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.

[1] 45 C.F.R. § 160.103 (2017).

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			

[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)).

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

---

[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 Plan2015-2020 (2015), *available at* https://www.healthit.gov/sites/default/files/9-5 federalhealthitstratplanfinal_0.pdf.

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.