The Office of the National Coordinator for Health Information Technology

Privacy and Security Framework for Patient-Centered Outcomes Research (PCOR)

FINAL REPORT

July 2020

TABLE OF CONTENTS

Introduction

Just as in healthcare delivery, the health research enterprise acknowledges that effectiveness of prevention and treatment options may depend on the preferences, values, and questions patients weigh when making healthcare choices. This type of research, patient-centered outcomes research (PCOR), is designed to produce new scientific evidence that informs and supports patients, families, and their healthcare providers.[1] PCOR depends on access to health data, which requires the protection of patient privacy in accordance with approved research protocols while providing sufficient granularity to allow meaningful conclusions to be drawn. Current laws and policies regarding use of individual data are nuanced and sometimes conflicting, creating confusion for researchers, providers, and patients. Researchers must navigate diverse state and federal requirements, as well as various consent requirements from local institutions and Institutional Review Boards (IRBs). Enabling and empowering individuals who are interested in sharing their health data is important to strengthening the validity of PCOR and setting the foundation of evidence for precision medicine. This project sought to create and identify resources for stakeholders as they navigate the complexities of sharing health data for research. The framework and resulting resources consider the legal and regulatory requirements relative to patient consent, privacy, and autonomy in examining the factors of collection, access, use, and disclosure of electronic health data that were current at the time of the project.

Project Overview

Funded by the Patient-Centered Outcomes Research Trust Fund administered by the Department of Health and Human Services (HHS) Assistant Secretary for Planning and Evaluation (ASPE), this project developed resources that support the protection of privacy and security of electronic health data as it is acquired and used for PCOR. The objectives for this project included:

- Conceptualizing and developing a privacy and security data architecture;
- Conceptualizing and developing the legal analysis and ethical framework needed to balance individual privacy rights with data use, sharing, and disclosure for PCOR; and
- Analyzing and developing, as needed, technical standards to implement and share individual consent (basic and granular choice) when sharing patient health data across health and research settings.

From June 16, 2015, through September 30, 2018, the work conducted resulted in a framework and lessons learned from project activities, which included the testing of technology that supports the use of health data for PCOR. The resources resulting from this project provide guidance to researchers, healthcare providers, and health systems through the responsible use and protection of electronic health data for PCOR, making data available to researchers and other stakeholders. This project, led by the Office of the National Coordinator for Health Information Technology (ONC) took place in parallel to a project led by the Centers for Disease Control and Prevention (CDC). The CDC project focused its efforts on the legal and ethical challenges posed by granting PCOR researchers access to public health data collected by

[1] https://aspe.hhs.gov/patient-centered-outcomes-research-trust-fund

the CDC. The resulting CDC work also informed the overall framework that ONC developed to address the various legal and ethical privacy and security-related issues that affect the use of data for PCOR.

To tackle the complex nature of privacy and security issues regarding the sharing of electronic health data for PCOR and clinical care, this project consisted of two complementary activities. The first aimed to produce a resource to help users of electronic health data navigate the complex privacy landscape. The resulting "Legal and Ethical Architecture for PCOR Data (Architecture)"[2] guides stakeholders through the responsible use and protection of electronic health data as it is acquired and used for PCOR. The second identified and tested the technology needed to enable patients to control how their data are shared for their care and research. This work involved pilot testing of existing technical mechanisms to enable interoperable exchange of patient consent directives for: 1) basic choice for treatment, payment, and operations, 2) basic choice for research, and (3) granular choice for research, and healthcare treatment, payment, and operations. The "Technology for Patient Choice"[3] activity resulted in development of multiple consent scenarios that identify and recommend data standards as well as several use cases that demonstrated the use of standards and eConsent technology. The activity also produced recommendations for the advancement of data standards that support an individual's consent preferences.

This project engaged with stakeholders at multiple points to develop common PCOR use cases and consent scenarios ensuring a level of realism related to issues when using health data for PCOR and when enabling patient-controlled consent for the sharing of health data. Together, the activities and resources resulting from this project create a practical, technology-neutral, blueprint that can be used by researchers, patients, and providers.

Development of the Legal and Ethical Architecture for PCOR Data (Architecture)

The Legal and Ethical Architecture for PCOR Data (Architecture) is intended for use by a variety of PCOR stakeholders to evaluate data needs and analyze data access requirements according to federal and state privacy, public health, and security laws and regulations.[4] The Architecture includes tools and resources that address the many privacy and security-related legal and policy issues that affect the use of health data for various types of PCOR. A key challenge in development of the Architecture was examining the myriad and often conflicting laws and policies regarding the use of patient-level data that often create confusion for researchers, providers, and patients.

To inform development of the Architecture, ONC convened and led discussions with relevant stakeholders. These discussions informed the development of research scenarios and data flows featured in the Architecture. This was followed by a review of the legal, regulatory, and policy environment governing the use of health data in these research scenarios and related uses for PCOR.

[2] https://www.healthit.gov/topic/scientific-initiatives/pcor/legal-and-ethical-architecture-patient-centered-outcomes-research-pcor-data-architecture

[3] https://www.healthit.gov/topic/scientific-initiatives/pcor/privacy-and-security-framework-pcor-psp

[4] Mapping reflects conditions that were current at the time of the Architecture's publication.

Five Architecture data flows and affiliated scenarios are outlined in Table 1. The Architecture data flow models were mapped to privacy and security legal requirements, definitions or updates to policies and minimum requirements for data de-identification and re-identification, and ethical implications for PCOR data use. These data flows encompass a variety of thematic areas present within PCOR, which have been expanded upon in the form of individual scenarios that describe real world research needs. The scenarios intend to showcase prevalent issues that emerge in the planning and conduct of PCOR. They also illustrate gaps in policy, regulation, and understanding that needed to be addressed to optimize the use of health data for PCOR and the protection of individuals contributing their data.

Table 1: Data Flows, Thematic Areas, and Scenarios

Data Flow	Thematic Area	Scenario
Data Flow 1: Combine Data for PCOR	Combining Independently Managed Data	Combining Clinical and Claims Data
		Secondary Analysis of Administrative Data on Substance Use Treatment
		Combine Claims and Birth Records
Data Flow 2: Consent Management	Age-Related Consent in Research Scenarios	Considerations Related to Consent and Transitions from Minor to Adult
	Research Data from Special Populations and With Protected Status	Obtaining Consent from Incarcerated, HIV-Positive Research Participants
		Consenting Individuals with Impaired Decision-Making Capacity
Data Flow 3: Release and Use of Protected Health Data for PCOR	Use of Behavioral Health Data	Combining Mental Health Data with Physical Health Data
	Precision Medicine	Consent to Disclose Genomic Data that Affects Family Members
		Genomic Testing and Disclosure from Minors
		Use of Genetic Biomarkers
	Individual and Population-Level Research Related to Sub-Populations	Privacy Concerns for American Indian/Alaska Native Individuals and/or Populations
Data Flow 4: Identification and Re-Identification of PCOR Data	Cumulative Re-Identification Risk	Re-identification Risk from the Mosaic Effect
	Multi-Site Identity Linking	Creating a Multi-Institutional Unique Identifier for Research
Data Flow 5: Use Patient-Generated Health Data for PCOR	Patient-Generated Health Data	Use of Sensor Data
		Creating a Registry that Includes Patient Reported Outcomes
		Use of a Registry that Includes Patient-Reported Outcomes
		Information Flow and Authentication in Linking Personal Devices to Clinical Data for Research

These data flows, scenarios, and analysis of federal and general state privacy, public health, and security laws and regulations were used to develop the Architecture which consists of the following five chapters.

Chapter 1: Overview of Legal and Ethical Architecture for PCOR Data

This chapter provides an overview of the key legal and ethical issues relevant to PCOR data as well as an overview of the Architecture and related efforts. This chapter also provides guidance on how to navigate and use the Architecture.

Chapter 2: Legal and Ethical Significance for Data for PCOR

This chapter explains fundamental concepts for organizing data according to categories and types enabling the application of legal requirements. The first section presents questions to guide the reader in identifying the key characteristics of health data used for PCOR. This chapter also includes an overview of the most significant health data types relevant to PCOR.

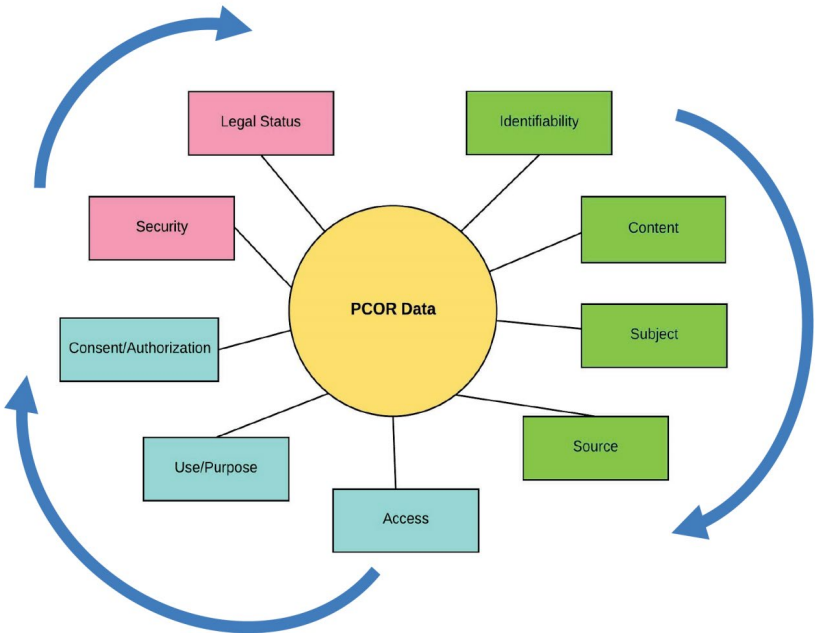
Chapter 3: Linking Legal and Ethical Requirements to PCOR Data

Some of the PCOR data characteristics identified in Chapter 2 are associated with specific legal requirements that can be found in the statutes and regulations that govern access and use of health data for PCOR. This chapter summarizes those specific legal requirements and links them directly to the key characteristics of PCOR data described in Chapter 2.

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

This chapter presents a series of visual decision tools that highlight the key considerations associated with data characteristics (Figure 1), PCOR data, and the nature of the relationships between researchers and other stakeholders. Each data characteristic is explored via decision aid that addresses key questions, implications, significance, considerations, and next steps.

Figure 1: Data Characteristics Within the PCOR Framework



Chapter 5: Mapping Research Data Flows to Legal Requirements

The representative data flows in this chapter identify common themes and gaps via narrative descriptions and visual illustrations of research scenarios for each data flow. Figure 2 provides an example of a data flow scenario. The scenarios describe common elements of the PCOR data use scenarios and indicate where and how they intersect with relevant federal laws and regulations.

Figure 2: Example of Data Flow Use Case 2: Consent Management

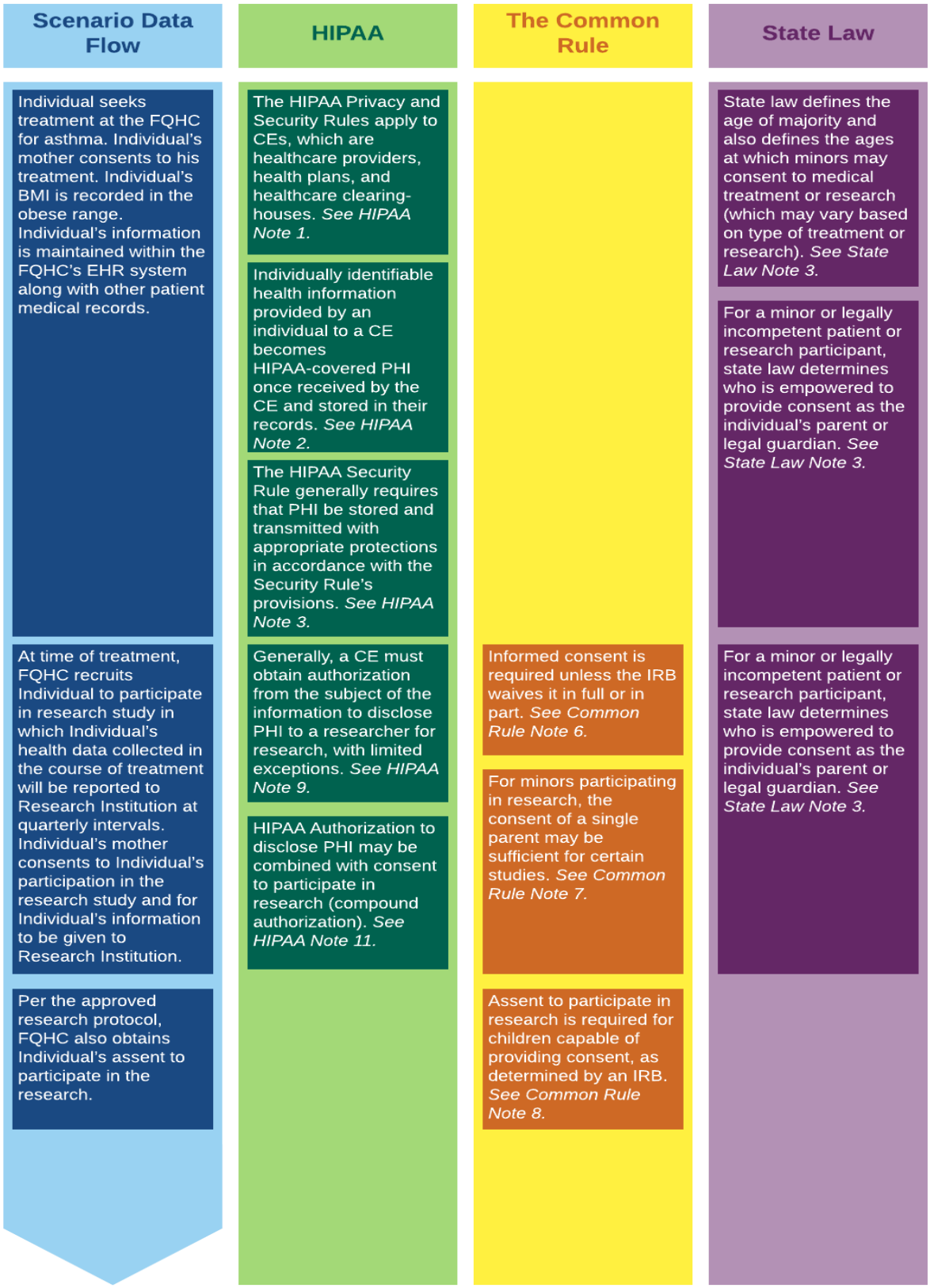


Table 2: Figure 2 Acronyms			
BMI	Body Mass Index	**HIPAA**	Health Insurance Portability and Accountability Act
CE	Covered Entity	**IRB**	Institutional Review Board
EHR	Electronic Health Record	**PHI**	Protected Health Information
FQHC	Federally Qualified Health Center		

Collectively, the assortment of tools and resources that are included in the Architecture offer a common structure and model for the analysis of legal requirements, ethical considerations, and responsibilities relevant to PCOR. The Architecture offers illustrative pathways for collecting and sharing data for research in compliance with relevant federal laws and regulations and state laws. Use of this framework can support a culture of trust among PCOR stakeholders as it supports the appropriate application of privacy and security considerations.

Technology for Patient Choice

In addition to developing an Architecture that focuses on how PCOR data needs intersect with privacy policies, laws and regulations, this project sought to develop, test, and support the adoption of technology and data standards to better understand how to share data based on different types of consent or how to electronically document consent. The need for an electronic version of a consent document and electronic data describing the consent, called metadata, is well understood. Currently, the electronic capture and exchange of consent forms is often an image of a paper document signed by the individual consenting to participate in a research study that has been encoded in an electronic format. The use of an image, for reasons of organizational policy or interpretation of law, provides a tangible representation of the terms and acceptance of a consent agreement. Technological advances, such as eConsent systems, offer alternatives to signing a paper document. For example, potential research participants may be given a tablet that leads the consenter through the consent directive. The use of electronic consent creates an uninterrupted electronic workflow that can incorporate specifics of the consent into attributes easily exchanged with other electronic systems. Organizations that still require printed and signed forms recognize the need to scan and extract information from those forms. This information is either entered into electronic systems manually or extracted electronically and stored as metadata. Generally, organizations accept consent as either a paper or electronic document that includes metadata describing the consent.

The need to exchange interoperable patient health data and consent between information systems is critical for research. Many organizations have worked together to define data models, semantics, role hierarchies, orchestration, security models, and security labels useful in constructing an interoperable health data exchange system. The resources resulting from this project build upon existing functionality of technology. For instance, the Substance Abuse and Mental Health Services Administration (SAMHSA)[5]

[5] https://www.healthit.gov/topic/health-it-health-care-settings/behavioral-health-consent-management

developed Consent2Share to guide health information technology (health IT) developers and policy makers in the implementation of technology that enables responsible use and protection of health data in PCOR and for data sharing. This project also builds on ONC's work since 2010 to expand electronic consent management.

ONC conducted an environmental scan and gap analysis of consent management technologies for research and engaged with stakeholders in the health IT and research communities. Stakeholder input helped identify consent scenarios and the technology needed for implementation for three types of patient consent for data sharing: 1) basic choice for treatment, payment, operations (TPO), 2) basic choice for research, and 3) granular choice.[6] Select consent scenarios and supporting technology were pilot tested to demonstrate how data standards could accommodate different protocols, representations, and implementations.

Basic Choice for Treatment, Payment, Operations (TPO)

For the purposes of this activity, basic choice refers to an individual's ability to opt-in or opt-out of having all of his or her protected health information (PHI) available for electronic exchange for TPO. To test the use of data standards and an electronic workflow, ONC partnered with two organizations, the Veterans Health Administration and the Michigan Health Information Network (MiHIN), to develop a basic consent use case and functional requirements. This model specifically addresses situations where there is a requirement to obtain patient consent before electronically exchanging health data when that consent requirement is imposed by state law or by the organizational policies of the disclosing organization. These use cases are for situations when patient consent is required, despite the federal rules under HIPAA that do not require such consent to exchange data for treatment.

Basic Choice for Research

To develop the model for the Basic Choice for Research Use Case, the team leveraged artifacts and lessons learned from the Basic Choice for TPO activities to support solutions that implement a basic choice model for research purposes. The resulting work supported efforts to successfully ballot the Health Level Seven International® (HL7®) Implementation Guide for Clinical Document Architecture (CDA®) Release 2, Privacy Consent Directives, Release 1.

The resulting Basic Choice for Research Use Case defines the interoperability requirements for health data exchange that uses a basic choice consent model for research. It provides operational context for data exchange, information regarding affected stakeholders, information flows that must be supported, types of data involved, and their required specifications for data exchange. The Basic Consent for Research Use Case include the following scenarios:

- **Participation in a Research Study with Revocation of Consent (the following describe scenarios that may build on one another)**
  - Patient consents to participation in a research study
  - An outside researcher contacts the patient regarding participation in a new research study
  - The patient revokes consent for re-contact

[6] Findings from these activities reflected the environment and technical capabilities that were current at the time this project was active.

- **Consent for Genetic Research by a Minor (the following describe four scenarios that may or may not build on one another)**
    - Patient assents to participate in a research study
    - Patient provides consent upon reaching adulthood and subsequently provides consent to participate in another research study to use her biospecimen for further research
    - Researcher sends results generated during the research study to patient's primary care provider (PCP)
    - Patient joins a research study and directs (leveraging the patient right of access) their PCP to release their medical records to the researcher

Granular Choice

Granular choice project activities included the development of use cases and scenarios to identify data standards to support an individual's detailed choice to share specific types of health data for TPO and research. The Granular Choice Use Case consent scenarios were designed to expand on artifacts from the Basic Choice for TPO and Basic Choice for Research work to demonstrate granular choice consent mechanisms within a health information exchange (HIE) setting. MiHIN continued to build upon their work conducted for basic choice and their experience with eConsent, which enabled seamless execution. For this project MiHIN leveraged an eConsent service, which can store multiple consent forms, to demonstrate support for consent scenarios where there are simultaneous healthcare concerns. MiHIN also demonstrated the incorporation of Health Level Seven International (HL7®) privacy tags to parse specific information out of messages. This can ensure protection of PHI as data can be routed based on patient consent preferences. The Granular Choice Use Case document utilizes the same approach to address interoperability requirements for health data exchange for the following scenarios:

- **Consent for Sharing of Specific Health Data for Treatment, Payment, Operations (the following scenarios may build on one another)**
    - Patient regularly attends an opioid treatment facility generating substance use disorder (SUD) data that is protected by 42 CFR Part 2
    - Patient seeks treatment from a new provider at an urgent care clinic
    - Patient grants consent for sharing of SUD data with a new provider
- **Consent for Sharing of Specific Health Data for Research (the following describe scenarios that may build on one another)**
    - Patient consents to participate in a new research study on effects of opioids
    - Patient directs (leveraging the patient right of access) their provider to share only SUD-specific data with the research study
    - Patient ceases participation in the research study and revokes authorization for research study to receive health data

Conclusion

Making health data accessible for PCOR requires addressing many privacy and security-related policy issues. This project addressed these issues by 1) conceptualizing and developing a privacy and security data architecture, 2) conceptualizing and developing the legal analysis and ethical framework that balance individual privacy rights with data use, sharing, and disclosure for PCOR, and 3) analyzing and testing

technical standards that support the implementation of electronic workflows for individual consent (granular choice) when sharing patient health data across health and research settings.

The changing healthcare policy and technical environment requires PCOR researchers and other health data users or data holders to frequently monitor and adjust the way they access or share health data. The Architecture developed under this project paved the way for stakeholders to navigate the legal and ethical landscape for PCOR. This project also developed and tested the technical mechanisms to enable interoperable exchange of patient consent for research and treatment, payment, and healthcare operations environments. This work demonstrated that health IT infrastructure can align with legal requirements and address ethical considerations.

Patient-level data are critical to understanding and improving health outcomes and effective research. These data need to be appropriately available to researchers in ways that ensure the protection of patient privacy and individual preferences while supporting a level of granularity that allows meaningful research to be conducted. Using data for purposes other than those originally intended at the time of data collection carries the concern of losing inherent agreements, legal protections, and patient understanding regarding how the data may be used. Shared data resources must have strong and transferable data protections visible to all stakeholders and be enforceable at every access level. The activities conducted under this project demonstrated that health data can be parsed and shared in a granular manner protecting patient privacy and preferences and supporting a greater array of data sharing options. Ongoing participation in all forms of data collection such as clinical trials, survey data collection, or allowance for the re-use of routinely collected data, critically depend on human subjects trusting that their data will be adequately protected.

Looking Ahead

Without available standards, implementation guides, and related resources, organizations may implement or default to more stringent data sharing workflows that restrict the availability of data for PCOR. The availability of standards-based tools and workflows for consent that support the evolving regulatory landscape and patient choice will be critical for enabling data sharing for treatment, payment, operations, and research.

As ONC continues to expand demonstration and standards development activities to foster data sharing for care and research, future projects will leverage the work conducted under this project. Since the completion of this project, consent standards have advanced to be available within the HL7 Fast Healthcare Interoperability Resources® (FHIR®) specifications for Resource Consent - Content for trial use within HL7 FHIR Release 4.[7]

Additionally, ONC recently awarded a grant under its Leading Edge Acceleration Projects (LEAP) in Health IT[8] that is implementing consent use cases for basic choice, using profiles for direct consent, and developing resources for partners to implement FHIR-based APIs that include consent information. The LEAP project will also use the Legal and Ethical Architecture for PCOR Data developed through this project.

[7] https://www.hl7.org/fhir/consent.html

[8] https://www.healthit.gov/topic/leading-edge-acceleration-projects-leap-health-information-technology-health-it