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

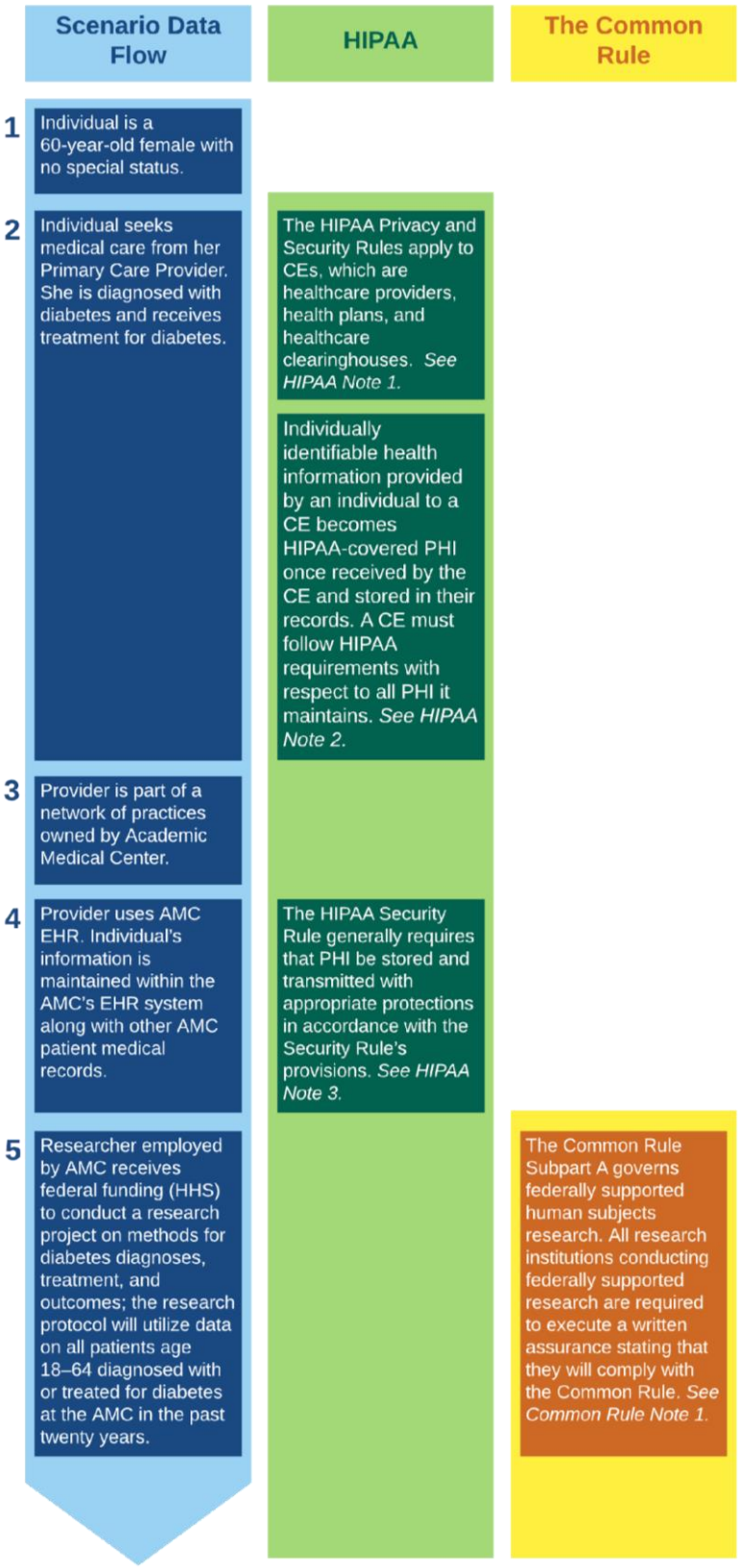
Scenario Narrative:

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)

	Scenario Data Flow	HIPAA	The Common Rule	42 C.F.R. Part 2
5	Health Plan has a BAA with a Coordinating Center to conduct data aggregation and other initiatives on its behalf.	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.*		Any recipient of Part 2 information is prohibited from re-disclosing it except as allowed by Part 2. *See Part 2 Note 2.*
6	Program has QSOA with Coordinating Center to provide it with data processing, data aggregation, and other professional services			A QSO is an entity that provides services to a Part 2 program; a QSOA is required between a program and a QSO. *See Part 2 Note 4.*
7	Researcher at independent Research Institution receives a federal grant to assess the cost-effectiveness and comparative effectiveness of several treatments, comparing pharmaceuticals and psychosocial treatment for opioid dependence.		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.*	
8	Researcher plans to request the following elements drawn from Part 2 Program clinical data and Health Plan claims data and compiled by Coordinating Center into an LDS: Age, All Diagnoses, Dates of Service, Treatments Received, and Cost of Services Provided.	An LDS is PHI that has had certain identifiers removed but is still considered PHI for purposes of HIPAA because it is not fully de-identified. *See HIPAA Note 7.* 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.* A researcher may obtain PHI for research without the subject's authorization under four circumstances. *See HIPAA Note 10.*		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 is subject to disclosure restrictions. *See Part 2 Note 1.*

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

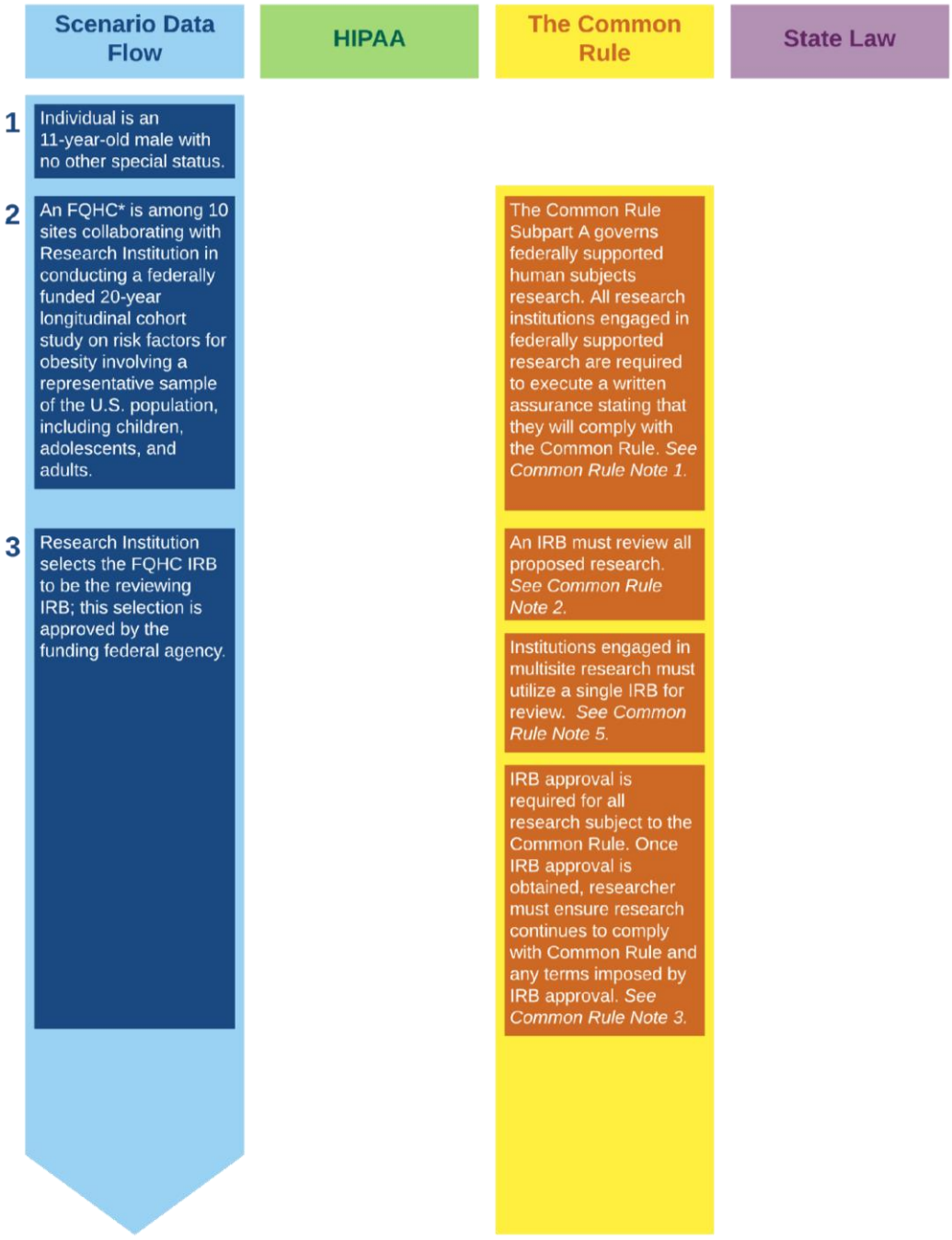
Scenario Narrative:

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.

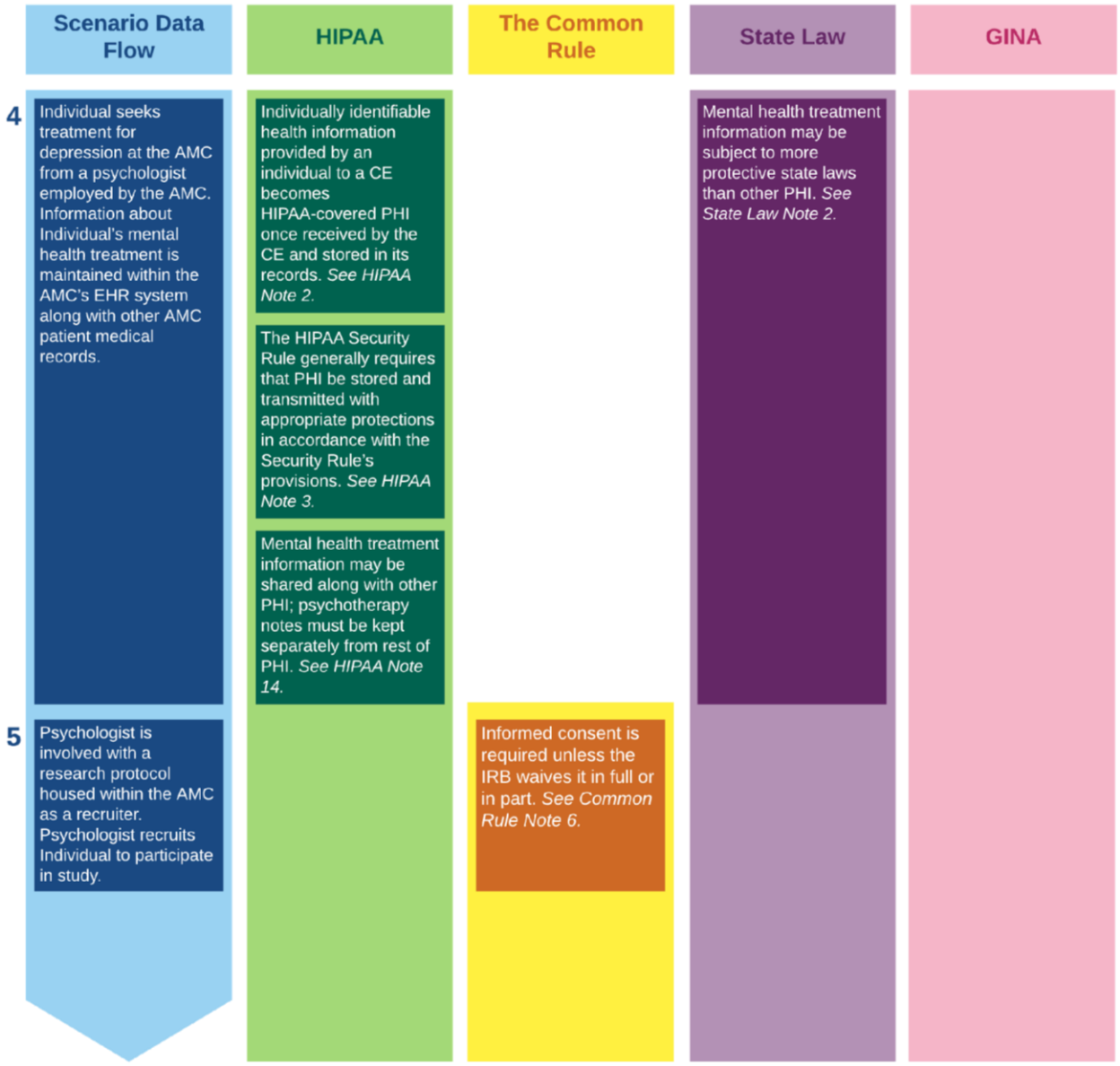
Statutes/Regulations implicated: HIPAA, Common Rule, State Law, GINA

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

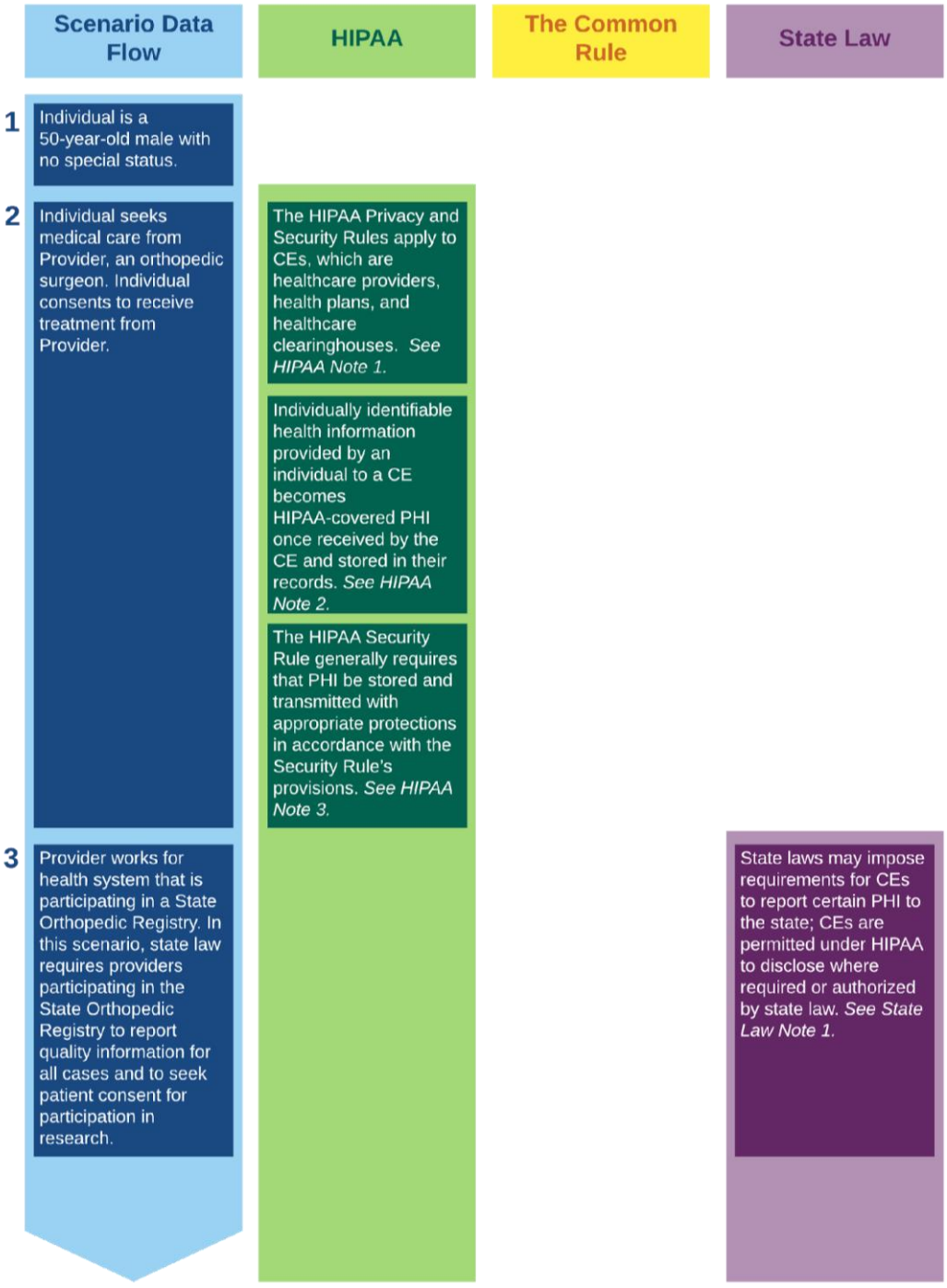
Scenario Narrative:

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

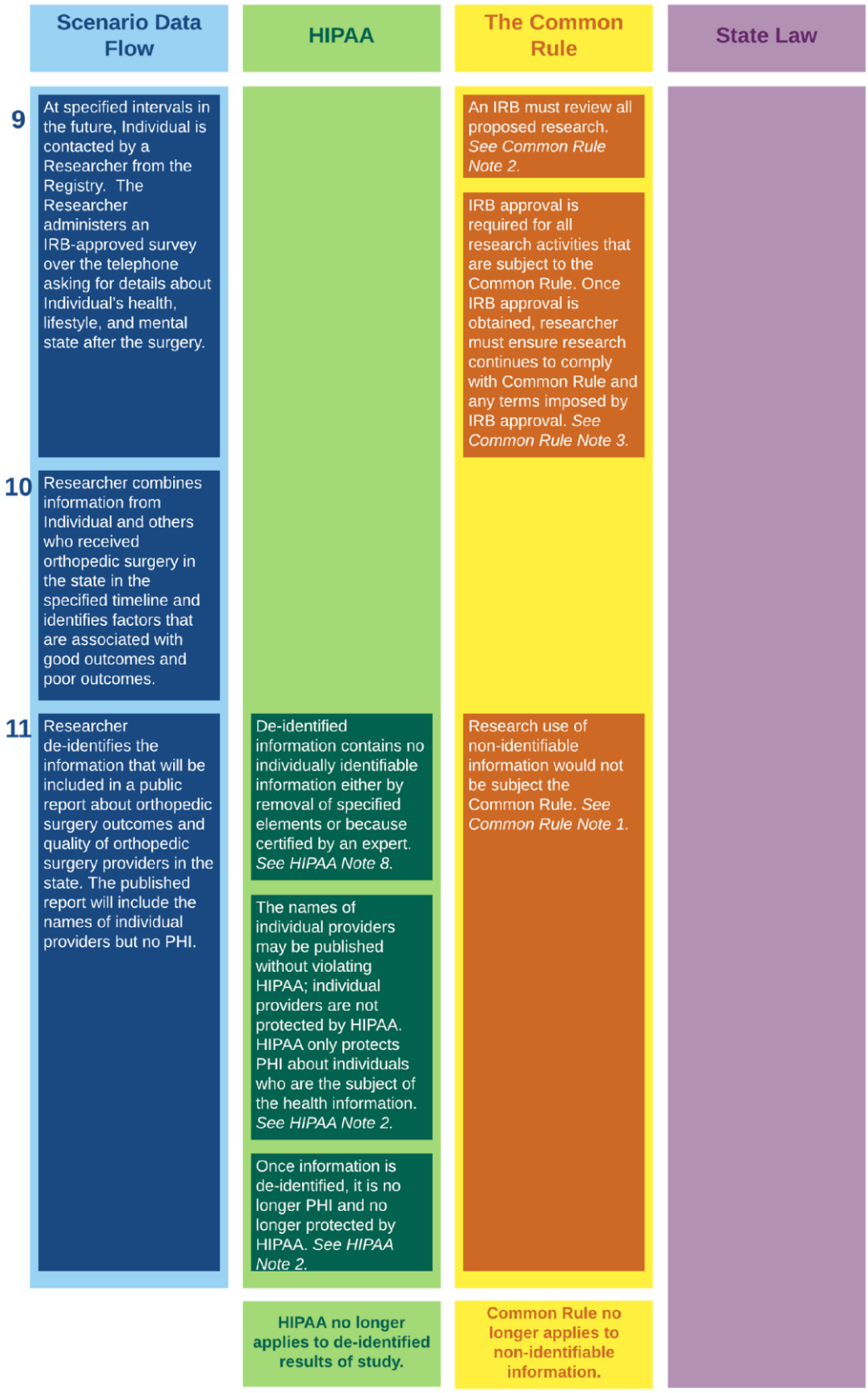
Data Flow 5—Use Case 5: Research Using Patient-Generated Health Data



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/.