The Office of the National Coordinator for Health Information Technology

Legal and Ethical Architecture for PCOR Data

APPENDIX C: SELECTED FEDERAL INITIATIVES

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

INTRODUCTION

The work of numerous U.S. Department of Health and Human Services (HHS) agencies and offices, particularly the Office of the National Coordinator for Health Information Technology, informed the development of this Architecture. The prior and current work of these stakeholders related to privacy and security of health information is summarized below as instructive references for researchers and other stakeholders.

HHS OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY (ONC)

Since its inception, ONC has focused on developing policy, programs, and initiatives designed to advance the interoperable exchange of electronic health information. These efforts have consistently addressed the important role that privacy and security play in any efforts involving the use, release, and exchange of health information.

Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (2008)[580]

In 2008 (prior to the HITECH changes to HIPAA reflected above), ONC released a Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. While this document may seem dated in the rapidly moving arena of health information and technology and relates specifically to the exchange of individually identifiable data via a network, the core principles remain important today and should be reflected in the legal and ethical framework for PCOR where relevant and appropriate. For example, the principles address: 1) ensuring reasonable individual access to their individually identifiable information; 2) enabling correction of information when appropriate; 3) ensuring openness and transparency related to policies and procedures; 4) enabling individual choice when relevant; 5) ensuring information is collected, used/or disclosed only to the extent necessary for the underlying purpose(s) (and never to discriminate); 6) ensuring data quality and integrity; 7) ensuring appropriate safeguards are met; and 8) ensuring accountability for non-adherence or breach. Importantly, this document and ONC resources reflect and are consistent with the Fair Information Practice Principles, or FIPPS. ONC and other stakeholders have routinely relied on FIPPS to develop and implement policies and procedures related to collection, use, and disclosure of personal information (see further description below).

HIE Governance (2013)

In 2013, ONC released a set of guiding principles related to the governance of health information exchanges.[581] While these principles focus on organizations engaging in activities related to the exchange of data as well as the actual exchange of data for health care purposes, they are also relevant to and

[580] The Office of the National Coordinator for Health Information Technology (ONC) Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information (2008), *available at* https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

[581] ONC Governance Framework for Trusted Electronic Health Information Exchange at 1-2 (2013), *available at* https://www.healthit.gov/sites/default/files/GovernanceFrameworkTrustedEHIE_Final.pdf.

should be considered in relation to research, specifically PCOR. The following principles provide the most relevant guidance applicable to PCOR efforts for inclusion in a legal and ethical framework: 1) establish mechanisms to ensure that the entity's policies and practices and applicable federal and state laws and regulations are adhered to; 2) promote inclusive participation and adequate stakeholder representation; and 3) provide a simple explanation of the privacy and security practices that are in place to protect personally identifiable information when it is electronically exchanged.

Shared Nationwide Interoperability Roadmap

In 2015, ONC released "Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap." One of the core principles of interoperability identified in the Roadmap is to "protect privacy and security in all aspects of interoperability."[582] The Roadmap focuses primarily on health care organizations, as the majority of health information "resides in and is stewarded by health care organizations," and their Business Associates, which are governed by HIPAA.[583] Health care organizations are a rich source of health information necessary to support PCOR. However, ONC also recognizes the increasing role played by organizations that are not governed by the HIPAA Privacy and Security Rule and calls for greater transparency of those organizations' data practices to ensure individuals understand the potential uses and disclosures of their information. Specifically, ONC addresses issues related to network security; verifiable identity and participant authentication; consistent principles for permission or consent to collect, share, and use identifiable health information, including FIPPS; and consistent representation of authorization to access health information.[584] This guidance and the continuing dialogue related to these issues will play an important role in the development of a legal and ethical framework for PCOR.

ONC notes that an interoperable health IT ecosystem supports critical public health functions as well as data aggregation for research.[585] The Roadmap also highlights the importance of a learning health system based on the best available evidence to further support these efforts (including patient-centeredness of care). It was the Institute of Medicine's (IOM) original vision of a learning health system that would "generate and apply the best evidence for the collaborative health care choices of each patient and provider; drive the process of discovery as a natural outgrowth of patient care; and ensure innovation, quality, safety and value in healthcare."[586] As noted above, this is the essence of PCOR.

---

[582] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 9 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[583] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 13 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[584] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 55 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[585] ONC Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap at 17 (2015), *available at* https://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf.

[586] Institute of Medicine (IOM) Learning Healthcare System (2007), *available at* https://iom.nationalacademies.org/Reports/2007/The-Learning-Healthcare-System-Workshop-Summary.aspx [purchase required].

Health Information Technology Policy Committee (HITPC) Privacy and Security Workgroup[587]

The Privacy and Security Workgroup of the HITPC (a Federal Advisory Committee Act (FACA) Committee), which reports to the HITPC and ONC, has focused its work solely on issues related to the privacy and security issues related to the electronic exchange of health information. Most recently, the Workgroup has addressed health big data[588] (including big data research), and their recommendations are instructive. There are many commonalities between big data and PCOR related to the use of patient health information. The Workgroup heard public testimony that raised a number of concerns related to commonly used tools to protect privacy (including de-identification, patient consent, data security, and transparency) and limitations on collection and use. The Workgroup also heard testimony on the barriers and challenges presented by the complex health information legal landscape. Much of the discussions focused on the challenges associated with the very different regulation of HIPAA Covered Entities and non-HIPAA entities, as well as decreasing confidence in de-identification methods and growing risk of re-identification. The Workgroup's resulting recommendations focused on addressing the "uneven" policy [legal] environment and changes to the de-identification methodologies as well as the secure use of data for learning. These recommendations and the collective work of the Privacy and Security Workgroup will help inform the development of the legal and ethical framework for PCOR.

Federal Health IT Strategic Plan 2015–2020[589]

Released in late 2015, the Federal Health IT Strategic Plan 2015–2020 builds on prior iterations of ONC's strategy to advance "widespread adoption of health IT." Advancing PCOR relates to several of the stated objectives in the Strategic Plan, including Objective 1A, empower individual, family, and caregiver health management and engagement; Objective 2B, improve health care quality, access, and experience through safe, timely, effective, efficient, equitable, and person-centered care; and Objective 2C, protect and promote public health and healthy, resilient communities.

The Strategic Plan calls for collaborative efforts by all stakeholders and highlights federal efforts to support PCOR, including improving accessibility, technical standards, services, policies, federal data, and governance structures for PCOR. With funding from/for PCORI, including funds to support this project, the goal is to "enable a comprehensive, interoperable, and sustainable data network infrastructure to collect, link, and analyze data from multiple sources to facilitate patient-centered outcomes research."[590]

The plan also highlights the importance of protecting the privacy and security of health information. Objective 4 of the Strategic Plan notes several strategies related to the clarification of legal requirements for privacy and security for entities covered by HIPAA and those not covered by HIPAA.

---

[587] *See* ONC "Privacy & Security" (*last updated* March 2, 2016), *available at* https://www.healthit.gov/facas/health-it-standards-committee/hitsc-workgroups/privacy-security

[588] HITPC Privacy and Security Workgroup Health Big Data Recommendations at 14 (2015), *available at*: https://www.healthit.gov/sites/faca/files/HITPC_Health_Big_Data_Report_FINAL.pdf.

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

[590] ONC Federal Health IT Strategic Plan 2015-2020 at 29 (2015), *available at* https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf.

Other ONC PCOR Projects

ONC also has a number of other projects relevant to PCOR underway. These include the Common Data Elements, Patient Matching, and Patient-Generated Health Data projects. As the work of these projects continues to evolve, researchers and other stakeholders should review the status and guidance materials generated by these projects. To the extent possible, existing efforts on these projects helped inform the development of the Architecture.

HHS OPEN DATA INITIATIVES

HHS has engaged in multiple open data initiatives pursuant to the HHS's Open Government Plan[591] and the associated Open Data Policy. These initiatives include the HHS Enterprise Data Inventory,[592] which lists all of the department's pubic, non-public, and restricted datasets and the release of publicly available datasets on healthdata.gov. The CMS website houses multiple datasets related to CMS programs. Interested parties can use the CMS Data Navigator to find data related to specific programs, settings, topics, and/or geographic locations.[593] CMS also offers access to research data through the CMS Chronic Conditions Data Warehouse.[594]

HHS OFFICE FOR CIVIL RIGHTS (OCR)

OCR, the federal office within HHS responsible for enforcement of the HIPAA Privacy, Security, and Breach Notification Rules has released guidance relevant to PCOR addressing: 1) individuals' right of access to their health information;[595]

2) privacy and security guidance for electronic health records;[596] 3) guidance for health app developers;[597] and 4) tools and resources for HIPAA Regulated Entities.[598] OCR enforcement action settlements also provide helpful guidance, particularly those related to medical devices and Internet applications. Collectively, these resources are instructive to PCOR.

---

[591] U.S. Department of Health and Human Services (HHS) HHS Open Government Plan: Version 4.0 (2016), *available at https://www.hhs.gov/sites/default/files/hhs-open-gov-plan-v4-2016.pdf*.

[592] HHS HHS Enterprise Data Inventory (*content updated* April 5, 2017), *available at* http://www.healthdata.gov/dataset/hhs-enterprise-data-inventory

[593] Centers for Medicare & Medicaid Services (CMS) "CMS Data Navigator" (2017), *available at* https://dnav.cms.gov/.

[594] CMS "Chronic Conditions Data Warehouse" (2017), *available at* https://www.ccwdata.org/web/guest/home

[595] HHS Office for Civil Rights (OCR) Questions and Answers About HIPAA's Access Right (*last updated* February 25, 2016), *available at* http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs

[596] OCR "Special Topics: Health Information Technology" (*last updated* June 16, 2017), *available at* http://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html

[597] HHS Health App Use Scenarios & HIPAA (2016), *available at* https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf

[598] OCR "HIPAA For Professionals" (*last updated* June 16, 2017, *available at* http://www.hhs.gov/hipaa/for-professionals

HHS OFFICE FOR HUMAN RESEARCH PROTECTIONS (OHRP)

OHRP, a federal office within HHS, is responsible for overseeing the protection of human participants involved in research that is conducted or supported by HHS. Specifically, OHRP provides guidance, maintains regulatory oversight, and provides advice on ethical and regulatory issues in biomedical and behavioral research. OHRP also supports the Secretary's Advisory Committee on Human Research Protections (SACHRP) (discussed below) that advises the HHS Secretary on issues of human participant protections. During the development of this Architecture, OHRP released material changes to the Common Rule that governs federally supported research involving human participants. Changes to the Common Rule were incorporated into the Architecture.

SECRETARY'S ADVISORY COMMITTEE ON HUMAN RESEARCH PROTECTIONS (SACHRP)

SACHRP provides guidance and recommendations to the HHS Secretary on matters pertaining to the protection of human participants research. While not directly specific to PCOR, SACHRP has provided recommendations related to big data research that bear consideration as they potentially relate to PCOR. For example, SACHRP suggested that OHRP provide guidance for and/or consider changes to the consent waiver standards applicable to human participants research and that OCR clarify if and how HIPAA applies to big data research. SACHRP also provided voluminous comments during the rulemaking process for the Common Rule (Final Rule effective February 2018).

NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS (NCVHS)[599]

The NCVHS advises HHS on matters related to health data, statistics, and national health information policy. Part of NCVHS' work is to review health data and advise on "statistical problems of national and international interest," to conduct simulations and/or studies of these problems, and to propose improvements for the US' health statistics and information systems. One of the NCVHS' roles is to foster collaboration on how to facilitate and accelerate multi-sector consensus around health system compatibility and information confidentiality.

PATIENT-CENTERED OUTCOMES RESEARCH INSTITUTE (PCORI)

The vision of PCORI is that "[p]atients and the public have information they can use to make decisions that reflect their desired health outcomes."[600] PCORI is responsible for supporting the development of PCORnet, the National Patient-Centered Clinical Research Network,[601] which is a PCORI initiative aimed

[599] HHS National Committee on Vital and Health Statistics (NCVHS) "About: About the Committee" *available at* https://www.ncvhs.hhs.gov/about/about-the-committee/ (*last visited* September 25, 2017).

[600] Patient-Centered Outcomes Research Institute (PCORI) "About Us," *available at* http://www.pcori.org/about-us (*last visited* September 25, 2017).

[601] PCORnet: The National Patient-Centered Clinical Research Network "Homepage" http://www.pcornet.org/ (*last visited* September 25, 2017).

at creating a national network for conducting PCOR. Through the PCORnet initiative, PCORI has grappled with issues related to use of patient health information for CER in particular, including health information privacy and security. Specifically, PCORnet has released its "Commitment to Patient Privacy and Data Security," including Guiding Principles.[602] The Guiding Principles articulate PCORnet's belief that the "protection of privacy, data confidentiality, and security is essential to the existence and success of healthcare data research networks." The Principles also state that all research practices within PCORnet "comply with current national and local regulatory and oversight provisions."[603] These Principles helped guide the development of the Architecture.

CENTERS FOR DISEASE CONTROL (CDC)

The CDC is a federal agency within HHS responsible for the protection of public health and the control of disease and injury. Parallel to the development of this Architecture, the CDC developed a Legal and Ethical Framework for Public Health Research. The process for the CDC project was similar to this project in that the project team developed scenarios with a multidisciplinary work group and applied legal and ethical analysis to develop a framework for research using public health data. That project's final document, the "Legal and Ethical Framework to Use Centers for Disease Control and Prevention Data for Patient-Centered Outcomes Research," sets forth three data use scenarios that the CDC workgroup created to highlight unique legal and ethical implications for use of CDC data. CDC collects data for public health purposes, including surveillance of disease, injury, exposure to health threats, and research to address population needs. Secondary use of CDC's existing public health data for PCOR purposes can have a substantial impact on patient and public health through research in areas such as epidemiology, drug safety, outcomes research, vaccines, and health services research.

FEDERAL TRADE COMMISSION (FTC)

The FTC is responsible for the protection of consumers and their information. In that role, they have released multiple materials that have been used to guide the efforts of other federal and state agencies, including ONC. In particular, the FTC FIPPs are widely cited. These principles resulted from the FTC's review of online entities that collect and use personal information to ensure that such efforts are fair and include appropriate privacy protections. The FIPPs address the following core elements related to information privacy: 1) notice to consumer prior to information collection; 2) choice/consent providing information on consumers' ability to control how their data is used (including opt-in and opt-out models); 3) limiting collection/use to stated purposes and enabling consumers to view and verify data

[602] PCORnet: The National Patient-Centered Clinical Research Network PCORnet: A Commitment to Patient Privacy and Data Security (2015), *available at*: http://www.pcornet.org/wp-content/uploads/2015/03/PCORnet_PrivacyStatement_Final_March2015.pdf.

[603] PCORnet: The National Patient-Centered Clinical Research Network PCORnet: A Commitment to Patient Privacy and Data Security (2015), *available at*: http://www.pcornet.org/wp-content/uploads/2015/03/PCORnet_PrivacyStatement_Final_March2015.pdf.

collected; 4) transparency about information collected; 5) ensuring reasonable security protections; and 6) accountability for information and compliance with relevant laws and regulations.[604]

SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION (SAMHSA)

The SAMHSA, an agency within HHS, leads public health efforts related to behavioral health, including substance abuse and mental health issues. During the development of the Architecture, SAMSHA released material revisions to 42 C.F.R. Part 2 (Part 2), the federal regulations that govern the use and disclosure of substance abuse patient health records. Changes to Part 2 were incorporated into the Architecture.

PRECISION MEDICINE INITIATIVE (PMI)[605]

PMI, announced by President Obama in his 2015 State of the Union Address, seeks to "provide clinicians with tools, knowledge, and therapies to select which treatments will work best for which patients." The primary objectives of the PMI include discovering more effective cancer treatments, creating a voluntary national research cohort, modernizing regulations, creating public-private partnerships, and identifying privacy and security issues related to precision medicine. The PMI has addressed this final objective by establishing the Privacy and Trust Principles and the Draft Data Security Policy Principles and Framework.

PMI Privacy and Trust Principles[606]

The Privacy and Trust Principles were developed by an interagency working group and are meant to guide PMI activities. The principles focus on: (1) governance; (2) transparency; (3) respecting participant preferences; (4) empowering participants by enabling access to information; (5) data sharing, access, and use; and (6) data quality and integrity.

PMI Draft Data Security Policy Principles[607]

The Draft Data Security Policy Principles, developed by an interagency process, are meant to guide the development and implementation of a security plan by PMI organizations. These principles include: 1) building a system that participants can trust; 2) making security a "core element of the organization's services"; 3) preserving data integrity; 4) identifying risks and developing risk management plans; 5)

[604] Federal Trade Commission (FTC) Fair Information Practice Principles (*last updated* June 25, 2007), *available at*: https://web.archive.org/web/20100309105100/http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Notice/Awareness

[605] The White House Fact Sheet: President Obama's Precision Medicine Initiative (2015), *available at* https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative

[606] The White House Precision Medicine Initiative: Privacy and Trust Principles (2015), *available at* https://obamawhitehouse.archives.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf.

[607] The White House Precision Medicine Initiative: Data Security Policy Principles and Framework (2016), *available at* https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_and_Framework_FINAL_022516.pdf.

maintaining transparency regarding security processes and expectations; 6) protecting data with security practices and controls, but not in a way that denies participants access to their data or limits proper research uses of the data; 7) acting responsibly, minimizing the exposure of participant data, and providing notification of breaches; and 8) communicating experiences and challenges with other PMI organizations. These organizations may achieve the Principles by complying with the core functions (i.e., Identify, Protect, Detect, Respond, and Recover) set forth in the Data Security Policy Framework.