115).

[141] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109).

[142] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(a)).

[143] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111).

[144] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110(b)) (Note: expedited review is available for: (1) research appearing on the list of categories published by the HHS Secretary in the Federal Register and available through OHRP unless the reviewer determines that the study involves more than minimal risk; (2) minor changes in previously approved research during the period for which approval is authorized; and (3) research for which limited review is a condition of exemption).

[145] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.110).

[146] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.109(e)).

[147] 82 Fed. Reg. 7149 at 7263 (to be codified at 45 C.F.R. § 46.109(f)(1)).

[148] 82 Fed. Reg. 7149 at 7259 (to be codified at 45 C.F.R. § 46.101(l)(2)).

[149] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(1)).

[150] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(b)(2)).

[151] 82 Fed. Reg. 7149 at 7265 (to be codified at 45 C.F.R. § 46.114(c)).

[152] 82 Fed. Reg. 7149 at 7264 (to be codified at 45 C.F.R. § 46.111(a)(4)).

[153] 82 Fed. Reg. 7149 at 7265-67 (to be codified at 45 C.F.R. § 46.116).

[154] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(f)).

[155] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(e)) (Note: this is distinct from research and demonstrations projects conducted or supported by a federal department or agency that are designed to study, evaluate, improve, or examine public benefit or service programs, which are exempt from Common Rule requirements entirely (see, 82 Fed. Reg. 7149 at 7262 (to be codified at 45 C.F.R. § 46.104(d)(5)).

[156] 82 Fed. Reg. 7149 at 7267 (to be codified at 45 C.F.R. § 46.116(g))

[157] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)).

[158] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(7)).

[159] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(8)).

[160] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(c)(9)).

[161] 82 Fed. Reg. 7149 at 7265-66 (to be codified at 45 C.F.R. § 46.116(a)(1)-(4), (6)).

[162] 82 Fed. Reg. 7149 at 7266 (to be codified at 45 C.F.R. § 46.116(d)(1)).

[163] 82 Fed. Reg. 7149 at 7266-67 (to be codified at 45 C.F.R. § 46.116(d)(2)-(7)).

[164] 45 C.F.R. § 46.201(a) (2017).

[165] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104(b)(1)).

[166] 45 C.F.R. § 46.301(a) (2017).

[167] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104(b)(2)).

[168] 45 C.F.R. § 46.401(a) (2017).

[169] 82 Fed. Reg. 7149 at 7261 (to be codified at 45 C.F.R. § 46.104(b)(3)).

[170] 82 Fed. Reg. 7149 at 7151 (2017).

[171] Title 21 C.F.R. Parts 50, 54, 56, 312, 812, 814 (2017).

[172] 82 Fed. Reg. 7149 at 7151 (2017).

[173] 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033, 1098-99, § 2063(b) (*codified at* 42 U.S.C. § 289) (2016).

[174] Title 21 C.F.R. § 56.105 (2017).

[175] 21 C.F.R. § 50.23(a)-(c) (2017).

[176] 21st Century Cures Act, 130 Stat. 1099, § 3024 at ¶¶ (a) (*amending* 21 U.S.C. § 360j(g)(3)) and (b) (*amending* 21 U.S.C. § 355(i)(4)) (2016).

[177] 21 C.F.R. § 56.103 (2017).

[178] 21 C.F.R. § 50.3 (2017).

[179] HUD are devices intended to benefit patients in treating or diagnosing a disease that affects or is manifested in 4,000 or fewer individuals in the United States annually.

[180] 45 C.F.R. § 164.512(i) (2017).

[181] 45 C.F.R. § 164.512(i)(1)(ii) (2017) (Note that the 21st Century Cures Act requires the HHS Secretary to issue guidance clarifying that remote access to PHI for research purposes is permitted so long as applicable privacy and security safeguards are maintained and the PHI is not copied or otherwise retained by the researcher (130 Stat. 1080-81, § 2063 at ¶ (a) (*codified at* 42 U.S.C. § 1320d-2, note)).

[182] 45 C.F.R. § 164.512(i)(1)(iii) (2017).

[183] 45 C.F.R. § 164.514(e)(3) (2017).

[184] 45 C.F.R. § 164.514(e)(2) (2017).

[185] 45 C.F.R. § 164.514(e)(4) (2017).

[186] 45 C.F.R. § 164.512(i)(2)(ii) (2017). (Note: waivers or alterations may only be approved if the use or disclosure of PHI involves no more than minimal risk to individuals' privacy. Minimal risk exists where the following elements exist: (1) an adequate plan to protect identifiers from improper use and disclosure; (2) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research (absent a health or research justification for retaining the identifiers or a legal requirement to retain the identifiers); (3) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the Privacy Rule; (4) the research could not practicably be conducted without a waiver or alteration; and (5) the research could not be practicably conducted without access to and use of the PHI (45 C.F.R. § 164.512(i)(2)(ii)(A) (2017))).

[187] 45 C.F.R. § 164.512(i)(2)(iv)(A) (2017).

[188] 45 C.F.R. § 164.512(i)(1)(i)(B) (2017).

[189] There are six "public health activities and purposes" for which PHI may be used or disclosed without individual authorization (*defined at* 45 C.F.R. § 164.512(b) (2017)).

[190] OCR. Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules 78 Fed. Reg. 5566 at 5612 (January 25, 2013); *see also*,OCR. "Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

[191] 45 C.F.R. § 164.508(c)(1)(v) (2017).

[192] 45 C.F.R. § 164.508(b)(3) (2017).

[193] 38 U.S.C. § 7332 (codified as amended in 38 C.F.R. §§ 1.460 *et seq.*) (2017).

[194] 38 C.F.R. § 1.460 (2017).

[195] 38 C.F.R. § 1.485 (2017).

[196] 38 C.F.R. § 1.488 (2017).

[197] 38 C.F.R. § 1.489 (2017).

[198] 38 C.F.R. § 1.486 (2017) (Note that physicians and counselors may also disclose HIV information to a patient's sexual partner(s) if they believe the patient will not disclose the information themselves and disclosure is necessary to protect the health of their partner(s) (38 C.F.R. § 1.487 (2017))).

[199] 38 C.F.R. § 1.484 (2017).

[200] 38 C.F.R. § 1.483 (2017).

[201] FERPA of 1974 (codified at 20 U.S.C. § 1232g; implementing regulations at 34 C.F.R. Part 99 (2017)).

[202] 34 C.F.R. § 99.1 (2017).

[203] 34 C.F.R. § 99.3 (2017).

[204] 34 C.F.R. § 99.3 (2017).

[205] 34 C.F.R. § 99.31 (2017).

[206] 42 C.F.R. § 59.11 (2017).

[207] 42 C.F.R. § 51c.110 (2017).

[208] 45 C.F.R. § 164.524; *see also* OCR. "Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. § 164.524" (*last updated* February 25, 2016), *available at* http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

[209] *See, e.g.* Health Information & the Law. Individual Access to Medical Records: 50 State Comparison (2013), *available at* http://www.healthinfolaw.org/comparative-analysis/individual-access-medical-records-50-state-comparison

[210] 45 C.F.R. § 164.502 (2017).

[211] 45 C.F.R. § 164.502 (2017).

[212] 45 C.F.R. § 164.508(c)(1) (2017).

[213] 82 Fed. Reg. 7149 at 7265-68 (2017) (to be codified at 45 C.F.R. Part 46 §§ 116, 117).

[214] GINA Title II, § 206(b) (2008), 42 U.S.C. § 2000ff-5(b) (2017).

[215] 42 C.F.R. § 2.31(a) (2017).

[216] 5 U.S.C. § 552a (as amended) (2016).

[217] Note that for a consent under Part 2, the information to be disclosed must be limited to the minimum amount of information necessary to accomplish the stated purpose of the disclosure (42 C.F.R. § 2.31(a)(5) (2017)).

[218] Note that in the case of an authorization for use or disclosure of PHI for future research purposes, the authorization must adequately describe such purposes so that it would be reasonable for the individual to expect his or her PHI could be used for such future research (82 Fed. Reg. 5566 at 5612 (2013)).

[219] *See, e.g.,* OCR. "Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html; OCR. Disclosures for Public Health Activities (2003), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf ; OCR. Research: 45 C.F.R. Part 164 §§ 501, 508, 512(i) (2003), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf; OCR. Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care (2015), *available at* http://www.hhs.gov/sites/default/files/provider_ffg.pdf.

[220] Disclosures for these purposes are not subject to the minimum necessary limitation (45 C.F.R. § 164.502(b)(2)(i) (2017)).

[221] A health oversight agency is defined by HIPAA as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the healthcare system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant" (45 C.F.R. § 164.501 (2017)).

[222] Providers must inform patients of directory disclosures and give them the opportunity to object to such disclosures or restrict them (may be accomplished via the provider's Notice of Privacy Practices or a verbal acknowledgement) (45 C.F.R. § 164.510(a)(2) (2017)). If patient is incapacitated, provider may make directory disclosures, but as soon as practicable, must inform patient of such disclosures and give patient the opportunity to object to or restrict further disclosures (45 C.F.R. § 164.510(a)(3) (2017)).

[223] Providers must give patients the opportunity to agree or object to such disclosures, by obtaining the patient's verbal or written approval, giving the patient the opportunity to object verbally or in writing, or inferring, based on professional judgment, that the patient does not object to such a disclosure and that disclosure is in the patient's best interest (45 C.F.R. § 164.510(b)(2) (2017)). If the patient is incapacitated, the provider may disclose if, using professional judgment, s/he determines that it is in the patient's best interest (45 C.F.R. § 164.510(b)(3) (2017)).

[224] OCR. "Research" (*last updated* June 5, 2013), *available at*: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

[225] Health plans may not use or disclose PHI that is genetic information for underwriting purposes (45 C.F.R. § 164.502(a)(5)(i) (2017)).

[226] Such activities include, but are not limited to: (1) Determining eligibility or coverage (including coordinating benefits or determining cost sharing amounts), and adjudicating or subrogating health benefit claims; (2) Risk adjusting amounts due based on enrollee health status and demographic characteristics; (3) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing; (4) Reviewing healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (5) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (6) Disclosing to consumer reporting agencies any of the following PHI relating to collecting premiums or reimbursement: (A) Name and address; (B) Date of birth; (C) Social security number; (D) Payment history; (E) Account number; and (F) Name and address of the healthcare provider and/or health plan (45 C.F.R. § 164.501 at "Payment" (2017)).

[227] Patient safety activities are: (1) Efforts to improve patient safety and the quality of healthcare delivery; (2) Collecting and analyzing patient safety work product; (3) Developing and disseminating information with respect to improving patient safety (e.g., recommendations, protocols, or information regarding best practices); (4) Utilizing patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk; (5) Maintaining procedures to preserve confidentiality with respect to patient safety work product; (6) Providing appropriate security measures with respect to patient safety work product; (7) Utilizing qualified staff; and (8) Activities related to operating a patient safety evaluation system and to providing feedback to participants in a patient safety evaluation system (45 C.F.R. § 164.501 at "Health care operations" ¶ (1) (2017) (referencing 42 C.F.R. § 3.20)).

[228] Psychotherapy notes may be disclosed without authorization for use in this activity (45 C.F.R. § 164.508(a)(2)(i)(B) (2017)).

[229] Where applicable, if a health plan receives PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such PHI for such purpose or as may be required by law (45 C.F.R. § 164.514(g) (2017)).

[230] This includes, but is not limited to: conducting cost-management and planning-related analyses related to managing and operating the entity; formulary development and administration; and development or improvement of methods of payment or coverage policies (45 C.F.R. § 164.501 at "Health care operations" ¶ (5) (2017)).

[231] This includes, but is not limited to: (1) Management activities relating to implementation of and compliance with the requirements of the HIPAA Administrative Simplification Rules (45 C.F.R. Parts 160, 162, and 164); (2) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer; (3) Resolution of internal grievances; (4) The sale, transfer, merger, or consolidation of all or part of the Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and (5) Consistent with applicable requirements, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity (45 C.F.R. § 164.501 at "Health care operations" ¶ (6) (2017)).

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX B:

ASSESSING POTENTIAL BARRIERS AND AMBIGUITY IN THE LEGAL LANDSCAPE

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Appendix B

Assessing Potential Barriers and Ambiguity in the Legal Landscape

INTRODUCTION

Stakeholder discussions organized during the early part of the development of the Architecture (described in further detail in Chapter 1) raised a number of issues and concerns related to the use of various types of data for PCOR (discussed in Chapter 2) and navigation of the statutes and regulations that govern the use of this data for PCOR (discussed in Chapters 3 and 4 and Appendix A). The stakeholders further identified topics of particular concern ranging from consent to special populations to merging clinical and claims data.

This Appendix identifies and defines categories of issues (referred to as *gaps*) related to privacy and security requirements for PCOR and catalogues challenges and concerns raised by stakeholders according to those categories. Identifying the "gaps" in privacy and security laws and regulations relevant to PCOR depends on how "gap" is defined. The term is generally understood to mean either a space between two objects or a difference in points of view and is not often used in relation to the issues that arise with the privacy and security laws that govern PCOR; rather stakeholders and experts in the field typically use "challenges," "issues," or "barriers" when referring to concerns with these laws. The categories below were developed to catalogue the core issues that stakeholders and the relevant literature raise with respect to PCOR. These categories are meant to clarify the scope and depth of the issues raised, as well as to serve as a foundation for application of the laws and regulations to these issues. The issues may not technically be a "gap" in the traditional sense, but they are areas of concern to stakeholders that may indicate a need for additional policies or clarification of existing policies.

A. Statutory, Regulatory, and Policy Void
B. Ambiguous or Overlapping Federal Authority
C. Informal Guidance ("Soft Law")
D. Ineffective Regulation and Regulatory Bottleneck
E. Incompatible Stakeholder Implementation or Institutional Policies
F. State Law Variation
G. Ethical Issues
H. Legal/Compliance/Operational Issues
I. Additional Areas of Stakeholder Concern and Suggestions

The stakeholder comments and queries are expanded upon where relevant with commentary, analysis, and additional content, with the exception of stakeholder comments that related to operational or individual issues (e.g., institutional policy, technical issues, or preferred practices). Comments that addressed such organizational or individual issues, as opposed to issues with the content and scope of laws and regulations themselves, are catalogued separately under the Legal/Compliance/Operational Issues category and "Additional Areas of Stakeholder Concern and Suggestions" section.

A. Statutory, Regulatory, or Policy Void

Laws and policies are generally drafted to reflect past, current, and anticipated circumstances. A statutory, regulatory, or policy void arises when unanticipated events occur that either render existing laws or regulations obsolete or insufficient. Technological innovations often lead to (or are themselves)

unanticipated events that make all or part of existing laws and policies incomplete. Recent examples of such innovations include the advent of mobile health technology and genetic testing. The use of virtual reality, 3D printing, synthetic biology, and nanotechnology in health care may lead to voids in the near future. Historical or structural changes also may render all or part of existing laws, regulations, and/or policies irrelevant. This may occur if a new administration implements new policies that undermine the efficacy of existing laws or policies, if Congress passes a law that makes existing regulations moot, or if the Supreme Court declares a law unconstitutional, rendering all enacting regulations void.

A valid law or regulation may exist that addresses a specific topic, product, issue, or concept but may not do so thoroughly enough to address the needs of the field. This is another example of a statutory, regulatory, and/or policy void. A law or regulation may initially be drafted in a way that does not completely address a particular topic, creating a gap from the outset.

Examples/Analysis

- The secondary use of data is critical to certain types of research (especially as it relates to big data analytics and CER). However, the existing legal framework does not consistently nor completely address secondary use and/or re-disclosure of information. Part 2 discusses information re-disclosure by recipients, and the Common Rule 2017 Final Rule finalized provisions applicable to secondary use of identifiable biospecimens and identifiable private information for research (though these provisions do not go into effect until 2018). However, other laws (HIPAA in particular, with respect to re-disclosure by non-Regulated Entity recipients) remain silent on this issue.
- How should researchers manage re-consent when a participant's proxy changes during a longitudinal study?
- The availability of personal data, the creation of big data sets, and advancements in machine learning have led to concerns that the Privacy Rule's methods of de-identifying data, particularly the Safe Harbor method, are no longer sufficient.

B. Ambiguous or Overlapping Federal Authority

When Congress issues legislation (i.e., federal statutes), it generally authorizes and/or requires relevant federal departments (or agencies) to develop detailed regulations implementing the statute's various provisions. Many statutes grant federal departments broad discretionary authority to craft these regulations; typically, the relevant department Secretary delegates specific rule-making tasks to various departmental agencies. Multiple departments and agencies have oversight and rulemaking authority over the functional elements that relate to PCOR (e.g., the FDA regulates medical devices that capture data used in PCOR, SAMHSA regulates any use and disclosure of substance abuse treatment information). When multiple departments and/or agencies assert (or *can* assert) authority over parts of the same processes, stakeholders, or outcomes, each agency or department must clearly establish how it intends to exercise that authority. A gap exists when these boundaries have not yet been clarified, creating ambiguous or overlapping regulatory authority. The same issues are mirrored at the state level.

Examples/Analysis

- Federal authority that is ambiguous or overlapping is particularly apparent in the regulation of patient-generated health data (PGHD) and patient reported outcomes (PRO) data. The Federal Trade Commission (FTC; an independent federal agency) and the Food & Drug Administration (FDA; an agency within HHS) can each assert administrative and/or enforcement authority over some of the technology used to collect or transmit PGHD and PRO data (the FDA over mHealth devices that meet the definition of "medical devices" and the FTC over all mHealth devices). Simultaneously, both the

FTC and the Office for Civil Rights (OCR; an HHS sub-agency) can assert administrative and/or enforcement authority over the collection, use, and disclosure of PGHD and PRO data.[1] Specifically, OCR has authority over the use and disclosure of PGHD and PRO data by a HIPAA Regulated Entity, where the data meets the definition of PHI. The FTC has authority to regulate against unfair and deceptive trade practices pursuant to the FTC Act[2] and may bring enforcement actions against any parties that use unfair or deceptive methods to collect, use, disclose, or secure PGHD/PRO data (e.g., failing to disclose the scope of information collected, failing to use the security standards identified in the entity's privacy policy). The FTC also has authority to enforce the breach notification rule as it pertains to certain non-HIPAA regulated entities.[3] The end result of this regulatory scheme is that the mobile collection of sensitive health data and transmission to or from a provider could be subject to regulation by: (1) the FDA, in relation to the actual device; (2) OCR, in regards to the privacy and security of the data received by a provider; and (3) the FTC, in regards to the trade practices related to the device's manufacture or sale. The FTC's mobile health interactive tool helps illustrate the overlapping nature of these agencies' authority.[4]

C. Informal Guidance ("Soft Law")

Federal and state regulatory agencies often issue informal guidance regarding the agency's interpretation of its own regulations. Agencies may issue such guidance in a standalone document or include guidance in the preamble of a Notice of Proposed Rulemaking (NPRM) or a Final or Interim Final Rule. These guidance documents generally outline what actions the agency considers to be compliant with and/or in violation of its regulations. Informal guidance documents are legally nonbinding; conforming actions to the guidance document does not make a stakeholder immune from legal liability or an agency enforcement action (where such authority exists). While guidance documents officially issued by regulatory agencies can be used in court or administrative actions to defend against an enforcement activity, they are not dispositive. This introduces ambiguity because stakeholders cannot rely on nonbinding sub-regulatory guidance in the same manner or to the same degree as with a law, regulation, or contract.

Examples/Analysis

- The HHS Office of the Secretary, OCR, and the Centers for Medicare & Medicaid Services[5] (CMS; an agency within HHS) have released multiple pieces of guidance regarding compliance with various provisions of the HIPAA Privacy and Security Rules. Topics addressed include an individual's right to access their own information, methods for de-identifying information, HIPAA compliance for app developers, and disclosing information to family members.[6]
- The FTC, OCR, and FDA have each issued guidance regarding mobile health devices and information collected from these devices (i.e., PGHD/PRO data).
- While not "guidance" in the traditional sense, certain department or agency actions may be considered "soft law." For example, the CMS policy to redact all substance abuse patient information from its identifiable data sets is based on its interpretation of the Part 2 regulations. While the changes to Part 2 made in the 2017 Final Rule addressed this issue by relaxing limitations on research disclosures of information obtained from Part 2 programs, the CMS interpretation remains in force until and unless it formally changes its policy. Because the Part 2 research provisions do not require disclosure for research purposes, other entities (private or public) may rely on the CMS interpretation of the rules in crafting their own data disclosure policies.

D. Regulatory Bottleneck

Regulations relevant to PCOR are often promulgated using a formal rulemaking process. An agency will publish an NPRM in the Federal Register, often accompanied by a request for [public] comment on some or all proposed provisions. After a specified time period, the agency reviews all comments received; if the agency chooses to take further action, it will modify, eliminate, or add to its proposed provisions based on this feedback. The agency publishes these modified provisions as a Final Rule in the Federal Register or, if the modifications warrant further public input, as a new NPRM or an Interim Final Rule (which contain binding regulations that may be changed or made permanent in a later Final Rule). Agencies may also issue an Advanced Notice of Proposed Rulemaking (ANPRM) or a Request For Information (RFI) as a means of soliciting feedback and information before proposing rules. The rulemaking process can take a long time to produce a Final Rule (if it produces one at all); this is particularly the case when the rules involve a complex and sensitive topic that requires careful deliberation. A Regulatory Bottleneck arises as a consequence of this process; a rulemaking signals that the regulatory structure applicable to a particular issue will [likely] change, so stakeholders do not know what the final provisions will be or when/if they will be finalized and the time between rulemaking and Final Rule keeps stakeholders in a holding pattern.

Examples/Analysis

- The changes to both the Part 2[7] and Common Rule regulations[8] significantly altered existing requirements regarding the use and disclosure of substance use information and federally supported research (in particular, mandating the use of a single IRB for multisite research, permitting broad consent for the secondary use of identifiable biospecimens and identifiable private information, and requiring changes to the informed consent process). However, regulators indicated at the time both Final Rules were published that further changes to each rule may be forthcoming. A Supplementary NPRM was published simultaneously with the Part 2 Final Rule seeking comment on numerous issues that make Part 2 incompatible with HIPAA (e.g., treatment and health care operations disclosures). No specific plans for further rulemaking were or have been announced since the SNPRM comment period closed in February 2017. In the preamble to the Common Rule 2017 Final Rule, the Secretary of HHS indicated that further changes to the Common Rule provisions are being contemplated and that harmonizing changes to Subparts B-E are anticipated. No formal rulemaking process was announced. Finally, the Common Rule 2017 Final Rule has an effective date one year after the Final Rule was published. It is possible that the effective date will be further delayed or that revisions to the updated regulations may occur prior to the effective date. Such uncertainty has led stakeholders to abstain from or delay conducting research rather than pursuing projects that could get undermined once the rules are finalized.

E. Incompatible Stakeholder Implementation or Institutional Policies

Laws and regulations often grant stakeholders discretion in deciding how to implement requirements. For example, the HIPAA Security Rule sets forth general standards for safeguards and allows Covered Entities to tailor their implementation to the Covered Entity's specific circumstances. Other laws and regulations may even allow stakeholders to decide which provisions, if any, to adopt. For example, the HIPAA Privacy Rule's permissive exceptions allow Covered Entities to select some, all, or none of the types/purposes of disclosures the rule allows. Gaps arise when stakeholders that must (or choose to) interact with each other have implemented flexible legal and regulatory requirements in ways that conflict, ultimately impeding their ability to conduct joint studies or share data. In addition, the law may be general enough to encompass many new fact patterns, but some stakeholders may be more risk-

averse than others with respect to undertaking new activities or methods absent explicit approval by the relevant regulator. For example, advances in technology have outpaced regulatory action, leaving stakeholders to apply laws to new technology not in existence nor contemplated when the statute or regulation was initially drafted. In such a situation, stakeholders may choose not to engage with new technology at all or may limit their use of it to a narrow interpretation of the existing law.

Examples/Analysis

- Research institutions may implement the discretionary provisions of HIPAA, the Common Rule, and other federal and state laws and regulations in their own way, depending on institutional culture, business needs, and available resources. Institutional policies and procedures reflect these unique perspectives and thus may govern the same activity in an entirely different way than another institution. For example, an institution that focuses on biospecimens research will likely have processes and procedures that differ from an institution that primarily conducts research using data in electronic form. Inconsistency in policies and practices across institutions can make multisite research challenging. Common areas of a inconsistency include: (1) institutions requiring their own IRB or Privacy Board to approve a multisite study even though the study has already received approval from another IRB or Privacy Board; (2) differing procedures for data management, transfer, and record linkage; (3) differing requirements for both the content of and process for executing Data Use Agreements (DUAs); (4) differing policies related to use of minors' information; or even (5) an unwillingness to share data with an institution perceived as a competitor.
- Inconsistent implementation is also an issue with respect to health data registry structures, as the lack of consistent technical standards may limit a given registry's ability to be used for certain purposes (or for multiple purposes) and/or housing data from multiple organizations/organization types.

F. State Law Variation

There is significant variation in state laws governing health information, health information technology, medical practice, and public health data collection. State law variation can create gaps when research is conducted across multiple states or data is exchanged across state lines.[9]

Examples/Analysis

- States laws create and govern many of the public health registries that contain data relevant to PCOR.[10] Because these laws vary by state, the registries vary in terms of the scope of data collected, the variables captured, and the ability to disclose the data for research purposes.
- State laws vary regarding the collection or sharing of minors' information.[11] These laws may prohibit the collection of a child's information or require a parent to opt in to the collection of their child's information. Opt-ins have the potential to significantly reduce the amount of data available for research.
- States allow minors varying degrees of control over certain health care decisions and thus also over the information associated with those decisions (e.g., in some states, minors may unilaterally consent to treatment for sexually transmitted diseases, reproductive health, mental health treatment, etc.).[12] These laws impact IRB policies for obtaining consent for a minor's participation in research, for seeking consent once the minor reaches a certain age (i.e., re-consent), and their procedures for protecting and preserving or destroying data. The disparate nature of these laws and IRB policies may create issues for studies conducted in multiple states.

- State laws and regulations vary in regards to the rights of persons under the supervision of the correctional system.[13] These rights may change based on the person's status as incarcerated, paroled, or on probation, so researchers must account for how a participant's changed status will impact their project.
- State laws vary in regards to the definition and authority of legally authorized representatives (LARs; persons authorized by law to consent to another person's participation in research). State laws may prohibit LARs from receiving compensation in return for providing consent or may limit compensation to the expenses associated with participating in the study.[14]

G. Legal/Compliance Questions

Some of the issues raised by stakeholders are better conceptualized as questions regarding whether and/or how a law applies to a particular scenario. These questions may appear to be "gaps" because: (1) stakeholders have not [yet] obtained an answer from an attorney or compliance officer and assume the question is unsettled law, even though it may not actually be unsettled; (2) stakeholders have obtained a legal or compliance opinion that inaccurately represents and/or applies the privacy and security laws and regulations; (3) applying complex laws and regulations to a particular situation can be extremely challenging (particularly for stakeholders without a legal background); or (3) institutional policies and procedures that include heightened protections reflecting the institution's culture, resources, and/or tolerance for risk are perceived as the floor for legal protections, even if those procedures are more stringent that what is legally required at the floor level. The questions below are answerable within the existing legal framework for privacy and security (i.e., do not represent gaps in those protections), and most are highly fact-specific (i.e., the answer will depend on the details of the exact scenario in question, including the state(s) in which the activity occurs, the relevant institution's policies and procedures, the characteristics of the individuals involved in the research, etc.). Stakeholder questions that fall under this category included the following:

Examples/Analysis

- How do the Part 2 regulations and state substance use privacy laws affect the secondary analysis of identifiable data?
- Does the decision by CMS to redact substance use claims from the ResDAC identifiable research data sets apply to state Medicaid agencies or other entities that release identifiable research data set? Does this decision by CMS impact state laws that govern the privacy of substance use information?
- Birth and death information are vital statistics that are required to be reported to states. Misuse of this information—e.g., identify theft—can cause significant harm. Given this concern, what are the legal implications of linking research data with vital statistics?
- Are researchers and third party entities legally required to use an internal IRB when linking data?
- How does a prisoner's incarceration status impact the consent process? For example, when a research participant is incarcerated, do they need to re-issue consent before a researcher uses data collected prior to their incarceration?
- What are the rights and responsibilities of Legally Authorized Representatives (LAR)? What legal obligations does a researcher have when a patient and their LAR disagree about a course of action (e.g., an LAR consents to a patient's participation in a study, but the patient asks for his or her data to be removed)?
- What are a researcher's legal obligations in regards to the disclosure of genetic information that affects the family members of a research participant? Can a researcher be held liable for disclosing or failing to disclose this information to affected family members?

- Do state laws impact the collection of data from workplace wellness programs?
- Do researchers have a legal obligation to disclose life-threatening diagnoses? Can they be held liable for disclosing or failing to disclose this information?
- How and when should a researcher contact participants about study results? Should informed-consent procedures address the method and timing of such disclosure?
- Many sensors allow individuals to transmit their information to their provider's EHR. Since the sensor data are combined with the individuals' other data (input by the provider in the EHR), researchers who have obtained consent to access EHR data can generally access the sensor data as well. How should researchers obtain consent if the sensor data flows to researchers through a non-EHR pathway?
- Are there legal implications to releasing research results through a patient portal?
- Do research protocols need to include a method for determining perspective participants' capacity to consent?
- Given the privacy concerns inherent in conducting research on American Indian/Alaskan Native (AI/AN) populations, are there best practices that can guide researchers' collection of identifiable information when these populations participate in a study?
- Does PRO data fall within the category of clinical data that providers must report to PH registries?

H. Ethical Questions and Concerns

PCOR potentially implicates many ethical concerns, as researchers and policymakers must balance patient privacy interests and the possibility that research might adversely impact or disproportionately advantage certain populations against potential research benefits. Ethical questions and concerns by stakeholders include the following:

Examples/Analysis

- If access to substance use data without direct patient consent is legally permissible, is such access by researchers ethical?
- Should researchers inform individuals of the privacy implications that arise when their birth certificate is used for research purposes?
- Is it ethical to use perpetual consent in the PCOR context?
- What are the ethical implications of using an opt-out consent for participation in PCOR as opposed to opt-in consent?
- Stakeholders believe that participants must retain autonomy over their data and that policies and procedures must exist to safeguard this autonomy. The importance of autonomy exists even if a participant's cognitive capacity is in decline.
- Stakeholders believe that research on prisoner populations must include additional measures to ensure proper consent for data release and safeguards against coercion. Stakeholders noted that data from incarcerated individuals raises unique privacy concerns (e.g., court-compelled data disclosures could affect the individual's release, parole, or probation).
- The collection of genetic information during a study may reveal that the participant has a genetic condition, is at risk of developing a genetic condition, and/or their family members are at risk of developing a genetic condition. Ethical concerns thus arise regarding the disclosure of such information by researchers to participants and/or their family members and disclosure by participants to their family members.
- Genetic research also raises issues in that the results could be used to discriminate against people with certain genetic characteristics.

- Research that involves small, culturally unique populations raises ethical issues. Notably, the risks to participant privacy might be greater because the small, unique nature of the population may make de-identified data easier to re-identify. The burdens associated with ensuring adequate protection of small, culturally unique populations might result in researchers choosing not to pursue research projects with these populations. This choice could be viewed as favoring population autonomy and privacy, but it also deprives populations of potentially beneficial insights that could help their communities. The stakeholders noted that researchers working with AI/AN populations must be aware of the sensitive nature of such research, given the historical oppression of these populations and abuses that have occurred within the research context.

I. Additional Areas of Stakeholder Concern and Suggestions

Finally, some of the stakeholder comments question the feasibility of certain compliance methods and/or suggest methods for complying. These suggestions are not "gaps" in law or policy and therefore will not be reflected in future deliverables for this project, such as the data flow mapping or framework. However, agencies may wish to consider these suggestions when developing guidance for stakeholders.

Examples/Analysis

- Stakeholders identified a decision tree as a potential tool to help researchers determine when and how to disclose study results to participants.
- Institutional policies and practices regarding data linking and IRB/Privacy Board review make multisite research studies difficult to conduct. Stakeholders suggested using a Memorandum of Understanding (MOU) as a method of reducing these challenges.
- The form and procedures associated with consent depend on the purpose of the consent (e.g., consent to use of data for PCOR versus consent to participate in clinical trial). Stakeholders suggested developing standards for IRBs regarding such context-based consent forms.
- Stakeholders suggested that a compound consent and authorization form could be used to facilitate the linking of data held by one research entity to data held by another entity.
- Is it feasible for a qualified independent entity to assess a potential research participant's capacity?
- Is there a feasible method for tracking prospective participants' capacity consent? Does this method work in longitudinal studies?

REFERENCES

[1] The Federal Trade Commission (FTC) regulates personal information pursuant to their authority over unfair and deceptive trade practices.

[2] 15 U.S.C. § 45; FTC, "FTC Policy Statement on Unfairness" (1980). *Available at*: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness (unfair acts or practices are those that cause or are likely to cause a substantial injury to consumers, cannot be reasonably avoided by consumers, and do not provide consumer or competitive benefits that outweigh the harms caused); FTC, "FTC Policy Statement on Deception" (1983). *Available at*: https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (deceptive acts or practices are those that include a material "representation, omission or practice that is likely to mislead the consumer).

[3] Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115) at § 13407; 16 C.F.R. Part 318. (Note: authority is limited to Personal Health Record (PHR) vendors, PHR-related entities, and third-party service providers to either PHR vendors or related entities).

[4] FTC, "Mobile Health Apps Interactive Tool" (2016). *Available at*: https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[5] Note: CMS had administrative and enforcement authority over the HIPAA Security Rule until the HHS Secretary delegated such authority to OCR on July 27, 2009. Consequently, CMS is the author of Security Rule guidance issued prior to this date (*See* U.S. Department of Health and Human Services Office for Civil Rights (OCR). Delegation of Authority, 74 Fed. Reg. 38630 (Aug. 4, 2009)).

[6] *See* OCR, "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524" (*content updated* February 25, 2016). *Available at*: http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html; OCR, "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule" (*content updated* November 6, 2015). *Available at*: http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html; OCR, "Health app developers, what are your questions about HIPAA?" *Available at*: http://hipaaqsportal.hhs.gov/ (*last visited* September 25, 2017); OCR, Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care (n.d.). *Available at*: http://www.hhs.gov/sites/default/files/provider_ffg.pdf.

[7] U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration (SAMHSA) Final Rule: Confidentiality of Substance Use Disorder Patient Records ("Part 2 Final Rule") 82 Fed. Reg. 5485 (January 18, 2017).

[8] "Common Rule" Departments and Agencies, Final Rule: Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149 (2017).

[9] 45 C.F.R. § 164.304 (2017).

[10] *See e.g.,* N.Y. Public Health § 2168 (Authorizing disclosure of identifiable information from the statewide immunization registry for research purposes); O.C.G.A. § 31-12-3.1 (Clarifying that the department may release vaccine registry data for scientific, educational, or public health purposes so long as the data are aggregated and do not contain names).

[11] *See e.g.,* MN 144.125 (Allows parents or legal guardians to consent to the use of their infant's blood sample and/or test results for research purposes); WAC § 246-650-050 (Requires the department to maintain newborn screening information and specimens until the child turns 21, but allows parents or guardians to request the destruction screening information/specimens once the screening process is complete).

[12] *See e.g.,* Arkansas Code Ann § 20-16-508 (Allowing minors to consent to STD treatment, but granting providers discretion to inform the minor's parents or guardian of the treatment); Idaho § 39-3801 (Allowing minors aged 14 or older to consent to the treatment of infection, contagious, or communicable diseases).

[13] *See e.g.,* CA Penal Code § 3501 et seq. (Prohibiting biomedical research on prisoners in California, but providing a limited exception for investigational drugs); A.R.S. § 31-321 (Allowing prisoners to consent to participate in research programs that receive approval from the director of the department of corrections).

[14] *See* CA Health & Safety Code 24178 (Identifying the persons that may provide surrogate consent to research participation and prohibiting surrogates from receiving compensation in exchange for consent).

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX C:

SELECTED FEDERAL INITIATIVES

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Appendix C

SELECTED FEDERAL INITIATIVES

INTRODUCTION

The work of numerous U.S. Department of Health and Human Services (HHS) agencies and offices, particularly the Office of the National Coordinator for Health Information Technology, informed the development of this Architecture. The prior and current work of these stakeholders related to privacy and security of health information is summarized below as instructive references for researchers and other stakeholders.

HHS Office of the National Coordinator for Health Information Technology (ONC)

Since its inception, ONC has focused on developing policy, programs, and initiatives designed to advance the interoperable exchange of electronic health information. These efforts have consistently addressed the important role that privacy and security play in any efforts involving the use, release, and exchange of health information.

Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (2008)[1]

In 2008 (prior to the HITECH changes to HIPAA reflected above), ONC released a Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. While this document may seem dated in the rapidly moving arena of health information and technology and relates specifically to the exchange of individually identifiable data via a network, the core principles remain important today and should be reflected in the legal and ethical framework for PCOR where relevant and appropriate. For example, the principles address: 1) ensuring reasonable individual access to their individually identifiable information; 2) enabling correction of information when appropriate; 3) ensuring openness and transparency related to policies and procedures; 4) enabling individual choice when relevant; 5) ensuring information is collected, used/or disclosed only to the extent necessary for the underlying purpose(s) (and never to discriminate); 6) ensuring data quality and integrity; 7) ensuring appropriate safeguards are met; and 8) ensuring accountability for non-adherence or breach. Importantly, this document and ONC resources reflect and are consistent with the Fair Information Practice Principles, or FIPPS. ONC and other stakeholders have routinely relied on FIPPS to develop and implement policies and procedures related to collection, use, and disclosure of personal information (see further description below).

HIE Governance (2013)

In 2013, ONC released a set of guiding principles related to the governance of health information exchanges.[2] While these principles focus on organizations engaging in activities related to the exchange of data as well as the actual exchange of data for health care purposes, they are also relevant to and should be considered in relation to research, specifically PCOR. The following principles provide the most

relevant guidance applicable to PCOR efforts for inclusion in a legal and ethical framework: 1) establish mechanisms to ensure that the entity's policies and practices and applicable federal and state laws and regulations are adhered to; 2) promote inclusive participation and adequate stakeholder representation; and 3) provide a simple explanation of the privacy and security practices that are in place to protect personally identifiable information when it is electronically exchanged.

Shared Nationwide Interoperability Roadmap

In 2015, ONC released "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap." One of the core principles of interoperability identified in the Roadmap is to "protect privacy and security in all aspects of interoperability."[3] The Roadmap focuses primarily on health care organizations, as the majority of health information "resides in and is stewarded by health care organizations," and their Business Associates, which are governed by HIPAA.[4] Health care organizations are a rich source of health information necessary to support PCOR. However, ONC also recognizes the increasing role played by organizations that are not governed by the HIPAA Privacy and Security Rule and calls for greater transparency of those organizations' data practices to ensure individuals understand the potential uses and disclosures of their information. Specifically, ONC addresses issues related to network security; verifiable identity and participant authentication; consistent principles for permission or consent to collect, share, and use identifiable health information, including FIPPS; and consistent representation of authorization to access health information.[5] This guidance and the continuing dialogue related to these issues will play an important role in the development of a legal and ethical framework for PCOR.

ONC notes that an interoperable health IT ecosystem supports critical public health functions as well as data aggregation for research.[6] The Roadmap also highlights the importance of a learning health system based on the best available evidence to further support these efforts (including patient-centeredness of care). It was the Institute of Medicine's (IOM) original vision of a learning health system that would "generate and apply the best evidence for the collaborative health care choices of each patient and provider; drive the process of discovery as a natural outgrowth of patient care; and ensure innovation, quality, safety and value in healthcare."[7] As noted above, this is the essence of PCOR.

Health Information Technology Policy Committee (HITPC) Privacy and Security Workgroup[8]

The Privacy and Security Workgroup of the HITPC (a Federal Advisory Committee Act (FACA) Committee), which reports to the HITPC and ONC, has focused its work solely on issues related to the privacy and security issues related to the electronic exchange of health information. Most recently, the Workgroup has addressed health big data[9] (including big data research), and their recommendations are instructive. There are many commonalities between big data and PCOR related to the use of patient health information. The Workgroup heard public testimony that raised a number of concerns related to commonly used tools to protect privacy (including de-identification, patient consent, data security, and transparency) and limitations on collection and use. The Workgroup also heard testimony on the barriers and challenges presented by the complex health information legal landscape. Much of the discussions focused on the challenges associated with the very different regulation of HIPAA Covered Entities and non-HIPAA entities, as well as decreasing confidence in de-identification methods and growing risk of re-identification. The Workgroup's resulting recommendations focused on addressing the "uneven" policy [legal] environment and changes to the de-identification methodologies as well as the secure use of data for learning. These recommendations and the collective work of the Privacy and Security Workgroup will help inform the development of the legal and ethical framework for PCOR.

Federal Health IT Strategic Plan 2015–2020[10]

Released in late 2015, the Federal Health IT Strategic Plan 2015–2020 builds on prior iterations of ONC's strategy to advance "widespread adoption of health IT." Advancing PCOR relates to several of the stated objectives in the Strategic Plan, including Objective 1A, empower individual, family, and caregiver health management and engagement; Objective 2B, improve health care quality, access, and experience through safe, timely, effective, efficient, equitable, and person-centered care; and Objective 2C, protect and promote public health and healthy, resilient communities.

The Strategic Plan calls for collaborative efforts by all stakeholders and highlights federal efforts to support PCOR, including improving accessibility, technical standards, services, policies, federal data, and governance structures for PCOR. With funding from/for PCORI, including funds to support this project, the goal is to "enable a comprehensive, interoperable, and sustainable data network infrastructure to collect, link, and analyze data from multiple sources to facilitate patient-centered outcomes research."[11]

The plan also highlights the importance of protecting the privacy and security of health information. Objective 4 of the Strategic Plan notes several strategies related to the clarification of legal requirements for privacy and security for entities covered by HIPAA and those not covered by HIPAA.

Other ONC PCOR Projects

ONC also has a number of other projects relevant to PCOR underway. These include the Common Data Elements, Patient Matching, and Patient-Generated Health Data projects. As the work of these projects continues to evolve, researchers and other stakeholders should review the status and guidance materials generated by these projects. To the extent possible, existing efforts on these projects helped inform the development of the Architecture.

HHS Open Data Initiatives

HHS has engaged in multiple open data initiatives pursuant to the HHS's Open Government Plan[12] and the associated Open Data Policy. These initiatives include the HHS Enterprise Data Inventory,[13] which lists all of the department's pubic, non-public, and restricted datasets and the release of publicly available datasets on healthdata.gov. The CMS website houses multiple datasets related to CMS programs. Interested parties can use the CMS Data Navigator to find data related to specific programs, settings, topics, and/or geographic locations.[14] CMS also offers access to research data through the CMS Chronic Conditions Data Warehouse.[15]

HHS Office for Civil Rights (OCR)

OCR, the federal office within HHS responsible for enforcement of the HIPAA Privacy, Security, and Breach Notification Rules has released guidance relevant to PCOR addressing: 1) individuals' right of access to their health information;[16] 2) privacy and security guidance for electronic health records;[17] 3) guidance for health app developers;[18] and 4) tools and resources for HIPAA Regulated Entities.[19] OCR enforcement action settlements also provide helpful guidance, particularly those related to medical devices and Internet applications. Collectively, these resources are instructive to PCOR.

HHS Office for Human Research Protections (OHRP)

OHRP, a federal office within HHS, is responsible for overseeing the protection of human participants involved in research that is conducted or supported by HHS. Specifically, OHRP provides guidance, maintains regulatory oversight, and provides advice on ethical and regulatory issues in biomedical and behavioral research. OHRP also supports the Secretary's Advisory Committee on Human Research Protections (SACHRP) (discussed below) that advises the HHS Secretary on issues of human participant protections. During the development of this Architecture, OHRP released material changes to the Common Rule that governs federally supported research involving human participants. Changes to the Common Rule were incorporated into the Architecture.

Secretary's Advisory Committee on Human Research Protections (SACHRP)

SACHRP provides guidance and recommendations to the HHS Secretary on matters pertaining to the protection of human participants research. While not directly specific to PCOR, SACHRP has provided recommendations related to big data research that bear consideration as they potentially relate to PCOR. For example, SACHRP suggested that OHRP provide guidance for and/or consider changes to the consent waiver standards applicable to human participants research and that OCR clarify if and how HIPAA applies to big data research. SACHRP also provided voluminous comments during the rulemaking process for the Common Rule (Final Rule effective February 2018).

National Committee on Vital and Health Statistics (NCVHS)[20]

The NCVHS advises HHS on matters related to health data, statistics, and national health information policy. Part of NCVHS' work is to review health data and advise on "statistical problems of national and international interest," to conduct simulations and/or studies of these problems, and to propose improvements for the US' health statistics and information systems. One of the NCVHS' roles is to foster collaboration on how to facilitate and accelerate multi-sector consensus around health system compatibility and information confidentiality.

Patient-Centered Outcomes Research Institute (PCORI)

The vision of PCORI is that "[p]atients and the public have information they can use to make decisions that reflect their desired health outcomes."[21] PCORI is responsible for supporting the development of PCORnet, the National Patient-Centered Clinical Research Network,[22] which is a PCORI initiative aimed at creating a national network for conducting PCOR. Through the PCORnet initiative, PCORI has grappled with issues related to use of patient health information for CER in particular, including health information privacy and security. Specifically, PCORnet has released its "Commitment to Patient Privacy and Data Security," including Guiding Principles.[23] The Guiding Principles articulate PCORnet's belief that the "protection of privacy, data confidentiality, and security is essential to the existence and success of healthcare data research networks." The Principles also state that all research practices within PCORnet "comply with current national and local regulatory and oversight provisions."[24] These Principles helped guide the development of the Architecture.

Centers for Disease Control (CDC)

The CDC is a federal agency within HHS responsible for the protection of public health and the control of disease and injury. Parallel to the development of this Architecture, the CDC developed a Legal and Ethical Framework for Public Health Research. The process for the CDC project was similar to this project in that the project team developed scenarios with a multidisciplinary work group and applied legal and ethical analysis to develop a framework for research using public health data. That project's final document, the "Legal and Ethical Framework to Use Centers for Disease Control and Prevention Data for Patient-Centered Outcomes Research," sets forth three data use scenarios that the CDC workgroup created to highlight unique legal and ethical implications for use of CDC data. CDC collects data for public health purposes, including surveillance of disease, injury, exposure to health threats, and research to address population needs. Secondary use of CDC's existing public health data for PCOR purposes can have a substantial impact on patient and public health through research in areas such as epidemiology, drug safety, outcomes research, vaccines, and health services research.

Federal Trade Commission (FTC)

The FTC is responsible for the protection of consumers and their information. In that role, they have released multiple materials that have been used to guide the efforts of other federal and state agencies, including ONC. In particular, the FTC FIPPs are widely cited. These principles resulted from the FTC's review of online entities that collect and use personal information to ensure that such efforts are fair and include appropriate privacy protections. The FIPPs address the following core elements related to information privacy: 1) notice to consumer prior to information collection; 2) choice/consent providing information on consumers' ability to control how their data is used (including opt-in and opt-out models); 3) limiting collection/use to stated purposes and enabling consumers to view and verify data collected; 4) transparency about information collected; 5) ensuring reasonable security protections; and 6) accountability for information and compliance with relevant laws and regulations.[25]

Substance Abuse and Mental Health Services Administration (SAMHSA)

The SAMHSA, an agency within HHS, leads public health efforts related to behavioral health, including substance abuse and mental health issues. During the development of the Architecture, SAMSHA released material revisions to 42 C.F.R. Part 2 (Part 2), the federal regulations that govern the use and disclosure of substance abuse patient health records. Changes to Part 2 were incorporated into the Architecture.

Precision Medicine Initiative (PMI)[26]

PMI, announced by President Obama in his 2015 State of the Union Address, seeks to "provide clinicians with tools, knowledge, and therapies to select which treatments will work best for which patients." The primary objectives of the PMI include discovering more effective cancer treatments, creating a voluntary national research cohort, modernizing regulations, creating public-private partnerships, and identifying privacy and security issues related to precision medicine. The PMI has addressed this final objective by establishing the Privacy and Trust Principles and the Draft Data Security Policy Principles and Framework.

PMI Privacy and Trust Principles[27]

The Privacy and Trust Principles were developed by an interagency working group and are meant to guide PMI activities. The principles focus on: (1) governance; (2) transparency; (3) respecting participant preferences; (4) empowering participants by enabling access to information; (5) data sharing, access, and use; and (6) data quality and integrity.

PMI Draft Data Security Policy Principles[28]

The Draft Data Security Policy Principles, developed by an interagency process, are meant to guide the development and implementation of a security plan by PMI organizations. These principles include: 1) building a system that participants can trust; 2) making security a "core element of the organization's services"; 3) preserving data integrity; 4) identifying risks and developing risk management plans; 5) maintaining transparency regarding security processes and expectations; 6) protecting data with security practices and controls, but not in a way that denies participants access to their data or limits proper research uses of the data; 7) acting responsibly, minimizing the exposure of participant data, and providing notification of breaches; and 8) communicating experiences and challenges with other PMI organizations. These organizations may achieve the Principles by complying with the core functions (i.e., Identify, Protect, Detect, Respond, and Recover) set forth in the Data Security Policy Framework.

REFERENCES

[1] The Office of the National Coordinator for Health Information Technology (ONC) Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (2008), *available at* https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

[2] ONC Governance Framework for Trusted Electronic Health Information Exchange at 1-2 (2013), *available at* https://www.healthit.gov/sites/default/files/GovernanceFrameworkTrustedEHIE_Final.pdf.

[3] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 9 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[4] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 13 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[5] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 55 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[6] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 17 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[7] Institute of Medicine (IOM) Learning Healthcare System (2007), *available at* https://iom.nationalacademies.org/Reports/2007/The-Learning-Healthcare-System-Workshop-Summary.aspx [purchase required].

[8] *See* ONC "Privacy & Security" (*last updated* March 2, 2016), *available at* https://www.healthit.gov/facas/health-it-standards-committee/hitsc-workgroups/privacy-security

[9] HITPC Privacy and Security Workgroup Health Big Data Recommendations at 14 (2015), *available at*: https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

[10] ONC Federal Health IT Strategic Plan 2015-2020 (2015), *available at* https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf.

[11] ONC Federal Health IT Strategic Plan 2015-2020 at 29 (2015), *available at* https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf.

[12] U.S. Department of Health and Human Services (HHS) HHS Open Government Plan: Version 4.0 (2016), *available at* https://www.hhs.gov/sites/default/files/hhs-open-gov-plan-v4-2016.pdf.

[13] HHS HHS Enterprise Data Inventory (*content updated* April 5, 2017), *available at* http://www.healthdata.gov/dataset/hhs-enterprise-data-inventory

[14] Centers for Medicare & Medicaid Services (CMS) "CMS Data Navigator" (2017), *available at* https://dnav.cms.gov/.

[15] CMS "Chronic Conditions Data Warehouse" (2017), *available at* https://www.ccwdata.org/web/guest/home

[16] HHS Office for Civil Rights (OCR) Questions and Answers About HIPAA's Access Right (*last updated* February 25, 2016), *available at* http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs

[17] OCR "Special Topics: Health Information Technology" (*last updated* June 16, 2017), *available at* http://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html

[18] HHS Health App Use Scenarios & HIPAA (2016), *available at* http://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf.

[19] OCR "HIPAA For Professionals" (*last updated* June 16, 2017, *available at* http://www.hhs.gov/hipaa/for-professionals

[20] HHS National Committee on Vital and Health Statistics (NCVHS) "About: About the Committee" *available at* https://www.ncvhs.hhs.gov/about/about-the-committee/ (*last visited* September 25, 2017).

[21] Patient-Centered Outcomes Research Institute (PCORI) "About Us," *available at* http://www.pcori.org/about-us (*last visited* September 25, 2017).

[22] PCORnet: The National Patient-Centered Clinical Research Network "Homepage" http://www.pcornet.org/ (*last visited* September 25, 2017).

[23] PCORnet: The National Patient-Centered Clinical Research Network PCORnet: A Commitment to Patient Privacy and Data Security (2015), *available at*: http://www.pcornet.org/wp-content/uploads/2015/03/PCORnet_PrivacyStatement_Final_March2015.pdf.

[24] PCORnet: The National Patient-Centered Clinical Research Network PCORnet: A Commitment to Patient Privacy and Data Security (2015), *available at*: http://www.pcornet.org/wp-content/uploads/2015/03/PCORnet_PrivacyStatement_Final_March2015.pdf.

[25] Federal Trade Commission (FTC) Fair Information Practice Principles (*last updated* June 25, 2007), *available at*: https://web.archive.org/web/20100309105100/http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Notice/Awareness

[26] The White House Fact Sheet: President Obama's Precision Medicine Initiative (2015), *available at* https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative

[27] The White House Precision Medicine Initiative: Privacy and Trust Principles (2015), *available at* https://obamawhitehouse.archives.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf.

[28] The White House Precision Medicine Initiative: Data Security Policy Principles and Framework (2016), *available at* https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_and_Framework_FINAL_022516.pdf.

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX D:

SELECTED FEDERAL RESOURCES

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

TABLE OF CONTENTS

Appendix D

SELECTED FEDERAL RESOURCES

INTRODUCTION

This Appendix includes an overview of key federal agencies and guidance they have released relevant to PCOR and CER. For each agency, a description of the agency's authority is provided, as well as titles of and links to relevant guidance documents released by that agency. The guidance documents listed beneath each agency are listed in chronological order, with the most recent guidance listed first. Where a guidance document was developed and released in collaboration with one or more additional federal agencies, a parenthetical after the document title lists the other agencies involved. Guidance documents are listed under the agency that posted the document: where multiple agencies post the same document, it is listed under each agency. The date of the document is included where available or, if unavailable, the date listed on the website as the date the material was last reviewed is included. Some documents do not have date information and are listed at the bottom of the list of resources for each agency with a note indicating no date information is available.

Centers for Disease Control and Prevention (CDC)

https://www.cdc.gov/

The Centers for Disease Control and Prevention (CDC) is a federal agency within the U.S. Department of Health and Human Services responsible for the protection of public health and the control of disease and injury. The CDC is responsible for conducting relevant research activities and collecting data on disease outbreaks.

- National Outbreak Reporting System (NORS) User Guidance—Waterborne Disease Outbreaks, February 2017. https://www.cdc.gov/nors/pdf/cdc_5212_guidance.pdf
- National Outbreak Reporting System Guidance—Foodborne Illness, February 2017. https://www.cdc.gov/nors/downloads/guidance.pdf
- HIPAA Privacy Rule and Public Health, April 2003. https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

Centers for Medicare & Medicaid Services (CMS)

https://www.cms.gov/

The Centers for Medicare & Medicaid Services (CMS) is a federal agency within the U.S. Department of Health and Human Services responsible for the administration of Medicare and working with state governments to administer Medicaid and the Children's Health Insurance Program (CHIP).

- HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules, August 2016. https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf

- Covered Entity Decision Tool, June 2016. https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/Downloads/CoveredEntitiesChart20160617.pdf
- Security Standards: Implementation for the Small Provider, December 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf?language=es
- Basics of Risk Analysis and Risk Management, March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf?language=es
- Security 101 for Covered Entities, March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es
- Security Standards: Administrative Safeguards, March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es
- Security Standards: Organizational, Policies and Procedures and Documentation Requirements, March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf?language=es
- Security Standards: Physical Safeguards, March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf?language=es
- Security Standards: Technical Safeguards, March 2007. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es

Federal Trade Commission (FTC)

https://www.ftc.gov/

The Federal Trade Commission (FTC) is a federal agency responsible for the protection of consumers and their information and competition. In that role, they have released multiple materials that have been used to guide the efforts of other federal and state agencies, including the ONC. In particular, the FTC Fair Information Practice Principles (FIPPs) are widely cited. These principles resulted from the FTC's review of online entities that collect and use personal information to ensure that such efforts are fair and include appropriate privacy protections. The FIPPs address the following core elements related to information privacy: 1) notice to consumer prior to information collection; 2) choice/consent providing consumers' ability to control how their data is used (including opt-in and opt-out models); 3) limiting collection/use to stated purposes and enabling consumers to view and verify data collected; 4) transparency about information collected; 5) ensuring reasonable security protections; and 6) accountability for information and compliance with relevant laws and regulations.

- Mobile Health App Developers: FTC Best Practices, April 2016. https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices
- Mobile Health Apps Interactive Tool (Developed with FTC, OCR, and ONC), April 2016. https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

- Medical Identity Theft: FAQs for Health Care Providers and Health Plans, January 2011. https://www.ftc.gov/tips-advice/business-center/guidance/medical-identity-theft-faqs-health-care-providers-health-plans
- Copier Data Security: A Guide for Businesses, November 2010. https://www.ftc.gov/tips-advice/business-center/guidance/digital-copier-data-security-guide-businesses

Food and Drug Administration (FDA)

https://www.fda.gov/

The Food and Drug Administration (FDA) is a federal agency within the U.S. Department of Health and Human Services responsible for regulating pharmaceutical drugs, medical devices, dietary supplements, tobacco products, food safety, and vaccines among other things.

- Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 C.F.R. Part 11—Questions and Answers—Guidance for Industry, June 2017. https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-gen/documents/document/ucm563785.pdf
- FDA Medical Device Cybersecurity, March 2017. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm
- Use of Electronic Health Record Data in Clinical Investigations: Guidance for Industry, May 2016. https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-gen/documents/document/ucm501068.pdf
- Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, February 2015. https://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf
- DSCSA Standards for the Interoperable Exchange of Information for Tracing of Certain Human, Finished, Prescription Drugs: How to Exchange Product Tracing Information—Guidance for Industry, November 2014. https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-gen/documents/document/ucm424895.pdf
- FDASIA Health IT Report (Developed by FDA, FCC and ONC), April 2014. https://www.fda.gov/MedicalDevices/DigitalHealth/ucm338920.htm
- Electronic Source Data in Clinical Investigations—Guidance for Industry, September 2013. https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-drugs-gen/documents/document/ucm328691.pdf
- Department of Health and Human Services Guidance Regarding Patient Safety Organizations' Reporting Obligations and the Patient Safety and Quality Improvement Act of 2005 (no date available). https://www.hhs.gov/sites/default/files/PSQIAFDA2guidance.pdf

National Committee on Vital and Health Statistics (NCVHS)

- Recommendations on De-identification of Protected Health Information under HIPAA, February 2017. https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf

National Institutes of Health (NIH)

https://www.nih.gov/

The National Institutes of Health (NIH) is a federal agency within the U.S. Department of Health and Human Services responsible for conducting biomedical and public health research. NIH is also responsible for awarding research grants to external researchers.

- Final NIH Policy on the Use of a Single Institutional Review Board for Multi-Site Research, June 2016. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-16-094.html
- NIH Precision Medicine Initiative, "All of Us" (no date available). https://allofus.nih.gov/
- Sync for Science Pilot (Developed by NIH in coordination with ONC) (no date available). http://syncfor.science/
- Certificate of Confidentiality FAQs (no date available). https://humansubjects.nih.gov/coc/faqs#eligibility

National Institute of Standards and Technology (NIST)

https://www.nist.gov/

The National Institute of Standards and Technology (NIST) is a non-regulatory agency within the U.S. Department of Commerce; it is a measurement sciences laboratory. NIST also develops technology standards utilized by the federal government, including security standards for storing sensitive information such as personal health information.

- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf?language=es

Office for Civil Rights (OCR)

https://www.hhs.gov/ocr/index.html

The Office for Civil Rights (OCR) is the federal agency within the U.S. Department of Health and Human Services responsible for enforcement of the HIPAA Privacy, Security, and Breach Notification Rules (see Appendix A for summaries of these rules). OCR has released guidance addressing: individuals' right of access to their health information, privacy, and security guidance for electronic health records; guidance for health app developers; and tools and resources for HIPAA Regulated Entities. OCR enforcement action settlements also provide helpful guidance, particularly those related to medical devices and Internet applications.

- Fast Facts for Covered Entities, last reviewed on June 16, 2017. https://www.hhs.gov/hipaa/for-professionals/covered-entities/fast-facts/index.html
- Guidance on HIPAA & Cloud Computing, last reviewed on June 16, 2017. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

- Privacy and Security Toolkit, last reviewed on June 16, 2017. https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html
- File Sharing and Cloud Computing: What to Consider?, June 2017. https://www.hhs.gov/sites/default/files/june-2017-ocr-cyber-newsletter.pdf
- My Entity Just Experienced a Cyber-attack! What Do We Do Now? A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR), June 2017. https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf
- Cybersecurity Incidents Will Happen... Remember to Plan, Respond, and Report!, May 2017. https://www.hhs.gov/sites/default/files/may-2017-ocr-cyber-newsletter.pdf
- Man-in-the-Middle Attacks and HTTPS Inspection Products, April 2017. https://www.hhs.gov/sites/default/files/april-2017-ocr-cyber-awareness-newsletter.pdf?language=es
- Workshop on the HIPAA Privacy Rule's De-Identification Standard, last reviewed on March 28, 2017. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/2010-de-identification-workshop/index.html
- Reporting and Monitoring Cyber Threats, February 2017. https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf?language=es
- Understanding the Importance of Audit Controls, January 2017. https://www.hhs.gov/sites/default/files/january-2017-cyber-newsletter.pdf?language=es
- Guidance and Resources for Electronic Information Technology: Ensuring Equal Access to All Health Services and Benefits Provided through Electronic Means, December 2016. https://www.hhs.gov/sites/default/files/ocr-guidance-electronic-information-technology.pdf
- Understanding DoS and DDoS Attacks and Best Practices for Prevention, November 2016. https://www.hhs.gov/sites/default/files/december-2016-cyber-newsletter.pdf?language=es
- Sharing Consumer Health Information? Look to HIPAA and the FTC Act, October 2016. https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act
- Mining More than Gold, October 2016. https://www.hhs.gov/sites/default/files/ocr-october-2016-cyber-newsletter.pdf?language=es
- Requirements of Title VI of the Civil Rights Act of 1964 (Developed with the Administration for Children and Families (ACF) and the U.S. Department of Justice (DOJ)), October 2016. https://www.hhs.gov/sites/default/files/title-vi-child-welfare-guidance-10-19-16.pdf
- What Type of Authentication Is Right for You?, October 2016. https://www.hhs.gov/sites/default/files/november-2016-cyber-newsletter.pdf?language=es
- Cyber Threat Information Sharing, September 2016. https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue8.pdf?language=es
- Do You Know Who Your Employees Are?, August 2016. https://www.hhs.gov/sites/default/files/Cyber-awareness-monthly-issue-7.pdf?language=es
- Help Emergency Preparedness, Response, and Recovery Providers Comply with Title VI of the Civil Rights Act, (Developed with the U.S. Department of Housing and Urban Development (HUD), U.S. Department of Homeland Security (DHS), U.S. Department of Justice (DOJ), and U.S. Department of Transportation (DOT)). August 2016. https://www.hhs.gov/sites/default/files/joint-guidance-titlevi-emergency-preparedness-august-2016.pdf
- HIPAA Audit Guidance & FAQ on HIPAA and Unique Device Identifiers, July 2016. https://www.hhs.gov/sites/default/files/2016HIPAADeskAuditAuditeeGuidance.pdf

- Fact Sheet: Ransomware and HIPAA, July 2016. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- Is Your Covered Entity or Business Associate Capable of Responding to a Cybersecurity Incident?, July 2016. https://www.hhs.gov/sites/default/files/HIPAA-cyber-awareness-monthly-issue-6.pdf?language=es
- Guidance and Resources for Long Term Care Facilities, June 2016. https://www.hhs.gov/sites/default/files/mds-guidance-2016.pdf
- What's in Your Third-Party Application Software?, June 2016. https://www.hhs.gov/sites/default/files/may-cyber-newsletter-05272016-final.pdf?language=es
- Cyber Awareness Monthly Update May 3, May 2016. https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue-4.pdf?language=es
- Cyber-Awareness Monthly Update March 30, March 2016. https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue3.pdf?language=es
- Cyber-Awareness Monthly Update March 3, March 2016. https://www.hhs.gov/sites/default/files/hipaa-cyber-awareness-monthly-issue2.pdf?language=es
- Patient Electronic Access to Health Information, March 2016. https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016_PatientElectronicAccess.pdf
- Cyber-Awareness Monthly Update February, February 2016. https://www.hhs.gov/sites/default/files/hippa-cyber-awareness-monthly-issue1.pdf?language=es
- HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework, February 2016. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf
- Questions and Answers about HIPAA's Access Right, last reviewed on February 25, 2016. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs
- Understanding Some of HIPAA's Permitted Uses and Disclosures, last reviewed on February 12, 2016. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/permitted-uses/index.html
- Individuals' Right under HIPAA to Access Their Health Information 45 C.F.R. § 164.524, January 2016. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
- HIPAA FAQs for Professionals, last reviewed on September 9, 2015. https://www.hhs.gov/hipaa/for-professionals/faq
- HIPAA Privacy and Security and Workplace Wellness Programs, last reviewed on April 20, 2015. https://www.hhs.gov/hipaa/for-professionals/privacy/workplace-wellness/index.html
- BULLETIN: HIPAA Privacy in Emergency Situations, November 2014. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/hipaa-privacy-emergency-situations.pdf
- HIPAA: Public Health Authority Disclosure Request Checklist (Developed with the Assistant Secretary for Preparedness and Response (ASPR)), October 2014. https://www.hhs.gov/sites/default/files/hippa-disclosure-chcklist102314.pdf
- HIPAA Privacy Rule and Sharing Information Related to Mental Health, February 2014. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/mhguidancepdf.pdf
- Sharing Information Related to Mental Health, February 2014. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/mhguidancepdf.pdf

- Health Information of Deceased Individuals, last reviewed on September 19, 2013. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html
- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule: A Guide for Law Enforcement (Developed with the U.S. Department of Justice (DOJ)), September 2013. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/final_hipaa_guide_law_enforcement.pdf
- Personal Representatives, last reviewed on September 19, 2013. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/personal-representatives/index.html
- The HIPAA Privacy Rule and Refill Reminders and Other Communications about a Drug or Biologic Currently Being Prescribed for the Individual, last reviewed on September 19, 2013. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/refill-reminders/index.html
- Student Immunizations, last reviewed on September 19, 2013. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/student-immunizations/index.html
- Is the HIPAA Privacy Rule Suspended during a National or Public Health Emergency?, last reviewed on July 26, 2013. https://www.hhs.gov/hipaa/for-professionals/faq/1068/is-hipaa-suspended-during-a-national-or-public-health-emergency/index.html
- Guidance on Significant Aspects of the Privacy Rule, June 2013. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/significant-aspects/index.html
- Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, November 2012. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf
- Guidance on Risk Analysis Requirements under the HIPAA Security Rule, July 2010. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records, (Developed with the U.S. Department of Education (DOE)). November 2008. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf
- HIPAA Security Guidance: Remote Use, December 2006. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf?language=es
- HIPAA Privacy Rule Compliance Guidance and Enforcement Statement for Activities in Response to Hurricane Katrina, September 2005. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/enforcementstatement.pdf
- Hurricane Katrina Bulletin: HIPAA Privacy and Disclosures in Emergency Situations, September 2005. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/katrinanhipaa.pdf
- Summary of the HIPAA Privacy Rule, May 2003. https://www.hhs.gov/sites/default/files/privacysummary.pdf
- Business Associates, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf

- Disclosures for Public Health Activities, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf
- Disclosures for Workers' Compensation Purposes, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/workerscompensation.pdf
- General Overview of Standards for Privacy of Individually Identifiable Health Information, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/overview.pdf
- Marketing, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf
- Minimum Necessary, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.pdf
- Notice of Privacy Practices for Protected Health Information, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/notice.pdf
- Research, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/research/research.pdf
- Restrictions on Government Access to Health Information, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/govtaccess.pdf
- Standards for Privacy of Individually Identifiable Health Information, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/introduction.pdf
- Uses and Disclosures for Treatment, Payment, and Health Care Operations, April 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf
- Incidental Uses and Disclosures, December 2002. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/incidentalu%26d.pdf
- A Health Care Provider's Guide to the HIPAA Privacy Rule: Communicating with a Patient's Family, Friends, or Others Involved in the Patient's Care (no date available). https://www.hhs.gov/sites/default/files/provider_ffg.pdf
- Frequently Asked Questions about Family Medical History Information (no date available). https://www.hhs.gov/sites/default/files/familyhealthhistoryfaqs.pdf
- Frequently Asked Questions about the Disposal of Protected Health Information (no date available). https://www.hhs.gov/sites/default/files/disposalfaqs.pdf
- HIPAA and Marriage: Understanding Spouse, Family Member, Marriage, and Personal Representatives in the Privacy Rule (no date available). https://www.hhs.gov/sites/default/files/hipaa-and-marriage.pdf
- Privacy, Security, and Electronic Health Records (no date available). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf

- Sharing Health Information with Family Members and Friends (no date available). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/sharing-family-friends.pdf
- Your Health Information Privacy Rights (no date available). https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf

Office for Human Research Protections (OHRP)

https://www.hhs.gov/ohrp/

The Office for Human Research Protections (OHRP) is a federal agency within the U.S. Department of Health and Human Services responsible for overseeing the protection of human participants involved in research that is conducted or supported by HHS. Specifically, OHRP provides guidance, maintains regulatory oversight, and provides advice on ethical and regulatory issues in biomedical and behavioral research. OHRP also supports the Secretary's Advisory Committee on Human Research Protections (SACHRP) (discussed below) that advises the HHS Secretary on issues of human participant protections. OHRP recently released revisions to the Common Rule that governs federally supported research involving human participants.

These changes become effective on January 19, 2018. See Appendix A for a summary of the Common Rule.

- 45 C.F.R. 46 (Common Rule) FAQs. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/45-cfr-46/index.html
- Clinical Data Registries—OHRP Correspondence (2015), June 2015. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/june-25-2015-letter-to-robert-portman/index.html
- National Health Registry Activities and 45 C.F.R. part 46 (2011), October 2014. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/regarding-application-of-45-cfr-46-to-national-health-registry/index.html
- National Health Registry Activities, OHRP, December 2011. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/december-29-2011-letter-to-dr-anthony-asher/index.html
- National Health Registry Activities, OHRP, August 2011. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/august-11-2011-letter-to-dr-anthony-asher/index.html
- Guidance on the Genetic Information Nondiscrimination Act: Implications for Investigators and Institutional Review Boards, March 2009. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/guidance-on-genetic-information-nondiscrimination-act/index.html
- Coded Private Information or Specimens Use in Research, Guidance, October 2008. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html
- Issues to Consider in the Research Use of Stored Data or Tissues (1996, 1997), November 1997. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/issues-to-consider-in-use-of-stored-data-or-tissues/index.html

Within the OHRP Office of the Director is:

Secretary's Advisory Committee on Human Research Protections (SACHRP)

https://www.hhs.gov/ohrp/sachrp-committee/index.html

The Secretary's Advisory Committee on Human Research Protections (SACHRP) provides expert guidance and recommendations to the HHS Secretary on matters pertaining to the protection of human participants research.

Office of the National Coordinator for Health Information Technology (ONC)

https://www.healthit.gov/

The Office of the National Coordinator for Health Information Technology (ONC) is a part of the Office of the Secretary at the U.S. Department of Health and Human Services. ONC is at the forefront of the department's health IT efforts. Since its inception, ONC has focused on developing policy, programs, and initiatives designed to advance the interoperable exchange of electronic health information. These efforts have consistently addressed the important role that privacy and security play in any efforts involving the use, release, and exchange of health information.

- State Health IT Privacy and Consent Laws and Policies, July 2017. https://www.healthit.gov/policy-researchers-implementers/state-health-it-privacy-and-consent-laws-and-policies
- State Health IT Privacy and Consent Laws and Policies Dashboard, July 2017. https://dashboard.healthit.gov/apps/state-health-it-privacy-consent-law-policy.php
- Patient Generated Health Data, April 2017. https://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data
- Building Data Infrastructure to Support Patient Centered Outcomes Research (PCOR), April 2017. https://www.healthit.gov/policy-researchers-implementers/building-data-infrastructure-support-patient-centered-outcomes
- Security Risk Assessment Tool, March 2017. https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- Permitted Uses and Disclosures: Exchange for Health Oversight Activities (Developed with OCR), January 2017. https://www.healthit.gov/sites/default/files/phi_permitted_uses_and_disclosures_fact_sheet_012017.pdf
- Permitted Uses and Disclosures: Exchange for Public Health Activities (Developed with OCR), December 2016. https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf
- Precision Medicine Initiative (PMI) Data Security Principles Implementation Guide, December 2016. https://www.healthit.gov/sites/default/files/pmi_security_ig_v16-clean.pdf
- Program Guidance #16-01—Applicability of Gap Certification and Inherited Certified Status, November 2016. https://www.healthit.gov/sites/default/files/policy/public_applicability_of_gap_certification_and_inherited_certified_status.pdf
- EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print, September 2016. https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf
- Health IT Playbook, September 2016. https://www.healthit.gov/playbook/

- Examining Oversight of the Privacy and Security of Health Data Collected by Entities Not Regulated by HIPAA, July 2016. https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf
- Permitted Uses and Disclosures: Exchange for Health Care Operations (Developed with OCR), January 2016. https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf
- Permitted Uses and Disclosures: Exchange for Treatment (Developed with OCR), January 2016. https://www.healthit.gov/sites/default/files/exchange_treatment.pdf
- ONC Certification Mark Terms of Use - Criteria and Terms of Use for ONC Health IT Certification Design and Mark, December 2015. http://www.healthit.gov/sites/default/files/hit_certificationterms_of_use_final.pdf
- Program Policy Guidance #15-01A - Surveillance Guidance for Calendar Year 2016, November 2015.
- Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, October 2015. https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf
- Program Guidance #15-02—Required Test Report Content for Health IT Certified to the 2014 Edition "Safely Enhanced Design" Certification Criterion, May 2015. https://www.healthit.gov/sites/default/files/policy/onchealthitcertificationprogramguidance1502.pdf
- Guide to Privacy and Security of Electronic Health Information, April 2015. https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- Program Guidance #15-01—Removal and Retirement of 2011 Edition EHR Certification Criteria and Related Standards, Terms, and Requirements, April 2015. https://www.healthit.gov/sites/default/files/onc_health_it_certificationprogramguidance15_01.pdf
- Your Mobile Device and Health Information Privacy and Security, last reviewed on March 21, 2014. https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security
- Managing Mobile Devices in Your Health Care Organization, January 2013. https://www.healthit.gov/sites/default/files/fact-sheet-managing-mobile-devices-in-your-health-care-organization.pdf
- A Guide to Understanding Your Organization's Mobile Device Policies and Procedures (no date available). https://www.healthit.gov/sites/default/files/fact-sheet-a-guide-to-understanding-your-organizations-mobile-device-policies.pdf
- Program Policy Guidance #14-01—Surveillance Guidance for Calendar Year 2015 (no date available). https://www.healthit.gov/sites/default/files/onc-acb_cy15annualsurveillanceguidance.pdf
- Program Policy Guidance #13-01—Surveillance Guidance for Calendar Year 2014 (no date available). https://www.healthit.gov/sites/default/files/onc-acb_2013annualsurveillanceguidance_final_0.pdf
- Take Steps to Protect and Secure Information When Using a Mobile Device (no date available). https://www.healthit.gov/sites/default/files/fact-sheet-take-steps-to-protect-information.pdf
- Your Practice and the HIPAA Rules (no date available). https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-2.pdf

Substance Abuse and Mental Health Services Administration (SAMHSA)

https://www.samhsa.gov/

The Substance Abuse and Mental Health Services Administration (SAMHSA) is a federal agency within the U.S. Department of Health and Human Services. SAMHSA leads public health efforts related to behavioral health, including substance abuse and mental health issues. Importantly for purposes of this project, SAMHSA recently released revisions to 42 C.F.R. Part 2 (Part 2), the federal regulations that govern the use and disclosure of substance abuse patient health records. These revisions became effective on February 17, 2017. See Appendix A for a summary of the Part 2 regulations.

- The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs, June 2004. https://www.samhsa.gov/sites/default/files/part2-hipaa-comparison2004.pdf

U.S. Department of Veterans Affairs (VA)

https://www.va.gov/

The Veterans Health Administration (VHA) is a component of the U.S. Department of Veterans Affairs that runs medical assistance programs for veterans through a network of hospitals and medical centers around the country. VA, especially VHA, are responsible for maintaining the electronic health records of all veterans who access their facilities and additionally have the ability to make some of that data available for research purposes.

- Revocation of HIPAA Authorization for Research, February 2017. https://www.research.va.gov/resources/policies/HIPAA-Revocation-FAQ.pdf
- VA Directive 6509—Duties of Privacy Officers, July 2015. https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=809&FType=2
- ORD Guidance on Certificates of Confidentiality, April 2015. https://www.research.va.gov/resources/policies/guidance/CertificatesConfidentiality.pdf
- VHA Handbook 1907.01—Health Information Management and Health Records, March 2015. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3088
- VA Directive 6066—Protected Health Information (PHI) and Business Associate Agreements Management, September 2014. https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=761&FType=2
- VHA Handbook 1907.06—Management of Release of Information, January 2013. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=2860
- Safeguarding Veterans' Personal Information (no date available). https://www.research.va.gov/for_veterans/Safeguarding-Veterans-Info.pdf

Research Data Assistance Center (ResDAC)

https://www.resdac.org/

The Research Data Assistance Center (ResDAC) is a contractor to the Centers for Medicare & Medicaid Services (CMS) and provides free user data support to nonprofit, academic, and government researchers interested in studying Medicare and Medicaid data. Resources include guides to choosing the right data files, preparing data requests, and data analysis tips; a data availability table; CMS fee information; and data file record layouts.

The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX E:

GLOSSARY

Submitted by:
The George Washington University
Milken Institute School of Public Health
Department of Health Policy and Management

Appendix E

Glossary
(In Alphabetical Order)

Accountable care organizations (ACOs). An ACO is a group of healthcare providers that is collectively reimbursed for a single patient's care. The goal of an ACO is to provide high-quality, low-cost, coordinated care. ACOs participating in the Medicare Shared Saving Program provide coordinated, high-quality care to Medicare patients in exchange for sharing in any savings the ACO realized for the Medicare program.[1]

Advanced Notice of Proposed Rulemaking (ANPRM). An ANPRM is formal invitation for stakeholders to participate in shaping a proposed rule and starts the notice-and-comment process in motion.[2]

Agency for Healthcare Research & Quality (AHRQ). AHRQ is a federal agency within the U.S. Department of Health and Human Services dedicated to improving the quality, safety, efficiency, and effectiveness of health care. AHRQ develops the knowledge, tools, and data needed to improve the healthcare system and enable informed decision-making.[3]

American Recovery and Reinvestment Act of 2009 (ARRA). ARRA (known as "the Stimulus Bill" or "the Recovery Act") was passed in response to the global economic decline in 2007 and 2008. Among other things, ARRA made investments in health care. ARRA included the Health Information Technology for Economic and Clinical Health (HITECH) Act, which called for the adoption and meaningful use of health information technology as a national policy priority and created the Electronic Health Record Incentive Programs.[4]

The Belmont Report. The Belmont Report summarizes the basic ethical principles identified by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research in the course of its deliberations. It is a statement of basic ethical principles and guidelines that should assist in resolving the ethical problems that surround the conduct of research with human subjects.[5]

Broad Consent. Broad consent refers to prospective consent given by an individual or his/her representative to unspecified future research. Under the Common Rule, it must include the 12 specified elements to be valid. Broad consent may be obtained in lieu of informed consent only for secondary research use, storage, and maintenance of identifiable private information and identifiable biospecimens.[6]

Business Associate (with respect to the HIPAA Rules). A Business Associate is a person or entity other than a member of a Covered Entity's workforce who:

(1) Creates, receives, maintains, or transmits protected health information for a HIPAA-regulated function or activity (e.g., claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management, and repricing) on behalf of a Covered Entity;
(2) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity;
(3) A Health information organization, E-prescribing gateway, or other person or entity that provides data transmission services with respect to protected health information to a Covered Entity and that requires access on a routine basis to such protected health information;
(4) A person that offers a personal health record to one or more individuals on behalf of a Covered Entity; or

(5) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate.[7]

Center for Medicare and Medicaid Innovation (CMMI). CMMI is an organization within the Centers for Medicare & Medicaid Services that was established by the Patient Protection and Affordable Care Act. Its purpose is to test out new payment and delivery models of care to reduce expenditures, while improving the quality of care within the Medicare, Medicaid, and Children's Health Insurance Program (CHIP) programs.[8]

Centers for Medicare & Medicaid Services (CMS). The federal agency within the U.S. Department of Health and Human Services that administers the Medicare, Medicaid, and Children's Health Insurance Program (CHIP) programs.[9]

Certification. Certification (in the context of the Common Rule) is the official notification by the institution to the supporting federal department or agency component, in accordance with the requirements of this policy, that a research project or activity involving human subjects has been reviewed and approved by an IRB in accordance with an approved assurance.[10]

Children's Health Insurance Program (CHIP). A health insurance program targeted to low-income children, established in 1997 and reauthorized in 2009, that is administered by the states either as a stand-alone program or as a Medicaid expansion and funded through a combination of federal and state payments.[11]

Clinical Decision Support System (CDSS). A CDSS is interactive computer software that provides health professionals with knowledge and person-specific information to aid in decision-making tasks, such as determining diagnosis for a patient or suggesting default values for a prescription. A CDSS usually includes multiple tools to enhance decision-making, including clinical guidelines, condition-specific order sets, patient data reports and summaries, and documentation templates.

Community Health Center. A Community Health Center is a healthcare provider that offers: primary and preventive health services to all residents of its catchment area and may also provide supplemental health services, referrals, environmental health services, and information on the availability and proper use of health services.[12] A CHC may receive a grant under Section 330 of the Public Health Service (PHS) Act[13] as a Federally Qualified Health Center.

Comparative effectiveness research. Comparative effectiveness research is the conduct and synthesis of research comparing the benefits and harms of different interventions and strategies to prevent, diagnose, treat and monitor health conditions in "real world" settings. The purpose of this research is to improve health outcomes by developing and disseminating evidence-based information to patients, clinicians, and other decision-makers, responding to their expressed needs, about which interventions are most effective for which patients under specific circumstances.[14]

Computerized Provider/Physician Order Entry/Management (CPOE). CPOE is an electronic system in which clinicians directly enter instructions for the treatment of patients under the practitioner's care, which then transmits the order directly to the medical staff or departments (such as pharmacy or laboratory) responsible for fulfilling the order.

Consent (to disclose information). The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule permits, but does not require, a Covered Entity voluntarily to obtain patient consent for uses and disclosures of protected health information (PHI) for treatment, payment, and healthcare operations. Covered Entities that do so have complete discretion to design a process that best suits their needs. By contrast, an "authorization" is required by the HIPAA Privacy Rule for uses and disclosures of

protected health information not otherwise allowed by the rule. To be valid, an authorization must include certain elements identified by the Privacy Rule, including the signature of the individual or his/her representative.[15]

Consent (to treatment). An individual consents to treatment when they give written or verbal permission prior to any medical exam or intervention. An individual who is unable to consent on his/her own may have an authorized surrogate who is permitted to consent for the individual.

Covered Entity (with respect to the HIPAA Rules). A Covered Entity is a health plan, healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a HIPAA-covered transaction.[16]

Critical Access Hospital (CAH). A Critical Access Hospital is a rural community hospital that receives cost-based reimbursement and meets certain conditions as set forth in the Medicare Conditions of Participation that are different for those for acute care hospitals.

Data Use Agreement (DUA) (with respect to the HIPAA Rules). A data use agreement is a contract use when nonpublic data is being transferred that spells out the terms of use of the data by the recipient. Under the HIPAA Privacy Rule, a data use agreement is required when a limited data set is shared and must identify who will receive the limited data set, establish how the data may be used and disclosed by the recipient, and provide assurances that the data will be protected.[17]

De-identified data. De-identified data is health information that does not identify an individual and does not provide any reasonable basis on which an individual could be identified. As de-identified data is no longer protected health information, HIPAA does not restrict the use or disclosure of de-identified data.

Department or agency head. This term refers to the head of any federal department or agency, such as the Secretary of HHS, and any other officer or employee of any federal department or agency to whom the authority provided by these regulations to the department or agency head has been delegated.[18]

Disclose (with respect to 42 C.F.R. Part 2). For the purposes of Part 2, disclose means to communicate any information identifying a patient as being or having been diagnosed with a substance use disorder, having or having had a substance use disorder, or being or having been referred for treatment of a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person.[19]

Disclose (with respect to the HIPAA Rules). For the purposes of HIPAA, disclose means to release, transfer, provide access to, or divulge in any manner of information outside the entity holding the information.[20]

Education records (with respect to FERPA). Education records under FERPA include those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.[21]

Electronic Health Record (EHR). An EHR is a digital version of an individual's health information and may include information from multiple providers or sources of health care. In contrast with EMRs, EHRs are interoperable, able to collect and share information with multiple healthcare providers, so they contain information from all the clinicians involved in the patient's care.[22]

Electronic Laboratory Reporting (ELR). ELR is the automated transmission of laboratory-related data from commercial, public health, hospital, and other labs to state and local public health departments.

Electronic medical record (EMR). An electronic medical record is a digital version of a patient's paper chart that contains the standard medical and clinical data gathered in a single provider's office. An EMR

is generally used by providers for diagnosis and treatment. Information from multiple EMRs for the same patient may be combined in an EHR.

Employer (for purposes of GINA). An employer is any person that employs an employee defined in § 1635.2(c) of 29 C.F.R. Part 1635.3 (GINA) and any agent of such person, except that, as limited by section 701(b)(1) and (2) of the Civil Rights Act of 1964, 42 U.S.C. 2000e(b)(1) and (2), an employer does not include an Indian tribe, or a bona fide private club (other than a labor organization) that is exempt from taxation under section 501(c) of the Internal Revenue Code of 1986.[23]

Expedited [IRB] review. Research activities that (1) present no more than minimal risk to human subjects, and (2) involve only procedures listed in one or more of the following categories may be reviewed by the IRB through the expedited review procedure authorized by 45 C.F.R. 46.110 and 21 C.F.R. 56.110. The activities listed should not be deemed to be of minimal risk simply because they are included on this list. Inclusion on this list merely means that the activity is eligible for review through the expedited review procedure when the specific circumstances of the proposed research involve no more than minimal risk to human subjects.[24]

The Fair Information Practice Principles (FIPPs). The FIPPs are a set of eight principles set forth by the Federal Trade Commission (FTC) that are rooted in the tenets of the Privacy Act of 1974. The eight principles include: transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, and accountability and auditing.[25]

Family Educational Rights and Privacy Act (FERPA). FERPA protects the privacy of education records, including elementary and secondary student health records (e.g., records maintained by school nurse, special education student records), held by all education agencies and institutions that receive federal funding.[26]

Family member. With respect to any individual, family member means:

(1) A person who is a dependent of that individual as the result of marriage, birth, adoption, or placement for adoption; or
(2) A first-degree, second-degree, third-degree, or fourth-degree relative of the individual, or of a dependent of the individual as defined in § 1635.3(a)(1).
    (i) First-degree relatives include an individual's parents, siblings, and children.
    (ii) Second-degree relatives include an individual's grandparents, grandchildren, uncles, aunts, nephews, nieces, and half-siblings.
    (iii) Third-degree relatives include an individual's great-grandparents, great-grandchildren, great-uncles/aunts, and first cousins.
    (iv) Fourth-degree relatives include an individual's great-great-grandparents, great-great-grandchildren, and first cousins once-removed (i.e., the children of the individual's first cousins).[27]

The Federal Information Security Management Act of 2002 (FISMA). FISMA requires every federal agency to develop and implement an agency-wide program to protect government information and information systems from unauthorized access, use, disclosure, or destruction.[28]

Federal Trade Commission Act Section 5. Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[29]

Federally assisted (under Part 2). For purposes of 42 C.F.R. Part 2, a program is considered to be federally assisted if:

(1) It is conducted in whole or in part, whether directly or by contract or otherwise by any department or agency of the United States (but see paragraphs (c)(1) and (2) of this section relating to the Department of Veterans Affairs and the Armed Forces);
(2) It is being carried out under a license, certification, registration, or other authorization granted by any department or agency of the United States including but not limited to:
    (i) Participating provider in the Medicare program;
    (ii) Authorization to conduct maintenance treatment or withdrawal management; or
    (iii) Registration to dispense a substance under the Controlled Substances Act to the extent the controlled substance is used in the treatment of substance use disorders;
(3) It is supported by funds provided by any department or agency of the United States by being:
    (i) A recipient of federal financial assistance in any form, including financial assistance that does not directly pay for the substance use disorder diagnosis, treatment, or referral for treatment; or
    (ii) Conducted by a state or local government unit that, through general or special revenue sharing or other forms of assistance, receives federal funds that could be (but are not necessarily) spent for the substance use disorder program; or
(4) It is assisted by the Internal Revenue Service of the Department of the Treasury through the allowance of income tax deductions for contributions to the program or through the granting of tax exempt status to the program.[30]

Federally Qualified Health Center (FQHC). An FQHC is a community health center that receives funding under Section 440 of the Public Health Service Act or a center that has been certified as meeting the same criteria.

Federalwide Assurance (FWA). The Federalwide Assurance (FWA) is the only type of assurance currently accepted and approved by OHRP. Through the FWA, an institution commits to HHS that it will comply with the requirements in the HHS Protection of Human Subjects regulations at 45 C.F.R. Part 46.[31]

Final Rule. The term "final rule" refers to the most current final disposition of a particular issue that includes a preamble, summary, effective date, and supplementary information. The final rule published in the *Federal Register* begins with a summary of the issue, regulatory goals, and why the rule is necessary.[32]

Freedom of Information Act (FOIA). FOIA gives any person the right to obtain access to information contained in the records of federal agencies, unless the information is specifically protected from disclosure under an exemption.[33]

Genetic information (with respect to GINA).

(1) Genetic information means information about:
    (i) An individual's genetic tests;
    (ii) The genetic tests of that individual's family members;
    (iii) The manifestation of disease or disorder in family members of the individual (family medical history);
    (iv) An individual's request for, or receipt of, genetic services or the participation in clinical research that includes genetic services by the individual or a family member of the individual; or
    (v) The genetic information of a fetus carried by an individual or by a pregnant woman who is a family member of the individual and the genetic information of any embryo legally held by the individual or family member using an assisted reproductive technology.

(2) Genetic information does not include information about the sex or age of the individual, the sex or age of family members, or information about the race or ethnicity of the individual or family members that is not derived from a genetic test.[34]

Genetic Information Nondiscrimination Act of 2008 (GINA). GINA protects individuals' genetic information from being used by health plans and issuers to make eligibility, coverage, underwriting, and premium-setting decisions about covered individuals. GINA also prohibits employers from discriminating against employees or applicants based on genetic information and from using genetic information in employment decisions.[35]

Genetic testing (with respect to GINA).

(1) "Genetic test" means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes.
(2) Genetic tests include, but are not limited to:
  (i) A test to determine whether someone has the BRCA1 or BRCA2 variant evidencing a predisposition to breast cancer, a test to determine whether someone has a genetic variant associated with hereditary nonpolyposis colon cancer, and a test for a genetic variant for Huntington's Disease;
  (ii) Carrier screening for adults using genetic analysis to determine the risk of conditions such as cystic fibrosis, sickle cell anemia, spinal muscular atrophy, or fragile X syndrome in future offspring;
  (iii) Amniocentesis and other evaluations used to determine the presence of genetic abnormalities in a fetus during pregnancy;
  (iv) Newborn screening analysis that uses DNA, RNA, protein, or metabolite analysis to detect or indicate genotypes, mutations, or chromosomal changes, such as a test for PKU performed so that treatment can begin before a disease manifests;
  (v) Preimplantation genetic diagnosis performed on embryos created using in vitro fertilization;
  (vi) Pharmacogenetic tests that detect genotypes, mutations, or chromosomal changes that indicate how an individual will react to a drug or a particular dosage of a drug;
  (vii) DNA testing to detect genetic markers that are associated with information about ancestry; and
  (viii) DNA testing that reveals family relationships, such as paternity.
(3) The following are examples of tests or procedures that are not genetic tests:
  (i) An analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes;
  (ii) A medical examination that tests for the presence of a virus that is not composed of human DNA, RNA, chromosomes, proteins, or metabolites;
  (iii) A test for infectious and communicable diseases that may be transmitted through food handling;
  (iv) Complete blood counts, cholesterol tests, and liver-function tests.
(4) Alcohol and Drug Testing—
  (i) A test for the presence of alcohol or illegal drugs is not a genetic test.
  (ii) A test to determine whether an individual has a genetic predisposition for alcoholism or drug use is a genetic test.[36]

Group health plan. The term "group health plan" means a plan (including a self-insured plan) of, or contributed to by, an employer (including a self-employed person) or employee organization to provide health care (directly or otherwise) to the employees, former employees, the employer, others associated or formerly associated with the employer in a business relationship, or their families.[37]

Health care (with respect to the HIPAA Rules). The term "health care" means care, services, or supplies related to the health of an individual (e.g., preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription).[38]

Healthcare Common Procedure Coding System (HCPCS). HCPCS is a two-level set of standard codes used by Medicare and other health insurance programs, with Level I being codes for medical services and procedures, known as CPT codes, and Level II being the coding system used primarily to identify products, supplies, and services not included in the CPT codes, such as ambulance services and durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) when used outside a physician's office. CPT codes are republished annually by the American Medical Association, whereas the Level II codes are maintained and distributed by CMS.

Healthcare operations (with respect to the HIPAA Rules). Healthcare operations means any of the following activities of a Covered Entity or a Business Associate to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined by the Patient Safety and Quality Improvement Act); population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or healthcare practitioners learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities;
(3) Except as otherwise prohibited, underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies;
(6) Business management and general administrative activities of the entity (e.g., management activities relating to implementation of and compliance with HIPAA; customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; resolution of internal grievances; the sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity); and
(7) Creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity.[39]

Healthcare payment (with respect to the HIPAA Rules). Healthcare payment means the activities of healthcare providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. The HIPAA Privacy Rule gives examples of common payment activities.[40]

Healthcare treatment (with respect to the HIPAA Rules). Healthcare treatment is the provision, coordination, or management of health care and related services among healthcare providers or by a healthcare provider with a third party, consultation between healthcare providers regarding a patient, or the referral of a patient from one healthcare provider to another.[41]

Health Information (with respect to the HIPAA Rules). Health information means any information, including genetic information, whether oral or recorded in any form or medium, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse and that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[42]

Health information exchange (HIE). Health information exchange can be used as either a verb or a noun. As a verb, HIE means the act of electronically sharing health-related information among organizations. As a noun, an HIE is an organization that provides services to enable the electronic sharing of health-related information.

Health information organization (HIO). An HIO is an organization that oversees and governs the exchange of health-related information among organizations in accordance with nationally recognized standards.

Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH is part of the American Recovery and Reinvestment Act of 2009 (ARRA). HITECH legislatively mandated the Office of the National Coordinator for Health Information Technology (ONC) to oversee the development of a national health information network as well as a strategic health information plan for the nation. HITECH strengthened standards for health information privacy and security and authorized financial incentives for certain healthcare providers and facilities that demonstrate meaningful use of certified electronic health record technology.[43]

The Health Insurance Portability and Accountability Act (HIPAA). HIPAA regulates health insurers and health benefit plans and provides privacy protection for health information. Among other provisions, HIPAA set forth guidelines for the privacy and security of individually identifiable health information. The HIPAA Privacy, Security, Enforcement, and Breach Notification Rules were established to implement those guidelines.[44]

Health insurance issuers. The term “health insurance issuer” means an insurance company, insurance service, or insurance organization (including a health maintenance organization). Such term does not include a group health plan.[45]

Health Plan (with respect to the HIPAA Rules). A health plan is an individual or group plan that provides, or pays the cost of, medical care.[46]

Healthcare Practitioner. A healthcare practitioner is any individual authorized to provide healthcare services, including a doctor of medicine, nurse practitioner, physician assistant, allied health professional, social worker, case worker, case manager, or case coordinator.

Healthcare Provider (with respect to the HIPAA Rules). A healthcare provider is a provider of services (as defined in the Medicare statute), a provider of medical or health services (as defined in the Medicare statute), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.[47]

Health Resources & Services Administration (HRSA). HRSA is an agency of the U.S. Department of Health and Human Services. It is the primary federal agency for improving health care to people who are geographically isolated and/or economically or medically vulnerable, helping those in need of high-quality primary health care, people living with HIV/AIDS, pregnant women, and mothers. HRSA also supports the training of health professionals, the distribution of providers to areas where they are needed most, and improvements in healthcare delivery. HRSA oversees organ, bone marrow, and cord blood donation. It compensates individuals harmed by vaccination and maintains databases that protect against healthcare malpractice, waste, fraud, and abuse.[48]

Human subject (with respect to the Common Rule). Under the Common Rule, a human subject is a living individual about whom an investigator (whether professional or student) conducting research:

(1) Obtains information or biospecimens through intervention or interaction with the individual and uses, studies, or analyzes the information or biospecimens; or
(2) Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.[49]

Human subject (with respect to the FDA Rule). Under the FDA Rule, a human subject is an individual who is or becomes a participant in research, either as a recipient of the test article or as a control. A subject may be either a healthy individual or a patient.[50]

Identifiable biospecimen. An identifiable biospecimen is a biospecimen for which the identity of the subject is or may readily be ascertained by the investigator or associated with the biospecimen.[51]

Identifiable private information. Identifiable private information is that for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.[52]

Individual (for purposes of the HIPAA Rules). The term “individual” means the person who is the subject of protected health information.[53]

Individually Identifiable Health Information (with respect to the HIPAA Rules). Individually identifiable health information is that which is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[54]

Informed consent (with respect to the Common Rule). Informed consent is the formal process by which researchers inform potential participants of a study’s purpose, scope, risk, harms, benefits, and other pertinent information that permits the potential participant to make an informed decision about participating in the research study.

Institution (with respect to the Common Rule). Institution means any public or private entity engaged in research.

Interaction (with respect to the Common Rule). Interaction means communication or interpersonal contact between investigator and participant.

International Classification of Disease (ICD). An ICD is a classification system for diseases and injuries that groups medical terms used by physicians, medical examiners, and coroners together for statistical

purposes (e.g., mortality data).[55] The ICD is revised regularly to incorporate changes in medical knowledge—the revision number is added after ICD (e.g., ICD-10).

International Classification of Disease, Clinical Modification (ICD-CM). ICD-CM is a classification system for diseases, injuries, health encounters, and inpatient procedures that groups medical terms used by healthcare providers together for billing and claims reimbursement and statistical purposes (e.g., morbidity data).[56]

Interoperability. Interoperability means the architecture or standards that enable diverse electronic health record (EHR) systems to work compatibly in an information network made up of multiple stakeholders (e.g., federal, state, and local governmental entities, private stakeholders, regional collaboratives).[57]

Intervention (with respect to the Common Rule). An intervention is a physical procedure or procedures by which information or biospecimens are gathered and manipulations of the subject or the subject's environment that are performed for research purposes.

Institutional Review Board (IRB). An IRB is a group that has been formally designated to review and monitor proposed research to ensure that appropriate steps are taken to protect the rights and welfare of research participants.[58] An IRB typically has authority to approve, require modifications in, and disapprove research proposals.

Institutional Review Board (IRB) approval. IRB approval is the determination that proposed research has been reviewed and may be conducted within the constraints set forth by the IRB and by other institutional and federal requirements.[59]

Legally authorized representative (for purposes of the Common Rule). Under the Common Rule, a legally authorized representative is an individual or judicial or other body legally authorized to consent on behalf of another individual to that individual's participation in the procedure(s) involved in the research.[60] Where there is no applicable law addressing this issue, a legally authorized representative is an individual recognized by institutional policy as acceptable for providing consent in the non-research context on behalf of the prospective participant to participation in the procedure(s) involved in the research.

Limited data set (with respect to the HIPAA Rules). A limited data set is protected health information from which 16 specific identifiers have been removed.[61]

Managed care. Managed care is an arrangement that integrates healthcare financing and delivery wherein payers contract with or employ providers to deliver a defined set of services to beneficiaries at an agreed-upon per-capita or per-service price.[62]

Medicaid. Medicaid is a jointly funded, federal-state program established under the Social Security Act in 1965 to provide health insurance to certain low-income families and individuals.[63]

Medical device (for purposes of FDA Research regulations). A medical device is an article, component part, or accessory that is: recognized in the official National Formulary or the United States Pharmacopoeia; intended for use in diagnosing diseases or other conditions, intended for use in curing, mitigating, treating, or preventing disease; or intended to affect the structure or any function of the body without relying primarily on chemical action within or on the body or on being metabolized.[64]

Medicare. Medicare is a federal program established in 1965 under the Social Security Act that provides government-sponsored health insurance to individuals aged 65 and older and certain individuals under age 65 with disabilities that meet federal requirements.[65]

Memorandum of Understanding (MOU). An MOU is a non-legally binding, formal agreement creating a relationship between two or more entities that outlines agreed-upon duties and responsibilities for each party in the context of the established relationship.

Minimal risk (with respect to the Common Rule). Minimal risk refers to a classification for a research protocol indicating that the probability and magnitude of harm or discomfort anticipated in the research is equal to or less than the probability and magnitude of harm or discomfort ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.

Minor. A minor is an individual who has not attained the age of majority specified under applicable state law, or if no age of majority is specified under applicable state law, 18 years of age.

National Committee for Quality Assurance (NCQA). NCQA is a private, non-profit organization that develops quality standards and performance measures for a broad range of healthcare entities and accredits health plans issued in all 50 states, the District of Columbia, and Puerto Rico.[66]

National Provider Identifier (NPI). The NPI is a unique identification number for healthcare providers issued by the Centers for Medicare and Medicaid Services (CMS) that is used by providers, health plans, and healthcare clearinghouses in administrative and financial transactions as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)'s Administrative Simplification provisions.[67]

National Quality Forum (NQF). NQF is a non-profit, nonpartisan, membership-based organization that endorses healthcare measures, advises the federal government and private sector payers on optimal measures for use in specific payment and accountability programs, and provides reports and tools and hosts events for healthcare decision-makers on performance measurement.[68]

Navigator. A navigator is an individual or organization trained to help consumers and small businesses and their employees look for health coverage options through the Marketplace, including completing eligibility and enrollment forms.[69]

Notice of Proposed Rulemaking (NPRM). An NPRM is the official document published in the *Federal Register* that announces and explains a federal agency's plan to address a problem or accomplish a goal and that gives the public an opportunity to submit feedback. [70] A proposed rule and the public comments received in response form the basis of the Final Rule.

Office of the National Coordinator for Health Information Technology (ONC). ONC is an office within the Office of the Secretary for the U.S. Department of Health and Human Services (HHS) charged with coordinating nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information.[71]

Office for Civil Rights (OCR). OCR is an office within the U.S. Department of Health and Human Services (HHS) that is responsible for enforcing laws against discrimination by certain healthcare and human service providers[72] as well as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules.[73]

Opt-in. Opt-in refers to technologies that require a self-selected choice to purposefully accept a situation or condition ahead of participation or receipt of services.[74]

Opt-out. Opt-out refers to technologies that assume user inclusion unless users explicitly state a decision to leave or withdraw from services.[75]

Patient (with respect to 42 C.F.R. Part 2). A patient is any individual who has applied for, is receiving, or has been given diagnosis, treatment, or referral for treatment for a substance use disorder at a Part 2 program.[76]

Patient Identifying Information (with respect to 42 C.F.R. Part 2). Patient identifying information means the name, address, social security number, fingerprints, photograph, or similar information by which the identity of a Part 2 program patient can be determined with reasonable accuracy either directly or by reference to other information.[77]

Patient Protection and Affordable Care Act (PPACA or ACA). The ACA is a law enacted in 2010 that represented a significant overhaul of the United States healthcare system, primarily focused on reducing the uninsured population through expanding Medicaid and developing a more robust individual healthcare marketplace, improving healthcare quality, and decreasing healthcare costs.[78]

Patient Registry. A patient registry is an organized system for the collection, storage, retrieval, analysis, and dissemination of information on individual persons who have a particular disease, a condition that predisposes them to the occurrence of a health-related event, or prior exposure to substances or circumstances known or suspected to cause adverse health effects.[79]

The Patient Safety and Quality Improvement Act of 2005 (PSQIA). PSQIA is a law creating a voluntary program for providers to share information with patient safety organizations related to patient safety events and imposing confidentiality and privilege requirements on such information to encourage providers to share the information without fear of liability.[80]

Patient-Centered Outcomes Research (PCOR). PCOR is a type of research comparing different medical treatments and interventions to provide evidence on the strategies that are most effective in different populations and situations, with the goal of empowering patients and their doctor(s) with additional information to make sound healthcare decisions.[81]

Payment (with respect to the HIPAA Rules). Payment includes the following functions undertaken by a health plan:[82]

(1) Activities to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan;
(2) Activities undertaken by a healthcare provider or health plan to obtain or provide reimbursement for the provision of health care and adjudication or subrogation of health benefit claims;
(3) Risk-adjusting amounts due based on enrollee health status and demographic characteristics;
(4) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related healthcare data processing;
(5) Reviewing healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
(6) Utilization review activities, including precertification and preauthorization of services and concurrent and retrospective review of services; and
(7) Disclosure of certain protected health information (PHI) to consumer reporting agencies relating to collection of premiums or reimbursement.

Person. A person is a natural individual, trust or estate, professional association, partnership, corporation, federal, state or local government agency, or any other legal entity, public or private.[83]

Personal health record (PHR). A PHR is an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in his or her own health care.[84]

Primary Health Services (with respect to Community Health Centers).[85] Primary health services at CHCs means all of the following services:

(1) Diagnostic, treatment, consultative, referral, and other services rendered by physicians, and/or physician's extenders;
(2) Diagnostic laboratory services and diagnostic radiologic services;
(3) Preventive health services;
(4) Emergency medical services;
(5) Transportation services as needed for adequate patient care, sufficient so that residents of the catchment area served by the center with special difficulties of access to services provided by the center receive such services; and
(6) Preventive dental services provided by a licensed dentist or other qualified personnel and the prescription of fluorides for systemic use when not available in the community water supply.

Prior authorization. Prior authorization is a tool used by a health plan requiring a healthcare provider to request approval before prescribing a drug for or providing a healthcare service to a patient in order for the drug or service to qualify for coverage under the terms of the patient's benefit plan.[86]

The Privacy Act of 1974. The Privacy Act governs the collection, use, and disclosure of personally identifiable information about individuals maintained in a system of records by federal agencies, where the records are retrievable by a personal identifier (such as an individual's name or social security number).[87]

Privacy Board. A Privacy Board is a review body established to act upon requests for a waiver or an alteration of the HIPAA Privacy Rule's authorization requirement for uses and disclosures of protected health information (PHI) for a particular research study.[88]

Private information (for purposes of the Common Rule). Private information is information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public.[89]

Program (with respect to 42 C.F.R. Part 2). Under Part 2, the term "program" means:

(1) An individual or entity (other than a general medical facility) or an identified unit within a general medical facility that holds itself out as providing and does provide substance use disorder diagnosis, treatment, or referral for treatment; or
(2) Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.[90]

Program Director (with respect to 42 C.F.R. Part 2). Under Part 2, the term "program director" means an individual (if the Part 2 program is that individual) or, if the Part 2 program is an entity, the individual designated as director or managing director or the individual otherwise vested with authority to act as chief executive officer of the Part 2 program.[91]

Protected Health Information (**PHI**) (with respect to the HIPAA Rules). PHI is individually identifiable information created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse and that relates to:

(1) The provision of care to an individual;
(2) An individual's past, present, or future physical or mental health condition; or
(3) An individual's payment for care, whether made in the past or present or expected in the future.[92]

Psychotherapy Notes (with respect to the HIPAA Rules). Psychotherapy notes are notes recorded by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record.[93]

Public health authority. A public health authority is an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, an Indian tribe, a foreign government, or a person or entity acting under a grant of authority from or contract with such public agency that is responsible for public health matters as part of its official mandate.[94]

Qualified Entity (QE). QEs are entities certified under the Medicare Qualified Entity Certification Program (QECP) and authorized to: obtain Medicare fee-for-service Parts A and B claims data and Part D prescription drug event data to generate reports for providers and suppliers on performance measures; to make performance reports available to the public; to provide or sell non-public reports or combined data; and to provide Medicare data at no cost to certain authorized users.[95]

Qualified health plan (QHP). A QHP is an insurance plan that is certified by the Health Insurance Marketplace, provides essential health benefits, follows established limits on cost-sharing (like deductibles, copayments, and out-of-pocket maximum amounts), and meets other requirements. A qualified health plan will have a certification by each Marketplace in which it is sold.

Qualified Service Organization (QSO) (with respect to 42 C.F.R. Part 2). A QSO is an individual or entity that provides services to a Part 2 program and has a written agreement with the program agreeing that it will comply with Part 2 requirements regulations when dealing with patient records from the program.[96]

Quality Improvement Organization (QIO). A QIO is a private, usually non-profit organization made up of health quality experts, clinicians, and consumers that reviews medical care, helps Medicare beneficiaries with quality-of-care complaints, and implements quality improvement strategies.[97]

Records (with respect to 42 C.F.R. Part 2). Under Part 2, the term "records" means any information (recorded or not) that is created by, received, or acquired by a Part 2 program relating to a patient.[98]

Regional Health Information Organization (RHIO). A RHIO is a type of health information exchange organization (HIO) that brings together healthcare stakeholders within a defined geographic area and governs health information exchange among them for the purpose of improving health and care in the community.[99]

Regulated Entities (with respect to the HIPAA Rules). The term "regulated entities" is a collective term used to refer to Covered Entities (CEs) and Business Associates (BAs) under HIPAA.

Research. Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.[100]

Rural Health Clinic (RHC). An RHC is a healthcare organization certified by the Medicare program to furnish primary care and preventive services in rural and underserved areas at a special payment rate, with the goals of addressing the lack of physician supply in rural areas. RHCs primarily serve Medicare patients and promote the use of non-physician practitioners in rural areas.[101]

Social Security Act. The SSA is a 1935 law establishing a federal old-age pension system that has been amended and expanded numerous times, including to establish the Medicare, Medicaid, and S-CHIP programs, and to provide funding to states to offer public health services to certain vulnerable populations and administer state unemployment compensation laws.[102]

Substance Abuse and Mental Health Services Administration (SAMHSA). SAMHSA is an agency within the U.S. Department of Health and Human Services (HHS) that leads public health efforts to advance the behavioral health of the nation and aims to reduce the impact of substance abuse and mental illness on U.S. communities.[103]

Substance use disorder (with respect to 42 C.F.R. Part 2). Under Part 2, the term "substance use disorder" means a cluster of cognitive, behavioral, and physiological symptoms indicating that the individual continues using the substance despite significant substance-related problems such as impaired control, social impairment, risky use, and pharmacological tolerance and withdrawal.[104]

Supplemental Health Services (with respect to Community Health Centers).[105] At CHCs, supplemental health services are non-primary health services that are:

(1) Inpatient and outpatient hospital services;
(2) Home health services;
(3) Extended care facility services;
(4) Rehabilitative services and long-term physical medicine;
(5) Mental health services;
(6) Dental services other than those provided as primary health services;
(7) Vision services;
(8) Allied health services;
(9) Pharmaceutical services;
(10) Therapeutic radiologic services;
(11) Public health services;
(12) Ambulatory surgical services;
(13) Health education services;
(14) Services, including the services of outreach workers, which promote and facilitate optimal use of primary health services and the above 13 services; or
(15) Services of outreach workers and other personnel fluent in the language or languages spoken by individuals in the population served by the Center, if a substantial number of such individuals are of limited English-speaking ability.

Supplemental Notice of Proposed Rulemaking (SNPRM). An SNPRM is a notice and request for public comment published in the Federal Register when an agency has made significant substantive changes to a proposed rule between issuance of the original Notice of Proposed Rulemaking (NPRM) and the subsequent Final Rule.[106]

System of records (for purposes of the Privacy Act of 1974). A system of records is a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.[107]

Test article. A test article is any drug (including a biological product for human use), medical device for human use, human food additive, color additive, electronic product, or any other article subject to regulation under the Food Drug and Cosmetics Act or under sections 351 and 354-360F of the Public Health Service Act.[108]

Title 21 C.F.R. Part 50—Protection of Human Subjects (FDA). These regulations apply to all clinical investigations regulated by the Food and Drug Administration (FDA) under the Food, Drug, and Cosmetic Act, as well as clinical investigations that support applications for research or marketing permits for products regulated by the FDA (including foods, dietary supplements that bear a nutrient content claim

or a health claim, infant formulas, food and color additives, drugs for human use, medical devices for human use, biological products for human use, and electronic products).[109]

Title 21 C.F.R. Part 54—Financial Disclosure by Clinical Investigators (FDA). These regulations require an applicant whose submission relies in part on clinical data to disclose certain financial arrangements between the sponsor(s) of the covered studies and the clinical investigators and certain interests of the clinical investigators in the product under study or in the sponsor of the covered studies.[110]

Title 21 C.F.R. Part 56—Institutional Review Boards (FDA). These regulations include general standards for the composition, operation, and responsibility of an Institutional Review Board (IRB) that reviews clinical investigations regulated by the Food and Drug Administration (FDA) under the Food, Drug, and Cosmetic Act, as well as clinical investigations that support applications for research or marketing permits for products regulated by the Food and Drug Administration (e.g., foods, dietary supplements that bear a nutrient content claim or a health claim, infant formulas, food and color additives, drugs for human use, medical devices for human use, biological products for human use, and electronic products).[111]

Title 21 C.F.R. Part 312—Investigational New Drug Application (FDA). These regulations govern all clinical investigations of products subject to section 505 of the Food, Drug, and Cosmetic Act or to the licensing provisions of the Public Health Service Act.[112]

Treating provider relationship (with respect to 42 C.F.R. Part 2). A treating provider relationship is where a patient is, agrees to, or is legally required to be diagnosed, evaluated, and/or treated, or agrees to accept consultation for any condition by an individual or entity that undertakes or agrees to undertake diagnosis, evaluation, and/or treatment of the patient or consultation with the patient, for any condition.[113]

Treatment (with respect to 42 C.F.R. Part 2). Under Part 2, the term "treatment" means care of a patient suffering from a substance use disorder, a condition which is identified as having been caused by the substance use disorder, or both, in order to reduce or eliminate the adverse effects upon the patient.[114]

Treatment (with respect to the HIPAA Rules). Under HIPAA, the term "treatment" means the provision, coordination, or management of health care and related services by one or more healthcare providers, including the coordination or management of health care by a healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for health care from one healthcare provider to another.[115]

U.S. Department of Health and Human Services (HHS). HHS is a federal department tasked with enhancing and protecting the health and well-being of all Americans by providing for effective health and human services and fostering advances in medicine, public health, and social services.[116]

Use (with respect to the HIPAA Rules). Under HIPAA, the term "use" means the sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information.[117]

Utilization Review. Utilization review is a tool utilized by health plans involving a critical evaluation by a healthcare provider of healthcare services provided to patients for purposes of controlling costs and monitoring care quality.

42 C.F.R. Part 2. Part 2 is a federal regulation that restricts the use and disclosure of substance use disorder patient records maintained in connection with the performance of any Part 2 program (i.e., a federally assisted program that provides substance use disorder diagnosis, treatment, or referral for treatment).[118]

REFERENCES

[1] Centers for Medicare & Medicaid Services (CMS). "Accountable Care Organizations (ACO)" (*last updated* May 12, 2017), *available at:* https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html.

[2] Office of the Federal Register. A Guide to the Rulemaking Process (2011), *available at*: https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

[3] Agency for Healthcare Research & Quality [home page], *available at:* https://www.ahrq.gov/ (*last visited* September 27, 2017).

[4] The American Recovery and Reinvestment Act (ARRA), P.L. 111-5, 123 Stat. 115 (2009); CMS, "Electronic Health Records (EHR) Incentive Programs" (*last updated* September 11, 2017), *available at:* https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms.

[5] U.S. Department of Health and Human Services (HHS), Office of the Secretary, The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report:

Ethical Principles and Guidelines for the Protection of Human Subjects of Research (1979); *available at:* https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html.

[6] 45 C.F.R. Part 46, Subparts A-E (2017).

[7] 45 C.F.R. § 160.103.

[8] Center for Medicare and Medicaid Innovation (CMMI), *available at:* https://innovation.cms.gov/ (*last visited* September 27, 2017).

[9] Centers for Medicare & Medicaid Services (CMS) [home page], *available at:* https://www.cms.gov/ (*last visited* September 27, 2017).

[10] 45 C.F.R. § 46.102.

[11] Social Security Act Volume I, Title 19, codified at 42. U.S.C. §§ 1396 –1396v.

[12] 42 C.F.R. § 51c.102.

[13] 42 U.S.C. § 254a.

[14] National Information Center on Health Services Research and Health Care Technology (NICHSR), "NLM Resources for Informing Comparative Effectiveness" [citing Federal Coordinating Council for Comparative Effectiveness Research definition] (June 26, 2009), *available at:* https://www.nlm.nih.gov/nichsr/cer/cerqueries.html#definition.

[15] HHS, "What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule (*last updated* July 26, 2013), *available at:* https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html.

[16] 45 C.F.R. § 160.103.

[17] 45 C.F.R. § 164.514(e)(4).

[18] 45 C.F.R. § 46.102.

[19] 42 C.F.R. § 2.11.

[20] 45 C.F.R. § 164.103.

[21] 34 C.F.R. § 99.3.

[22] The National Alliance for Health Information Technology, "Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information" (April 28, 2008). *Available online at*: http://www.hitechanswers.net/wp-content/uploads/2013/05/NAHIT-Definitions2008.pdf.

[23] 29 C.F.R. § 1635.3.

[24] HHS, Office for Human Research Protections (OHRP), "OHRP Expedited Review Categories (1998)" (*last updated* March 21, 2016), *available at:* https://www.hhs.gov/ohrp/regulations-and-policy/guidance/categories-of-research-expedited-review-procedure-1998/index.html.

[25] U.S. Department of Homeland Security, Privacy Office, Memorandum: "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security" (December 29, 2008), *available at:* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[26] Family Educational Rights and Privacy Act (FERPA) of 1974 (codified at 20 U.S.C. 1232g; implementing regulations at 34 C.F.R. Part 99).

[27] 29 C.F.R. § 1635.3.

[28] Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3544 (2006).

[29] 15 U.S.C. § 45.

[30] 42 C.F.R. § 2.11.

[31] OHRP, "Federalwide Assurances (FWAs)," (*last updated* March 18, 2016), *available at:* https://www.hhs.gov/ohrp/federalwide-assurances-fwas.html.

[32] Office of the Federal Register. A Guide to the Rulemaking Process (2011), *available at*: https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

[33] The Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (amending 5 U.S.C. 552) (1966).

[34] 29 C.F.R. § 1635.3.

[35] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (Title I amended scattered provisions of 29 U.S.C. § 1182 et seq., 42 U.S.C. § 300gg-1 et seq., 42 U.S.C. § 1395ss, 42 U.S.C. § 1320d-9, and 26 U.S.C. § 9802 et seq.; Title II is codified at 42 U.S.C. 2000f et seq.); implementing regulations found throughout the Code of Federal Regulations.

[36] 29 C.F.R. § 1635.3.

[37] 26 U.S.C. § 5000.

[38] 45 C.F.R. § 160.103.

[39] 45 C.F.R. § 160.103.

[40] 45 C.F.R. § 160.103.

[41] 45 C.F.R. § 160.103.

[42] 45 C.F.R. § 160.103.

[43] ARRA, Pub. L. No. 111-5, Div. A, Title XIII, § 13410(e), 123 Stat. 271-76 (2009).

[44] HIPAA, Pub. L. No. 104-191, 110 Stat. 139 (1996) (codified as amended in scattered sections of 42 U.S.C.).

[45] 26 U.S.C. § 9832.

[46] 45 C.F.R. § 160.103.

[47] 45 C.F.R. § 160.103.

[48] Health Resources & Services Administration (HRSA), "About HRSA," *available at:* https://www.hrsa.gov/about/ (*last visited* September 27, 2017).

[49] 45 C.F.R. § 46.102.

[50] 21 C.F.R. § 50.3(g).

[51] 45 C.F.R. § 46.102.

[52] 45 C.F.R. § 46.102.

[53] 45 C.F.R. § 160.103.

[54] 45 C.F.R. § 160.103.

[55] Centers for Disease Control and Prevention (CDC). International Classification of Diseases: 10th Revision (ICD-10) (2001), *available at*: https://www.cdc.gov/nchs/data/dvs/icd10fct.pdf; *see also* World Health Organization (WHO). "Classifications: International Classification of Diseases (ICD) Information Sheet," *available at*: http://www.who.int/classifications/icd/factsheet/en/ (*last visited* September 26, 2017).

[56] CDC National Center for Health Statistics. "Classification of Diseases, Functioning, and Disability: International Classification of Diseases, (ICD-10-CM/PCS) Transition—Background" (*last updated* October 1, 2015), *available at*: https://www.cdc.gov/nchs/icd/icd10cm_pcs_background.htm

[57] U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC). "Frequently Asked Questions: What does "interoperability" mean and why is it important?" (*last updated* January 15, 2013), *available at*: https://www.healthit.gov/providers-professionals/faqs/what-does-interoperability-mean-and-why-it-important.

[58] *See, e.g.,* Food and Drug Administration (FDA). "Institutional Review Boards Frequently Asked Questions—Information Sheet: Guidance for Institutional Review Boards and Clinical Investigators" at § I: IRB Organization, Question 1 (*last updated* January 25, 2016), *available at*: https://www.fda.gov/RegulatoryInformation/Guidances/ucm126420.htm.

[59] "Common Rule" Departments and Agencies. Final Rule: Federal Policy for the Protection of Human Subjects Research. (2017) 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(h)).

[60] 82 Fed. Reg. 7149 at 7260 (to be codified at 45 C.F.R. § 46.102(i)).

[61] 45 C.F.R. § 160.103 at "Limited data set" (2017).

[62] *See, e.g.*, Sekhri NK. Managed Care: The US Experience. *Bulletin of the World Health Organization,* 78(6): 830-44 at 831 (2000). *Available online at*: http://www.who.int/bulletin/archives/78(6)830.pdf.

[63] Social Security Act Volume I, Title 19, codified at 42. U.S.C. §§ 1396 –1396v.

[64] FDA. "Is The Product A Medical Device?" (*last updated* September 12, 2014), *available at:* https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm.

[65] *See, e.g.,* Social Security Administration. "Medicaid Information: What Is Medicaid?" *available at*: https://www.ssa.gov/disabilityresearch/wi/medicaid.htm (*last visited* September 26, 2017).

[66] National Committee for Quality Assurance (NCQA). "About NCQA: Overview," *available at*: http://www.ncqa.org/about-ncqa (*last visited* September 26, 2017).

[67] *See, e.g.,* HHS Office for the Assistant Secretary of Planning and Evaluation (ASPE). "Frequently Asked Questions About the National Provider Identifier (NPI)," at "What Is the National Provider Identifier (NPI)?" (2000), *available at*: https://aspe.hhs.gov/report/frequently-asked-questions-about-national-provider-identifier-npi

[68] National Quality Forum (NQF). "What We Do," *available at*: http://www.qualityforum.org/what_we_do.aspx (*last visited* September 26, 2017).

[69] Centers for Medicare & Medicaid Services (CMS). "Glossary: Navigator," *available at*: https://www.healthcare.gov/glossary/navigator/ (*last visited* September 26, 2017).

[70] Office of the Federal Register. A Guide to the Rulemaking Process (2011), *available at*: https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

[71] HHS Office of the National Coordinator for Health Information Technology (ONC). "Newsroom: About ONC" (*last updated* May 12, 2016), *available at*: https://www.healthit.gov/newsroom/about-onc.

[72] OCR. "Civil Rights for Individuals and Advocates" (*last updated* October 28, 2015), *available at*: https://www.hhs.gov/civil-rights/for-individuals/index.html.

[73] OCR. "HIPAA Enforcement" (*last updated* July 25, 2017), *available at* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html.

[74] HHS Assistant Secretary for Administration (ASA) Office of the Chief Information Officer (OCIO). Implementation of OMB M-10-22 and M-10-23 (2010), *available at*: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/implementation-of-omb-m-10-22-and-m-10-23/index.html.

[75] OCIO. Implementation of OMB M-10-22 and M-10-23 (2010), *available at*: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/implementation-of-omb-m-10-22-and-m-10-23/index.html.

[76] 42 C.F.R. § 2.11 at "Patient" (2017).

[77] 42 C.F.R. § 2.11 at "Patient identifying information" (2017).

[78] Patient Protection and Affordable Care Act, Pub. L. No. 111-148 (2010).

[79] National Committee on Vital and Health Statistics (NCVHS). "Frequently Asked Questions About Medical and Public Health Registries" (2012), *available at*: http://ncvhs.hhs.gov/9701138b.htm.

[80] Patient Safety and Quality Improvement Act (PSQIA), Pub. L. No. 109-41, 119 Stat. 424 (amending scattered sections of the Public Health Services Act at 42 U.S.C. 299 *et seq*.) (2005).

[81] Healthcare.gov "Glossary: Patient-Centered Outcomes Research," *available at*: https://www.healthcare.gov/glossary/patient-centered-outcomes-research/ (*last visited* September 27, 2017).

[82] 45 C.F.R. § 160.103 at "Payment" (2017).

[83] *See, e.g.*, 45 C.F.R. § 160.103 at "Person" (2017) (with respect to the HIPAA Rules) and 42 C.F.R. § 2.11 at "Person" (2017) (with respect to Part 2).

[84] OCR. Personal Health Records and the HIPAA Privacy Rule at p. 1 (2016), *available at*: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

[85] 42 C.F.R. § 51c.102(h) (2017).

[86] *See, e.g.*, Academy of Managed Care Pharmacy. Concepts in Managed Care Pharmacy: Prior Authorization at p. 1 (2012), *available at*: http://www.amcp.org/prior_authorization/.

[87] The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a).

[88] HHS National Institutes of Health (NIH). Privacy Boards and the Privacy Rule at p. 2 (*last updated* 2004), *available at*: https://privacyruleandresearch.nih.gov/pdf/privacy_boards_hipaa_privacy_rule.pdf.

[89] 82 Fed. Reg. at 7260 (to be codified at 45 C.F.R. § 46.102(e)(4)).

[90] 42 C.F.R. § 2.11 (2017).

[91] 42 C.F.R. § 2.11 (2017).

[92] 45 C.F.R. § 160.103 at "Protected health information" (2017).

[93] 45 C.F.R. § 160.103 at "Psychotherapy notes" (2017).

[94] 82 Fed. Reg. at 7260 (to be codified at 45 C.F.R. § 46.102(k)).

[95] *See, e.g.*, CMS Qualified Entity Certification Program. QECP Frequently Asked Questions (FAQs), at pp. 1-2 (*last updated* 2017), *available at*: https://www.qemedicaredata.org/QECP_Docs/QECP_FAQS%20__9.15.2017.pdf.

[96] 42 C.F.R. § 2.11 at "Qualified service organization" (2017).

[97] CMS. "Quality Improvement Organization" at 'What Are QIOs?' (*last updated* November 30, 2016), *available at*: https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityImprovementOrgs/index.html?redirect=/QualityImprovementOrgs/.

[98] 42 C.F.R. § 2.11 at "Records" (2017).

[99] *See generally*, Healthcare Information and Management Systems Society (HIMSS). "Privacy & Security for RHIOs/HIEs," *available at*: http://www.himss.org/privacy-security-rhioshies-0 (*last visited* September 27, 2017).

[100] 82 Fed. Reg. at 7260-61 (to be codified at 45 C.F.R. § 46.102(l)) and 45 C.F.R. § 160.103 at "Research" (2017).

[101] *See generally* CMS. Rural Health Clinic (2017), *available at*: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/RuralHlthClinfctsht.pdf.

[102] Martin PP and Weaver DA. Social Security: A Program and Policy History. *Social Security Bulletin* 66(1) (2005), *available at*: https://www.ssa.gov/policy/docs/ssb/v66n1/v66n1p1.html.

[103] Substance Abuse and Mental Health Services Administration (SAMHSA). "About Us," *available at*: https://www.samhsa.gov/about-us (*last visited* September 27, 2017).

[104] 42 C.F.R. § 2.11 at "Substance use disorder" (2017).

[105] 42 C.F.R. § 51c.102(j) (2017).

[106] 33 C.F.R. § 1.05-40 (2017).

[107] 5 U.S.C. § 552a (2017).

[108] 21 C.F.R. § 50.3(j) (2017).

[109] 21 C.F.R. Part 50 (2017).

[110] 21 C.F.R. Part 54 (2017).

[111] 21 C.F.R. Part 56 (2017).

[112] 21 C.F.R. Part 312 (2017).

[113] 42 C.F.R. § 2.11 at "Treating provider relationship" (2017).

[114] 42 C.F.R. § 2.11 at "Treatment" (2017).

[115] 45 C.F.R. § 160.103 at "Treatment" (2017).

[116] HHS. "About HHS," *available at*: https://www.hhs.gov/about/ (*last visited* September 27, 2017).

[117] 45 C.F.R. § 160.103 at "Use" (2017).

[118] *See generally* 42 C.F.R. § 2.2 (2017).