AGGREGATING PATIENT-LEVEL DATA

REGULATORY, ETHICAL, AND PRIVACY ISSUES FOR COMMUNITIES

Les Morgan and Joanne Lynn / March 2018

Gordon and Betty Moore Foundation Grant # 5662

Report 1.2.4

ALTARUM

SOLUTIONS THAT MATTER. HEALTH CARE THAT WORKS.

Table of Contents

Disclaimer: The information here is not intended to serve as legal advice nor should it substitute for legal counsel.

Introduction

Our team is working with communities where leaders are interested in improving the reliability, quality, and costs of care for elderly persons living with disabilities, mostly associated with aging. These communities need trustworthy data to use in setting priorities and in monitoring improvements. One appealing approach is to aggregate existing health-related records and analyze the data for key indicators of how their local system is functioning. However, for most of our communities, on a practical level the aggregation of this sort of data seems to be very difficult or impossible, given widely-known concerns over privacy and the serious penalties associated with breaches of privacy obligations. Furthermore, community leaders generally do not yet see a clinical, business, or public interest rationale that has been sufficient to overcome these concerns.

This report gives an overview and assessment of regulatory, ethical, and privacy issues specifically related to the use of aggregated care plan and related health data for analytical use across defined geographical catchment areas. The literature covering regulation and privacy of healthcare data is extensive and often contentious. Our review here highlights some major sources for authoritative guidance, then moves on to the specific situation of using aggregated and de-identified data sets for geographic analysis. Regulations that are specific to requirements for maintaining care plans were covered in a prior project report and are not repeated here.[1]

A key conclusion of our review is that using aggregated and de-identified data on a broad geographic basis is probably *not* restricted as much as many of our community stakeholders and leaders think. Some uses of such data are specifically exempted from key privacy laws when appropriate protections are in place. Some regional health care payer systems and Health Information Exchanges (HIEs) have mechanisms to enable such research now, using very large data sets they have already compiled. This means that it is feasible to carry out pilot projects to demonstrate practical methods for data aggregation and analysis for a community or region in many parts of the United States.

Overview of the Regulatory Environment for Healthcare Data

Primary sources for regulatory and privacy information include the following key laws, guidelines, and policy materials. In this section we define a number of terms we will use later when discussing how data can be aggregated for analytical use by communities. We refer frequently to the Code of Federal

[1] Lynn, J., and Morgan, L. (October 20, 2017). *Interim Report on the Variety and Merits of Care Plan Templates and Regulations in Use, Including Implications for Information Technology*.

Regulations (CFR), which offers a convenient online interface for those wishing to read CFR provisions in detail.[2]

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, required the U.S. Department of Health and Human Services (HHS) to adopt national regulatory and technical standards for electronic health care transactions. The Privacy and Security Rules promulgated under HIPAA were the first Federal regulations to broadly address the privacy and security of health information.[3] These rules cover a broad range of topics required for effective exchange of health information, including code sets, unique health identifiers, privacy, and security. HIPAA establishes a federal floor for privacy practices, meaning states can, and in many cases have, put in place more protective and restrictive standards, particularly for certain categories of protected health information (PHI).

Health care providers and health plans that are subject to HIPAA, including the HIPAA Privacy Rule, are known as HIPAA covered entities, or simply *covered entities*. Their *business associates* (BA) are persons or entities providing certain functions or activities involving PHI. A legal contract between a covered entity and a business associate is called a *business associate agreement* (BAA). For definitions of "covered entity" and "business associate" see 45 CFR 160.103.

- HIPAA defines a *covered entity* as 1) a health care provider that conducts certain standard administrative and financial transactions in electronic form; 2) a health care clearinghouse; or 3) a health plan.[4]
- A *business associate* is a person or entity (other than a member of the covered entity's workforce) that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of *protected health information* (PHI). Examples of business associates are lawyers, accountants, and firms that analyze patient data. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e).

Since increased adoption of electronic information technology could erode privacy, Congress incorporated into HIPAA certain provisions that mandated the adoption of Federal privacy protections for individually identifiable health information. HIPAA regulations are voluminous, detailed, and subject

---

[2] The *Electronic Code of Federal Regulations* (e-CFR) is not an official legal edition of the CFR. The e-CFR is an editorial compilation of CFR material and Federal Register amendments produced by the National Archives and Records Administration's Office of the Federal Register (OFR) and the Government Publishing Office. Retrieved February 13, 2018, from https://www.ecfr.gov

[3] Office of the National Coordinator for Health Information Technology. (December 15, 2008). *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information*. Page 3. Retrieved March 8, 2018, from https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

[4] Detailed definitions of varying types of covered entities, business associates (45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)), and associate agreements can be found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (Retrieved February 2, 2018).

to strict enforcement. A high-level summary of their contents, with links to detailed regulatory guidance, can be found on the HHS HIPAA web site, which includes information both for professionals and for the public.[5]

The HIPAA Privacy Rule protects most "individually identifiable health information." The term for information subject to the rule is *protected health information* (PHI), which is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium (45 CFR 160.103).[6] The Privacy Rule gives individuals the right to receive an accounting of certain disclosures of PHI made by a covered entity.[7] The Privacy Rule gives patients the right to make complaints to the covered entity and to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).[8]

Many common identifiers such as name, address, birth date, and Social Security Number are considered PHI when they can be associated with health information such as a health condition, health care provision, or payment data. By contrast, reports and analytical documents that are developed by aggregating information from many health records are not considered PHI if they do not identify any individuals and there is no reasonable basis to conclude that specific people could be identified through use of such reports. The use of aggregated health data is essential for many secondary purposes such as health system management, policy assessment, quality improvement, and equity analysis. Aggregating data involves a process called *de-identification* by which personal identifiers are removed from PHI. De-identification mitigates privacy risks to individuals. Specific standards for performing de-identification are discussed below in this report [page 24].

HIPAA provides special protection for psychotherapy notes.[9] Covered entities must obtain authorization from the patient or an appropriate surrogate to use or disclose psychotherapy notes, except for (1) use in the person's treatment or (2) certain narrow exceptions, such as use by the covered entity itself in training programs or to defend itself in a legal proceeding, or to avert a serious and imminent threat to

---

[5] The main web site is at https://www.hhs.gov/hipaa/index.html. Professional guidance is in the branch of that site at https://www.hhs.gov/hipaa/for-professionals/index.html (Retrieved January 21, 2018).

[6] The definition exempts a small number of categories of individually identifiable health information, such as individually identifiable health information found in employment records held by a covered entity in its role as an employer. HIPAA defines health information with a set of nested definitions: health information, individually identifiable health information, and protected health information. (45 C.F.R. § 160.103, *Definitions*) The effective result is that HIPAA covers all identifiable information held by a covered entity related to health care treatment or to payment for the provision of health care. In practical terms, all identifiable data processed by a HIPAA covered entity is PHI subject to the HIPAA rules. See: U.S. Department of Health and Human Services. Gellman, R. (December 13, 2017). *Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges*. A Report for the National Committee on Vital and Health Statistics (NCVHS) and its Privacy, Security, and Confidentiality Subcommittee. Page 3. Retrieved February 26, 2018, from https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf

[7] 45 CFR § 164.528.

[8] HHS.gov. Health Information Privacy. *Filing a Complaint*. Retrieved February 13, 2018, from https://www.hhs.gov/hipaa/filing-a-complaint/index.html

[9] 45 CFR § 164.508(a)(2). Cornell Law School. Legal Information Institute. *§ 164.508 Uses and disclosures for which an authorization is required*. Retrieved February 4, 2018, from https://www.law.cornell.edu/cfr/text/45/164.508

public health or safety. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes, not with other types of protected health information.[10] Substance abuse records are governed by 42 CFR part 2 (previously known as the confidentiality of drug abuse and alcohol abuse records), as discussed below in a separate section of this report (page 24).

The privacy rule permits disclosure of protected health information without the patient's authorization, subject to various conditions and limitations, for some specific purposes. In some cases, disclosure is permitted for uses other than clinical patient care. Examples of permitted disclosures that serve a non-clinical purpose include research, public health activities, protection of public safety, law enforcement, legal proceedings, and health oversight activities. Research is defined in the Privacy Rule as, "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[11]

In approaching the complex issues of how HIPAA rules affect data exchange, it is important to remember that standards have been put in place to facilitate appropriate exchanges, not block them. The Office of the National Coordinator for Health Information Technology (ONC) publishes a series of fact sheets giving numerous examples of when electronic health information can be exchanged without first requiring an authorization or a writing of some type from the patient, so long as other protections or conditions are met. ONC Privacy Officers have said that:[12]

> *At ONC, we hear all of the time that the Health Insurance Portability and Accountability Act (HIPAA) makes it difficult, if not impossible, to move electronic health data when and where it is needed for patient care and health. This is a misconception, but unfortunately one that is widespread. This blog series and accompanying fact sheets aim to correct this misunderstanding so that health information is more often available when and where it is needed.*
>
> *What many people don't realize is that HIPAA not only protects personal health information from misuse, but also enables that personal health information to be accessed, used, or disclosed interoperably, when and where it is needed for patient care.*

---

[10] 45 CFR § 164.508(b)(3)(ii).

[11] For documentation on research disclosures specifically, see: HHS.gov. Health Information Privacy. *Research*. Retrieved February 13, 2018, from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/research/index.html

[12] Brooks, A., & Savage, L.. Office of the National Coordinator for Health Information Technology. (February 4, 2016). *The Real HIPAA Supports Interoperability*. HealthITBuzz. Series of four blog posts. Retrieved January 30, 2018, from https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/the-real-hipaa-supports-interoperability/

This theme was restated in the proposed Fiscal Year 2019 budget request for ONC that was released by the Trump Administration on February 12, 2018. The request stated that ONC will continue working with OCR to demonstrate how HIPAA and other privacy laws and regulations "support, rather than impede, information flow in an electronic environment."[13]

Demonstrating respect for privacy is essential to building an atmosphere of trust that will enable appropriate use of shared data. Strong privacy protections unlock the potential benefits of health information technology, as these remarks from ONC's principles for a nationwide privacy and security framework make clear.[14]

> *The principles [in the national policy framework] establish a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the legal framework that may apply to a particular organization. The goal of this effort is to establish a policy framework for electronic health information exchange that can help guide the Nation's adoption of health information technologies and help improve the availability of health information and health care quality. ...*
>
> *Numerous forces are driving the health care industry towards the use of health information technology, such as the potential for reducing medical errors and health care costs, and increasing individuals' involvement in their own health and health care. To facilitate this advancement and reap its benefits while reducing the risks, it is important to consider individual privacy interests together with the potential benefits to population health.*

21ST CENTURY CURES ACT

The 21st Century Cures Act (the "Cures Act") was enacted by Congress in December 2016.[15] Section 4003 of the 21st Century Cures Act directed ONC to create a framework and agreement for the secure exchange of health information between networks. That portion of the law is being implemented now in

---

[13] Slabodkin, G. February 13, 2018). *Trump budget eliminates AHRQ, makes major cuts to OCR, ONC*. Health Data Management. (Retrieved February 13, 2018, from https://www.healthdatamanagement.com/news/trump-budget-eliminates-ahrq-makes-major-cuts-to-ocr-onc

[14] Office of the National Coordinator for Health Information Technology. (December 15, 2008). *Nationwide Privacy and Security Framework For Electronic Exchange of Individually Identifiable Health Information*. Page 1. Retrieved March 8, 2018, from https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

[15] For a summary of the law see: Congress.gov. *H.R. 34 – 21st Century Cures Act*. Retrieved March 5, 2018, from https://www.congress.gov/bill/114th-congress/house-bill/34/ For the full text see: Congress.gov. *Public Law 114–255—Dec. 13, 2016*. https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf

the form of a draft Trusted Exchange Framework and Common Agreement (TEFCA), discussed below [page 24].

The Cures Act also includes provisions to prevent information blocking.[16,17] Section 4002(a) of the Cures Act requires HHS through notice and comment rulemaking to require, as a condition of certification and maintenance of certification, that the HIT developer or entity does not take any action that constitutes information blocking (as defined in Section 3022(a) of the Public Health Service Act, as amended), or "any other action that may inhibit the appropriate exchange, access, and use of electronic health information".[18] The Cures Act defines "information blocking" broadly as a "practice that ... is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information" if that practice is known by a developer, exchange, network, or provider as being likely to "interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information."[19]

ONC is developing a proposed rule on information blocking that is expected to be released in early 2018.[20] The ONC blocking rule will be used by the Office of the Inspector General in HHS to guide investigations and enforcement actions against entitities that impede the electronic flow of healthcare information between organizations. The law provides for penalties of up to $1 million per violation. In connection with the new data blocking provisions, HHS will educate providers about data sharing misunderstandings that could hinder better interoperability. Improved awareness about the need for data sharing as part of the Cures Act reinforces our findings that providers are often more conservative than they need to be about some uses of data that could ultimately benefit both patients and care delivery systems.

AUDIT PROTOCOLS AND RISK ASSESSMENT

Studying standard auditing protocols is a good way to get an overview of key risk factors for groups wanting to begin data aggregation projects. Currently, the HHS HIPAA audit protocol covers 169 areas of performance evaluation, including 81 related to the Privacy Rule, 10 related to the Breach Notification

---

[16] (§ 4002) The bill requires developers of health IT, for their health IT to be certified, to meet certain requirements, including that the developer not engage in information blocking, which is preventing, discouraging, or interfering with the access, exchange, or use of information. (§ 4004) Developers of health IT and health care providers may be penalized for engaging in information blocking. Congress.gov. *H.R. 34 – 21st Century Cures Act*. Retrieved March 5, 2018, from https://www.congress.gov/bill/114th-congress/house-bill/34/

[17] For a review of information blocking issues see: Office of the National Coordinator for Health Information Technology. (April 2015). *Report to Congress: Report on Health Information Blocking*. Retrieved March 5, 2018, from https://www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf

[18] Morris, G., and Anthony, E. (January 8, 2018). *21st Century Cures Act Overview for States*. SIM State Educational Session 1. An Overview of the 21st Century Cures Act for States. Retrieved March 5, 2018, from https://www.healthit.gov/sites/default/files/curesactlearningsession_1_v6_10818.pdf

[19] 42 U.S.C. § 300jj-52(a).

[20] Slabodkin, G. (December 20, 2017). *ONC plans to release rule to tackle information blocking in early 2018*. Health Data Management. Retrieved March 5, 2018, from https://www.healthdatamanagement.com/news/onc-plans-to-release-rule-to-tackle-information-blocking-in-early-2018

Rule, and 78 related to the Security Rule. The audit protocol is available at the HHS OCR Privacy website, and provides an integrated description of key regulation components.[21]

The Security Rule requires that covered entities and, per The Health Information Technology for Economic and Clinical Health (HITECH) Act, business associates, conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity.[22] The Security Rule requires the risk assessment to be documented but does not require a specific format.[23]

A comprehensive review should include modern technologies such as electronic mail, text messaging, mobile devices, smartphones, flash drives, web-based applications, use of encryption, and dependency on vendors, including cloud-based systems. In some cases, these newer technical methods have risk profiles that are not well-understood and are subject to novel forms of attack.

GENERAL PRIVACY REGULATION IN THE UNITED STATES

HIPAA is not the only law affecting privacy and security of data in the United States. General privacy law in the United States includes many protections in addition to specific privacy of healthcare data. A variety of Federal, State, and local laws apply to specific jurisdictions and business situations.

State laws may affect the confidentiality of a patient's health information, both before and after death.[24] In general, HIPAA establishes a Federal floor for health care privacy protection and preempts contrary state laws that provide less protection for individual health information.[25] The basic tenets of § 160.203 are that if state law is "contrary" to HIPAA, then the latter preempts and is controlling; but if state law is "more stringent" than HIPAA, then in essence the federal and state laws are complementary and both apply. Both "contrary" and "more stringent" are terms of art defined in Subpart B.[26] In general, a “more stringent” law is one that increases either the duties of providers or the rights of patients. ONC’s Health

---

[21] U.S. Department of Health & Human Services. *(Updated April 2016). Health Information Privacy: Audit Protocol* Retrieved November 2, 2017, from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

[22] 45 CFR § 164.308(a)(1)(ii)(a). A useful presentation on practical aspects of audit risk is available from the American Health Lawyers Association. See: Kirk, K.S., and Rostolsky, B.M. *The Evolution of HIPAA: Impact of HITECH and Increased HIPAA Enforcement on Physician Practices*. For slides of that presentation see: Retrieved February 9, 2018: https://www.healthlawyers.org/Events/Programs/Materials/Documents/PHY13/C_kirk_rostolsky_slides.pdf. For a written document on those issues see: Retrieved February 9, 2018, from https://www.healthlawyers.org/Events/Programs/Materials/Documents/PHY13/C_kirk_rostolsky.pdf.

[23] 45 CFR § 164.316(b)(1). See: Cornell Law School. Legal Information Institute. (January 25, 2013). *45 CFR 164.316 - Policies and procedures and documentation requirements*. Retrieved February 13, 2018, from https://www.law.cornell.edu/cfr/text/45/164.316

[24] For an example of how state laws intersect with HIPAA regulations, see: Orlando, J. Connecticut General Assembly. Office of Legislative Research. *OLR Research Report 2013-R-0124. Disclosure Of Deceased Person’s Medical Records*. (February 13, 2013). Retrieved February 4, 2018, from https://www.cga.ct.gov/2013/rpt/2013-R-0124.htm

[25] Key sections that address the interactions between HIPAA rules and state laws are § 160.201, § 160.202, § 160.203, § 160.204 and § 160.205. Questions on these matters should be reviewed by legal counsel with expertise in the domain under study.

[26] This characterization of the legal approach is from *HIPAA and State Law*. Retrieved February 4, 2018, from http://www.hipaasurvivalguide.com/hipaa-state-law.php

IT Dashboard includes a feature in its State Health IT Policy Levers Compendium that contains over 300 examples of how states promote health IT and advance interoperability via 32 distinct policy levers, including the lever of "State Privacy and Security Policies." An interactive map gives an overview of state efforts for any policy lever chosen.[27] The Health IT Dashboard has another feature that gives an overview of State health IT privacy and consent laws and policies that can be visualized online or downloaded as an open data set.[28] The Agency for Healthcare Research and Quality (AHRQ) distributes a Health Information Security and Privacy Collaboration Toolkit that provides guidance for conducting organization-level assessments of business practices, policies, and State laws that govern the privacy and security of health information exchange.[29] The toolkit was developed as part of the AHRQ and ONC joint-funded Health Information Security and Privacy Collaboration (HISPC) project.

Examples of state laws that are "more stringent" include placing stronger limits on provider disclosures of health information, allowing patients greater access to their health data, or increasing minimum times for medical record retention.[30] State laws that are "more stringent" often pertain to public health uses such as collection of, and access to, records regarding births and deaths, child abuse, substance abuse, and communicable diseases. For example, the State of Connecticut has state laws that establish privileged communications, with exceptions that allow for disclosure without consent, for five categories of health care providers (psychologists, physicians, psychiatrists, social workers, and professional counselors) as well as for marriage and family therapists and battered women's or sexual assault counselors.[31]

This complex patchwork of laws places multiple requirements on any entity, not just healthcare providers that are classifed as covered entities. For example, community-based-organizations (CBOs) that handle PHI may not be classified as healthcare entities themselves, but may be in a business agreement (BA) with a covered entity and therefore covered by HIPAA rules. They will also be bound by any privacy laws that are defined separately from HIPAA requirements.

Recognizing that state laws and Medicaid policy are an important influence on health care, the National Governors Association developed a road map specifically for complex care programs[32] and a road map

---

[27] Office of the National Coordinator for Health Information Technology. *State Health IT Policy Levers Compendium*. Health IT Dashboard. Retrieved 8 March, 2018, from https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations/state-hit-policy-levers-compendium

[28] Office of the National Coordinator for Health Information Technology. (July 2017). *State Health IT Privacy and Consent Laws and Policies*. Health IT Dashboard. Retrieved March 8, 2018, from https://dashboard.healthit.gov/apps/state-health-it-privacy-consent-law-policy.php

[29] Agency for Healthcare Research and Quality. *Health Information Security and Privacy Collaboration Toolkit*. Retrieved March 8, 2018, from https://healthit.ahrq.gov/health-it-tools-and-resources/health-information-security-and-privacy-collaboration-toolkit

[30] Craig, D. (October 10, 2016). *What You Need to Know About HIPAA and Your State's Laws*. Retrieved February 6, 2018, from https://blog.sprucehealth.com/need-know-hipaa-states-laws/

[31] Orlando, J. (February 13, 2013). Connecticut General Assembly. Office of Legislative Research. OLR Research Report 2013-R-0124. *Disclosure Of Deceased Person's Medical Records*. Retrieved February 4, 2018, from https://www.cga.ct.gov/2013/rpt/2013-R-0124.htm

[32] Wilkniss, S., Pandit, S., Arabo, F., Malone, S., & Tewarson, H. (June 2017; Revised October 2017). *Building Complex Care Programs: A Road Map for States.* Washington, DC: National Governors Association Center for Best

"to help states evaluate and implement changes to achieve better health, better care and lower costs by increasing the flow of clinical health care information between health care providers, while protecting patient privacy, as a step toward nationwide interoperability."[33] In that road map, state strategies to address legal barriers include:

- ***Fully Align State Privacy Laws With HIPAA***: Pass a law that supersedes all more restrictive state privacy laws to allow providers and hospitals to exchange information in accordance with HIPAA.
- ***Partially Align State Privacy Laws With HIPAA***: Amend select statutes to allow certain types of information, such as information exchanged electronically, to be exchanged in accordance with HIPAA.
- ***Create Standardized Consent Forms***: Create a standardized consent form that provides a "one stop" approach to gaining patient permission for sharing information.
- ***State Guidance and Education***: Issue guidance and provide education to providers about how to comply with state and federal law, including clarifying legal intent and addressing common misconceptions.

A recent report for the National Committee on Vital and Health Statistics (NCVHS) provided an "environmental scan" of privacy and security implications of uses of health information that are outside or beyond the scope of HIPAA. The goal was "to explore existing and emerging policy frameworks, practices, and technologies to better frame key issues and drivers of change" in several key areas. The first issue on their list was, "Big data and expanding uses and users."[34] The report goes "beyond HIPAA" in the sense that, while PHI is defined by and regulated by HIPAA, and therefore subject to controls in the hands of covered entities, there is also a vast and growing amount of health data circulating that is not subject to specific HIPAA statutory regulation for privacy (though some of this data may fall under the scope of other privacy law). The magnitude of the privacy risks for that class of health information must not be underestimated. Consider this extract from the NCVHS report (page 1):

> *"Many but not all of the activities in the non-HIPAA category involve organizations that rely on health data as an element of a commercial activity, including data brokers, advertisers, websites, marketers, genetic testing companies, and others. The unregulated category includes some governmental and non-profit activities as well. The size of the unregulated world of health data*

Practices. Retrieved March 4, 2018, from https://www.nga.org/files/live/sites/NGA/files/pdf/2017/ComplexCare_RoadMap_12.17_Health.pdf

[33] Johnson, K., Kelleher, C., Block, L., & Isasi, F. (2016). *Getting the right information to the right health care providers at the right time: A road map for states to improve health information flow between providers*. Washington, DC: National Governors Association Center for Best Practices. Retrieved March 5, 2018, from http://gettingtherightinformationtoproviders.cwsit.org/

[34] U.S. Department of Health and Human Services. Gellman, R. (December 13, 2017). *Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges*. A Report for the National Committee on Vital and Health Statistics (NCVHS) and its Privacy, Security, and Confidentiality Subcommittee. Page 1. Retrieved February 26, 2018, from https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf

> *is hard to estimate, but one health media expert said that in 2016, there were more than 165,000 health and wellness apps available through the Apple App Store alone. Those apps represent a small fraction of the unregulated health data sphere."*

THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). Provisions of HITECH are designed to promote the adoption and meaningful use of health information technology in the United States.[35] Sections 13400-13411 of HITECH address privacy, security, and breach notification provisions for electronic exchange and use of health information.

The HITECH Act empowers ONC to carry out efforts to improve health care quality, safety, and efficiency through the promotion of health information technology. ONC operates under the U.S. Department of Health and Human Services. ONC activities include setting the standards and certification criteria that electronic health records (EHRs) must meet, and standards for private and secure electronic health information exchange.[36] ONC also provides regulatory resources, including FAQs and links to other health IT regulations. ONC's Nationwide Interoperability Roadmap provides a strategic vision extending to 2024 for many issues.[37] Protecting privacy and security in all aspects of interoperability and respecting individual preferences are among the guiding principles for that Roadmap. ONC, in coordination with OCR, offers a *Guide to Privacy and Security of Electronic Health Information* to help providers integrate privacy and security into their practices.[38]

SUBSTANCE ABUSE RECORDS (42 CFR PART 2)

Congress has established special laws regarding the confidentiality of substance use disorder patient records in order to address the stigma associated with those conditions. Since 2017, the law has been governed by 42 CFR Part 2 REVISED (previously known as the "confidentiality of drug abuse and alcohol

---

[35] HHS.gov. Health Information Privacy. *HITECH Act Enforcement Interim Final Rule*. Retrieved February 4, 2018, from https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

[36] HHS.gov. *Health IT Legislation and Regulations*. Retrieved February 12, 2018, from https://www.healthit.gov/policy-researchers-implementers/health-it-legislation-and-regulations

[37] Office of the National Coordinator for Health Information Technology. *Connecting Health and Care for the Nation A Shared Nationwide Interoperability Roadmap. Final Version 1.0*. Retrieved February 4, 2018, from https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperability-roadmap-final-version-1.0.pdf

[38] The Office of the National Coordinator for Health Information Technology (ONC). *Guide to Privacy and Security of Electronic Health Information*. Retrieved January 7, 2018, from https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information

abuse records"). Further revisions to this law became effective from February 2, 2018.[39] The 2018 law is detailed, and providers are trying to understand what they must do to comply with its provisions. Patient consent is required for disclosures, with some exceptions. The conditions for granting consent, and the ability to have that consent cover multiple uses of the data, is an actively evolving area of regulation. We have learned from interviews that providers are taking a very cautious stance with regard to this category of data in particular and are reluctant to share the information, even with authorized partners.

The relationship between 42 CFR Part 2 and State laws is similar to that between HIPAA and state laws, in that it establishes a Federal floor on privacy protections. 42 CFR § 2.20, states that "no State law may authorize or compel any disclosure prohibited by these [Part 2] regulations." However, States may impose additional confidentiality protections. Thus, § 2.20 provides that, "If a disclosure permitted under these regulations is prohibited under State law, neither these regulations nor the authorizing statutes may be construed to authorize any violation of that State law."[40]

In 2010, the HHS Substance Abuse and Mental Health Services Administration (SAMHSA) and ONC published Frequently Asked Questions (FAQ), "Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)".[41] The FAQ document was prepared by SAMHSA staff, in collaboration with staff from ONC and contractors, but it should not be considered to be definitive legal advice. That FAQ made clear that, even under older and more restrictive versions of the law, the revised federal law that protects the confidentiality of alcohol and drug abuse patient records does allow information about patients with substance use disorders to be included in electronic health information exchange systems, so long as appropriate consent requirements are met. As noted in Question 1 of the FAQ, "This consent requirement is often perceived as a barrier to the electronic exchange of health information. However, as explained in other FAQs, it is possible to electronically exchange drug and alcohol treatment information while also meeting the requirements of Part 2." Additionally, Question 16 notes that demographic information about patients with PHI documenting substance abuse (which therefore comes under Part 2) may be released without patient consent if the demographic information does not reveal anything that would identify the person, either directly or indirectly, as having a current or past drug or alcohol problem or as being a patient in a Part 2 program.

In January 2017, SAMHSA issued proposed rules to update 42 CFR Part 2 in order to allow patients to provide consent for a general disclosure of substance abuse information, rather than limiting

---

[39] The finalized 2018 rule has been posted to the Federal Register for public inspection. 42 CFR Part 2 [SAMHSA-4162-20] RIN 0930-ZA07. Retrieved January 29, 2018, from https://s3.amazonaws.com/public-inspection.federalregister.gov/2017-28400.pdf

[40] For Frequently Asked Questions (FAQ) on applying the substance abuse confidentiality regulations of 42 CFR Part 2 (REVISED) see: Substance Abuse and Mental Health Services Administration. *Substance Abuse Confidentiality Regulations*. Retrieved February 13, 2018, from https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs

[41] Legal Action Center for the Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services. Sarah A. Wattenberg, MSW, Project Officer. Contract # OMB0990-0115. *Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*. Retrieved January 28, 2018, from https://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf

authorization to a specific provider. The changes made in 2017 were the first substantive revisions to the regulations in nearly 30 years. SAMHSA's intention was to facilitate the sharing of information within the healthcare system to support new models of integrated healthcare, but some providers criticized the approach taken and called for closer alignment with HIPAA. Some associations felt that the rule made sharing clinical information more difficult.[42]

The finalized 2018 rule builds on the 2017 changes to 42 CFR Part 2. It permits healthcare providers, with patients' consent, to more easily conduct such activities as quality improvement, claims management, patient safety, training, and program integrity efforts. In a statement, Elinore F. McCance-Katz, M.D., the nation's first Assistant Secretary for Mental Health and Substance Use, said, "This final rule underscores our commitment to ensuring persons with substance use disorders receive integrated and coordinated care."[43]

Efforts to align Part 2 rules with HIPAA through legislation are pending. U.S. Senators Joe Manchin (D-WV) and Shelley Moore Capito (R-WV) have introduced S.1850, Protecting Jessica Grubb's Legacy Act (Legacy Act), in the Senate.[44] The Legacy Act would bring the regulations governing treatment records for substance use disorders in better alignment with the privacy rules and protections for other medical records.[45]

HEALTH INFORMATION FOR DECEASED INDIVIDUALS

The HIPAA Privacy Rule protects individually identifiable health information about a decedent for 50 years following the date of death of the individual.[46] After this, it can be disclosed. Prior to that time, an authorized individual (a family member or other persons involved in the individual's health care or payment for care prior to the individual's death) can authorize release.

Health information for deceased individuals is noted as a special case in 45 CFR 160.103, paragraph (2)(iv) of the definition of "protected health information".

---

[42] Landi, H. (January 3, 2018). *SAMHSA Issues Final Rule Updating Substance Abuse Confidentiality Regulations*, Healthcare Informatics, includes the statement that, "In that rule, SAMHSA aimed to facilitate the sharing of information within the healthcare system to support new models of integrated healthcare. But some associations attested at the time that the rule makes sharing clinical information for treatment purposes more difficult." Retrieved January 28, 2018, from https://www.healthcare-informatics.com/news-item/privacy/samhsa-issues-final-rule-updating-substance-abuse-confidentiality-regulations

[43] Characterization of the 2018 changes and quotation from Elinore F. McCance-Katz, M.D. is from Landi, H. (January 3, 2018). *SAMHSA Issues Final Rule Updating Substance Abuse Confidentiality Regulations*. Healthcare Informatics. Retrieved January 28, 2018, from https://www.healthcare-informatics.com/news-item/privacy/samhsa-issues-final-rule-updating-substance-abuse-confidentiality-regulations

[44] Congress.gov. *S.1850 - Protecting Jessica Grubb's Legacy Act*. 115th Congress (2017-2018). Retrieved January 29, 2018, from https://www.congress.gov/bill/115th-congress/senate-bill/1850

[45] Characterization of the Legacy Act is from Leventhal, R. (September 27, 2017). *New Legislation Intends to Align Substance Abuse Treatment Records with HIPAA*. Healthcare Informatics. Retrieved January 29, 2018, from https://www.healthcare-informatics.com/news-item/privacy/new-legislation-intends-align-substance-abuse-treatment-records-hipaa

[46] HHS.gov. Health Information Privacy. *Health Information of Deceased Individuals*. Retrieved February 4, 2018, from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html

> ***From § 160.103 Definitions:*** *Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition,[….]*
>
> *(2) Protected health information excludes individually identifiable health information: [….] (iv) Regarding a person who has been deceased for more than 50 years.*
>
> ***§ 164.502(f) Standard: Deceased individuals:*** *A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.*

States may amend or create statutes that modify the circumstances under which the person's authorized representative can assert privilege after the person's death.

Unless blocked by HIPAA or state law, a covered entity that maintains identifiable health information on individuals who have been deceased for more than 50 years may use or disclose the information without regard to the Privacy Rule because the information is not considered protected health information.

The HHS audit protocol for compliance with § 164.502(f) includes two questions for auditors:[47]

- Do the covered entity's policies and procedures protect the deceased individual's PHI consistent with the established performance criterion? Inquire of management.
- Obtain and review policies and procedures regarding use and disclosure of deceased individuals' PHI. Evaluate whether the policies and procedures are consistent with the established performance criterion.

The Privacy rule includes provisions that permit a covered entity to disclose a decedent's protected health information in some specific circumstances:

- § 164.510(b)(5) to a family member, or other person who was involved in the individual's health care or payment for care prior to the individual's death, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the covered entity. This may include disclosures to spouses, parents, children, domestic partners, other relatives, or friends of the decedent, provided the information disclosed is limited to that which is relevant to the person's involvement in the decedent's care or payment for care.
- § 164.512(f)(4) to alert law enforcement to the death of the individual, when there is a suspicion that death resulted from criminal conduct.
- § 164.512(g)(1) to coroners and medical examiners for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that

[47] HHS.gov. (*Updated April 2016)*. Health Information Privacy. *Audit Protocol*. Retrieved February 4, 2018, from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

also performs the duties of a coroner or medical examiner may use protected health information for the purposes described in this paragraph.

- § 164.512(g)(2) to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, the covered entity may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.
- § 164.512(h) to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation.
- § 164.512(i)(1)(iii) for research that is solely on the protected health information of decedents.

For uses or disclosures of a decedent's health information not otherwise permitted by the Privacy Rule, a covered entity must obtain a written HIPAA authorization from a personal representative of the decedent who can authorize the disclosure. Under Privacy § 164.502(g) [Personal representatives], a covered entity must recognize certain personal representatives of a deceased individual:

> *§ 164.502(g)(4) Implementation specification: Deceased individuals. If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation.*

Under Breach § 164.404(d) [Methods of Notification], notification of breaches involving deceased individuals is noted as a special case:

> *The notification required by paragraph (a) of this section shall be provided in the following form:*
>
> *(ii) If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under § 164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual is required. The notification may be provided in one or more mailings as information is available.*

PRIVACY ISSUES FOR PERSONAL HEALTH RECORDS (PHR)

The term "personal health record" (PHR) refers to a relatively new category of information technology systems that enable individuals to participate in direct management of their own health records.[48] The

[48] For a detailed review of issues specific to PHR systems see: Maximus Federal Services. (December 13, 2012). *Non-HIPAA Covered Entities: Privacy and Security: Policies and Practices of PHR Vendors and Related Entities Report*. Prepared for the Office of the Chief Privacy Officer, Office of the National Coordinator for Health

HITECH Act defines a PHR as, "an electronic record of ….PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[49] The most common sources for data in PHR systems are:

- *Health care provider data from Electronic Health Record (EHR) systems*. Some health care providers offer PHRs via portals into their EHRs.
- *Health insurer claims data*. Some Insurers offering beneficiaries access to PHRs that draw data from the insurer's claims data, sometimes with added functions to educate and offer guidance to beneficiaries on how to improve their health status.
- *Consumer/patient-entered data*. Some PHR systems allow users to add information about things such as glucose levels and weight to help monitor health status.
- *Device data, including real-time data trackers*. Information can be collected directly from devices such as glucose monitors, exercise trackers, weighing scales, etc., often with options to display trend analysis directly to the patient.

Several types of PHR systems are available, with varying capabilities. Some PHR systems are offered by health care providers and health plans that are covered by the HIPAA Privacy Rule (i.e., they are "covered entities" or "business associates").[50] PHR systems offered by vendors that are not HIPAA covered entities generally do not fall under HIPAA regulation, including the HIPAA Privacy Rule. PHR privacy policies for non-HIPAA entities are governed by vendor policies and by other applicable laws. PHR systems that are outside the scope of HIPPA regulation lack uniformity in their privacy and security practices. One study found that less than half of the non-HIPAA PHR systems examined held any form of private sector certification for privacy and security.[51]

ONC has published a Model Privacy Notice (MPN) as a voluntary, openly available resource to help developers of consumer-oriented applications clearly convey information about privacy and security policies to their users.[52] Like the FDA Nutrition Facts Label, the MPN provides a standardized summary of a company's privacy practices to encourage transparency and help consumers make informed choices. The MPN does not mandate specific policies or substitute for more comprehensive or detailed privacy policies.

PHRs not subject to HIPAA can be under the general jurisdiction of the Federal Trade Commission, which has a breach notification rule for non-HIPAA PHR vendors and related parties (16 CFR. Part 318), but no

---

Information Technology. Retrieved February 26, 2018, from https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf

[49] HITECH Act § 13400(11).

[50] Under HITECH Act §§ 13401, 13404, and 13408, vendors who contract with covered entities to offer PHRs on their behalf are considered business associates and must comply with most of the provisions of the HIPAA Security and Privacy Rules.

[51] The most common certifying bodies associated with the PHRs examined in this study were URAC (formerly the Utilization Review Accreditation Committee), TRUSTe and the Health on the Net Foundation (HON). Certification standards vary across these certifying organizations. Maximus Federal Services. (December 13, 2012). *Non-HIPAA Covered Entities: Privacy and Security: Policies and Practices of PHR Vendors and Related Entities Report*. Page 5. Retrieved February 26, 2018, from https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf

[52] HealthIT.gov. *Privacy & Security Policy: Model Privacy Notice (MPN)*. Retrieved March 8, 2017, from https://www.healthit.gov/policy-researchers-implementers/model-privacy-notice-mpn

other privacy rules for PHRs.[53] OCR provides a a review of how the HIPAA Privacy Rule applies to various uses of PHR systems.[54] In addition to federal protections, some states have enacted privacy laws that apply to PHRs.[55]

Ethical Issues

The regulations and practices given above and the strategies worked out below have deep roots in the values of Americans. In general, citizens are worried about the risks inherent in having deeply personal information shared with others. We are worried about embarrassment, causing family discord, losing employment, or just having private matters being exposed. However, we also see the advantages of having a complete record across service provider settings, especially if that record is available to the person. Although much less commonly noted, most people also recognize the merit of having aggregated analyses that show how groups of people are faring, so that improvements in overall processes and systems can be implemented. The tension between the interest in personal privacy and the interest in having reliable and efficient social systems is persistently unsettled and is adjudicated with a substantial body of social policy as expressed in regulations, statutes, court cases, and pronouncements of civil authorities. That balance of risks and benefits is likely to continue to change over time. This persistent tension and ongoing reassessment leaves many people perplexed and inconsistent. The same person whose every movement is catalogued by his car manufacturer's built-in GPS may feel outraged if a Health Information Exchange tells hospital B that he was at hospital A last week for the same complaint.

Most of these conflicts are endemic to information management generally, but there are a few considerations that arise in our work on improving care for frail and disabled elderly people that bring novel considerations to bear.

First, in a public health context, it is commonly considered acceptable to grant a broader license for transmitting and use of personal information, both identified and de-identified. Therefore, if the data management, analyses, and use of the resulting insights come under the aegis of public health authorities, most states and commentators grant broad access to personal data. That access comes with strong prohibitions on releasing identifiable data beyond what is essential in order to protect the person and the public. However, as public health endeavors to move to geo-mapping "hot spots" of high need, or generate areas with predictions of unmet need, specific persons may be identifiable in the data

[53] See: U.S. Department of Health and Human Services. Gellman, R. (December 13, 2017). Health Information *Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges*. A Report for the National Committee on Vital and Health Statistics (NCVHS) and its Privacy, Security, and Confidentiality Subcommittee. Page 4. Retrieved February 26, 2018, from https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf

[54] Office for Civil Rights. *Personal Health Records and the HIPAA Privacy Rule*. Retrieved January 23, 2018, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf

[55] Maximus Federal Services. (December 13, 2012). *Non-HIPAA Covered Entities: Privacy and Security: Policies and Practices of PHR Vendors and Related Entities Report*. Page 4. Retrieved February 26, 2018, from https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf

unless particular care is taken. For example, a public health worker might be sent to visit a home where supportive services are thought to be needed, but the address of the home should not be identified on a map that is made public. Instead, some broader aggregation, such as publishing the center of a ZIP code area, could be made public in most cases.[56] It may be useful for communities aiming to improve eldercare to locate important aspects of data management in public health offices in order to build on the broad accord that data analysis that is conducted in the public interest can use either identified or de-identified data in ways that enhance understanding, guide priority-setting, allow monitoring of steps to improve, and inform the public, so long as the public health staff do not release identifiable information to the public. This paper provides an overview of the applicable rules in a section on Public Health below [page 37].

Second, some of the insights from aggregating patient records could use records of persons who have died. Until HIPAA, the legal protections for the records of decedents were scant or non-existent. The heirs and relations of dead persons cannot assert privacy rights on behalf of the dead persons. However, as we develop above [page 14], HIPAA protects the records of dead persons for 50 years, providing penalties to the covered entities in much the same way as for living persons. In a particular circumstance, it may be attractive to seek the permissions of survivors to use records of decedents, for example, in a sampling frame of death certificates from a particular community. Certainly, experiences from the last few years are often sufficiently timely to serve to anchor priority setting and monitoring of improvement. While we have not found this question specifically addressed in the rules, it seems that a person could authorize use of his or her records in advance of death, just as a person can authorize organ donation or autopsy for themselves in advance.

Third, today there is greater recognition that persons living with serious, worsening, chronic conditions are regularly served by multiple providers of a various types. For example, an elderly woman living alone in rent-supported housing might have home-delivered meals, a homemaker, a volunteer from the local volunteer support network, a primary care physician, a care coordinator, and three specialist physicians. For a variety of reasons, there may be coordination and cooperation, which is increasingly formalized in contractual relationships, among these service providers that aim to increase desired outcomes such as reliability, efficiency, participant satisfaction, or participant independence in daily activities. In order to do so, they may need to discuss both aggregate data analyses and the woman's individual case. They would do well to have insights as to their system's outputs and costs, and otherwise work as if they were in one organization aiming for improvement in quality and costs. Historically, much of the work on ethics, regulations, and law has considered the records of one organization, but the need to work smoothly across organizational boundaries is increasingly recognized as being essential and valuable. Additional concern must be focused on data security, governance, access, and privacy when the technological attack surface is large, and the individuals who are given access report to different organizational structures. One strategy for resolving these pressures is the Organized Health Care Arrangement (OHCA) described below [page 44].

[56] Zip codes with low populations may be subject to special restrictions as determined by OCR.

In sum, the ethical mandate to act to enhance social welfare and equity creates a strong call to change traditional norms that have each organization closely hold patient-related data they have accumulated. With thoughtful protections for individuals, aggregating data in order to enhance public welfare and equity should be permissible. This can be accomplished through leadership of public health offices, broader use of data from the experiences of deceased persons, and collaborations among organizations that jointly serve a population.

Data Sources For Aggregated Use

This section explains some key ideas and terms of art in data management that are relevant to public reporting. Choosing the data to review is critical for any community undertaking seeking to improve care for its frail elderly population through data-driven guidance mechanisms. Policy makers need a fact-based overview of health care patterns in their area, and sharing insights through public reports builds citizen understanding of and support for community improvement projects. The issue is not whether public review of data would be valuable, but rather, what data will be both revealing and actionable. Due to the great importance of maintaining privacy and security over health records, the methods for moving health care data from protected clinical environments to public use must be studied closely. The goal is to help communities assemble, analyze, and report on aggregated data in a manner that ensures privacy and security. An IT design issue here is the difference between a dynamic clinical system, where information on specific individuals may change from minute to minute, and a static public reporting system that carries either aggregated historical records or relatively unchanging information that is being stored pending future use, such as a repository for advance directives.

In clinical settings, full identification of a patient is essential to treatment. At the point of collection, covered entities collect *protected health information* (PHI) that must be closely held within their care delivery system. If some, but not all, of the personal identifiers are removed from PHI, a covered entity may shared a *limited data set* for use outside its own care system, but only with entities that have entered into a Business Agreement (BA) with the covered entity, and under the specific terms of a Data Use Agreement (DUA). If all of the personal identifiers are removed, a covered entity may share *de-identified data* more freely for a wide range of purposes. De-identified data is not considered PHI, so Business Agreements and Data Use Agreements are generally not required in such cases, but other types of usage arrangements may be formalized as needed.

In all situations, identifiable data must be securely transferred and stored, and destroyed when no longer needed. Secure procedures are necessary to maintain privacy, and often are required as part of a DUA or an Institutional Review Board (IRB) protocol. Electronic PHI must be encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is

a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).[57] HHS guidance specifies:

- Valid encryption processes for data at rest must be consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*.[58]
- Valid encryption processes for data in motion must comply, as appropriate, with NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*[59]; 800-77, *Guide to IPsec VPNs*[60]; or 800-113, *Guide to SSL VPNs*[61], or others which are Federal Information Processing Standards (FIPS) 140-2[62] validated.

The media on which the PHI is stored or recorded must be destroyed in one of the following ways:

- Paper, film, or other hard copy media must be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
- Electronic media must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*[63] such that the PHI cannot be retrieved.

LIMITED DATA SETS

The term "limited data set" refers to a limited set of identifiable patient information as defined in the HIPAA regulations.[64] A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual. Because a limited data set may contain some information that could be used to identify specific patients, it is still considered to be PHI under

---

[57] HHS.gov. Health Information Privacy. *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals*. Retrieved March 7, 2018, from https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

[58] Scarfone, K.,, Souppaya, M., and Sexton, M. (November 2007). NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*. Retrieved March 7, 2018, from https://csrc.nist.gov/publications/detail/sp/800-111/final

[59] Polk, T., McKay, K., and Chokhani, S. (April 2014). NIST Special Publication 800-52 Rev. 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. Retrieved March 7, 2018, from https://csrc.nist.gov/publications/detail/sp/800-52/rev-1/final

[60] Frankel, S., Kent, K., Lewkowski, R., Orebaugh, A., Ritchey, R., and Sharma, S. (December 2005). NIST Special Publication 800-77, *Guide to IPsec VPNs*. Retrieved March 7, 2018, from https://csrc.nist.gov/publications/detail/sp/800-77/final

[61] Frankel, S., Hoffman, P., Orebaugh, A., and Park, R. (July 2008). NIST Special Publication 800-113, *Guide to SSL VPNs*. Retrieved March 7, 2018, from https://csrc.nist.gov/publications/detail/sp/800-113/final

[62] For information about FIPS 140-2 (effective 15-Nov-2001) and other related standards see: National Institute for Standards and Technology. *Cryptographic Module Validation Program*. Retrieved March 7, 2018, from https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards

[63] Kissel, R., Regenscheid, A., Scholl, M., and Stine, K. (December 2014). NIST Special Publication 800-88 Rev. 1, *Guidelines for Media Sanitization*. Retrieved March 7, 2018, from https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[64] To find HHS.gov FAQs related to limited data sets, see https://www.hhs.gov/hipaa/for-professionals/faq/limited-data-set (Retrieved February 3, 2018). For a practical overview of limited data set regulations see: John Hopkins Medicine. Office of Human Subjects Research— Institutional Review Board. (April 2015). *Definition of Limited Data Set*. Retrieved February 3, 2018, from https://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/limited_data_set.html

HIPAA rules. This differentiates *limited* data sets from fully *de-identified* data sets, which are are not classified as PHI.

A covered entity may disclose a limited data set to an outside party without a patient's authorization under certain conditions. First, under 45 CFR 164.514(e), the purpose of the disclosure may only be for research, public health, or health care operations. Second, the person receiving the information must sign a data use agreement (DUA) with the covered entity that provides the limited data set and defines the intent and the boundaries of permitted use.

Limited data sets are not subject to the HIPAA Accounting for Disclosures provisions. Under 2013 revisions to HIPAA, unauthorized uses or disclosures of a limited data set may constitute a "breach" for breach notification rule purposes.

All the following identifiers must be removed in order for health information to be a "limited data set". This list is less restrictive than the list of identifiers that must be removed to create a fully de-identified data set using the "Safe Harbor" method (see Appendix D).

- Names;
- Street addresses (other than town, city, state and zip code);
- Telephone numbers;
- Fax numbers;
- E-mail addresses;
- Social Security numbers;
- Medical records numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate license numbers;
- Vehicle identifiers and serial numbers, including license plates;
- Device identifiers and serial numbers;
- URLs;
- IP address numbers;
- Biometric identifiers (including finger and voice prints); and
- Full face photos (or comparable images).

The health information that may remain in the information disclosed in a limited data set includes:

- Dates such as admission, discharge, service, date of birth, date of death;
- City, state, five digit or more zip code; and
- Ages in years, months, days or hours.

DATA USE AGREEMENTS

Covered entities must enter into data use agreements with recipients of limited data sets, which are considered to be PHI. Data use agreements must meet standards specified in HIPAA privacy regulations. Draft templates for a data use agreement for those who wish to disclose a limited data set are available

from Johns Hopkins Medicine[65] and the Harvard Clinical and Translational Science Center (Harvard Catalyst).[66]

A data use agreement must:

- establish the permitted uses and disclosures of the limited data set;
- identify who may use or receive the information;
- prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law;
- require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement;
- require the recipient to report to the covered entity any unauthorized use or disclosure of which it becomes aware;
- require the recipient to ensure that any agents (including a subcontractor) to whom it provides the information will agree to the same restrictions as provided in the agreement; and
- prohibit the recipient from identifying the information or contacting the individuals.

Limited data sets are excepted from the accounting requirement at 45 CFR 164.528(a)(1)(viii). Where a covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function, the HIPAA Privacy Rule does not require the covered entity to enter into both a business associate agreement and a data use agreement with the business associate.[67] The covered entity satisfies the Rule's requirements that it obtain satisfactory assurances from its business associate with the data use agreement.The HHS FAQ on this issue says,

> *For example, where a State hospital association receives only limited data sets of protected health information from its member hospitals for the purposes of conducting and sharing comparative quality analyses with these hospitals, the member hospitals need only have data use agreements in place with the State hospital association.*

---

[65] To download templates, see: Johns Hopkins Medicine. Office of Human Subjects Research - Institutional Review Board. (April 2015). *Definition of Limited Data Set.* Retrieved February 4, 2018, from https://www.hopkinsmedicine.org/institutional_review_board/hipaa_research/limited_data_set.html For the template *HIPAA Form 9 (Version 4). Data Use Agreement*, see: https://www.hopkinsmedicine.org/institutional_review_board/forms/form9.doc (Retrieved March 5, 2018).

[66] Harvard Catalyst Data Protection subcommittee of the Regulatory Knowledge & Support Program. This work was conducted with support from Harvard Catalyst, The Harvard Clinical and Translational Science Center (National Center for Research Resources and the National Center for Advancing Translational Sciences, National Institutes of Health Award 8UL1TR000170-05 and financial contributions from Harvard University and its affiliated academic health care centers. *Harvard Catalyst Data Use Agreement For Limited Data Sets*. Retrieved February 4, 2018, from https://catalyst.harvard.edu/docs/regulatory_support/Harvard_Catalyst_Template_LDS_DUA.docx

[67] HHS.gov. Health Information Privacy. *If the only protected health information a business associate receives is a limited data set, does the HIPAA Privacy Rule require the covered entity to enter into both a business associate agreement and data use agreement with the business associate?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/251/what-agreements-are-needed-limited-data-set/index.html

CREATING LIMITED DATA SETS

A covered entity may use either of the following approaches to create a limited data set:

- The covered entity may use its own personnel to create the limited data set, or
- Under the HIPAA Privacy Rule, a covered entity may contract with a business associate to create a limited data set the same way it can use a business associate to create de-identified data.[68] The business associate agreement must meet the conditions of the privacy regulations. Once the conversion to a limited data set is completed under the business associate agreement, all of the PHI that includes direct identifiers must be returned to the covered entity or destroyed.

When a covered entity provides a recipient of a data set with protected health information that includes direct identifiers, a business associate agreement is required in addition to the data use agreement to protect the information. If the final user of the limited data set is also acting as the covered entity's business associate to create the limited data set from a broader set of PHI, the recipient will need to sign both a data use agreement and a business associate agreement. A data use agreement can be combined with a business associate agreement into a single agreement that meets the requirements of both provisions of the HIPAA Privacy Rule.[69]

METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Section 13424(c) of the HITECH Act requires the Secretary of HHS to issue guidance on how best to implement the requirements for the deidentification of health information contained in the Privacy Rule. Section 164.502(d) of the Privacy Rule permits a covered entity or its business associate to create information that is not individually identifiable by following the de-identification standard and implementation specifications in § 164.514(a)-(b). Under those provisions, an entity may use and disclose information that neither identifies nor provides a reasonable basis to identify an individual, but other protections may apply as well, such as those found in Family Educational Rights and Privacy Act (FERPA) or the Federal Policy for the Protection of Human Subjects, known as the "Common Rule." A covered entity may use a business associate to de-identify PHI on its behalf only to the extent such activity is authorized by their business associate agreement.

OCR has developed a 32-page guidance document on methods and approaches to achieve deidentification in accordance with the HIPAA Privacy Rule.[70] The guidance document uses a question

---

[68] HHS.gov. Health Information Privacy. *Under the HIPAA Privacy Rule, may a covered entity contract with a business associate to create a limited data set the same way it can use a business associate to create de-identified data?* Retrieved February 3, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/249/may-I-use-a-business-associate-to-create-a-limited-data-set/index.html

[69] HHS.gov. Health Information Privacy. *I want to hire the intended recipient of a limited data set to also create the limited data set as my business associate. Can I combine the data and use agreement and business associate contract?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/250/may-a-data-use-agreement-be-combined/index.html

[70] Office for Civil Rights. (November 26, 2012). *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy*

and answer format to explain many technical details of the de-identification process, including risk assessment factors and the two methods that can be used to satisfy the Privacy Rule's de-identification standard: Expert Determination and Safe Harbor. For details on these two de-identification methods, refer to Appendix D. For alternatives on when to apply de-identification in the overall data analysis process, see Figure 1, *Examples of Alternative Data Flows* [page 32].

Briefly summarized, the two methods are:

- **Expert Determination § 164.514(b)(1)**
  - Apply statistical or scientific principles
  - Very small risk that anticipated recipient could identify individual
- **Safe Harbor § 164.514(b)(2)**
  - Removal of 18 types of identifiers
  - No actual knowledge residual information can identify individual

When properly applied, both methods yield de-identified data where the risk that data could be linked back to specific patients is very small, but not zero. The guidance document states:[71]

> *Regardless of the method by which de-identification is achieved, the Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information.*

Clearly, when and how to de-identify data has deriviative implications for the analyses possible and the risks of improper disclosure or use. De-identification necessariy results in loss of information and limits some of the potential analyses. De-identification early in the process, just after merging data sets, limits risks to unauthorized use or release of data. Full de-identification loses more analytic opportunity than using a limited data set, but protects data better. The OCR guidance document recognizes that such information loss may limit the usefulness of the resulting health information in certain circumstances and suggests various de-identification strategies that minimize such loss. Deciding how to proceed requires balancing these risks and opportunities in the particular situation.

ALTERNATIVE MODELS FOR COMMUNITY DATA ANALYSIS

When approaching the question of how a community could obtain helpful and actionable information about how well it is addressing the needs of the frail elderly, there are several possible models of what data could be used. In Table 1 [page 31], we summarize six alternatives to illustrate major themes. These six methods present increasingly difficult technical challenges and privacy risks. A community that

---

Rule. Retrieved February 2, 2018, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

[71] Office for Civil Rights. (November 26, 2012). *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. Page 6. Retrieved February 2, 2018, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

wanted to begin work may choose to try simple models first because they are the easiest to do, and pose the least risk. A community need not go with the most demanding scenario in order to get started with the work.

Obviously, a less risky strategy in terms of breaching privacy is either to work only with de-identified data if that is all that is necessary, or to use PHI only early in the process, e.g., at the time of merging prior to de-identification. It is possible to provide adequate security to protect merging of PHI (which is fully identified) and then de-identify at a later step.

At its point of origin, data is fully identified for use in clinical work. Identified data requires more protection than de-identified data, but de-identified data still requires security and has constraints on use. The place in the information flow where data becomes de-identified is a critical point for security and privacy protections. Aggregation and deidentification are specialized technical tasks that must be performed under secure conditions, following a chain of custody model. The point in the chain of custody where de-identification takes place needs to be clear.

We can envision situations where a large network has a large enough market share to make their data useful by themselves. Also, in some public health scenarios, all providers in a community could submit de-identified data on specific conditions, allowing for creation of a community-wide view of specific things, with no exchange of PHI. That type of distributed approach probably would engender unidentified duplications (when a person is in multiple data sets and the overlap can't be identified). In a community where there is a dominant provider or a strong HIE, this problem might be small or at least stable. It may be wiser for a community to try something simple that can be implemented reasonably easily than insist on a perfect master plan that cannot be executed. Doing small pilots would enable a community to gain practical experience with the opportunities and pitfalls of data work and get a hands-on sense for what data would actually make a difference to their policy approach and resource allocation.

Analysis of data from more than one source requires that records be merged somehow. Since this report primarily addresses privacy issues, we will not elaborate too much on the technical challenges of merging data, but some discussion of merging is necessary to understand the aggregation alternatives a community could choose from. Another reason for including merging in a privacy review is that combining data from multiple sources can result in a cumulative privacy risk from matching that is greater than the sum of its parts.[72] Combining data from multiple sources creates the possibility that

---

[72] This increase in privacy risk due to merging of data is well-known in IT circles. For example, for discussion of correlation of information from multiple sources see: Rowland, D., Kohl, U., & Charlesworth, A. (2016). Chapter 9, *Privacy and data protection*. In *Information Technology Law*. Fifth edition. Routledge. Those authors use the term "function creep" to describe the gradual use of data for purposes other than those for which it was collected. and make the observation that in the case of data matching, "... correlation of information from disparate sources may produce an impression that is greater than the sum of its parts." Retrieved February 18, 2018, from https://books.google.com/books?id=8IKKDQAAQBAJ&pg=PT576&lpg=PT576&dq=privacy+risks+are+greater+than+the+sum+of+the+parts&source=bl&ots=qaMx3ZcAft&sig=s6H72v0DMWmuZtyqQTxPznr78z0&hl=en&sa=X&ved=0ahUKEwiNpbbBg7HZAhUGw2MKHXN2BF4Q6AEIKzAB#v=onepage&q=privacy%20risks%20are%20greater%20than%20the%20sum%20of%20the%20parts&f=false

while each of the individual data elements involved may have been authorized for use separately within their own contexts, the combination of the elements in novel ways may never have been explicitly envisioned or authorized. Emergent privacy risks from such combinations are becoming more apparent with the increase in online data from social media, purchasing behavior, and other activities that are unrelated to health care.[73]

The very definition of PHI may need to be expanded to address emergent privacy risks arising from aggregation. Consider the well-known case in which Target Department store used purchase data to infer that a teenage customer was pregnant. The customer's father, the last to know of his daughter's pregnancy, protested receiving advertisements for baby products. The NCVHS privacy report reviews this example and asks a pointed question:[74]

> *"The specific methodology Target used to make the inference is not public, but it is fair to assume that Target did not have access to health information from any HIPAA-covered source. Nevertheless, Target determined to a reasonable degree of commercial likelihood something that almost everyone is likely to agree is health information. Does the accuracy of the algorithm make a difference to whether the data is health information? If as a result of commercial or other inferences, an individual is treated as if she were pregnant, had HIV/AIDS, or had cancer, does that make the information health information even if the information is wrong or if the algorithm used to develop the information is highly, moderately, or not-very accurate?"*

The options for merging depend on the type of data being combined. You can only merge on a data element that is present in both of the records being compared. Furthermore, there are challenges when consolidating data from multiple sources without shared semantic coding standards.[75]

---

[73] The observation that, "the overall effect is greater than the sum of the individual parts," referring to the example of Google's ability to combine search data with other sources, is from: Bernal, P. (2014). *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge University Press. Page 71. Retrieved February 18, 2018, from https://books.google.com/books?id=0TI4AwAAQBAJ&pg=PA71&lpg=PA71&dq=privacy+risk+for+merging+data+greater+than+the+sum+of+the+parts&source=bl&ots=cDn9PiHkpT&sig=6dE48sZdaAcuUFiqO7ElzriunJk&hl=en&sa=X&ved=0ahUKEwjq_e74j7HZAhUB6mMKHedzCjoQ6AEIMjAB#v=onepage&q=privacy%20risk%20for%20merging%20data%20greater%20than%20the%20sum%20of%20the%20parts&f=false

[74] U.S. Department of Health and Human Services. Gellman, R. (December 13, 2017). *Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges*. A Report for the National Committee on Vital and Health Statistics (NCVHS) and its Privacy, Security, and Confidentiality Subcommittee. Page 6. Retrieved February 26, 2018, from https://www.ncvhs.hhs.gov/wp-content/uploads/2018/02/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf

[75] ONC publishes an assessment of implementation methods for vocabularies, code sets, and terminology as part of its Interoperability Standards Advisory (ISA). However, the ISA notes (page 1) that, "It is for informational purposes only. It is non-binding and does not create nor confer any rights or obligations for or on any person or entity." See: Office of the National Coordinator for Health IT. (2018). *2018 Interoperability Standards Advisory*

If the data being merged differ in type (de-identified, limited, or PHI), merging can only occur using a "lowest common denominator" present in both sources. For example, if one source is a de-identified data set containing a three-digit zip code, it could be merged with a limited data set containing a five-digit zip code, but only after the level of precision in the limited data set was reduced to the less-granular level of the de-identified data set. Similarly, if full PHI containing an exact street address for a patient were combined with a limited data set containing only a five-digit zip code, the match level could be only at the five-digit zip code level.

Merging need not be limited to combining patient-level data from more than one source. For things such as equity analysis, it may be desirable to study associations between community demographic factors such as average income, age, or education and observed health care transactions in a geographic unit such as a zip code or census tract. In that example, the merge operation would operate on a common geographic unit, not a common person specifically. We must be thoughtful about the risks of counting one person multiple times if the merging is done at a level more general than the person. In some cases, that doesn't matter. For example, if the issue were the load levels from falls with injury in the community's Emergency Rooms (ERs), it could be correct to count one person each time for each incident.

Growing interest in social determinants of health and "whole person care" are driving interest in combining health care data with other types of information to create a combined service profile for clients, and perhaps for all residents of an area. Information from food security programs, community-based organizations, and other social service providers creates new opportunites to improve the total quality of service for the most challenged clients. Frail elders with mutiple needs are particularly likely to require support from a range of service providers, not just health care.

Standard definitions and expressions of core data elements is necessary to support interoperability and electronic exchange of data between health and human service programs such as Medicaid, Children's Health Insurance Program (CHIP), Supplemental Nutrition Assistance Program (SNAP), and Temporary Assistance for Needy Families (TANF). This fundamental technical requirement was spelled out by the Health Information Technology (HIT) Policy Committee and the HIT Standards Committee in recommendations made to the National Coordinator for Health Information Technology.[76] Appendix B of that report summarized findings from a sample of 34 health and human services programs across ten States used to identify gaps and similarities in data element definitions across the programs. The complexity of data harmonization was assessed as high, medium, or low using the following factors, all of which would be relevant to any community-level attempt to merge data across programs:

(Reference Edition). Section I: Vocabulary/Code Set/Terminology Standards and Implementation Specifications. Retrieved February 21, 2018, from https://www.healthit.gov/isa/sites/default/files/2018%20ISA%20Reference%20Edition.pdf

[76] Office of the National Coordinator for Health Information Technology, Report from Committees. *Patient Protection and Affordable Care Act Section 1561 Recommendations*. Retrieved February 18, 2018, from https://www.healthit.gov/sites/default/files/rules-regulation/aca-1561-recommendations-final2.pdf; and especially *Appendix B: Core Data Analysis*. Retrieved February 18, 2018, from https://www.healthit.gov/sites/default/files/rules-regulation/appendix-b.pdf

- Variation of data name and definition across programs;
- Prevalence of similar variations across programs;
- Similarity and range of data values sets across programs; and
- Existing data standards such as those identified in HL7, X12, and the National Information Exchange Model (NIEM).[77]

The report's table of complexity ratings shows that there is a great deal of inconsistency in how many data elements are handled across programs. Even data elements that were rated as having low complexity, such as name, date of birth, and social security number may have semantic variation in how they are encoded in databases. Examples of data elements that were rated as having medium complexity included such things as address, citizenship, and immigration status. Examples of high complexity data elements included ethnicity, household composition, income, and primary care providers. The point of this for community aggregation work is that, while combining data from multiple programs is not impossible, it is not necessarily easy. Careful attention to a preliminary survey of what data elements are available from multiple sources should be done as part of a data normalization and reconciliation study to determine the level of effort that will be required for cross-program aggregation.

Merging of PHI from multiple sources is complicated by the fact that there are inconsistencies in patient identifiers and medical vocabulary coding, and varying levels of completeness in records such as care plans. Creating a Master Patient Index (MPI) requires a great deal of attention to detail, and reliance on automated matching for patient deduplication presents risks of mis-matches that could have serious clinical consequences. There is also a problem with how to handle conflicting data. For all these reasons, building a MPI that is complete, accurate, and able to be updated consistently is a resource-intensive operation. Our survey of IT vendors working in the care coordination sector identified some examples where data cleaning and matching services were a highlight of their sales focus, but the majority of vendors seem not to emphasize these issues.

ONC's public *Comment Summary* on a draft of the proposed Trust Exchange Framework and Common Agreement (TEFCA) notes that, "many respondents suggested patient matching between networks should be addressed as a components of the TEFCA."[78] That observation underlines the reality that patient matching is a common requirement that is not consistently addressed in existing interchange frameworks. The same public comment report included a call for patient matching standards (*Comment Summary*, page 3), noting that (*Comment Summary*, page 8), "A large number of respondents expressed concerns regarding patient identification/authentication, citing misidentification as a barrier to interoperability which directly impacts patient safety." To elevate data integrity and patient safety, comments urged ONC to:

- Advance patient record matching to verify the data belongs to the correct individual.
- Establish data review standards so inaccurate information in a patient record is identified and

---

[77] The National Information Exchange Model (NIEM) is an XML-based information exchange framework for sharing data across all levels of the United States government, as well as with public and private institutions. See https://www.niem.gov (Retrieved February 18, 2018)

[78] Office of the National Coordinator for Health Information Technology. (January, 2018).*Trust Exchange Framework and Common Agreement Public Comment Summary*. Page 5. Retrieved February 18, 2018, from https://www.healthit.gov/sites/default/files/tefca-comment-summary.pdf

corrected, meets a legal standard to provide some assurance of accuracy and contains all necessary information, including metadata that provides a clearer picture of a patient's health record.

Identity management for patient users of information systems is another issue that is not well-settled in existing frameworks. ONC's summary of comments on TEFCA notes that, "The burdens related to the various levels of identity management can differ significantly in terms of cost and level of effort," with a call for "additional guidance as to how we can all make it easier for patients to authenticate while still preserving security."[79] For general consumer use, OAuth 2.0 and OpenID are currently the most widely accepted standards for internet security.

We should recognize that population-level metrics can tolerate more failed or erroneous matching than clinical services can. Having the wrong patient's information in a clinical record can endanger the patient and cause a great deal of waste. However, in aggregation work, if the errors and failed matches are small and stable across time and do not disproportionately affect a population of interest, they may not be a barrier to merging the data for these purposes. If the error rate can be reliably estimated, an adjustment factor can be applied to the findings.

A simpler case where data from multiple providers may already exist in merged form would be with some large health care networks or OHCAs, which have a business case for putting in the effort to create a consolidated patient view across multiple care settings and providers. Networked providers of this type that have a large market share within a community may be able to produce consolidated data from existing systems that would give a reasonable picture of at least a major percentage of a community population. Another driver for consolidated merging is payment systems where the majority of health care transactions are covered by Medicare or Medicaid. Access to payment data presents its own set of problems. Many states are experimenting with all-payer claims databases that deserve close study.[80] We conducted an interview with a Public Health official in Colorado, who was aware of the potential benefits of data analysis that could be done with such a database.[81] There was an unsuccessful effort in Vermont to move to a single-payer arrangement.[82]

The nature of the legal agreement between the partners must be at the highest level to which any of the data sets rises. For example, if there is a merge of PHI with any other data, a BA must be in place. If there is a merge of de-identified data with any other data, at a minimum there must be a DUA in place, and possibly a BA if PHI is also involved. Strictly speaking, an OHCA may not need an additional BA or

---

[79] Office of the National Coordinator for Health Information Technology. (January, 2018). *Trust Exchange Framework and Common Agreement Public Comment Summary*. Page 8. Retrieved February 18, 2018, from https://www.healthit.gov/sites/default/files/tefca-comment-summary.pdf

[80] For a state-by-state review of the status of all-payer databases, see: All-Payer Claims Database Council. *Welcome to the APCD Council.* Retrieved February 18, 2018, from https://www.apcdcouncil.org

[81] APCD Council. *Colorado All Payer Claims Database*. Retrieved February 18, 2018, from https://www.apcdcouncil.org/state/colorado

[82] Linda Blumberg of the Urban Institute interviewed by Ari Shapiro. (September 13, 2017). National Public Radio. All Things Considered. *Why Bernie Sanders' Single-Payer Health Care Plan Failed In Vermont*. Retrieved February 18, 2018, from https://www.npr.org/2017/09/13/550757713/why-bernie-sanders-single-payer-health-care-plan-failed-in-vermont

DUA among the partners if the data is used for purposes of patient care or system management and the usage falls within their existing OCHA agreements, though the OHCA's data would need these tools if the data were used outside of the OHCA.

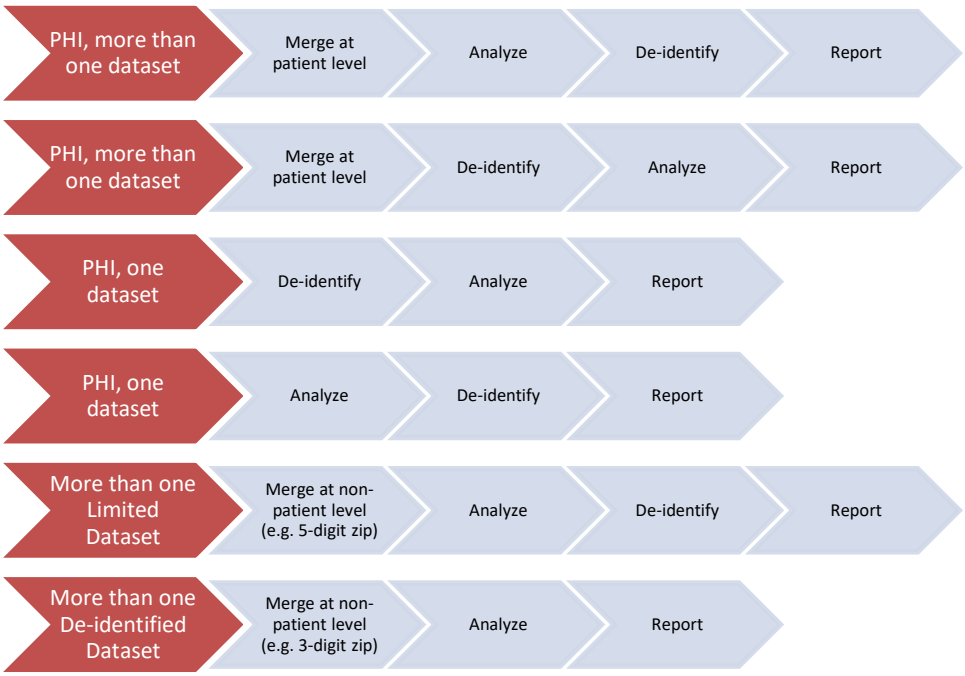
Finally, before any public use there must be a complete de-identification of the summary results. A group such as a Public Health Department could conduct analysis of PHI internally, for example, and could make internal use of findings, but any public reporting would require full de-identification, necessarily limiting the level of detail that can be shared outside the organization.

TABLE 1
Scenarios for Community Data Analysis

Scenario	Is PHI?	Needs BA or DUA?	Needs Merge of Records?	Merge Level	Public Use
1. Analysis of de-identified data from a single source	no	no	no	Not applicable	Not restricted
2. Analysis of de-identified data from more than one source	no	no	yes	Aggregated unit such as a three-digit zip code, with some restrictions based on the number of persons within each aggregation unit.	Not restricted, with some restrictions based on the number of persons within each aggregation unit.
3. Analysis of a limited data set from a single source	yes	DUA	no	Not applicable	Requires final de-identification
4. Analysis of a limited data set from more than one source	yes	DUA	yes	Aggregated unit such as a five-digit zip code, with some restrictions based on the number of persons within each aggregation unit.	Requires final de-identification
5. Analysis of PHI from a single source	yes	BA	no	Not applicable	Requires final de-identification
6. Analysis of PHI from more than one source	yes	BA	yes	Aggregated at the patient level if matching patient identifier(s) can be determined with sufficient accuracy.	Requires final de-identification

Table 1 illustrates some of the possible scenarios in which data from one or more sources could be used to obtain community metrics. The following figure (Figure 1) shows some prominent examples of possible data flows by which a community could analyze and report on different types of input data. Other sequences could be developed in which the number and type of input data sets varies. In situations where the goal is to aggredate data from more than one data set, merging must take place before whatever data element is used for merging must be dropped for de-identification purposes. For example, if there will be a merge of PHI using a patient number, the patient number must be present in both files at the time of merge but must be dropped prior to final publication of the results of analysis. If there will be a merge of two Limited Data sets for geographic aggregation based on a five-digit zip code, the five-digit zip code must be present in both files at the time of merge, but must be reduced to a three-digit zip code aggregation unit or dropped completely prior to public uses. Depending on the processing scenario in which data sets would be merged, analysis might take place either before or after de-identification. In all cases, complete de-identification is necessary for public reporting.

FIGURE 1
Examples of Alternative Data Flows



THE SPECIAL ROLE OF HEALTH INFORMATION EXCHANGE ORGANIZATIONS

ONC defines a Health Information Exchange (HIE) as follows:[83]

> *An HIE organization is an entity that oversees or facilitates the exchange of health information among a diverse group of health care stakeholders within and across regions, according to nationally recognized standards.*

HIE organizations can do much more than just serve as a transport layer for information. They can be large-scale integrators of data from multiple sources, in many cases capturing data from the majority of health care providers in the region they serve. This data warehousing function creates exceptional opportunities to develop integration services necessary to gain a composite picture of healthcare delivery for a community. We expect that the emerging business model for HIEs will increasingly includes analytic services and/or provision of de-identified or limited data sets that can be used for aggregated reporting for various populations, including those living in broad geographic catchment areas.

ONC has published a report exploring how public health jurisdictions use HIE organizations as a method to exchange information with health care providers.[84] The report is based on interviews with 16 jurisdictions. It documents best practices and lessons learned from public health and HIE integration across six major categories: leadership, technical, financial, privacy and security, legal and policy, and health IT developers.

That report notes instances where public health data transmitted from HIE organizations is superior in quality to data obtained from clinical information systems.[85] This points to the data enrichment services that an HIE organization can provide.

Other major sources of information about the operation of HIE organizations, including privacy and security issues, include:

- ONC Exemplar HIE Governance Program. *EHR|HIE Interoperability Workgroup's Governance Best Practices & Standards Alignment Project Federated Provider Directories Pilots Final Report*.[86]

---

[83] The Office of the National Coordinator for Health Information. (June 2016). *Health Information Exchange: What is it and why is it useful?* Retrieved February 13, 2018, from https://www.healthit.gov/sites/default/files/ltpac_value_prop_factsheet_6-21-16.pdf

[84] The Office of the National Coordinator for Health Information Technology. (September 2017). *Connecting Public Health Information Systems and Health Information Exchange Organizations: Lessons From The Field*. Retrieved February 13, 2018, from https://www.healthit.gov/sites/default/files/FINAL_ONC_PH_HIE_090122017.pdf

[85] The Office of the National Coordinator for Health Information Technology. (September 2017). *Connecting Public Health Information Systems and Health Information Exchange Organizations: Lessons From The Field*. Page 4. Retrieved February 13, 2018, from https://www.healthit.gov/sites/default/files/FINAL_ONC_PH_HIE_090122017.pdf

[86] Desai, A., Amato, E., Robinson, C., Coughlin, C., & Donnelly, J. (March 24, 2014). EHR|HIE Interoperability Workgroup. *Governance Best Practices & Standards Alignment Project Federated Provider Directories Pilots Final*

- The Sequoia Project. *eHealth Exchange Onboarding Overview*.[87]

ONC's Trusted Exchange Framework and Common Agreement (TEFCA)

Section 4003 of the 21st Century Cures Act (states that:[88,89]

> *The ONC must: (1) convene stakeholders to develop or support a framework and agreement for the secure exchange of health information between networks, (2) provide for testing of the framework and agreement, and (3) publish a list of networks that adopt the agreement.*
>
> *HHS must establish an index of digital contact information for health professionals, health facilities, and others to encourage the exchange of health information.*
>
> *The bill replaces the Health IT Policy Committee and the Health IT Standards Committee with the Health IT Advisory Committee. The ONC must periodically convene the Health IT Advisory Committee to report on priority uses of health IT and standards and implementation specifications that support the use and exchange of electronic health information.*

To carry out the directive of the 21st Century Cures Act, on January 5, 2018, ONC released a Draft Trusted Exchange Framework and Common Agreement (TEFCA) outlining a common set of principles for

---

Report. Prepared for The Office of the National Coordinator for Health Information Technology under contract # 90HG0001.. Retrieved February 18, 2018, from https://www.healthit.gov/sites/default/files/iwg_hie_exemplar_report_04042014_final.pdf

[87] Rosas, J., & Odom, K. (2017). An initiative of the Sequoia Project. *eHealth Exchange Onboarding Overview*. Retrieved February 18, 2018, from http://sequoiaproject.org/wp-content/uploads/2017/06/eHealth-Exchange-Onboarding-Overview-May2017-rev.pdf

[88] Congress.gov. H.R. 34 – 21st Century Cures Act. Retrieved March 5, 2018, from https://www.congress.gov/bill/114th-congress/house-bill/34/

[89] For background on the need for the Trusted Exchange Framework, and its authorization in the 21st Century Cures Act, see: Morris, G., and Anthony, E. (January 8, 2018). *21st Century Cures Act Overview for States*. SIM State Educational Session 1. An Overview of the 21st Century Cures Act for States. Retrieved March 5, 2018, from https://www.healthit.gov/sites/default/files/curesactlearningsession_1_v6_10818.pdf

trusted exchange and minimum terms and conditions for trusted exchange.[90,91,92] The final version of the TEFCA will be published in the Federal Register in late 2018. The draft specifically addresses how the Trusted Exchange Framework aligns with HIPAA regulations.

The Draft TEFCA is designed to enable interoperability and data exchanges across disparate health information networks (HINs) that operate locally, regionally, and nationally. Currently, organizations often do not exchange information due to differences in participation agreements and competitive interests. Establishing clear trust frameworks will make it easier for individuals, providers, health systems, public health, and others to maximize the benefits of shared data while minimizing the risks of inappropriate use.

Once the TEFCA is finally adopted, ONC will collaborate with a single Recognized Coordinating Entity (RCE) "to advance the single on-ramp to interoperability," the agency stated.[93] The RCE will use the Trusted Exchange Framework to develop a single Common Agreement that Qualified Health Information Networks (Qualified HINs) and their participants can choose to adopt. If the market moves in the direction that ONC is intending, only a small number of Qualified HINs (~10) may come into existence.[94]

The proposed Trusted Exchange Framework is divided into two parts. Part A, "Principles for the Trusted Exchange Framework", provides general guidance based on the existing trusted exchange frameworks. Part B, "Minimum Required Terms and Conditions," operationalizes the principles to help ensure that common practices are required of all participants.

In connection with this forward planning, ONC is working with HL7 and the Smart on FHIR team to build out a FHIR specification that will allow people to query for more than one patient record at a time to address population health use cases. Genevieve Morris, Principal Deputy National Coordinator for Health Information Technology, has said that, "In other words, I give you my patient panel, and a broadcast query would be done for all the ePHI, and all the records would be sent back in one query

---

[90] The draft TEFCA was open to public comment through February 20, 2018. HealthIT.gov. *Trusted Exchange Framework and Common Agreement*. Retrieved January 21, 2018, from https://beta.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement

[91] Morris, G. (January 5, 2018). *Trusted Exchange Framework and Common Agreement: A Common Sense Approach to Achieving Health Information Interoperability*. HealthITBuzz. Retrieved January 28, 2018, from https://www.healthit.gov/buzz-blog/interoperability/trusted-exchange-framework-common-agreement-common-sense-approach-achieving-health-information-interoperability/

[92] Snell, E. (January 8, 2018). *Secure Data Exchange Part of ONC Trusted Exchange Framework Draft*. HealthIT Security. Retrieved February 5, 2018, from https://healthitsecurity.com/news/secure-data-exchange-part-of-onc-trusted-exchange-framework-draft

[93] Snell, E. (January 8, 2018). *Secure Data Exchange Part of ONC Trusted Exchange Framework Draft*. HealthIT Security. Retrieved February 5, 2018, from https://healthitsecurity.com/news/secure-data-exchange-part-of-onc-trusted-exchange-framework-draft

[94] Leventhal, R. (February 1, 2018). *Industry Executive Outlines Opportunities, Concerns with ONC's TEFCA*. Healthcare Informatics. Retrieved February 14, 2018, from https://www.healthcare-informatics.com/news-item/interoperability/industry-executive-outlines-opportunities-concerns-onc-s-tefca

instead of having to do them one at a time. We think that is a really important use case, but that standard is just being built now. We know that it is two or three years away."[95]

Another related development is that on January 5, 2018, ONC published the Draft U.S. Core Data for Interoperability (USCDI), which will establish a minimum set of data classes that are required to be interoperable nationwide.[96] Adoption of the USCDI standards will help normalize what providers can expect to find in data systems. While market forces will determine which of the data classes are in greatest demand, giving a clear roadmap simplifies the work of system developers and accelerates creation of interoperable systems.

Because of the large number of possible data elements that are relevant to health records, the USCDI approach of having phased classes of data is understandable. Unfortunately, many of the data elements that are critical in the care of frail elders are not on the list of data that must be implemented first. Instead, they have been placed in Candidate Status and Emerging Status, two lower-priority groups that are scheduled for implementation on a longer time frame. It would be helpful if some of these data elements could be prioritized for specific use cases, such as eldercare, so that vendors that wish to advertise their systems as having "enhanced" data features can note them specifically. The concept of building specialized data profiles for specific use cases fits clinical practice in many domains. It would be advantageous for vendors who sell into specific markets, such as eldercare, to note compliance with custom use case data packages.

The following data classes listed in USCDI Candidate Status and Emerging Status are particularly important in the care of frail elderly patients. We hope they will receive higher priority, either by accelerating their planned adoption dates, or by noting them through a use case paradigm:

USCDI Candidate Status Data Classes

- Cognitive Status
- Family Health History
- Functional Status
- Care Team Members Contact Information
- Care Team Member Roles/Relationships
- Individual Goals and Priorities
- Provider Goals and Priorities

Emerging Status Data Classes

- Advance Care Planning, including Advance Directive, Power of Attorney, and Physician Orders for Life Sustaining Treatment (POLST) Form
- Communication Facilitators

---

[95] Quote from Genevieve Morris is from a January 23, 2018, webinar as reported in: Raths, David. (January 30, 2018). *What Will TEFCA Mean For Regional HIEs? ONC's Genevieve Morris on putting together all the puzzle pieces*. Healthcare Informatics. Retrieved February 14, 2018, from https://www.healthcare-informatics.com/blogs/david-raths/interoperability/what-will-tefca-mean-regional-hies

[96] The Office of the National Coordinator for Health Information Technology. (January 5, 2018). *Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process*. Retrieved February 17, 2018, from https://www.healthit.gov/sites/default/files/draft-uscdi.pdf

- Disability Status
- Durable Medical Equipment
- Overall Financial Resource Strain
- Personal Representative (a person allowed access to PHI on behalf of an individual they are representing, such as a child's parent or legal guardian, or a family member providing care for an aging relative)
- Social, psychological, and behavioral data, including in particular Social Connection/Support and Isolation, and Physical Activity
- Special Instructions or Precautions for Ongoing Care

Regarding possible missing elements in the Draft USCDI, we have suggested to ONC that the work of ONC's electronic Long-Term Services & Supports (eLTSS) Initiative be recognized explicitly in at least the Emerging Status class.[97] The eLTSS Initiative developed a specification that includes two types of data elements: core and non-core. We have proposed that any common data exchange agreement should include support for all the core eLTSS data elements, with support for non-core elements encouraged as well. The eLTSS specification is moving into the HL7 review process now, but it is not too early to encourage awareness and adoption of this important class of data. Inclusion of eLTSS core elements will empower many community service providers that are now unable to easily integrate their work as vital contributors in comprehensive care management.

The Concept of Attack Surface in Federated Systems

Effective privacy control requires effective security control. The technical term "attack surface" refers to the totality of different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an IT environment. Understanding the attack surface of a specific IT system requires detailed understanding of the system architecture. In environments where data are being shared among multiple providers and payers, such as in HIE organizations and some large healthcare systems, the attack surface spans multiple IT systems.

Data Access Control refers to who can see and/or modify information. Data Governance refers to issues of responsibility for data currency and accuracy. These issues are closely connected with data privacy and deserve study in connections with any plan to combine data from multiple sources.

PUBLIC HEALTH AS A SPECIALIZED APPLICATION

Public health departments receive both identified and de-identified data. Public health has been dealing with the linking and matching of multiple records on an individual long before HIEs existed. Public Health uses of data have special standing under federal and state law. Under 45 CFR 164.501, a "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. The public health provision of the HIPAA Privacy Rule permits, but

[97] Public comment on Draft TEFCA submitted to ONC on February 19, 2018.

does not require, covered entities to make public health disclosures.[98] Many specific situations for public health reporting are outlined in the HHS FAQ, "Public Health Uses and Disclosures."[99]

The HHS summary of health information privacy rules for Public Health under 45 CFR 164.512(b) states that the regulation permits covered entities to disclose protected health information, without authorization from the patient or the patient's representative, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability.[100]

> *The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose protected health information without authorization for specified public health purposes.*

Specific rules cover specialized situations that permit permit covered entities to disclose protected health information, without patient authorization, to persons or entities other than public health authorities for public health activities. Some examples include things such as:[101]

- Information to ensure public health or safety
- To prevent or lessen imminent danger
- Disclosure to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal
- Child abuse or neglect
- Quality, safety or effectiveness of a product or activity regulated by the FDA
- Persons at risk of contracting or spreading a disease
- Workplace medical surveillance

---

[98] HHS.gov. Health Information Privacy. *Does the public health provision of the HIPAA Privacy Rule require covered entities to make public health disclosures?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/295/does-the-public-health-provision-require-covered-entities-to-make-public-health-disclosures/index.html

[99] HHS.gov. Health Information Privacy. *Public Health Uses and Disclosures*. Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/public-health-uses-and-disclosures

[100] HHS.gov. Health Information Privacy. *Public Health*: *45 CFR 164.512(b)*. Retrieved January 29, 2018, from https://www.hhs.gov/hipaa/for-professionals/special-topics/public-health/index.html

[101] For additional information on when covered entities may disclose PHI without patient authorization, see: The Office of the National Coordinator for Health Information Technology. *Guide to Privacy and Security of Electronic Health Information. Chapter 2: Your Practice and HIPAA Rules*. Pages 15-17. Retrieved February 17, 2018, from https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-2.pdf

Covered entities may disclose facially identifiable protected health information, such as name, address, and social security number, for public health purposes in some cases. For disclosures not required by law, covered entities may disclose "without authorization, the information that is reasonably limited to that which is minimally necessary to accomplish the intended purpose of the disclosure." As the HHS FAQ on this topic explains:[102]

> *The HIPAA Privacy Rule permits covered entities to disclose the amount and type of protected health information that is needed for public health purposes. In some cases, the disclosure will be required by other law, in which case, covered entities may make the required disclosure pursuant to 45 CFR 164.512(a) of the Rule.*
>
> *For disclosures that are not required by law, covered entities may disclose, without authorization, the information that is reasonably limited to that which is minimally necessary to accomplish the intended purpose of the disclosure. For routine or recurring public health disclosures, a covered entity may develop protocols as part of its minimum necessary policies and procedures to address the type and amount of information that may be disclosed for such purposes. Covered entities may also rely on the requesting public health authority's determination of the minimally necessary information.*

Covered entities generally are required to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose, with the exception of public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law.[103]

ONC and OCR provide a fact sheet that explains how the rules work for disclosures of PHI for public health activities to public health agencies that are authorized by state or federal law to collect the information they seek.[104] The information in the fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet notes that:

---

[102] HHS.gov. Health Information Privacy. *May covered entities disclose facially identifiable protected health information, such as name, address, and social security number, for public health purposes?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/296/may-covered-entities-disclose-facially-identifiable-protected-health-information/index.html

[103] See 45 CFR 164.502(b).

[104] Office of the National Coordinator for Health Information Technology (ONC) & the U. S. Department of Health and Human Services Office for Civil Rights. (December, 2016). *Permitted Uses and Disclosures: Exchange for Public Health Activities 45 Code of Federal Regulations (CFR) 164.512(b)(1)*. Retrieved January 29, 2018, from https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf

> *While HIPAA requires that the information disclosed is the minimum information necessary for the purpose, it permits the discloser to reasonably rely on a public health authority's request as to what information is necessary for the public health activities.*

Nine scenarios given in that Fact Sheet are summarized in Appendix C. While none of the scenarios involve eldercare, some of the issues they raise have direct parallels to what could be done with aggregated public health reporting care for frail elders in a community. We present four examples below.

- ***Scenario 2: Exchange for Conduct of Public Health Surveillance***. The example involves collection of data for a cancer registry authorized by State law.[105] In this scenario, a Public Health Department has been authorized to collect data on cancer occurrence (including the type, extent, and location of the cancer) and the type of initial treatment. Under 45 CFR 164.512(b)(1)(i), a hospital may use certified health IT to disclose electronic PHI to the Health Department's central cancer registry. In deciding how much and what information to supply to the Department of Health, HIPAA permits the hospital to reasonably rely on the Department of Health's statement of what information is necessary for the public health activities. Disclosure of electronic PHI requires HIPAA Security Rule compliance.
    - In our population of interest, a state could authorize the public health department to maintain a registry of advance directives which includes identifying information and information as to diagnoses, preferences, and surrogates. All covered entities holding advance directives could rely upon the data request from the public health department to contribute data to the registry. The public health department could analyze the data for such public health concerns as the rate of advance directives and the compliance with them in end of life care (a function that would require merging death certificates and data from Medicare claims).
- ***Scenario 4: Exchange for Public Health Interventions***. The example involves a situation where a city water supply is found to be contaminated with lead. The Health Department implements a lead poisoning intervention program and needs lead exposure test results of children who might have been exposed. Because of the known long-term neurological effects of lead poisoning in children, the Health Department is authorized by law to obtain the test results of each tested child and to track those children's health and development over time. The Department contracts with a local Health Information Exchange (HIE) to collect, on the Health Department's behalf from local providers, PHI about the tested children. Under 45 CFR 164.512(b)(1)(i), providers may disclose the PHI to the Health Department using certified health IT.
    - In our population of interest, the Public Health Department might note a striking rise in rehospitalizations and then deaths of elderly people as part of their surveillance of an Admissions, Discharges, and Transfers database that was established as part of emergency preparedness. This database is very thin on details, so the public health office might need to investigate more about the situation and gather records from

[105] A registry is defined as a data base of identifiable persons containing a clearly defined set of health and demographic data collected for a specific public health purpose. See: Solomon, D., Henry, R., Hogan, J., Van Amburg, G., & Taylor, J. (1991). *Evaluation and implementation of public health registries*. Public Health Rep. Mar-Apr; 106(2): 142–150. Retrieved February 18, 2018, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1580226/

hospitals and post-hospital providers for persons rehospitalized. Under this Scenario, the covered entities could send that data without specific patient authorization.

- ***Scenario 5: Exchange for Public Health Interventions***. A Public Health Department is responsible under state law for implementing a CMS State Innovation Model (SIM) program in their state. The Department was awarded a SIM grant to conduct a public health intervention and then measure outcomes for patients that have both diabetes and depression and whose primary care provider (PCP) coordinates their patients' care. The Authority requests that PCPs within the state disclose PHI to the state's Public Health Authority to assist in the evaluation of care coordination outcomes. Under 45 CFR 164.512(b)(1)(i), PCPs within the Department's jurisdiction may disclose PHI to the appropriate Public Health Department official using certified health IT. While PCPs must only disclose the minimum necessary for the purpose of the public health intervention, they may reasonably rely on representations from the Public Health Department that the requested PHI is the minimum needed. Disclosure of electronic PHI requires HIPAA Security Rule compliance.
    - In our population of interest, a parallel endeavor could be that the Public Health Department may have a SIM grant to provide substantial education to providers in order to reduce the rate of pressure ulcers in frail and disabled persons. The Department could request of PCPs the PHI for persons who were coded as having pressure ulcers in order to monitor the rate and therefore the effectiveness of the intervention.
- ***Scenario 9: Using Certified Electronic Health Record Technology***. This scenario merely notes that, "Providers who need to share PHI with agencies or organizations for public health activities may use certified health IT to send the information to the requesting agency or organization. Disclosure of electronic PHI by certified health IT or other electronic means requires HIPAA Security Rule compliance by the provider."
    - In any of the scenarios above, and in the many others where public health officials have a need to gather PHI from covered entities, the transmission of the data can by done electronically, so long as the covered entity uses certified health IT in compliance with the HIPAA Security Rule.

OCR provides a checklist to help public health authorities be prepared to provide a covered entity with the information and representations necessary for the covered entity to ensure that a disclosure meets the specific requirements and conditions outlined in the HIPAA Privacy Rule.[106] The requestor of the PHI should be able to demonstrate or represent that:

- The requestor is a "public health authority" as defined in the Privacy Rule. The Privacy Rule defines "public health authority" as an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.
- The requestor has legal authority to collect or receive the information it is requesting for the stated public health purpose.
- The information being requested is the minimum necessary for the stated public health purpose.

---

[106] U. S. Department of Health and Human Services Office for Civil Rights. *HIPAA: Public Health Authority Disclosure Request Checklist*. Retrieved January 30, 2018, from https://www.hhs.gov/sites/default/files/hippa-disclosure-chcklist102314.pdf

In addition, the requestor should be prepared to verify its identity by:

- Presenting an agency identification badge, other official credentials, or other proof of government status if the request is made in person;
- Making the request on the appropriate government letterhead if the request is made in writing; or
- If the request is by a person acting on behalf of a public official, providing a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

HHS FAQs note that:[107]

> *The Privacy Rule does not require a notation in each medical record that has been accessed by public health authorities, as long as the information required under the Privacy Rule is included in the accounting for disclosures. Where, as with many public health disclosures, access to an entire universe of records is involved, tracking disclosures can be accomplished without the need for documentation in each record. This flexibility in the manner of documentation facilitates complying with the accounting requirement. ...*
>
> *Public health surveillance activities often involve a retrospective review by a public health authority of a universe of patient records to identify reportable events. When a reportable case is identified, the specific data items pertinent to the public health surveillance activity are extracted and reported to the public health authority. ...*
>
> *Because of the universal nature of the access provided, the documentation required for the disclosure can be easily maintained. The covered entity need only document the identity (and address if known) of the public health authority to which access was provided, a description of the records and PHI subject to access, the purpose for the disclosure, and when access was provided. This documentation need not be noted in each record. It would be sufficient, for instance, for the covered entity to maintain a separate notation of such*

[107] HHS.gov. Health Information Privacy. *To provide individuals with an accounting for disclosures, does a covered entity have to document each medical record that may be accessed by a public health authority in the course of surveillance activities that involve all patient records?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/465/does-a-covered-entity-have-to-document-each-medical-record-that-may-be-accessed-by-a-public-health-authority/index.html

> *disclosures, applicable to all records so accessed. Then, if an individual requests an accounting, the covered entity need only determine whether the individual's records were among the universe of records to which the public health authority was granted access.*

LIMITED DATA SETS IN PUBLIC HEALTH

Public Health Department uses of data are greatly simplified when only a limited data set is exchanged.[108] For definition of a limited data set, see page 21. Limited data sets are excepted from the accounting requirement at 45 CFR 164.528(a)(1)(viii). The HHS FAQ on this issue explains that:

> *Must a covered entity provide an accounting for disclosures if the only information disclosed to a public health authority is in the form of a limited data set?*
>
> *Answer: No, a covered entity is not required to provide an accounting for a disclosure where the only information disclosed is in the form of a limited data set, and the covered entity has a data use agreement with the public health authority receiving the information. (See 45 CFR 164.514(e) for limited data set and data use agreement requirements.)*
>
> *Moreover, a covered entity is not required to provide an accounting when it uses protected health information to create a limited data set.*

A covered entity may enter into a business associate agreement with a public health authority for the sole purpose of creating a limited data set, even if the same public health authority is also the intended recipient of the information (45 CFR 164.514(e)(3)(ii)).[109]

---

[108] HHS.gov: Health Information Privacy. *Must a covered entity provide an accounting for disclosures if the only information disclosed to a public health authority is in the form of a limited data set?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/467/must-a-covered-entity-provide-an-accounting-for-disclosures/index.html

[109] HHS.gov. *May a covered entity hire a business associate to create a limited data set, and may the public health authority be a business associate for that purpose, even if the public health authority is also the intended recipient of the limited data set?* Retrieved January 30, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/468/may-a-covered-entity-hire-a-business-associate-to-create-a-limited-data-set/index.html

OHCA ORGANIZED HEALTH CARE ARRANGEMENT (UNDER HIPAA EXEMPTION)

HIPAA provides for cooperative work among entities through the use of an Organized Health Care Arrangement (OHCA).[110] OHCAs may be a vehicle for regionalized data aggregation in our context. In an OHCA, participant providers and organizations may share PHI about their patients in order to benefit the common enterprise.

Under the regulations, an OHCA has the following characteristics:[111]

- More than one provider is involved in a clinically integrated setting to provide patient care;
- Participants hold themselves out to the public as an organized system of healthcare in which providers in different organizations have a joint arrangement that includes at least one of certain specified joint activities, such as payment activities, quality assessment, improvement activities, or utilization review;
- A combination of group health plans or group health plans and insurers.

OHCAs may vary in legal structure, but a key component of these arrangements is that individuals who obtain services from them have an expectation that the arrangements are integrated and that they jointly manage their operations. Providers who are participating in an OHCA may offer a joint privacy notice and may obtain a joint consent for release of protected health information from the patient.

Participating in an OHCA can give organizations substantial flexibility in sharing of PHI. HHS provides guidance on how providers and health care systems that participate in an OHCA can comply with the HIPAA Privacy Rule's requirements for providing notices and obtaining individuals' acknowledgements of the notice.[112]

Since the entities that create the OHCA are all covered entities and health care providers, Community-Based Organizations would need to participate through BAAs.

THE OFFICE FOR HUMAN RESEARCH PROTECTIONS (OHRP)

The Office for Human Research Protections (OHRP), a function of the U. S. Department of Health and Human Services (DHHS), is responsible for ethical oversight of clinical research conducted by the

---

[110] The Oregon Association of Hospitals and Health Systems provides a good overview of what OHCAs are and how they can benefit data sharing in particular. Oregon Association of Hospitals and Health Systems. *Organized Health Care Arrangements*. Retrieved January 23, 2018, from http://www.oahhs.org/organized-health-care-arrangements

[111] For formal definitions of the terms “organized health care arrangement” and “health care operations” see: U. S. Department of Health and Human Services. Office of the Assistant Secretary for Planning and Evaluation. (December 28, 2000). *Standards for Privacy of Individually Identifiable Health Information. Final Privacy Rule Preamble. Organized Health Care Arrangement*. Retrieved January 23, 2018, from https://aspe.hhs.gov/report/standards-privacy-individually-identifiable-health-information-final-privacy-rule-preamble/organized-health-care-arrangement

[112] HHS FAQ: *337-We participate in an OHCA how do we provide notices and obtain individuals' acknowledgements*. Retrieved January 23, 2018, from https://www.hhs.gov/hipaa/for-professionals/faq/337/how-can-ohca-participants-obtain-acknowledgement/index.html

Department.[113] OHRP is part of the Office of the Assistant Secretary for Health in the Office of the Secretary of HHS. OHRP also supports the Secretary's Advisory Committee on Human Research Protections (SACHRP), which advises the HHS Secretary on issues related to protecting human subjects in research. SACHRP is authorized under 42 U.S.C. 217a, Section 222 of the Public Health Service (PHS) Act, as amended.[114]

OHRP implements HHS regulations for the protection of human subjects as defined in 45 CFR part 46, which has four subparts:

- Subpart A, also known as the Federal Policy for the Protection of Human Subjects, known as the "Common Rule". The "Common Rule" was published in 1991 and codified in separate regulations by 15 Federal departments and agencies.[115];
- Subpart B, additional protections for pregnant women, human fetuses, and neonates;
- Subpart C, additional protections for prisoners; and
- Subpart D, additional protections for children.

In order to receive support for research involving human subjects, institutions must enter into a formal agreement with OHRP covering ethical oversight. This agreement is called a "Federalwide Assurance (FWA) for the Protection of Human Subjects".[116] Each FWA must designate at least one Institutional Review Board (IRB) registered with OHRP.[117] An Institution may register its own IRB (an "internal" IRB) or designate a previously registered IRB operated by another organization.

A portion of the OHRP Quality Improvements FAQ is reproduced in Appendix A.[118] The examples given there make it clear that use of de-identified, aggregated data for quality improvement purposes is generally not prohibited so long as appropriate administrative procedures are followed.

Summary

In our preliminary work with communities, many participants are worried that the plans will be thwarted by concerns over privacy and security. Our review shows that multiple pathways can make it

---

[113] HHS.gov: Office for Human Research Protections. Retrieved January 28, 2018, from https://www.hhs.gov/ohrp/

[114] HHS.gov: Office for Human Research Protections. *Recommendations on the Notice of Proposed Rulemaking entitled "Federal Policy for the Protection of Human Subjects"*. Retrieved January 28, 2018, from https://www.hhs.gov/ohrp/sachrp-committee/recommendations/2016-january-5-recommendation-nprm-attachment-a/index.html

[115] HHS.gov. Office for Human Research Protections. *Federal Policy for the Protection of Human Subjects ("Common Rule")*. Retrieved January 28, 2018, from https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html

[116] HHS.gov. Office for Human Research Protections. *Federalwide Assurance (FWA) for the Protection of Human Subjects*. Retrieved January 28, 2018, from https://www.hhs.gov/ohrp/register-irbs-and-obtain-fwas/fwas/fwa-protection-of-human-subjecct/index.html

[117] OHRP provides procedures to register IRBs and obtain FWAs. See: HHS.gov. Office for Human Research Protections. *Register IRBs & Obtain FWAs*. Retrieved January 28, 2018, from https://www.hhs.gov/ohrp/register-irbs-and-obtain-fwas/index.html

[118] HHS.gov. Office for Human Research Protections. *Quality Improvement Activities FAQs*. Retrieved January 28, 2018 from https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/quality-improvement-activities/index.html

quite possible to generate community-level data from patient information held by multiple providers, both PHI and non-PHI information, and both medical care information and information from providers of social and supportive services. In some cases, having the work under the aegis of the public health department would make access easier. Some sets of providers might well already effectively be an OHCA and could constitute themselves as such and inform their public, thus making it easier to proceed without multiple business associate agreements. Using data from decedents does not eliminate the barriers to aggregating data in a geographic community, but there are some data strategies such as mortality followback studies that could focus upon decedents. Security will always be a concern and gets more challenging as the attack surface enlarges, which is why teams will have to be quite thoughtful about working with data to make it limited or completely de-identified. However, the bottom line is that privacy and security rules do not stand in the way of the work to generate useful geographically-anchored metrics concerning the performance of the local eldercare system.

Acknowledgements

We would like to thank the following people for reviewing this report:

- Gregory Becker
- Rick Keller
- Katharine McVeigh, PhD, MPH
- Anne Montgomery
- Terrence A. O'Malley, MD
- Sharon Perlman, MPH
- Laura Rappleye
- Ted Rooney, RN, MPH
- Sarah Slocum, MA
- Forrest White
- Michael Yaskanin, MBA

Appendix A: OHRP Quality Improvement Activities FAQs

This Appendix reproduces a portion of the Office for Human Research Protections (OHRP) Quality Improvement Activities FAQs as found on the OHRP website.[119] The examples make it clear that use of de-identified, aggregated data for quality improvement purposes is generally not prohibited so long as appropriate administrative procedures are followed and no special conditions apply. While the examples given below highlight situations where regulations for human research subject protections do not apply, exceptions to these cases can occur. Assessment of any specific situation should be done with regard to the full provisions of the OHRP guidelines, not just these sample questions.

Quality Improvement Activities FAQs

QUESTION: How does HHS view quality improvement activities in relation to the regulations for human research subject protections?

Protecting human subjects during research activities is critical and has been at the forefront of HHS activities for decades. In addition, HHS is committed to taking every appropriate opportunity to measure and improve the quality of care for patients. These two important goals typically do not intersect, since most quality improvement efforts are not research subject to the HHS protection of human subjects regulations. However, in some cases quality improvement activities are designed to accomplish a research purpose as well as the purpose of improving the quality of care, and in these cases the regulations for the protection of subjects in research (45 CFR part 46) may apply.

To determine whether these regulations apply to a particular quality improvement activity, the following questions should be addressed in order:

1. does the activity involve research (45 CFR 46.102(d));
2. does the research activity involve human subjects (45 CFR 46.102(f));
3. does the human subjects research qualify for an exemption (45 CFR 46.101(b)); and
4. is the non-exempt human subjects research conducted or supported by HHS or otherwise covered by an applicable FWA approved by OHRP.

For those quality improvement activities that are subject to these regulations, the regulations provide great flexibility in how the regulated community can comply. Other laws or regulations may apply to quality improvement activities independent of whether the HHS regulations for the protection of human subjects in research apply.

QUESTION: Do the HHS regulations for the protection of human subjects in research (45 CFR part 46) apply to quality improvement activities conducted by one or more institutions whose purposes are limited to: (a) implementing a practice to improve the quality of patient care, and (b) collecting

[119] HHS.gov. Office for Human Research Protections. *Quality Improvement Activities FAQs*. Retrieved January 7, 2018, from https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/quality-improvement-activities/index.html

patient or provider data regarding the implementation of the practice for clinical, practical, or administrative purposes?

No, such activities do not satisfy the definition of "research" under 45 CFR 46.102(d), which is "...a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge..." Therefore the HHS regulations for the protection of human subjects do not apply to such quality improvement activities, and there is no requirement under these regulations for such activities to undergo review by an IRB, or for these activities to be conducted with provider or patient informed consent.

Examples of implementing a practice and collecting patient or provider data for non-research clinical or administrative purposes include:

- A radiology clinic uses a database to help monitor and forecast radiation dosimetry. This practice has been demonstrated to reduce over-exposure incidents in patients having multiple procedures. Patient data are collected from medical records and entered into the database. The database is later analyzed to determine if over-exposures have decreased as expected.
- A group of affiliated hospitals implements a procedure known to reduce pharmacy prescription error rates, and collects prescription information from medical charts to assess adherence to the procedure and determine whether medication error rates have decreased as expected.
- A clinic increasingly utilized by geriatric patients implements a widely accepted capacity assessment as part of routine standard of care in order to identify patients requiring special services and staff expertise. The clinic expects to audit patient charts in order to see if the assessments are performed with appropriate patients, and will implement additional in-service training of clinic staff regarding the use of the capacity assessment in geriatric patients if it finds that the assessments are not being administered routinely.

Do quality improvement activities fall under the HHS regulations for the protection of human subjects in research (45 CFR part 46) if their purposes are limited to: (a) delivering healthcare, and (b) measuring and reporting provider performance data for clinical, practical, or administrative uses?

No, such quality improvement activities do not satisfy the definition of "research" under 45 CFR 46.102(d), which is "…a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge…" Therefore the HHS regulations for the protection of human subjects do not apply to such quality improvement activities, and there is no requirement under these regulations for such activities to undergo review by an IRB, or for these activities to be conducted with provider or patient informed consent.

The clinical, practical, or administrative uses for such performance measurements and reporting could include, for example, helping the public make more informed choices regarding health care providers by communicating data regarding physician-specific surgical recovery data or infection rates. Other practical or administrative uses of such data might be to enable insurance companies or health maintenance organizations to make higher performing sites preferred providers, or to allow other third parties to create incentives rewarding better performance.

Can I analyze data that are not individually identifiable, such as medication databases stripped of individual patient identifiers, for research purposes without having to apply the HHS protection of human subjects regulations?

Yes, whether or not these activities are research, they do not involve “human subjects.” The regulation defines a “human subject” as “a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information….Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.” Thus, if the research project includes the analysis of data for which the investigators cannot readily ascertain the identity of the subjects and the investigators did not obtain the data through an interaction or intervention with living individuals for the purposes of the research, the analyses do not involve human subjects and do not have to comply with the HHS protection of human subjects regulations.

Appendix B: SAMHSA/ONC 2010 FAQs

In 2010, the HHS Substance Abuse and Mental Health Services Administration (SAMHSA) and the HHS Office of the National Coordinator for Health Information Technology (ONC) published FAQs, *Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*.[120] This Appendix reproduces two questions and answers found in that FAQ. The FAQ was prepared by SAMHSA staff, in collaboration with staff from ONC and contractors and should not be considered legal advice.

Q1. Does the federal law that protects the confidentiality of alcohol and drug abuse patient records allow information about patients with substance use disorders to be included in electronic health information exchange systems?

A1. Yes. The federal confidentiality law and regulations (codified as 42 U.S.C. § 290dd-2 and 42 CFR Part 2 ("Part 2")), enacted almost three decades ago after Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, has been a cornerstone practice for substance abuse treatment programs across the country. Part 2 permits patient information to be disclosed to Health Information Organizations (HIOs)2 and other health information exchange (HIE) systems; however, the regulation contains certain requirements for the disclosure of information by substance abuse treatment programs; most notably, patient consent is required for disclosures, with some exceptions.

This consent requirement is often perceived as a barrier to the electronic exchange of health information. However, as explained in other FAQs, it is possible to electronically exchange drug and alcohol treatment information while also meeting the requirements of Part 2.

Q16. Under Part 2, may an HIO release demographic information about Part 2 patients without patient consent?

A16. Yes. However, one must be sure to be in compliance with Part 2, which prohibits the disclosure of patient-identifying information. (42 CFR § 2.11 and § 2.13) Therefore, releasing demographic information would only be allowed under Part 2 if the demographic information does not reveal any information that would identify the person, either directly or indirectly, as having a current or past drug or alcohol problem or as being a patient in a Part 2 program.

[120] Wattenberg, S. *Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)*. Legal Action Center for the Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services. Contract # OMB0990-0115. Retrieved January 28, 2018, from https://www.samhsa.gov/sites/default/files/faqs-applying-confidentiality-regulations-to-hie.pdf

Appendix C: Public Health Scenarios

The Office of the National Coordinator for Health Information Technology (ONC) and the U. S. Department of Health and Human Services Office for Civil Rights (HHS OCR) provide a fact sheet that explains how the rules work for disclosures of PHI for public health activities to public health agencies that are authorized by state or federal law to collect the information they seek.[121] The information in the fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel.

This Appendix provides a summary of the nine scenarios given in that fact sheet. While none of the scenarios involve eldercare, some of the issues they raise have direct parallels to what could be done with public health reporting of eldercare in a community.

Scenario 1: Exchange for Reporting of Disease. The example involves reporting PHI on an ongoing basis for all prior and prospective cases of patients exposed to the Zika virus.

Scenario 2: Exchange for Conduct of Public Health Surveillance. The example here is collection of data for a cancer registry authorized by State law. The hypothetical Department has been authorized to collect data on cancer occurrence (including the type, extent, and location of the cancer) and the type of initial treatment. Under 45 CFR 164.512(b)(1)(i), a hospital may use certified health IT to disclose electronic PHI to the Health Department's central cancer registry. In deciding how much and what information to supply to the Department of Health, HIPAA permits the Hospital to reasonably rely on the Department of Health's statement of what information is necessary for the public health activities. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

Scenario 3: Exchange for Public Health Investigations. The example involves investigation of the source of a recent measles outbreak in a local school. State law authorizes access to medical records to complete the investigations. The Department of Public Health asks all health providers in the state to report confirmed diagnoses of measles, including patient identity, demographic information, and positive test results. Under 45 CFR 164.512(b)(1)(i), providers within the State may use certified health IT to disclose PHI to the Department of Health.

Scenario 4: Exchange for Public Health Interventions (First Example). The example involves a situation where a city water supply is found to be contaminated with lead. The Health Department implements a lead poisoning intervention program and needs lead exposure test results of children who might have been exposed. Because of the known long-term neurological effects of lead poisoning in children, the Health Department is authorized by law to obtain the test results of each tested child and to track those children's health and development over time. The Department contracts with a local Health Information Exchange (HIE) to collect, on the Health Department's behalf from local providers, PHI about the tested

[121] Office of the National Coordinator for Health Information Technology (ONC) and the U. S. Department of Health and Human Services Office for Civil Rights. (December, 2016). *Permitted Uses and Disclosures: Exchange for Public Health Activities 45 Code of Federal Regulations (CFR) 164.512(b)(1)*. Retrieved January 29, 2018, from https://www.healthit.gov/sites/default/files/12072016_hipaa_and_public_health_fact_sheet.pdf

children. Under 45 CFR 164.512(b)(1)(i), providers may disclose the PHI to the Health Department using certified health IT.

Scenario 5: Exchange for Public Health Interventions (Second Example). A Public Health Authority is responsible under state law for implementing a CMS State Innovation Model (SIM) program in their state. The Authority was awarded a SIM grant to conduct a public health intervention measuring of outcomes for patients that have both diabetes and depression and whose primary care provider (PCP) coordinates their patients' care. The Authority requests that PCPs within the state disclose PHI to the state's Public Health Authority to assist in the evaluation of care coordination outcomes. Under 45 CFR 164.512(b)(1)(i), PCPs within the Authority's jurisdiction may disclose PHI to the Coastalview Public Health Authority using certified health IT. While PCPs must only disclose the minimum necessary for the purpose of the public health intervention, they may reasonably rely on representations from the Public Health Authority that the requested PHI is the minimum needed. Disclosure of electronic PHI requires HIPAA Security Rule compliance.

Scenario 6: Exchange Subject to Food and Drug Administration (FDA) Jurisdiction. The example involves a recall of an implanted medical device. Medical devices are subject to the jurisdiction of the U.S. Food and Drug Administration (FDA). A device manufacturer announces a Class I Medical Device Recall for a specific device. Providers who implanted the devices prior to the recall may employ certified health IT to identify patients affected by the recall and may disclose PHI, such as patient contact information and other health information about the affected patients, to the FDA under 45 CFR 164.512(b)(1)(iii)(c).

Scenario 7: Exchange for Persons Exposed to Communicable Disease and for Related Public Health Investigation. The example involves control of an outbreak of an airborne communicable virus. Local law permits providers to notify individuals that may have been exposed to a communicable disease.A provider may use PHI and certified health IT to identify patients who were potentially exposed and may send notices to the exposed patients about their exposure based on 45 CFR 164.512(b)(1)(iv). The local Department of Health is authorized by law to collect disease information and access medical records to conduct investigations and implement disease control measures and may collect PHI of patients exposed to the virus based on 45 CFR 164.512(b)(1)(i).

Scenario 8: Exchange in Support of Medical Surveillance of the Workplace. The example involves the safety of working conditions in a workplace where Federal law requires monitoring the safety of working conditions, also known as medical surveillance of the workplace. The employer provides medical evaluation services so the company may comply with Federal and state laws. Under 45 CFR 164.512(b)(1)(v), providers may disclose Worker workplace medical surveillance-related PHI to the company.

Scenario 9: Using Certified Electronic Health Record Technology. This scenario merely notes that, "Providers who need to share PHI with agencies or organizations for public health activities may use certified health IT to send the information to the requesting agency or organization. Disclosure of electronic PHI by certified health IT or other electronic means requires HIPAA Security Rule compliance by the provider."

Appendix D: HIPAA Privacy Rule De-Identification Methods

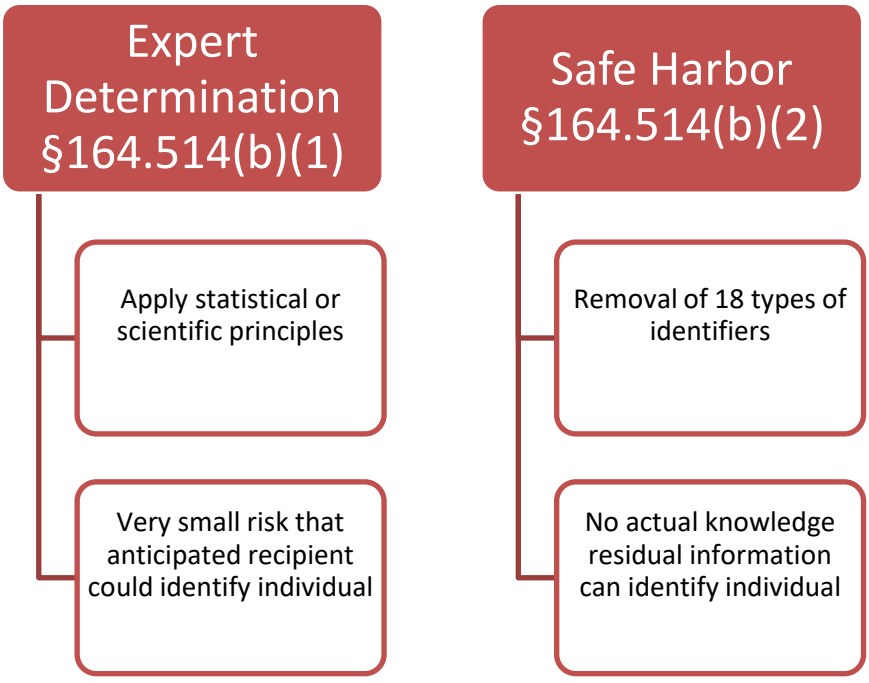
This summary of HIPAA Privacy Rule De-identification Methods is based the Office for Civil Rights (OCR) document, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*.[122]

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual. The Rule states:

> *§ 164.514 Other requirements relating to uses and disclosures of protected health information. (a) Standard: de-identification of protected health information. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.*

Sections 164.514(b) and(c) of the Privacy Rule contain the implementation specifications that a covered entity must follow to meet the de-identification standard. Two methods are acceptable: Expert Determination and Safe Harbor. Satisfying either method would demonstrate that a covered entity has met the standard in § 164.514(a) above. De-identified health information created following these methods is no longer protected by the Privacy Rule because it does not fall within the definition of PHI.

[122] Office for Civil Rights. (November 26, 2012). *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. Pages 7-8. Retrieved February 2, 2018, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf



Section 164.514(b) Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

[The "Expert Determination" method:]

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

> (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
>
> (ii) Documents the methods and results of the analysis that justify such determination; or

[The "Safe Harbor" method:]

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

> (A) Names
>
> (B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
>
> > (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000[123]

(C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

(D) Telephone numbers

(E) Fax numbers

(F) Email addresses

(G) Social security numbers

(H) Medical record numbers

(I) Health plan beneficiary numbers

(J) Account numbers

(K) Certificate/license numbers

(L) Vehicle identifiers and serial numbers, including license plate numbers

(M) Device identifiers and serial numbers

(N) Web Universal Resource Locators (URLs)

(O) Internet Protocol (IP) addresses

(P) Biometric identifiers, including finger and voice prints

(Q) Full-face photographs and any comparable images

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below]; and

---

[123] OCR published a final rule on August 14, 2002, that modified certain standards in the Privacy Rule. The preamble to this final rule identified the initial three digits of ZIP codes, or ZIP code tabulation areas (ZCTAs), that must change to 000 for release. 67 FR 53182, 53233-53234 (Aug. 14, 2002)). ZCTAs are generalized area representations of U.S. Postal Service (USPS) ZIP code service areas. Each ZCTA is built by aggregating the Census 2000 blocks, whose addresses use a given ZIP code, into a ZCTA which gets that ZIP code assigned as its ZCTA code. To produce a deidentified data set utilizing the safe harbor method, all records with three-digit ZIP codes corresponding to these three-digit ZCTAs must have the ZIP code changed to 000. Covered entities should not, however, rely upon the listing found in the August 14, 2002 regulation if more current data has been published. See: Office for Civil Rights. (November 26, 2012). *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*. Page 24. Retrieved February 18, 2018, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Re-identification

The implementation specifications further provide direction with respect to reidentification, specifically the assignment of a unique code to the set of de-identified health information to permit re-identification by the covered entity.

(c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

Appendix E: Audit Protocol for Limited Data Sets and Data Use Agreements

The following audit protocol for Limited Data Sets and Data Use Agreements is extracted from the HIPAA Audit Program protocol updated April 2016.[124]

Privacy §164.514(e)	Limited Data Sets and Data Use Agreements	§164.514(e)(1) Standard: Limited data set. A covered entity may use or disclose a limited data set that meets the requirements of paragraphs (e)(2) and (e)(3) of this section, if the covered entity enters into a data use agreement with the limited data set recipient, in accordance with paragraph (e)(4) of this section. §164.514(e)(2) Implementation specification: Limited data set: A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images. §164.514(e)(3) Implementation specification: Permitted purposes for uses and disclosures. (i) A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only for the purposes of research, public health, or health care operations. (ii) A covered entity may use protected health information to create a limited data set that meets the requirements of paragraph (e)(2) of this section, or disclose protected health information only to a business associate for such purpose, whether or not the limited data set is to be used by the covered entity. §164.514(e)(4) Implementation specifications:	Are data use agreements in place between the covered entity and its limited data set recipients, if any? Obtain and review policies and procedures and evaluate the content in relation to the established performance criterion to determine if data use agreements are in place between the covered entity and its limited data set recipients. Obtain and review a sample data use agreement to determine if the agreements comply with the established performance criterion. Obtain and review a sample limited data set to determine whether it complies with the established performance criterion.

[124] HHS.gov. (Updated April 2016). *Health Information Privacy. Audit Protocol*. Retrieved February 4, 2018, from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

		Data use agreement (i) Agreement required. A covered entity may use or disclose a limited data set under paragraph (e)(1) of this section only if the covered entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the protected health information for limited purposes. (ii) Contents. A data use agreement between the covered entity and the limited data set recipient must: (A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity; (B) Establish who is permitted to use or receive the limited data set; and (C) Provide that the limited data set recipient will: (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (4) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (5) Not identify the information or contact the individuals. (iii) Compliance. (A) A covered entity is not in compliance with the standards in paragraph (e) of this section if the covered entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful: (1) Discontinued disclosure of protected health information to the recipient; and (2) Reported the problem to the Secretary. (B) A covered entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with the standards, implementation specifications, and requirements of paragraph (e) of this section.	