



The Office of the National Coordinator for
Health Information Technology

Milken Institute School
of Public Health

THE GEORGE WASHINGTON UNIVERSITY

Legal and Ethical Architecture for PCOR Data

NIH Collaboratory Grand Rounds

April 6, 2018

Jane Hyatt Thorpe, Lara Hartwright-Smith, Elizabeth Gray

The George Washington University Milken Institute School of Public Health



@ONC_HealthIT



@HHSOnc



Agenda

- Introductions
- Project Overview: PCOR Privacy and Security Research Scenario Initiative and Legal Analysis and Ethics Framework Development Project
- Final Product: Legal and Ethical Architecture for PCOR Data

Project Overview

The PCOR Privacy and Security Research Scenario Initiative and Legal Analysis and Ethics Framework Development project supported the development of a legal and ethical architecture to enable robust PCOR while providing sufficient assurance to stakeholders that data used for PCOR and CER will be protected and secured as required by applicable statutes and regulations.

Funded by: The U.S. Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC)

Project Overview, cont'd

Phase 1:

- Convene discussions with stakeholders in PCOR community.
- Develop research scenarios and data use cases.

(Led by NORC)

Phase 2:

- Assess the legal, regulatory, and policy environment governing the use of health information for PCOR/CER.
- Develop a legal and ethical framework and architecture for access to data for PCOR while protecting patient privacy.

(Led by the George Washington University)

Legal and Ethical Architecture for PCOR Data

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

Legal and Ethical Architecture for PCOR Data

- Technology-neutral
 - » Does not address or recommend any particular technology or technical standards
- Reference Resource
 - » Does not constitute legal advice and should not be used as a substitute for legal advice or guidance
 - » Does not present single path; rather provides tools to help researchers and other stakeholders identify and navigate legal and ethical requirements that may vary depending upon the data needs of a particular research project
 - » Users advised to always consider state-specific statutes and regulations that may vary, in addition to federal law
- Longevity
 - » Legal analysis is current as of September 28, 2017. Users encouraged through-out Architecture to review status of statutes and regulations (e.g., Common Rule) as well as any relevant guidance.

Designed for Broad Audience

- Primary Audience
 - » Researchers engaged in PCOR and CER
 - » IRBs
 - » Contracting Officers
 - » Research and Development Officers
 - » Compliance and Privacy Officers
 - » Internal/External Legal Counsel
- Wider Audience
 - » Federal and state legislative and regulatory bodies
 - » Foundations and other organizations that fund research
 - » Policy analysts
 - » Patient advocates
 - » Lawmakers
 - » Academics
 - » Students

Architecture Overview

- Chapter 1: Overview
- Chapter 2: Legal and Ethical Significance of Data for PCOR
- Chapter 3: Linking Legal and Ethical Requirements to PCOR Data
- Chapter 4: Framework for Navigating Legal and Ethical Requirements for PCOR
- Chapter 5: Mapping Research Data Flows to Legal Requirements
- Appendices
 - » A: Summary of Statutes and Regulations Relevant to PCOR
 - » B: Assessing Potential Barriers and Ambiguity in the Legal Landscape
 - » C: Selected Federal Initiatives
 - » D: Selected Federal Resources
 - » E: Glossary

- **Overview of legal and ethical considerations relevant to PCOR**
- **Background**
 - » Architecture Development
 - » Audience
- **How to Navigate and Use the Architecture**

Chapter 2: Legal and Ethical Significance of Data for PCOR

- **Identifies relevant legal and ethical questions; answers provide foundation for the Architecture**
 - » Legal and ethical requirements vary depending on type of data sought, accessed, or used by a researcher
- **Identifies key characteristics of health information used for PCOR**
 - » Identifiability, Content, Subject, Source, Access, Use/Purpose, Consent/Authorization, Security, and Legal Status
- **Describes the types of health information data relevant to PCOR**
 - » *Includes: clinical data, administrative data, patient-generated health data (PGHD), patient reported outcomes (PROs), genetic information, biospecimens, surveillance data, and quality improvement data*

Why would a stakeholder use Chapter 2?

To identify and understand the legally relevant characteristics of data necessary for PCOR as well as the types of data commonly used for PCOR.

Chapter 3: Linking Legal and Ethical Requirements to PCOR Data

- **Links specific legal requirements to key questions and data characteristics identified in Chapter 2**
- **Describes various statutes and regulations that stipulate different requirements and vary in their applicability to PCOR**
- **Organizes relevant legal provisions according to six key data characteristics:**
 - » *Identifiability and Content; Subject; Source; Access and Use/Purpose; Consent/Authorization; and Security*

Why would a stakeholder use Chapter 3?

To identify and understand the relevant statutes and regulations applicable to the characteristics and data types described in Chapter 2 that may be triggered by the use of/access to data for PCOR.

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

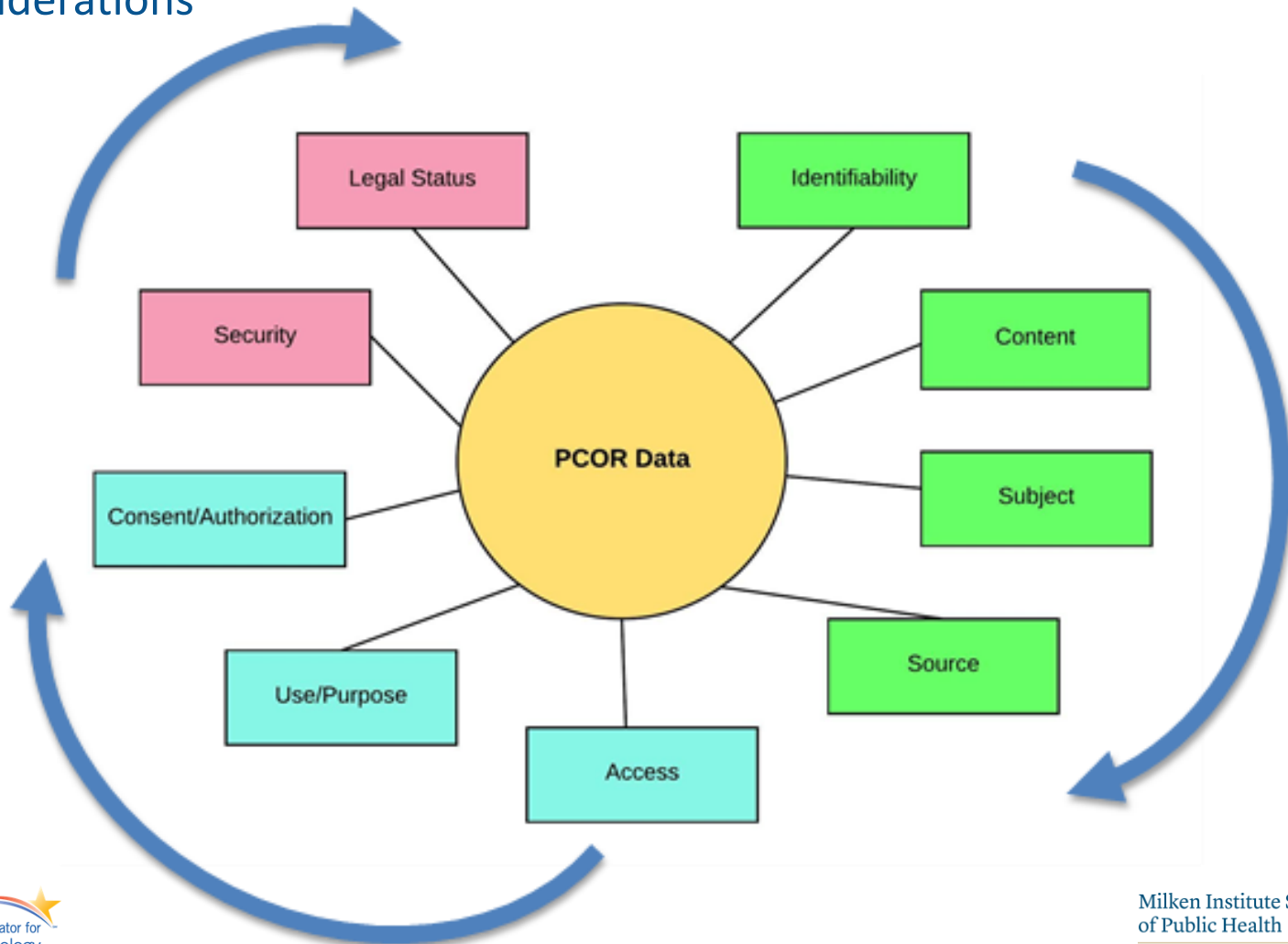
- **The Framework is a visual decision tool that highlights key characteristics and considerations associated with the spectrum of data used for PCOR and the nature of the relationships between researchers and other stakeholders.**
- **Groupings and color coded key characteristics direct stakeholders to factors determining:**
 - » Whether a statute or regulation applies to the data;
 - » How a researcher should navigate statutes/regulations that apply to the data; and
 - » Whether there are case-specific determinations relating to data collection and use.

Why would a stakeholder use Chapter 4?

To identify relevance and importance of legal requirements and ethical principles detailed in Chapter 3 that may apply to the use of/access to data for PCOR depending on specific data characteristics described in Chapter 2.

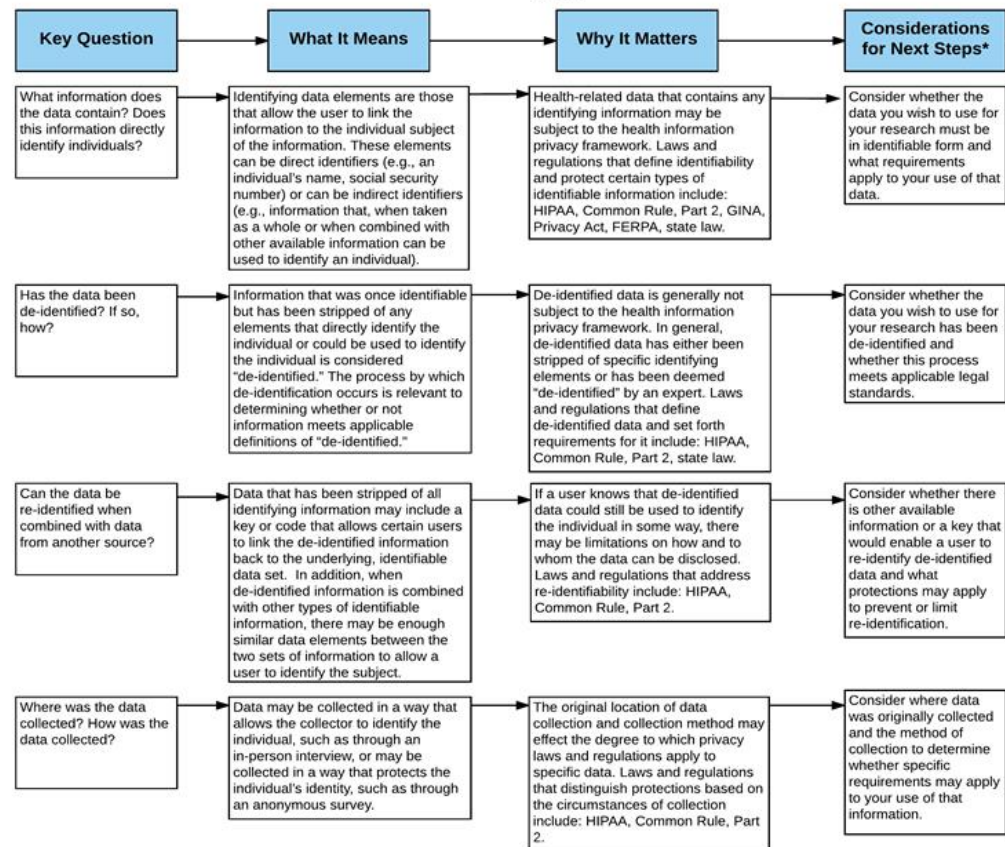
Organization of Framework

- Reflecting Primary (Green), Secondary (Blue), and Tertiary (Pink) Considerations



Example of the Framework

Identifiability pg. 2



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

Ensure that your proposed research protocol complies with applicable legal and ethical requirements.

Chapter 5: Mapping Research Data Flows to Legal Requirements

- **Data Flows adapted from Phase 1 research data use scenarios**
 - » General Data Flow (provides a foundational example of the mapping process)
 - » Combining Data for PCOR
 - » Consent Management
 - » Release and Use of Specially Protected Health Data
 - » Identification and Re-Identification of PCOR Data
 - » Research Using Patient-Generated Health Data
- **Data Flow Maps**
 - » Outline **key steps** likely to be encountered in the course of PCOR research
 - » Analyze legal trigger/decision points as applicable: **HIPAA, Common Rule, 42 CFR Part 2, State Law, GINA**
 - » Include **legal explanatory notes** as a supplement as well as references to legal summaries in Appendix A

Why would a stakeholder use Chapter 5?

To understand how relevant statutes and regulations apply to specific research scenarios (step-by-step illustrations).

Data Flow 2: Consent Management

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 US 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 institute 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 institute. 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 Individuals' 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 5 years of data in de-identified, aggregated form (planning to publish updates every 5 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.

Data Flow

Example

p. 1

Scenario Data Flow	HIPAA	The Common Rule	42 CFR Part 2	Acronyms for Data Flow 1
1 Individual is 60-year-old female with no special status.				BA = Business Associate
2 Individual seeks treatment for opioid dependence at a federally-assisted substance abuse (Part 2) Program.	<p>The HIPAA Privacy and Security Rules apply to CEs, which are healthcare providers, health plans, and healthcare clearinghouses. See <i>HIPAA Note 1</i>.</p> <p>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 <i>HIPAA Note 2</i>.</p>		<p>42 CFR Part 2 (Part 2) applies to all federally-assisted substance use disorder programs. See <i>Part 2 Note 1</i>.</p> <p>42 CFR Part 2 (Part 2) protects any information identifying an individual as having or having had a substance use disorder. See <i>Part 2 Note 1</i>.</p>	BAA = Business Associate Agreement CE = Covered Entity DUA = Data Use Agreement EHR = Electronic Health Record IRB = Institutional Review Board
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 <i>HIPAA Note 3</i> .		Records maintained by Part 2 programs must comply with certain security requirements. See <i>Part 2 Note 5</i> .	LDS = Limited Data Set PHI = Protected Health Information
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 <i>Part 2 Note 4</i> .	QSO = Qualified Service Organization QSOA = Qualified Service Organization Agreement

Data Flow Example p. 2

Scenario Data Flow	HIPAA	The Common Rule	42 CFR 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. <i>See HIPAA Note 5.</i>		Any recipient of Part 2 information is prohibited from re-disclosing it except as allowed by Part 2. <i>See Part 2 Note 2.</i>
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 QSO is required between a program and a QSO. <i>See Part 2 Note 4.</i>
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. <i>See Common Rule Note 1.</i>	
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 which has had certain identifiers removed but is still considered PHI for purposes of HIPAA because it is not fully de-identified. <i>See HIPAA Note 7.</i> Generally, a CE must obtain authorization from the subject of the information to disclose PHI to a researcher for research, with limited exceptions. <i>See HIPAA Note 9.</i> A researcher may obtain PHI for research without the subject's authorization under four circumstances. <i>See HIPAA Note 10.</i>		A QSO is an entity that provides services to a Part 2 program; a QSO is required between a program and a QSO. <i>See Part 2 Note 4.</i>

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

Appendices

- Appendix A: Summary of Statutes and Regulations Relevant to PCOR
- Appendix B: Assessing Potential Barriers and Ambiguity in the Legal Landscape
- Appendix C: Selected Federal Initiatives
- Appendix D: Selected Federal Resources
- Appendix E: Glossary

Full Architecture Available on HealthIT.gov

- www.healthit.gov/topic/legal-and-ethical-architecture-patient-centered-outcomes-research-pcor-data-architecture

The screenshot shows the HealthIT.gov website. The header includes the HealthIT.gov logo, the text 'Official Website of The Office of the National Coordinator for Health Information Technology (ONC)', and navigation links for 'CONTACT' and 'EMAIL UPDATES'. Below the header is a dark blue navigation bar with links for 'TOPICS', 'HOW DO I?', 'BLOG', 'NEWS', and 'ABOUT ONC', along with a search bar. The main content area has a breadcrumb trail: 'Home > Topics > Scientific Initiatives > Building Data Infrastructure to Support Patient Centered Outcomes Research (PCOR) > Privacy and Security Framework for PCOR (PSP) > Legal and Ethical Architecture for Patient-Centered Outcomes Research (PCOR) Data ("Architecture")'. On the left is a sidebar with a 'Scientific Initiatives' section containing links to 'Precision Medicine', 'Building Data Infrastructure to Support Patient Centered Outcomes Research (PCOR)', 'Data Access Framework (DAF)', 'Patient Matching, Aggregating and Linking (PMAL)', 'Patient-Generated Health Data (PGHD)', 'Privacy and Security Framework for PCOR (PSP)', 'Legal and Ethical Architecture for Patient-Centered Outcomes Research (PCOR) Data ("Architecture")' (which is highlighted), and 'Structured Data Capture (SDC)'. Below this is an 'Additional Reports' section. The main content area is titled 'Legal and Ethical Architecture for Patient-Centered Outcomes Research (PCOR) Data ("Architecture")'. It contains a paragraph describing the Architecture as a collection of tools and resources. It lists three bullet points: 'Provides a common structure and model for the analysis of legal requirements and ethical consideration and responsibilities in research, particularly PCOR;', 'Supports PCOR by illustrating pathways to collect and share data for research that is in compliance with relevant federal laws and regulations and in consideration of state law; and', and 'Supports a culture of trust among stakeholders by applying meaningful and appropriate privacy and security parameters.' It then states that the Architecture and its components are technology-neutral and do not address nor recommend any particular technical standards. It mentions that the legal summaries and analyses are current as of September 2017. It also states that the Architecture consists of five chapters, which can be viewed online through hyperlinks. It provides links for 'Chapter 1: Overview of Legal and Ethical Architecture for PCOR Data [PDF - 1.09 MB]', 'Chapter 2: Legal and Ethical Significance of Data for PCOR [PDF - 1.13 MB]', and 'Chapter 3: Linking Legal and Ethical Requirements to PCOR Data [PDF - 637 KB]'.

Secure | <https://www.healthit.gov/topic/legal-and-ethical-architecture-patient-centered-outcomes-research-pcor-data-architecture>

HealthIT.gov

Official Website of The Office of the National Coordinator for Health Information Technology (ONC)

CONTACT | EMAIL UPDATES

Connect with us: [in](#) [t](#) [f](#) [r](#)

TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC

Search

Home > Topics > Scientific Initiatives > Building Data Infrastructure to Support Patient Centered Outcomes Research (PCOR) > Privacy and Security Framework for PCOR (PSP) > Legal and Ethical Architecture for Patient-Centered Outcomes Research (PCOR) Data ("Architecture")

Scientific Initiatives

- Precision Medicine
- Building Data Infrastructure to Support Patient Centered Outcomes Research (PCOR)**
- Data Access Framework (DAF)
- Patient Matching, Aggregating and Linking (PMAL)
- Patient-Generated Health Data (PGHD)
- Privacy and Security Framework for PCOR (PSP)
- Legal and Ethical Architecture for Patient-Centered Outcomes Research (PCOR) Data ("Architecture")**
- Structured Data Capture (SDC)

Additional Reports

Legal and Ethical Architecture for Patient-Centered Outcomes Research (PCOR) Data ("Architecture")

This Architecture is a collection of tools and resources that help researchers and others navigate an overview of the legal requirements related to data use, sharing, and disclosure for PCOR. Specifically the Architecture:

- Provides a common structure and model for the analysis of legal requirements and ethical consideration and responsibilities in research, particularly PCOR;
- Supports PCOR by illustrating pathways to collect and share data for research that is in compliance with relevant federal laws and regulations and in consideration of state law; and
- Supports a culture of trust among stakeholders by applying meaningful and appropriate privacy and security parameters.

This Architecture and its components are technology-neutral and do not address nor recommend any particular technical standards for a health information technology system. Readers should note that laws may change over time. The legal summaries and analyses in this Architecture are current as of September 2017. In the case of the Common Rule, the analysis reflects the Final Rule that was published in 2017 and due to take effect in 2018.

The Architecture consists of the following five chapters, which can be viewed online through the hyperlinks below. [Download the entire Architecture \[PDF - 6.8 MB\]](#)

Chapter 1: Overview of Legal and Ethical Architecture for PCOR Data [PDF - 1.09 MB]

Provides background information on the project, an overview of the key legal and ethical issues relevant to PCOR data and an overview of the Architecture.

Chapter 2: Legal and Ethical Significance of Data for PCOR [PDF - 1.13 MB]

Explores fundamental concepts to help readers understand the features of the data they are working with and any privacy, security, consent, and ethics issues that may arise while conducting PCOR.

Chapter 3: Linking Legal and Ethical Requirements to PCOR Data [PDF - 637 KB]

NORC and George Washington University Project Teams and Contact Information

- Jane Hyatt Thorpe, JD
 - » 202-994-4183
 - » jthorpe@gwu.edu
- Lara Cartwright-Smith, JD, MPH
 - » 202-994-8641
 - » laracs@gwu.edu
- Elizabeth Gray, JD, MHA
 - » 202-994-4163
 - » egray11@gwu.edu



The Office of the National Coordinator for
Health Information Technology

Milken Institute School
of Public Health

THE GEORGE WASHINGTON UNIVERSITY

Thank You



@ONC_HealthIT



@HHS ONC

