Health Information Privacy Beyond HIPAA: A Framework for Use and Protection

A Report for Policy Makers

June 18, 2019

National Committee on Vital and Health Statistics

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

NCVHS Members and Staff

William W. Stead, MD, **NCVHS Chair**

Linda L. Kloss, MA, RHIA,* **Chair, Subcommittee on Privacy, Confidentiality and Security**

Bruce Cohen, PhD[+]

Llewellyn J. Cornelius, PhD, LCSW

Nicholas L. Coussoule*

Alexandra Goss

Richard W. Landen, MPH, MBA

Denise E. Love, BSN, MBA

Vickie M. Mays, PhD, MSPH*

Jacki Monson, JD*

Frank Pasquale, JD*

Robert L. Phillips, Jr, MD, MSPH

Debra Strickland, MS

Roland J. Thorpe, Jr, PhD

*Member of the Subcommittee on Privacy, Confidentiality and Security

[+]Term expired May 31, 2019

Rachel Seeger, MA, MPA
Lead Staff to the Subcommittee on Privacy, Confidentiality and Security
Senior Advisor, Public Affairs and Outreach
Office for Civil Rights, HHS

Rebecca Hines, MHS
NCVHS Executive Secretary/Designated Federal Officer
Health Scientist
National Center for Health Statistics, CDC, HHS

Sharon Arnold, PhD
NCVHS Executive Staff Director
Associate Deputy Assistant Secretary for Science and Data Policy
Office of the Assistant Secretary for Planning and Evaluation, HHS

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory public advisory body to the Secretary of the Department of Health and Human Services (HHS) in the areas of health data, standards, statistics, national health information policy, and the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. § 242k(k)). In this capacity, the Committee provides advice and assistance to HHS and serves as a forum for interaction with relevant private-sector groups on important health data issues. Its membership includes experts in the fields of health statistics, electronic interchange of health care information, privacy, confidentiality, and security of electronic information, population-based public health, purchasing or financing of health care services, integrated computerized health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. The Secretary of HHS appoints sixteen members for terms of four years each. Two additional members are selected by Congress. **www.ncvhs.hhs.gov**

June 18, 2019

Table of Contents

Executive Summary

The complex U.S. framework of privacy and data protection is evolving. Today, there is a greater focus on privacy and security protections for a digital and mobile environment than in the recent past. These laws, regulations and guidance are often characterized as a patchwork because they are not comprehensive in scope; they may apply only to a particular industry—such as financial services or health care—or they may apply narrowly to effect particular protections—such as those prohibiting discrimination based on genetic information or requiring fair credit reporting. Digital information has rapidly broken through boundaries, challenging our information privacy and data protection frameworks. Medical records were the traditional repository of information about one's health history, status, and care. Today, health information includes lifestyle, wellness, genetic and other information that may or may not be part of a formal medical record. The scope of health information has expanded, but the privacy and data protection laws, regulations, and guidance have not kept pace.

The U.S. has nearly two decades experience administering privacy and security of health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Carefully defined custodians have clearly defined responsibilities under HIPAA's Privacy and Security Rules, and there are enforcement consequences when a custodian violates the privacy rights of protected individuals. However, when a custodian discloses health information from the HIPAA controlled space or when it originates outside this space, today's privacy and protection patchwork breaks down.

The United States Congress charged the National Committee on Vital and Health Statistics (NCVHS) with studying and identifying "privacy, security and access measures to protect individually identifiable health information in an environment of electronic networking and multiple uses of data." The Committee undertook a 'Beyond HIPAA' initiative to examine emerging health information privacy and security challenges that are beyond the scope of the HIPAA law and its regulations, and to consider a health data privacy and security framework for the 21st century. This Report:

- Describes the environment beyond HIPAA and how it differs from the assumptions that frame HIPAA;
- Lays out essential elements for a new Framework for protection and use of health information beyond HIPAA;
- Discusses the principles that should guide protection of health information that underlie the new Framework;
- Recommends key actions at the federal level to advance the Framework; and
- Calls on private sector entities to improve privacy and security practices beyond HIPAA.

This Report is subtitled, "A Report for Policy Makers," a call to action addressed to those who set federal and state policy and those who set health information privacy and security policies for private sector entities. Public and private sector collaboration and an informed and engaged public would expand protections for health information beyond HIPAA.

Introduction

The Congress of the United States charged the National Committee on Vital and Health Statistics (NCVHS) with studying and identifying "privacy, security and access measures to protect individually identifiable health information in an environment of electronic networking and multiple uses of data." Over the past two decades, NCVHS has advised the Secretary of Health and Human Services (HHS) on a range of matters relating to the implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). At the same time, it offered advice on areas where health information protections are lacking or inadequate.[1,2,3]

This Report addresses privacy of health information when it is beyond the scope of the HIPAA law and it lays out a framework for foundational privacy protections for health information "beyond HIPAA." It is the result of two years of NCVHS hearings, research, and deliberations to understand the environment and consider a workable framework. The goal of this framework is to support innovative uses of health information to advance health and wellness while protecting the rights of the subjects of that information. In the Committee's assessment, the nation must adopt enhanced privacy protections for health information beyond HIPAA – and this should be a national priority.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a multi-part law enacted primarily to allow members of the workforce to continue to receive health insurance coverage between jobs. Another major purpose was to facilitate electronic transfers of health information for billings and other administrative efficiencies. It required health care organizations to implement standards that reduce paperwork burden and facilitate the efficient transfer of health care data between health care organizations and insurers. HIPAA also called for the promulgation of regulations requiring custodians to protect the privacy of patients and secure their data—provisions added to the bill when separate privacy legislation failed to advance in Congress. Congress' inability to pass legislation to protect privacy and security within three years after HIPAA's enactment triggered HHS's obligation to develop the Privacy and Security Rules.

Ironically, most people know HIPAA for those requirements added by the HIPAA Privacy Rule of 2000, not what is in the statute itself. HHS finalized the HIPAA Security Rule in 2003, and in

2009, the Breach Notification Rule introduced the requirement for notifying individuals of a breach of their protected health information (PHI). Patients routinely sign documents acknowledging their "HIPAA Rights, and patients can obtain access to their PHI by asserting their HIPAA rights. While HIPAA dictates what uses and disclosures may be made of PHI, nevertheless, well-meaning but over-cautious attorneys or compliance analysts often misrepresent its requirements.

Health information "beyond HIPAA" refers to all information about, or related to, individuals' health outside the coverage boundaries of the Privacy and Security Rules. These rules apply only to "covered entities," defined as health care providers who conduct insurance transactions electronically, health plans, and clearinghouses; and "business associates" of these covered entities, defined as those who have access to protected health information in the course of performing functions for HIPAA covered entities. If health information leaves this protected realm, it is "beyond HIPAA." So is health information generated outside of the covered entity.

With this report, NCVHS advocates for a new Framework of protections to cover health information collected for health care purposes when it leaves the protections of HIPAA *and* health information that originates in environments not covered by HIPAA. The volume, scale, and scope of this health information represents an ecosystem that largely did not exist when Congress passed the HIPAA law and when HHS designed the Privacy and Security Rules. The Framework has the potential to serve as a new floor complementing, not supplanting, HIPAA.

The HIPAA World

When the Congress enacted HIPAA in 1996, most confidential health information was locked in color-coded paper medical records. Many of the controls for capturing, analyzing, releasing, and archiving records protected physical medical records over the life cycle of those records. Clerks manually abstracted selected information from the record and entered it into registries, reported it as quality measures, transferred it for use in clinical trials, or indexed it for statistical purposes. Electronic billing was becoming more common, and analysts used tools such as "groupers" and severity adjustment algorithms to calculate payment adjustments and comparable outcome measures.[4]

The Congress, HHS, and industry shared a vision and imperative for electronic health records at the time, and HIPAA's focus on standards and privacy was an important catalyst. As NCVHS's 13th Report to Congress states, "HIPAA put the country on a path toward standardizing electronic health care transactions and protecting patients' health care information."[5] HIPAA includes both Privacy and Security Rules because Congress and HHS understood that privacy and security protections go hand-in-hand. The Privacy Rule establishes management safeguards

for confidential health data and mechanisms for patient control over the sharing of data. The Security Rule establishes physical, administrative, and technical safeguards for health data; it guards against data destruction, loss, corruption, or theft. The threats associated with cybersecurity have increased sharply since HHS adopted the Security Rule. Now, there are real consequences for covered entities, business associates, and patients—as well as for health information that is beyond the protections of HIPAA. These Rules provide much-needed guardrails without which, adoption of health information technologies could well have been stalled.

A major goal of the HIPAA Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule covers health information sharing between covered entities and their business associates for treatment, payment and health care operations (TPO). It also provides guidance on sharing for research uses, public health uses, regulatory uses, judicial and law enforcement uses and other uses that are beyond TPO. The Rule intends to strike a balance that permits important uses of information, while protecting the privacy of individuals who seek care and healing. Given that the health care marketplace is diverse, the drafters designed the Rule to be flexible and comprehensive, and to address the variety of uses and disclosures that they could anticipate.

HIPAA has proved a workable framework for regulating the flow of protected health information (PHI) within the boundaries set forth in the law. Patient authorization is generally required for disclosure of identifiable health information by covered entities unless a specific exception applies, such as treatment, payment, or health care operations. The Privacy Rule permits covered entities to use and disclose PHI without authorization for certain research activities. For example, a covered entity can use or disclose PHI for research if it obtains documentation that an Institutional Review Board (IRB) or Privacy Board waived the requirement for authorization or allowed an alteration, or if the individual authorizes disclosure in an IRB-approved informed consent. The Rule also allows a covered entity to enter into a data use agreement for sharing a "limited data set" for research purposes. The data use agreement may also permit activities preparatory to research and for research on decedents' information.

Health Information Definitions

The HIPAA Privacy Rule defines Protected Health Information (PHI) as information created or received by a covered entity about past, present, or future physical or mental health, or the condition of an individual for provision of health care services to an individual or the payment for those services.

"PHI remains subject to controls in the hands of covered entities. When disclosed outside the HIPAA domain of covered entities, HIPAA data is no longer subject to HIPAA controls, although some disclosed data may occasionally fall under the scope of another privacy law. In general, however, the data disclosed by a HIPAA covered entity (or by the individual) passes into the second category of unregulated data."[6] Importantly, information that is no longer in the hands of a covered entity is no longer PHI. In addition, information that is no longer individually identifiable is also not PHI.

Responsibilities and Obligations

HIPAA assigned compliance responsibility to "covered entities" strictly defined as providers of health care services, payers for those services and the clearinghouses that connected them by processing electronic transactions. "Business associates" are obligated to comply when performing contractual services involving health information on behalf of and under formal agreement with covered entities. Covered entities and business associates are responsible for safeguarding information including limiting access, use, and disclosure.

Essential HIPAA Guardrails:

- Health information definitions
- Responsibilities and obligations
- Rights of Information subjects
- Enforcement

Rights of Information Subjects

The Privacy Rule's baseline protection is to require a valid authorization or request for individual access prior to use or disclosure of data. Its default stance is to let the individual who is the primary subject of the protected health information, rather than a covered entity, define the scope of information that a covered entity can use or disclose."[7] The Rule specifies a number of exceptions where covered entities may use or disclose information without the authorization of information subjects. Examples include disclosure for public health, research covered by IRB waiver, disclosures required by law, workers' compensation and for "treatment, payment and operations."

Enforcement

HHS may impose civil monetary penalties on covered entities and business associates for violations of the HIPAA Rules. A complaint from an information subject or a breach that meets or exceeds the cut-off for reporting may trigger a penalty. HHS has imposed substantial penalties in the years since the enforcement rules went into effect, often accompanied by remedial compliance plans.

HIPAA provided a federal "floor" of privacy protections; states may, if they so wish, enact more stringent protections than this federal minimum, and many states have added provisions to the HIPAA floor. Like many complex laws, HIPAA included compromises that have since become

problematic. Congress rejected the call of some experts at the time that it should preempt state laws to ensure greater uniformity. It has grown more difficult and more costly for multi-state regulated entities to navigate compliance challenges of a complex patchwork of laws. In addition, entities that were explicitly exempt from HIPAA are more deeply involved in health information processing today than they were two decades ago.

The HHS Office for Civil Rights (OCR) is reviewing opportunities for regulatory change to the HIPAA Privacy Rule to encourage information-sharing for treatment and care coordination and to eliminate procedural requirements that may no longer be productive.[8] HHS is actively promoting interoperability and taking steps to prevent information blocking. Timely information sharing among providers improves care coordination and quality and reduces cost. OCR has also taken steps to remove barriers preventing patients from gaining access to their own health records. HIPAA exists in a largely digital health environment today and updates represent important advances.

These updates cannot, however, address the issues in the health information world of 2019 that are outside the scope of HIPAA.

Beyond HIPAA

Today's health information environment is a complex digital ecosystem comprised of countless "non-covered" entities that handle, process, and use some form of health information for a broad range of purposes. These entities include health app developers, device manufacturers, genetic companies, private disease and treatment registries, social media, marketing and analytic organizations, retail outlets, and more. If they are outside of HIPAA, they have a variety of limited obligations to protect the privacy of the health information subjects. They are not subject to the uniformity that patients now expect from the HIPAA rules. Today, safeguards for individually identifiable health information too often are weak or nonexistent.

The range of use cases of health information beyond HIPAA is vast. To guide its inquiry, NCVHS focused first on entities that receive identifiable health information directly from covered entities. Private disease or patient registries, widely valued tools for disease and treatment tracking and trending, are examples of entities that work at the intersection of the HIPAA covered and uncovered worlds. Covered entities may use available HIPAA mechanisms such as requiring these organizations to sign business associate agreements or adhere to a data sharing or data use agreement before releasing PHI to registries. Research shows, however, that many registries operate without even these basic protections.[9]

NCVHS also considered personal health devices used for monitoring patients with chronic diseases, often used under an order written by a health care provider. Creators of these valuable devices too often do not design them to ensure privacy and security.[10] The devices might not link directly to patient electronic health records, and their creators may not function as business associates of covered entities, which would bring them within the domain of HIPAA. They are but the tip of a growing range of devices and applications (apps) that collect data and transmit health-relevant data via the web. No current U.S. regulations address the "Internet of Things" (IoT) holistically.

NCVHS also looked at geo-fencing apps that use the Global Positioning System (GPS) or Radio-Frequency Identification (RFID) technology to create a virtual geographic boundary, enabling third parties to identify individuals via their cell phones while receiving medical care. This occurs without the individual's consent or even their awareness of the intrusion. Even if individuals knew that third parties were tracking them, they would have no practical recourse other than to turn off cellular services. The purpose of this stealth intrusion is presumably target marketing, but just as there is no control over the data gathering, there is also no transparency or control over the purpose of its usage or how it might be shared.[11]

In its Environmental Scan,[12] NCVHS examined the ever-expanding world of "big data," health data analytics, and the related policy considerations regarding privacy. Big data refers to extensive datasets—primarily in the characteristics of volume, velocity, and variability—from which an analyst can extract patterns, correlations, and information to support important decision-making.[13] Health companies now amass data from numerous sources including electronic health records (EHRs), medical imaging, pharmacy, therapeutics, genomics, payment, demographics, and many other sources. Data types and sources have expanded from traditional medical care to include a range of dimensions including geographic, population, public health, environmental, and others.[14] Companies may enhance the analytic and commercial value of big data by combining data sets. Research analytics may be subject to IRB controls affording a range of protections. Commercial analytics are under no such obligations.

A persistent assumption exists that when non-covered entities analyze data, de-identification protects privacy. However, the increasing availability of information generated outside health care settings, coupled with advances in technology to combine data sets, undermines the historical assumption that data can be forever technically de-identified.[15] In a 2017 report, NCVHS found that companies should no longer view technical de-identification of health information as a permanent privacy safeguard, and that re-identification is a growing reality.[16] The economic drivers to re-identify health data to create enhanced datasets make this a central issue for consideration in the world beyond HIPAA. Without additional rigor or administrative controls, technical de-identification may convey a false veneer of privacy.

The dilemmas about health information beyond HIPAA are complex and compelling.

What is Health Information?

A framework for use and protection of health information beyond HIPAA must grapple with the fundamental definitional challenge of what constitutes health information. Our modern conception of health-relevant information goes well beyond that created or received by a covered entity for treatment and payment. Health-relevant information includes social determinants of health, environment, lifestyle, diet, fitness, and other factors. Patient-generated health data is a growing source of relevant information.

***Beyond HIPAA* Dilemmas:**

- What is health information?
- Who owns the information?
- What are the rights of information subjects?
- To what degree is de-identification a safeguard?
- What are the rights and responsibilities of data holders or processors?
- What are the courses for remediation for harms?

The NCVHS Health Data Framework emphasizes that "the benefits of the explosion and liberation of health related data can only be realized if the systems for making sense of data keep pace with their burgeoning volume and complexity."[17] In the judgment of NCVHS, an approach that defines health information in terms of its custodian is unworkable for the world beyond HIPAA. Policy officials must define health-relevant information beyond HIPAA in a way that is flexible enough to reflect personal preferences, uses, and contexts.

Who Owns the Information?

The HIPAA law does not adopt information ownership as an approach. Instead, it enumerates specific rights that people have with respect to their data and assigns covered entities custodial responsibility for health information, including responsibilities for managing access to, and disclosure of, information in accordance with the provisions of the Privacy and Security Rules. Information subjects retain broad access rights, and new laws and regulations have underscored and expanded those rights over time. While certain state laws may bestow ownership of physical medical records to providers, patients may determine who accesses and uses their information. Similarly, a corporation that owns a CT scanner may arguably own the data produced by the equipment, but patients have unlimited rights to access and use the findings.

The ownership question arises more and more frequently as the commercial value of information products and services increases, and as companies make greater investments in technologies and intellectual property. While several states have laws that assign property rights to individuals for their genetic information and results of DNA analysis, for the most part, state laws are silent or vague on the matter of ownership of medical record information. In the

information age, “some continue to promote patient ownership even as the notion of ownership becomes seemingly less meaningful.”[18] Ownership is not a relevant issue for framing the protection of health information in the world beyond HIPAA.

What are the Rights of Information Subjects?

Rather than ownership, the right questions in the world beyond HIPAA may be who has access to the information, in what form, for what purpose, and what rights do information subjects retain? Recent research confirmed that people generally seek three assurances. First, they seek respect for the rights and interests of individuals whose data are stored in databases, including access to information about themselves and a meaningful voice in how custodians use and disclose their data. They support the societal benefits that will flow from having their data accessible for research, public health, and other important uses. They also expect information security and other basic protections for their information.[19]

People are generally unaware of the many ways their health data may be used when it leaves the protections of HIPAA or when they voluntarily disclose it while using an app or data service, such as for commercial genetic testing. Most consumers do not understand the concept that data protections significantly change when the data move from one environment to another. Even if one executes an informed consent for an initial use, the custodian likely does not disclose subsequent reuse and re-disclosure. Most people do not understand the scale of commercial interests’ dependent on unencumbered access to information and the risks of re-identification. Further, because technology changes so rapidly, it is not reasonable to expect people to be responsible for anticipating future risks.[20]

To What Degree is Technical De-identification a Safeguard?

“De-identification is a process that is applied to a dataset with the goal of preventing or limiting informational risks to individuals, protected groups, and establishments, while still allowing for the production of aggregate statistics.”[21] Once de-identified, protected health information is no longer subject to the provisions of the HIPAA Rules and may be disclosed and used for a variety of purposes. The widespread availability of de-identified health data, liberated from HIPAA, is the raw material for the big data industry. De-identification is justification for virtually unlimited use of health data with no residual obligations to the underlying information subjects.

The threat of data re-identification, however, is increasing as powerful analytic tools combine data sets and extract information from large volumes of data. “There are economic drivers for re-identification of health data to create enhanced datasets that make it an increasingly important topic. For example, combining health care service patterns and personal web search patterns may be valuable for marketing products and services.”[22] In the unregulated world of data and health data there are no limits on use despite the growing risk, even certainty, that

data can and will be re-identified. Once a safeguard, de-identification at least in its present state is rapidly becoming a myth.[23]

What are the Rights of Data Holders or Processors?

"Data holder" is an inclusive term referring to entities that design and maintain proprietary databases and algorithms, sell data products, or design and build apps and devices that capture, transmit or use health data. A range of mechanisms is in place to protect the rights of such entities. These include ownership, copyright, patent, trade secrets, and other laws protecting commercial interests. Business-to-business contracts for data sales are commonplace and enjoy all the protections of contract law. Protections are generally on the side of businesses and not the individuals whose information is the basis for the business. To pursue business interests, companies may voluntarily agree to meet HIPAA-like standards when covered entities impose them through data sharing, data use, or business associate agreements.

Many commercial entities engaged in processing health information not covered by HIPAA fall under the jurisdiction of the Federal Trade Commission (FTC). While the FTC has broad jurisdiction under its general powers to take action in individual cases against unfair and deceptive trade practices, it may promulgate rules only in very rare cases where authorized by Congress. The United States has a matrix of privacy and breach laws across jurisdictions that do not complement one another and do not address contemporary dilemmas. Recent exposure of social media data practices and vulnerabilities has opened the eyes of many about the need to step up protections. The United States lacks safety nets if someone does bad things with our data.

What are the Courses for Remediation for Harms?

Health information contributes to the public good. People do benefit from scientific research, personal health devices and apps, big data, and other innovations that are outside the privacy controls of HIPAA. However, the same innovations may expose individuals to increased risk of harms such as discrimination, stigmatization, and loss of autonomy. Government and industry should protect individuals from such harms by putting in place reasonable levels of protection and paths for remediation. Approaching protection solely based on harm that causes economic damage is too high a bar "in that it allows almost any use or disclosure unless the data subject can provide (in a court of law) that a direct economic harm resulted."[24] Policymakers and industry developers must also consider values such as autonomy, integrity, dignity and quality of life.

Technology is having a profound effect in shaping the world beyond HIPAA, but the reasons why we need a broader privacy framework are not solely technological. There must be a range of well-understood mechanisms designed to mitigate the risk of harm, redress the

consequences of harm, and punish outright fraud. These will inevitably include sound information management and governance, including responsible security practices, application of ethical principles for use of information, and legal protections and recourse.
There is growing interest in personal privacy and greater potential for people to access and use their health records. At the same time, many people do not know how to access their information or exercise their rights under HIPAA. The barriers to individuals' abilities to understand, much less consent, to how their information is used, are greatly magnified when it leaves the HIPAA controlled environment.

Guiding Principles for Use and Protection of Health Information

Uses for health information have unimaginable potential to benefit our understanding of health and wellness generally and to improve the health and health care to individuals. In this context, NCVHS recommends the following as Guiding Principles for Use and Protection of Health Information Beyond HIPAA:

1. **Privacy protections should promote greater health equity.**

Paula Braverman asserted in 2017 that health equity means, "everyone has a fair and just opportunity to be as healthy as possible." [25] Yet gaps in health and health care for individuals are pervasive and consequential. To achieve equity in how health information affects some individuals, policymakers and data holders should incorporate into health information privacy policies protections from discrimination, stigma, and exploitation resulting from use and sharing of health information, particularly for vulnerable individuals.

2. **Individuals should have options to exercise their privacy preferences and assert their information rights.**

Most individuals have scant understanding of how data holders use their health information, when and to whom they disclose in identifiable or de-identified form. A data holder may present terms of service, use, and consent to subject individuals for their approval, but generally do not provide details of use and potential sharing of the information, which makes those details difficult to assess. An individual may not understand how to exercise rights such as requesting limitations, seeking an accounting of disclosures, or requesting their providers to sequester certain information. In addition, because individuals cannot assume that de-identification techniques, even where in use, will permanently protect privacy,[26] individuals should have the right to expect that data holders and downstream recipients of their data will not re-identify it without their permission.

3. Data holders should disclose what information they hold, and how they secure it.

A framework beyond HIPAA should allow individuals a right of access to information that data holders store about them. This right should include an accounting of information that data holders have disclosed about them, to whom, in what form, and how subsequent data holders are using it. Data holders should also inform individuals about the way they secure data to prevent its theft, breach, damage, destruction, or manipulation. This principle should be in force regardless of the intended use, whether commercial or non-commercial. When individuals know what data holders are collecting and why, they can consider how the intended uses align with their preferences. They should have the right and opportunity to ask questions, understand the goals of data collection and use, and become more comfortable participating in these endeavors.[27]

Guiding Principles for Use and Protection of Health Information

1. Privacy protections should promote greater health equity.
2. Individuals should have options to exercise their privacy preferences and assert their information rights.
3. Data holders should disclose what information they hold, and how they secure it.
4. Data holders should specify the purposes for which they collect, use, and disclose information.
5. Health information collection in the world beyond HIPAA should be limited to that needed for the current purposes.
6. Consent requirements for disclosure should be meaningful and understandable.
7. Unconsented uses and disclosures are limited and clearly specified.
8. Based upon risk analysis, ongoing risk management and rigorous protections should be in place for more granular and sensitive information.
9. Data sharing should only occur under a data use agreement that prohibits re-identification and re-disclosure.

4. **Data holders should specify the purposes for which they collect, use, and disclose information.**

In the beyond HIPAA ecosystem, both data holders and individuals must understand the business purpose and intended uses for which data are captured, compiled, and stored. This specification helps individuals judge the risks associated with participation and make informed decisions when granting permission or limiting uses. For example, individuals may view clinical research differently than marketing uses, and, based on these views, make different choices.

Purposes and uses evolve over time as new insights and opportunities emerge from use. Policymakers and data holders cannot successfully implement this principle with a one-time, static notice. Going forward, data subjects will demand greater transparency and flexibility along with opportunities to change permissions based on their own assessment of the risk associated with evolving business purposes and uses.

5. **Health information collection in the world beyond HIPAA should be limited to that needed for the current purposes.**

Once information exists, it persists. Thus, limiting collection in the first place is an important privacy protection principle. Data holders should take greater care with the information they are collecting. For example, information grocery stores should not sell information collected for inventory control to a commercial entity that seeks information to make inferences about individuals' health.

6. **Consent requirements for disclosure should be meaningful and understandable.**

People make choices continually about what health-related information they share, some deliberate and many inadvertent. Too often private services compel uncomfortable choices or do not fully disclose the implications of the choices presented. For example, the offer to get a discounted drug price may be contingent on providing information about one's condition to the drug manufacturer. Giving up personal health information to get necessities one needs to live by may represent compelled consent.

7. **Unconsented uses and disclosures are limited and clearly specified.**

This principle extends purpose specification by limiting unconsented uses and disclosures that are incompatible with the original purpose. Limiting, rather than prohibiting, reflects the need to promote innovation and develop new knowledge and insights. Policymakers and industry should protect Individuals against analyses and inferences that are unwelcome, harmful, discriminatory, or unreasonable. For example, while the accelerometer in one's mobile device may be able to detect tremors indicative of Parkinson's disease, consumers do not expect their

phone's manufacturer to be making such inferences without advance notice. The rapidly changing landscape of the space beyond HIPAA underscores the need for industry to give greater consideration prior to permitting uses of data, and great thought to what uses should be restricted or prohibited.

8. **Based upon risk analysis, ongoing risk management and rigorous protections should be in place for more granular and sensitive information.**

Not all information carries an equal risk of harm. Genetic information has greater potential for wider discriminatory use than do, for example, patterns of an individuals' physical exercise. This principle advances a risk-based approach to data protection and use. The notion that certain types of health information are particularly sensitive, such as mental health, substance use disorders, and HIV/AIDS, is a helpful and broadly understood risk based approach.

9. **Data sharing should only occur under a data use agreement that prohibits re-identification and re-disclosure.**

A Framework for Use and Protection of health information beyond HIPAA requires that there be accountability as data holders pass information one to another. Data use agreements and other contractual mechanisms make explicit the responsibilities of parties involved in sharing and obtaining health information. These can reinforce essential privacy and security-protecting mechanisms in the Guiding Principles. While no guarantee that recipients will not misuse data, such agreements benefit data holders acting in good faith and the subjects of the shared data.

The Committee identified these nine guiding principles for use and protection of health information to guide governance of emerging uses of health information beyond HIPAA. The Committee does not intend them as rules or absolutes but rather as guidelines to inform the design of a Framework for health information. Without reasonable guardrails for sharing and use of health information beyond HIPAA, individuals may be unwilling to give or share their data because of the risks and unknown consequences to them and their families. Advancing both protection for individual privacy and the use of information to improve health equity and advance the health status of populations is the privacy challenge of our time.

Framework for Use and Protection of Health Information Privacy Beyond HIPAA

The following Framework for Use and Protection of Health Information Privacy Beyond HIPAA is intended to:

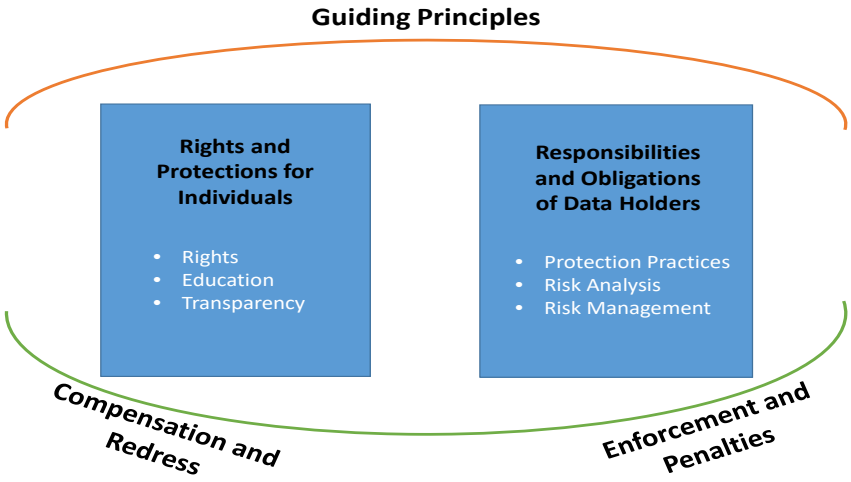
- Advance understanding and dialogue about the issues;

- Help HHS and other federal agencies consider the levers they have under current laws to improve protections for health information beyond HIPAA;
- Promote greater public and private collaboration to advance a range of viable approaches with urgency; and
- Encourage greater initiative through high impact actions that individuals, covered entities, business associates, and the currently non-HIPAA covered industry can take.

The Framework, based on the guiding principles above, reflects a set of ideas and beliefs about how the US should approach the privacy of health information beyond HIPAA while enabling use of information to pursue health and wellness improvements. It encompasses the rights and protections for individuals and the redress they have when their information is misused. The Framework also encompasses the responsibilities and obligations of data holders and the mechanisms for enforcement, including penalties, for violations that harm individuals or the public.

The Framework presumes that the federal floor secured by the HIPAA Privacy and Security Rules is in place, and it calls on covered entities, business associates, and non-HIPAA-covered entities to take the initiative where expanded care and vigilance in disclosure practices will enhance protections for individuals.

Figure 1. Framework for Use and Protection of Health Information Beyond HIPAA



The Framework reflects six key characteristics. First, the Framework requires a foundation of rules that includes public, private, commercial, and nonprofit data holders. This foundation of rules includes laws, controls, policies, agreements, contracts, and management practices

executing the guiding principles described above. Only a broad approach will account for the fluidity of health information and the range of uses; only a broad foundation will accommodate rapid change and innovation.

Second, the rights and protections for individual data subjects transect the range of uses by data holders. All data holders should strengthen protective practices. These include mechanisms such as use-based consent and convenient and understandable authorization processes, mechanisms for sequestration and segmentation and other approaches that can substantially improve the exercise of individual rights and preferences. Certain vulnerable individuals, such as individuals who have a disease or disability that could limit the ability to exercise their rights, may need greater protections. Further, protections should follow the data or at least be consistent across data holders, particularly for data that is of moderate or higher risk when considered in terms of the potential for real or perceived harms.

Third, data holders will benefit from an explicit foundation of laws, governance rules, and best information management practices. Mechanisms for data holders also include information exchange, security, data anonymization practices and other best practices. NCVHS underscored security, because security is foundational to achieving privacy. Like generally accepted accounting principles, principles for use and protection of health information should be explicit, understandable, and regularly maintained to reflect new circumstances that arise as the health data privacy environment evolves. In addition, like accounting principles, performance should be transparent, and there should be a way in which entities can assess their conformance to contribute to shared learning and improved performance over time.

Fourth, given the many uses for health information beyond HIPAA, the Framework acknowledges that not all uses for health information carry the same potential risks and benefits. The Framework calls for development of a use-based risk model to identify potential harms. Uses beyond HIPAA include at least the following: mobile applications, personal health devices, genetic information services and products, consumer-generated testing kits, health registries, and commercial data analytics. Protective mechanisms can vary based on clearer understanding of the risks associated with types of uses.

This fourth characteristic also calls for examining levels of information associated with higher risks of harm. A higher level of protective practices should apply to information that carries a greater risk of harm.

The National Institute of Standards and Technology (NIST) distinguishes impacts to confidentiality using a high-medium-low scale reflecting potential levels of harm that could affect the individual or the data holder.[28] The higher the perceived risk, the greater the obligation to inform individuals so they can make choices about how they prefer to exercise

their rights. For example, historically, privacy regimes hold substance use and mental health information to more rigorous standards.[29] Restrictions on use of genetic information for employment and for insurance underwriting are key features of the Genetic Information Nondiscrimination Act.[30]

Fifth, the Framework asserts that enforcement mechanisms are needed to redress data holder failures to implement protective and security practices. The federal government should identify gaps in enforcement mechanisms and close them by law, regulation, or by a combination of public-private collaboration backstopped by law. A meaningful enforcement scheme could serve as an incentive for adoption of further appropriate controls.

Sixth and finally, the Framework spotlights the need for a more complete understanding of harms—to individuals, to communities, and to vulnerable populations. This in turn will lead to identifying gaps in legal protections including compensation and redress.

Key Characteristics for a Use and Protection Framework:

1. Foundation of rules that cover public, commercial and nonprofit data holders;
2. Consistent rights and protections for individual data subjects;
3. Explicit obligations for data holders that are adapted over time;
4. Special protections for uses and types of information associated with higher risks of harm;
5. Enforcement and penalties for data holders that fail to carry out individuals' preferences, who misuse or fail to protect data;
6. Codified range of harms to individuals, communities and vulnerable populations.

NCVHS envisions a Beyond HIPAA Framework built on a foundation of guiding principles, law, and protective best practices. Improving protections for health information uses beyond HIPAA need not be highly regulated and prescriptive. Rather, as the Framework indicates, key levers can provide targeted protections, serving as rules of the road and guardrails. However, the adoption of laws and practices based on Framework elements can advance the interests of individuals and those of a responsible health data industry. Failing to take steps to protect health information beyond HIPAA could be harmful to individuals, to public health, and to health care innovations by US stakeholders.

The Path Forward

NCVHS calls on government and private sector stakeholders to commit to a long-term course of action to develop and implement this Framework for Use and Protection of Health Information that is not protected by HIPAA. Putting in place a policy framework that serves as a cross sector

foundation requires participation by federal, state and local government jurisdictions, health industry stakeholders, commercial entities, and engaged citizens.

The key lesson of NCVHS's Beyond HIPAA initiative is that effective privacy and security practices cannot stop when information leaves the environment in which HIPAA protections apply. In the digital world, custodial obligations do not stop at the door and no entity is exempt from some level of custodial responsibility if they are in the health information business, whether as an app developer or as a passive exchange entity.

Similar to the implementation of the HIPAA Privacy and Security Rules, extending protections beyond HIPAA represents major policy and social change. Fortunately, NCVHS and the broader health industry have learned lessons in the nearly two decades working with the HIPAA Privacy and Security Rules that can serve as guideposts. Consumer data protection initiatives such as the European Union's General Data Protection Regulation and other recent developments[31] reflect additional equities and approaches. The challenge for the United States is to mobilize a multi-sectoral and multi-phased effort to build upon and extend what is now in place.

Private Sector Near-Term Actions

NCVHS calls upon the private sector and information subjects to take steps to improve current practices. These actions, which require no changes to laws or regulations, can improve the current state and demonstrate a commitment to advancing the guiding principles.

As the table below shows, if covered entities consider their information custodial role beyond what is strictly required to comply with today's Privacy and Security Rules, they could extend protections in very important ways today that not only improve their own reputations and risk mitigation positions, but also better serve their patients and communities.

Being a good steward of health information is not only a legal compliance obligation, it is a moral and ethical one. In this context, NCVHS calls upon health care providers, insurers, and clearinghouses and their business associates to take actions.

Near Term Actions for Covered Entities and Business Associates
• Require data sharing and data use agreements before disclosing individually identifiable health information. • Improve informed consent practices. • Strengthen de-identification methods and match methods to the sensitivity of the dataset. • Improve ease of access for individuals to their information and provide guidance on how to protect it. • Become more transparent about the actual uses being made of personally identifiable and de-identified health information. • Improve accounting of disclosures including disclosure of de-identified data sets. • Implement more robust information and data governance programs particularly focused on access and disclosure management and security. • Adopt personal health technology products only if they meet rigorous privacy and security specifications. • Proactively upgrade security practices needed to protect the information from a cyber-attack.

Data holders, as broadly defined above, have the opportunity and the obligation to make privacy and security a core value and even a market differentiator. While not legally bound by HIPAA, any business or nonprofit that uses health information, and seeks success in their mission, should understand the trends that are leading to the need for greater data protection. The table below suggests some near term actions that data holders can take on their own and in collaboration with other industry partners.

Near Term Actions for Data Holders
• Adopt privacy-by-design practices and adhere to security best practices. • Require data sharing agreements before re-disclosing identifiable health information. • Implement information and data governance programs to upgrade the policies and practices for managing health information. • Improve understanding and adherence to Fair Information Practices Principles. • Become more transparent about the actual uses of personally identifiable and de-identified health information. • Educate employees on health information confidentiality and hold them responsible for breaches or any misuse of information.

As health care recipients, we are all information subjects, and many of us have become more aware of our HIPAA rights and more literate about how to exercise them. We should be just as vigilant when companies that are not delivering health care ask for health-related information or data from which they can infer health information.

Near Term Actions for Information Subjects
• Learn how to exercise your health information rights. • Be diligent about protecting health information in your possession. • Question entities that want your health-related information about its intended use, resale and re-disclosure policies, and privacy and security practices. • Read and understand consent forms, including electronic consents, before signing them.

Public Sector Near-Term and Longer Term Actions

Implementation of the Framework will require Congressional and cross-agency federal leadership through a series of legal and regulatory changes and the supporting research to inform these changes. NCVHS recommends that the Secretary of Health and Human Services lead efforts to improve the protection of health information beyond HIPAA because the Department has nearly two decades of experience in advancing and enforcing nationwide information privacy and security policy.

HHS is currently advancing policies that promote information interoperability and exchange. This presents an opportunity to take several actions that could reduce vulnerabilities at the intersection of the regulated and unregulated worlds. The Committee suggests timely action in the four areas shown in the following table:

Near Term Actions by HHS
• Establish federal health information security and privacy standards for sponsors of health data registries. • Establish federal health information security and privacy standards for medical device and mobile application manufacturers. • Develop consumer guidance concerning use and protection of direct-to-consumer testing, such as genetic analysis, when not protected by HIPAA. • Support a federal research agenda on de-identification methods including the risks of re-identification related to various methods for de-identification.

NCVHS also recommends longer-term actions that are key to implementing the Framework to improve the protection of health information beyond HIPAA. NCVHS urges HHS to advance these as part of its strategic leadership plan. HHS is ideally positioned to lead and convene other agencies to advance the important initiatives shown below.

Longer Term Actions by HHS and other Federal Agencies

- Support a federal study of how consumers might exercise their rights to seek redress in the case of unauthorized access, misuse, or harm attributable to use of their identifiable health information.
- Develop federal baseline standards for privacy and security protection of individually identifiable and de-identified health information held by commercial organizations outside the scope of HIPAA.
- Develop a model for tiers or categories of harms and risks regarding unauthorized access or misuse of health information beyond HIPAA.
- Develop scalable consumer and school-based education curricula about health information privacy and security.

The Importance of Public-Private Collaboration

NCVHS recognizes that the protection of health information beyond HIPAA represents a challenge of great importance and complexity and must be supported by strong industry collaboration. The government should serve as the convener for public-private collaboration to coalesce research, development, and the call to action to adopt a beyond HIPAA Framework. The years preceding the adoption of HIPAA saw intense public-private stakeholder collaboration to shape workable policy – so too in the run-up to health IT adoption. Key stakeholders include federal, state and local governments, health industry stakeholders, research and public health, developers, commercial entities, and engaged citizens. While trade, standards developers, and industry groups are expending significant efforts that are relevant to building the beyond HIPAA protections NCVHS envisions, these efforts could be more impactful with broader, government-sponsored collaborative leadership.

The beyond HIPAA world is dynamic and public-private collaboration it likely to be required for some time to come. NCVHS calls on HHS and other federal agencies to lead a collaborative effort to build the call to action and then put in place a cross-industry system of governance to advance the Framework over time based on experience and the changing environment.

NCVHS is poised to advise and support the Secretary and HHS in these important undertakings.

Citations

[1] National Committee on Vital and Health Statistics (hereinafter, NCVHS), *Enhancing Protections for Uses of Health Data: A Stewardship Framework – Summary for Policy Makers*, Dec. 19, 2007, https://ncvhs.hhs.gov/wp-content/uploads/2014/05/080424rpt.pdf (visited June 17, 2019).
[2] NCVHS, *A Stewardship Framework for the Use of Community Health Data (*hereinafter *Stewardship Framework)*, Dec. 5, 2012, Letter to Secretary Kathleen Sebelius, Department of Health & Human Services (HHS), https://ncvhs.hhs.gov/wp-content/uploads/2014/05/121205lt.pdf (visited June 17, 2019).
[3]NCVHS, *Recommendations on De-identification of Protected Health Information Under HIPAA* (hereinafter *De-identification Recommendations)*, Feb. 23, 2017, Letter to Secretary Thomas E. Price, HHS, https://ncvhs.hhs.gov/wp-content/uploads/2018/03/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf (visited June 17, 2019).
[4] Centers for Medicare and Medicaid Services. *MS-DRG Classifications and Software*, (page last modified Aug. 3, 2018), https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/AcuteInpatientPPS/MS-DRG-Classifications-and-Software.html (visited June 17, 2019).
[5]NCVHS, *The Thirteenth Report to Congress on the Implementation of the Administrative Simplification Provisions of the Health Insurance Portability and Accountability Act of 1996*, Mar. 14, 2019, https://ncvhs.hhs.gov/wp-content/uploads/2019/03/13th-Report-to-Congress.pdf (visited June 17, 2019).
[6] NCVHS, *Report on Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges (hereinafter Environmental Scan),* prepared by Robert Gellman on behalf of NCVHS, Dec. 13, 2017, https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf (visited June 17, 2019).
[7] NCVHS, *Recommendation on the HIPAA Minimum Necessary Standard,* Letter to Secretary Sylvia M. Burwell, Nov. 9, 2016, https://ncvhs.hhs.gov/rrp/november-9-2016-letter-to-the-secretary-recommendation-on-the-hipaa-minimum-necessary-standard/ (visited June 17, 2019).
[8] Request for Information on Modifying HIPAA Rules to Improve Coordinated Care, 83 Fed. Reg. 64302 (Dec. 14, 2018), https://www.govinfo.gov/content/pkg/FR-2018-12-14/pdf/2018-27162.pdf (visited June 17, 2019).
[9] Leslie P. Francis, *Patient Registries: Patient Consent when Children Become Adults,* 7(2) ST. LOUIS U. J. HEALTH L. & POL'Y 389 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2563320 (visited June 17, 2019).
[10] Joshua Franklin et al., *Mobile Device Security: Cloud and Hybrid Builds, Volume B, Approach, Architecture, and Security Characteristics*, National Institute of Standards and Technology (NIST) Special Publication 1800-4B (Feb. 2019), https://www.nccoe.nist.gov/publication/1800-4/VolB/ (visited June 17, 2019).
[11] Debra Cassens Weiss, *Law firms hire company to send ads to ER patients' cellphones; Is it a HIPAA violation?* AM. BAR ASSOC. J. (May 30, 2018), http://www.abajournal.com/news/article/law_firms_hire_company_to_send_ads_to_er_patients_cellphones_is_it_a_hipaa/?utm_source=maestro&utm_medium=email&utm_campaign=weekly_email (visited June 17, 2019).
[12] *Environmental Scan, at 20-36*.
[13] Andrea De Mauro et al., *A Formal definition of Big Data based on its Essential Features*, 65 LIBR. REV. 122–135 (2016).
[14] NCVHS, *The NCVHS Health Data Framework* (hereinafter *Health Data Framework*) Mar. 21, 2017, https://ncvhs.hhs.gov/wp-content/uploads/2018/03/Framework-White-Paper-v9-2017-03-21.pdf (visited June 17, 2019).
[15] I.G. Cohen and M.M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320(3) J. AM. MED. ASSOC. 231 (2018).
[16] *De-identification Recommendations*, at 5.
[17] *Health Data Framework*, at 2.
[18] *Environmental Scan*, at 14.
[19] Amy L. McQuire et al., *Who Owns the Data in a Medical Information Commons?* 47 J.L. MED. & ETHICS 62-69 (Mar. 2019, first published online April 17, 2019).
[20] Harold Thimbleby, *Technology and the Future of Healthcare*, 2(3) J. Pub. Health Res. e28 (Dec. 1, 2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4147743/ (visited June 20, 2019).

[21] Simson L. Garfinkel, *De-identifying Government Datasets*, NIST Special Pub. 800-188 (2d DRAFT) (Dec. 2016), at 8, http://csrc.nist.gov/publications/drafts/800-188/sp800_188_draft2.pdf (visited June 20, 2019).
[22] *De-identification Recommendations*, at 9.
[23] Mark A. Rothstein, *Is Deidentification Sufficient to Protect Health Privacy in Research?* 10(9) Am. J. Bioeth. 3 (Sep. 2010), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3032399/ (visited June 20, 2019).
[24] *Environmental Scan*, at 29.
[25] Paula Braverman, *A New Definition of Health Equity to Guide Future to Guide Future Efforts and Measure Progress*. HEALTH AFF. (June 22, 2017) https://www.healthaffairs.org/do/10.1377/hblog20170622.060710/full/.
[26] President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, at 38-39 (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (visited June 17, 2019).
[27] *Stewardship Framework*, at 4.
[28] Erika McCallister, NIST Special Pub. 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Science and Technology (Apr. 2010)*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.
[29] *See, e.g.*, Confidentiality of Substance Abuse Disorder Patient Records, 42 C.F.R. Part 2 (2018), https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2.
[30] Genetic Information Nondiscrimination Act of 2008, Pub. L. 110–233, 122 Stat. 881 (May 21, 2008), https://www.govinfo.gov/content/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf (visited June 20, 2019).
[31] *See, e.g.*, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679 (visited June 20, 2019); California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100-199 (*Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3*, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121 (visited June 20, 2019).