Privacy and Security Protections for Health Information

Participation in and use of a learning health system will be highly dependent upon reliable mechanisms to ensure that (1) a secure network infrastructure is widely available; (2) privacy is protected; (3) health information and services are accessed only by participants whose identity has been verified and who have been authenticated to access the system they are seeking to access; (4) users have access only to data they are authorized to access, where authorization is determined by individuals' choices, or, if no choices are recorded, what the statutes, regulations and consensus rules say a user may access, use, disclose and receive. All of these components are necessary for enabling broad scale interoperability and a learning health system.

Ubiquitous, Secure Network Infrastructure

LHS Requirement

E. ***Ubiquitous, secure network infrastructure****:* Enabling an interoperable, learning health system requires a stable, secure, widely available network capability that supports vendor-neutral protocols and a wide variety of core services.

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

- Advance a national communications infrastructure that supports health, safety and care delivery
- Protect the privacy and security of health information
- Increase access to and usability of high-quality electronic health information and services

Background and Current State

Security of the network infrastructure is pivotal to ensuring success of a learning health system. It is the basis for enabling necessary trust that data can be shared in a way that keeps it secure and private, unaltered in an unauthorized or unintended way and available when needed by those authorized to access it. There are a number of components that will ultimately enable a ubiquitous, secure network infrastructure, including cybersecurity and encryption. Additionally, in a learning health system, the security of the systems and their underlying security infrastructure will continuously evolve as necessary to maintain its secure state.

As health IT systems have become increasingly connected to each other, cyber threats have concurrently increased at a significant rate. In an interoperable, interconnected health system, an intrusion in one system could allow intrusions in multiple other systems. Additionally, there is high variability in the capabilities and resources healthcare organizations have at their disposal to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cybersecurity; however, small and mid-sized health care organizations, like other small businesses, may not have these resources and may not be able to afford them. Finally, there is a significant behavioral and cultural change necessary in the industry regarding the relevance of

cybersecurity risks. Many in the industry do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks. Despite being identified as critical infrastructure for the nation, the healthcare system could do more to prepare for a cyber-security attack.[34]

Encryption of data is a second component of a ubiquitous, secure network infrastructure. Encryption is a method of scrambling or encoding data, so that it cannot be read without the appropriate key to unscramble the content. Encryption is applied when data is sent (particularly over networks that are not secure otherwise, like the Internet) and when it is stored. These are sometimes referred to as information in transit and information at rest, respectively. In both cases, the core mechanism is the same. A software program takes a piece of information (a string of data bytes) and changes it into another piece of information (a different string of bytes, not necessarily the same number of bytes). For encryption to work, it must be possible for another program (or possibly another algorithm in the same program) to reverse the process and change the encrypted information back into the information in the clear. This is called decrypting. Another constraint is that the algorithm to decrypt should itself be secure; otherwise, unwanted recipients would be able to recover the original information.

Encryption is a safe harbor provision under the Breach Notification Rule.[35,36] This means that if a HIPAA Covered Entity (CE) or Business Associate (BA) (who may have custody of the protected health information or PHI), such as a cloud-based EHR and data services provider, chooses to encrypt PHI consistent with guidance in the Breach Notification Interim Final Rule, 74 Fed. Reg. 42740 (Aug. 24, 2009) and discovers a breach of that encrypted information, neither a CE nor a BA is required to provide the breach notifications specified under the Rule. See Appendix C for more information on cybersecurity and encryption.

Moving Forward and Critical Actions

A learning health system's cybersecurity program encompasses, but is not limited to, the following:

- Contracts, such as Data Use Agreement, Memorandum of Understanding/Memorandum of Agreement (MOU/MOA), Interconnection Security Agreement (ISA), and Business Associate Agreement (BAA). These documents, which are typically bi-lateral between two parties, exist in addition to each party's own compliance documents such as HIPAA Privacy & Security Policies and Procedures, or other documents required by law. Collectively, the bilateral documents *and* the individual organization's policy and compliance documents document the regulatory and other requirements for-security controls, technical implementation as well as business to business requirements for connecting between health IT systems;

[34] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

[35] 45 CFR 164.404(a). October 2011. http://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-404.pdf

[36] 74 FR 42740 pg. 42742. August 2009. http://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf

- Cross-organizational threat information sharing and mature incident response capabilities;
- Incident Management and Response policies and procedures are in place and a response team is identified within the organization;
- The functional contents of all network messages are fully encrypted; and,
- All data stored in any database connected to the network (whether through a companion system, interface engine, or gateway) is fully encrypted.

Table 5: Critical Actions for Ubiquitous, Secure Network Infrastructure

Category	**2015-2017** Send, receive, find and use a common clinical data set to improve health and health care quality	**2018-2020** Expand interoperable health IT and users to improve health and lower cost	**2021-2024** Achieve a nationwide learning health system
E1. Cybersecurity	1. ONC will work with OCR to release an updated Security Risk Assessment tool and hold appropriate educational and outreach programs. 2. ONC will coordinate with the Office of the Assistant Secretary for Preparedness and Response (ASPR) on priority issues related to cyber security for critical public health infrastructure. 3. HHS will continue to support, promote and enhance the establishment of a single health and public health cybersecurity Information Sharing and Analysis Center (ISAC) for bi-directional information sharing about cyber threats and vulnerabilities between private health care industry and the federal government. 4. ONC will work with NIST and OCR to finalize and publish the NIST Critical Infrastructure Cybersecurity Framework and Health Insurance Portability and Accountability Act (HIPAA) Security Rule Crosswalk. 5. HHS will work with the industry to develop and propose a uniform approach to enforcing cybersecurity in healthcare in concert with enforcement of HIPAA Rules.	6. Stakeholder input requested	7. Stakeholder input requested
E2. Encryption	1. ONC will work with OCR and industry organizations to develop "at rest" standards for data encryption and provide technical assistance. OCR will consider whether additional guidance or rulemaking is necessary. 2. ONC will work with OCR and industry organizations to develop "in transit" standards for data encryption and provide technical assistance. OCR will consider whether additional guidance or rulemaking is necessary. 3. ONC will develop guidance for implementing encryption policies. 4. ONC will work with payers to explore the availability of private sector financial incentives to increase the rate of encrypting, starting with discussions with casualty insurance carriers who offer cybersecurity insurance.	5. Stakeholder input requested	6. Stakeholder input requested

Verifiable Identity and Authentication of All Participants

LHS Requirement

F. ***Verifiable identity and authentication of all participants:*** Legal requirements and cultural norms dictate that participants be known, so that access to data and services is appropriate. This is a requirement for all participants in a learning health system regardless of role (individual/patient, provider, technician, etc.)

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

- Protect the privacy and security of health information

Background and Current State

Legal requirements and cultural norms dictate that the identity of participants who are accessing electronic health information be known so that access to data and services is appropriate. A learning health system will require that all participants, regardless of role (e.g., patient, provider, researcher), be identified and authenticated so that there is a high level of trust that participants are who they say they are and participants cannot fraudulently pose as someone else. Without appropriate identification and authentication policies, processes and technologies, individuals will not trust that their health information and other data are secure and private.

The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information (PHI). PHI is defined as personal health information that is created, received, used, or maintained by a covered entity or business associate. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic PHI. These safeguards are designed to prevent unauthorized or inappropriate access, alteration, use, or disclosure. The Security Rule also includes a Person or Entity Authentication Standard,[37] which requires covered entities to implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed. However, the Security Rule does not specify authentication options, assurance levels, or verification requirements, as entities are to determine themselves what is appropriate in their particular environments. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

Identity proofing is the process of verifying that a person is who he says he is through representative identifiers, usually for the purpose of assigning a credential that carries a token (*e.g.*, password or certificate pin) to be used later by the individual to access an information system. Identity proofing of providers and patients is necessary for a number of purposes. From the provider's perspective, it could include accessing the EHR at their hospital or practice, sending an electronic prescription, accessing a

[37] 164.312(d)

health information organization's query portal, or sending secure messages (whether Direct messages or other types of secure messages). For a patient, it could be accessing their health information from a patient portal. The identity proofing process requires the participant to present supporting documentation for verification. In general, two forms of identification are required and at least one of those must be a government issued form of identification (*e.g.,* driver's license, passport, etc.). Additional forms of identification, such as a utility bill, financial record, or the patient's health plan card, are often accepted. The level of verification ranges widely from visually inspecting and photocopying what was presented to contacting the source of the information during the registration process.

Authentication is the process of establishing confidence in the identity presented to gain access to a system. Authentication sometimes utilizes tokens (also called factors for authentication) that a participant provides to demonstrate they are the person who should have access. Tokens can be something a participant knows (a password), something a participant has (ID badge or hardware token/fob), or something a participant is (typically a biometric like a fingerprint). Depending on the risks of authentication errors, one or more factors may be required for authentication.

Federal agencies are required to adhere to OMB M-04-04, E-Authentication Guidance for Federal Agencies. OMB M-04-04 defines four levels of assurance (LOA) as a means to weigh the risks associated with authentication errors and misuse of credentials. Level 1 is the lowest assurance level (little or no effect) and Level 4 is the highest (may cause great harm). The NIST document SP 800-63-2 provides technical guidance that includes the identity proofing process and all aspects of credential management based on the OMB M-040-04 weight scale. While federal agencies require specific LOAs for their own use cases and while other industries have standard LOA requirements for their sector's cybersecurity, the health care industry has not standardized its LOA requirements for identity proofing and authentication.

The lack of consistently applied methods and criteria for both identity proofing and authentication has significantly hampered the exchange of data across organizations. For example, Direct was intended to work much like email and lower the barrier for exchange for providers and hospitals by eliminating the need for complex legal agreements between individual organizations. However, many health information service providers (HISPs) have different identity proofing and authentication policies and requirements. Or, HISPs may not acknowledge the identity proofing and authentication undertaken upstream by another organization. This variation has led to the creation of multiple trust organizations and individual agreements between organizations. Ultimately, providers and hospitals are limited to exchanging data only with those individuals or organizations with whom they (or their HISP) have created an agreement. In a learning health system, in contrast, the providers and hospitals should exchange with any other provider or hospital appropriately identity proofed and authenticated and especially with providers or hospitals that a patient directs them to share with.

The ONC HIT Policy Committee (HITPC) has put significant effort into recommendations to ONC for addressing both provider and patient identity proofing and authentication issues over the last three years. Its recommendations recognize that multi-factor authentication is feasible and is consistent with the direction the industry is headed, just like other industries with more mature information

infrastructures. Additionally, HITPC's recommendations have strongly encouraged providers to use multi-factor authentication for provider remote access to PHI and for patient access to patient portals. The HITPC did not give any specific requirements for identity proofing beyond support of the existing HIPAA Security Rule guidance, but did encourage ONC to disseminate and distribute best practices for identity proofing and authentication.[38]

In 2010, the National Strategy for Trusted Identities in Cyberspace (NSTIC) was launched as a public-private collaborative to help, "individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation."[39] NSTIC has worked over the last few years to develop pilots to test various electronic means for ensuring identity and authenticating users and ultimately develop an identity ecosystem that can be utilized to mitigate cybersecurity issues and maintain the privacy of individuals. Based on the NSTIC's work, as well as wide agreement across various sectors (financial, health, defense, etc.), multi-factor authentication and solid identity proofing processes have been acknowledged as the new norm. A recent Executive Order also pushes for alignment with NSTIC.[40]

Moving Forward

The use of mobile phones, email and other factors for authentication has become commonplace in many sectors such as banking and e-commerce. With the emergence of Internet accessible medical devices, monitors and the yet-to-be-developed Internet of Things,[41] it is not too far-fetched to imagine a time in the near future in which a mobile device may be used to identity proof and authenticate a patient and their associated devices at the point of care. This in turn could serve to promote a person-centric environment that would minimize the need for intermediaries to facilitate trust.

To prepare, the nation can take some simple steps to pave the way today: establish common identity proofing practices at the point of care; require multi-factor authentication for all patient and provider access to health IT systems in a way that aligns with what is required in other industries; leverage existing mobile technologies and smart phones to provide efficient, effective paths for patient or provider identity authentication; and integrate the RESTful approaches to authentication in anticipation of that vision of tomorrow.

[38] http://www.healthit.gov/facas/health-it-policy-committee/health-it-policy-committee-recommendations-national-coordinator-health-it

[39] http://www.nist.gov/nstic/index.html

[40] Improving the Security of Consumer Financial Transactions. October 17, 2014. http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

[41] The Internet of Things (IoT) refers to the connection of a wide variety of uniquely identifiable devices across the existing Internet infrastructure (e.g., smart phones, wearable and implantable devices, etc.).

Table 6: Critical Actions for Verifiable Identity and Authentication of All Participants

Category	**2015-2017** Send, receive, find and use a common clinical data set to improve health and health care quality	**2018-2020** Expand interoperable health IT and users to improve health and lower cost	**2021-2024** Achieve a nationwide learning health system
F1. Policies and Best Practices	1. Policies established through the coordinated governance process will adopt the concept of multi-factor authentication for all roles that access health information, subject to contextual appropriateness and consistency with the HIPAA Security Rule.[42] 2. ONC will identify and undertake (where necessary) work to harmonize other standards with those adopted for multi-factor authentication. 3. Through coordinated governance, stakeholders (with input from OCR) will establish and adopt best practices for identity proofing that are consistent with standards already adopted for other, comparable industries and with the HIPAA Security Rule.	4. Stakeholder input requested	5. Stakeholder input requested
F2. Standards	1. Health IT developers will leverage existing mobile technologies and smart phones to provide efficient, effective paths for patient or provider identity authentication. 2. SDOs will work with health IT developers to conduct Pilots using RESTful approaches for authentication.	3. Stakeholder input requested	4. Stakeholder input requested

[42] In September 2012 and May 2013, the HITPC recommended to the ONC that multi-factor authentication be utilized for providers and patients respectively. In October 2014, an Executive Order required National Security Council staff, the Office of Science and Technology Policy and OMB to draft a plan for ensuring "that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate."

Consistent Representation of Permission to Collect, Share and Use Identifiable Health Information

LHS Requirement

G. ***Consistent representation of permission to collect, share and use identifiable health information:*** Though legal requirements differ across the states, nationwide interoperability requires a consistent way to represent an individual's permission to collect, share and use their individually identifiable health information, including with whom and for what purpose(s).

FEDERAL HEALTH IT STRATEGIC PLAN OBJECTIVES SUPPORTED

- Protect the privacy and security of health information

Background and Current State

The success of health IT and interoperability is dependent on individuals' trust that their health information will be kept private and secure and that their rights with respect to this information will be respected.[43] The parameters of individual choice regarding collection, sharing and use of an individual's health information are defined across three broad categories that impact interoperability: statutes and regulations, organizational policy and technology. Statutes and regulations include federal and state laws and regulations that set individual privacy protections for health information. Laws and regulations serve three purposes: First, they specify requirements of data holders to protect a person's individually identifiable health information. Second, they specify the conditions under which an individual's health information can be accessed, used and disclosed with or without the individual or his/her representative's explicit authorization. Third, they specify the purposes or conditions under which an individual's information can be accessed, used, or disclosed only with the individual or their representative's express authorization.

HIPAA and its implementing regulations set a national baseline of federal health information privacy and security protections. The HIPAA Rules create requirements that health plans, most health care providers and health care clearinghouses, as well as their business associates, must follow. The HIPAA Rules also provide rights for individuals to obtain access to their PHI and rules governing when protected health information may be used or disclosed without individual's express authorization. A number of other current federal and state health information privacy laws and regulations exist that have heightened privacy protections and require documented, individual choice to share certain types of health information. Some examples of federal regulations that contain these special protections are the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations (42 U.S.C. § 290dd-2) that

[43] http://www.hhs.gov/strategic-plan/patient-privacy.html

apply to behavioral health treatment information[44] and federal laws (38 USC § 7332) protecting certain types of health information coming from covered U.S. Department of Veterans Affairs facilities and programs.[45]

Many states have laws and regulations to protect the privacy of health information that have stricter privacy protections and requirements on use and disclosure than the HIPAA Rules. These laws and regulations vary from state-to-state, often narrowly targeting a particular population, health condition, data collection effort or specific types of health care organizations. As a result, states have created a "patchwork" of health information privacy laws and protections that address individual choice and are not uniform across state lines or care settings/encounters. This patchwork is also not easily understood by individuals.

Organizational policies are organization-level rules regarding individual choice for use and disclosure of health information (within the bounds of state and federal regulations). Organizational policies vary even within single states and create an additional layer of differing approaches and parameters for individual choice. Unlike laws, organizational policies may be and often are, developed within a specific organization and therefore are not typically subject to public debate or public consensus building. Moreover, organizational policies often include requirements not specifically mandated by law.

Technological advances are creating opportunities to share data and allow patient preferences to electronically persist through an interoperable learning health system. Technology provides a means for electronically identifying, capturing, tracking, managing and communicating an individual's choice preferences regarding the use and disclosure of health information from the originating source to other technical systems. Health IT enables not only the capture of a documented choice, but also the capture of what permissions apply, even when there is no documented choice. Health IT can enable users to comply with relevant use and disclosure laws, regulations and policies in an electronic health information environment. (See Appendix D for deeper background on these three categories.)

Fair Information Practice Principles[46]

Adoption and effective implementation of privacy protections is essential to establishing the public trust necessary for broad scale interoperability of health information. The Fair Information Practice Principles (FIPPs) are a common set of overarching principles that guide information practices while advancing

---

[44] http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=02b3d31742318b503b8d4ba0111d0e35&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

[45] http://www.gpo.gov/fdsys/pkg/USCODE-2011-title38/pdf/USCODE-2011-title38-partV-chap73-subchapIII-sec7332.pdf

[46] In 1973, the Department of Health, Education and Welfare (HEW) released its report, Records, Computers and the Rights of Citizens, which outlined a Code of Fair Information Practices that would create "safeguard requirements" for certain "automated personal data systems" maintained by the Federal Government. This Code of Fair Information Practices is now commonly referred to as fair information practice principles (FIPPs). See Department of Health, Education and Welfare, *Records Computers and the Rights of Citizens* (July 1973), available at http://www.justice.gov/opcl/docs/rec-com-rights.pdf.

technology. They are foundational to many laws, regulations and policies in the public and private sector, including the HIPAA Privacy Rule, the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information and many state laws and organization-level policies.[47] So too, this roadmap uses the FIPPS as a touchstone for building a privacy and security framework for interoperability. The Nationwide Privacy and Security Framework (based on the FIPPs) are specific objectives identified by ONC in earlier work. Proposals below reference these principles.

The FIPPs identify that individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information (choice) and that individuals need to understand their choice and how their data is used. In an interoperable learning health system, that means there must be both policies and technology that:

1. Provide individuals the opportunity to make meaningful decisions about their health information;
2. Capture information about choice in a manner that can be communicated and recognized across a broad ecosystem of technology;
3. Represent choice in a consistent manner so that it can be appropriately acted upon (ideally over time, in automated ways between technical systems);
4. Enable providers to deliver health care to individuals using appropriately exchanged electronic health information even when the individual has not stated a preference; and
5. Allow individuals, especially those who have not stated a choice, to understand how the information system works, especially for number four above.

[47] There are many versions of the FIPPs; the ONC FIPPs are in the Nationwide Privacy and Security Framework for Electronic Health Information Exchange ("Nationwide Privacy and Security Framework") released in 2008: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf. In 2012, ONC issued privacy and security guidance to the state health information exchange cooperative agreement program that is based on the Nationwide Privacy and Security Framework for Electronic Health Information Exchange. See ONC's State Health Information Exchange Program Instruction Notice (PIN), Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program, March 2012, http://www.healthit.gov/sites/default/files/hie-interoperability/onc-hie-pin-003-final.pdf.

Figure 7: Nationwide Privacy & Security Framework

Nationwide Privacy and Security Framework (based on the FIPPs)

1. **INDIVIDUAL ACCESS:** Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
2. **CORRECTION:** Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied.
3. **OPENNESS AND TRANSPARENCY:** There should be openness and transparency about policies, procedures and technologies that directly affect individuals and/or their individually identifiable health information.
4. **INDIVIDUAL CHOICE:** Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.
5. **COLLECTION, USE, AND DISCLOSURE LIMITATION:** Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
6. **DATA QUALITY AND INTEGRITY:** Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
7. **SAFEGUARDS:** Individually identifiable health information should be protected with reasonable administrative, technical and physical safeguards to ensure its confidentiality, integrity and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
8. **ACCOUNTABILITY:** These principles should be implemented and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

SOURCE: http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf

Basic Choice v. Granular Choice

"Basic choice" is the choice an individual makes about the use and disclosure of their health information generally, including electronic exchange of health information that is not subject to heightened use and disclosure restrictions under state or federal law. HIPAA rules permit the use and disclosure of PHI for, among other purposes, treatment, payment and health care operations of a HIPAA covered entity (TPO) without an individual's express permission (often called "consent"). Nevertheless, many health care organizations still choose to obtain an individual's written permission for use and disclosure of PHI for TPO.[48] This type of consent activity represents "basic choice."[49] Basic choice builds on existing standards

[48] For more information about health information privacy law pertaining to individual choice, see ONC's Meaningful Choice Resource Center, http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy.

HIPAA Privacy Rule standards of “minimum necessary,” [50] “role based access,” and use of de-identification when possible.[51] Basic choice" does not refer to circumstances where special legal requirements about identified clinical conditions apply; for the purposes of the Roadmap, those are treated under the concept of "granular choice."

“Granular choice” refers to the choice an individual makes to share specific types of information, including (1) information that fits into categories to which, by law, protections in addition to HIPAA apply; (2) the choice afforded an individual based on their age; and (3) the choice to share health information by specific provider or payer types. Many stakeholders believe, and several laws reinforce, that individuals should have the ability to control use and disclosure of specific health information, or to specify which providers may have electronic access to it. For example, the results of a nationwide ONC survey on consumer attitudes found that when their health information is exchanged electronically, nearly all respondents (about 92%) want to be able to share only portions of their medical records with others.[52]

This is consistent with the individual choice principle in FIPPs. One example is federal law (e.g., 42 U.S.C. § 290dd-2), which requires health care providers to obtain patients’ written consent before they disclose information about a patient’s substance abuse treatment to other people and organizations, even for treatment. Granular choice refers, therefore, not only to granular choice among clinical conditions that are protected by laws in addition to HIPAA, but eventually, granular choice, should a patient wish to express it, regarding other data distinctions to be determined, but which are consistent with a learning health system, such as research purposes in which an individual has chosen to participate.

Moving Forward

The U.S. legal, regulatory and policy landscape for sharing health information is complex. While the laws are designed to protect health information and individual rights, they also must enable appropriate

---

[49] The National Governors Association has published a landscape analysis of these laws that concern whether the patient wants to allow any of their information to be exchanged, the oft-called “opt in/opt out.” http://www.nga.org/files/live/sites/NGA/files/pdf/1103HIECONSENTLAWSREPORT.PDF; see also RTI International prepared for ONC, *Report on State Law Requirements for Patient Permission to Disclose Health Information*, August 2009, http://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

[50] 45 CFR 164.502(b), 164.514(d)

[51] U.S. Department of Health and Human Services, Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

[52] U.S. Department of Health and Human Services, Office of the National Coordinator, Health Information Security and Privacy Collaboration: Survey of Attitudes toward Electronic health Information Exchange and Associated Privacy and Security Aspects, (Wash. D.C.: January 2011), http://www.healthit.gov/policy-researchers-implementers/health-information-security-privacy-collaboration-hispc. The survey used the term "privacy settings," defined as allowing permission for some portions of an individual's health records to be shareable and other portions to not authorized to be accessed, used, or disclosed.

information sharing to support health and health care. Despite efforts to address potential technology standards and solutions for individual choice across this complex ecosystem, it has become clear that the complexity of the rules environment will continue to hinder the development and adoption of a consistent nationwide technical framework (e.g., data elements, definitions, vocabularies) for electronically managing individuals' basic and granular choices until the complexity is resolved.[53] Reducing variation in the current legal, regulatory and organizational policy environment related to privacy that is additive to HIPAA will help facilitate the development of technical standards and technology that can adjudicate and honor basic and granular choices nationwide in all care settings, while ensuring that special protections that apply as a result of deliberative legislative processes remain conceptually in place. Through the course of harmonization, however, individual privacy rights as specified in state and federal laws must not be substantively eroded. For example, where a law protects reproductive health or behavioral health information (to name but two sensitive conditions), harmonization would not mean the substantive weakening of such protections.

Consistent with the governance principle of individual choice outlined elsewhere in this Roadmap, HHS is committed to encouraging the development and use of organizational policy and technology to advance individuals' rights to make choices about the use and disclosure of their electronic health information. HHS also supports the development of standards and technology to facilitate individuals' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, domestic or sexual violence, or HIV/AIDS) in an electronic environment.[54]

Methods to consistently capture, communicate and automate processing of individual choice will be essential as additional systems and stakeholders are interoperable. These same automated processes are essential to support clinical research, population health and public health. Both an individual's "basic choice" and "granular choice" will also need to persist as data is shared from the point of origin to each subsequent system.

To ensure consistent technical representation of an individual's choice regarding use and disclosure of their health information across the learning health system, the nation will need to make aggressive progress to understand, align and harmonize laws and organizational policy so that individuals can more fully understand how data about them is being used (consistent with FIPPs.) In particular, the following three areas of policy will require attention before addressing technology standards to capture, communicate and process individual choice across the learning health system:

1. **Exchange permitted for certain purposes without an individual's written permission.** Working to help all stakeholders understand the protections of existing laws will establish a clear foundation for the public's understanding and expectations for how most PHI (that does not

[53] http://www.healthit.gov/facas/calendar/2014/12/17/standards-transport-security-standards-workgroup

[54] Excerpt from HHS Secretary Strategic Initiative focused on Privacy. March 2014: http://www.hhs.gov/strategic-plan/patient-privacy.html

have applicable special legal protections) can be used and disclosed (including through electronic exchange), if an individual takes no action to document a basic choice, no matter where an individual or their health information resides.

2. **Individuals understand their basic choice:** Individuals understand how their information is being moved (exchanged) for TPO (as primary uses), what their choices are for "basic choice" (choice regarding electronic exchange) and how their information will be protected, used, or disclosed even if the individual makes no active choice.

Standardize the meaning of sensitive health information laws. Individuals can understand their granular choice related to these categories (e.g., protected by laws in addition to HIPAA, or by provider). These categories and rules should be consistently applied to health information across the United States, no matter where an individual or their health information is.

Table 7: Critical Actions for Consistent Representation of Permission to Disclose Identifiable Health Information

Category	**2015-2017** Send, receive, find and use a common clinical data set to improve health and health care quality	**2018-2020** Expand interoperable health IT and users to improve health and lower cost	**2021-2024** Achieve a nationwide learning health system
G1. Improve Health IT stakeholders' understanding of existing HIPAA rules and how they support Interoperable exchange through permitted access, use and disclosure for TPO	1. Through education and outreach, federal government/Office for Civil Rights (OCR) will consider where additional guidance may be needed to help stakeholders understand how the HIPAA Privacy Rule permits health information to be exchanged (use and disclosure) for TPO without consent. 2. Federal and state governments, in coordination with organizational health information privacy policymakers, conduct outreach and disseminate educational materials and OCR guidance to LHS participants about Permitted Uses and Disclosure of health information and Individual Choice. 3. ONC will brief key stakeholders, possibly including NCSL, NGA, privacy advocates and Congress on findings regarding the complexity of the rules environment, especially the diversity among more restrictive state laws that seek to regulate the same concept, impedes computational privacy. 4. ONC, in collaboration with states, national and local associations, and other federal agencies will convene a Policy Academy on Interoperability with a particular focus on privacy as an enabler of interoperability.	5. Stakeholder input requested	6. Stakeholder input requested

Category	2015-2017 Send, receive, find and use a common clinical data set to improve health and health care quality	2018-2020 Expand interoperable health IT and users to improve health and lower cost	2021-2024 Achieve a nationwide learning health system
G2. Align stakeholder adopted policies with existing HIPAA regulations for health info that is regulated only by HIPAA	For information that is regulated by HIPAA only, ONC will 1. adopt at a policy level a standard definition of what is "Basic Choice" 2. adopt technical standards regarding how to ensure individuals are offered Basic Choice in a manner that can be captured electronically and in a manner in which the individual's choice persists over time and in downstream environments, unless the individual makes a different choice.	3. A majority of state governments and stewards of health information (health care organizations, HIEs, etc.) revise regulations and policies to align with the federal definitions of permitted uses for data regulated solely by HIPAA and also aligning with the ONC standard on what constitutes Basic Choice and how it should be implemented, with the result being an established consensus background rules for the nation.	4. All of state governments and stewards of health information (health care organizations, HIEs, etc.) revise regulations and policies to align with the consensus on non-sensitive information that is permissible to exchange—or access, use and disclose—for TPO without an individual's written consent establishing consensus background rules for the nation.
G3. Align regulations and policies for electronic health info that is protected by laws in addition to HIPAA		1. State governments standardize existing laws pertaining to "sensitive" health information, particularly those regarding clinically sensitive and age-based rules, so that those laws mean the same things in all U.S. jurisdictions, without undermining privacy protections individuals have today. 2. Federal government, a majority of state governments and stewards of health information (health care organizations, HIEs, etc.) begin revising regulations, policies and programs for granular choice to align with the consensus categories of sensitive health information and rules for granular choice that establish consensus background rules for the nation.	3. Federal government, all state governments and stewards of health information (health care organizations, HIEs, etc.) revise regulations, policies and programs for granular choice to align with the consensus categories of sensitive health information and rules for granular choice that establish consensus background rules for the nation.

Category	**2015-2017** Send, receive, find and use a common clinical data set to improve health and health care quality	**2018-2020** Expand interoperable health IT and users to improve health and lower cost	**2021-2024** Achieve a nationwide learning health system
G4. Technical standards for basic choice	1. ONC, standards development organizations, health IT developers and appropriate stakeholders harmonize technical standards and implementation guidance for consistently capturing, communicating and processing basic choice across the ecosystem. 2. Technology developers begin implementing harmonized standards that document and communicate an individual's basic choice.	3. Technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual choice. Adoption has begun, with 5% of exchangers using the standards regularly.	4. Technology developers implement technical standards and implementation guidance for consistently capturing, communicating and processing individual basic choice. Adoption continues, with a majority of exchangers using the standards regularly. 5. Basic choice standards are used widely to electronically capture individuals' desire to have their health information included in research.
G5. Associate individual choice with data provenance	1. ONC, standards development organizations, health IT developers, health care providers and appropriate stakeholders harmonize technical standards and develop implementation guidance for associating individual choice with data provenance to support choice 2. Technology developers begin to implement technical standards for associating individual choice with data provenance to support choice.	3. Technology developers implement harmonized technical standards for associating individuals' choice with data provenance; adoption has begun, with 5% of exchangers using the harmonized standards regularly.	4. Technology developers implement harmonized technical standards for associating individuals' choice with data provenance; adoption has begun, with a majority of exchangers using the harmonized standards regularly.

Appendix C: Background Information on Cybersecurity and Encryption

Cybersecurity

There are increasing cyber-attacks on electronic health information, particularly large stores of information. In 1998, Presidential Decision Directive (PDD) 63, acknowledged the need to protect the nation's critical infrastructure from both physical and cyber-attacks.[96] A major outcome of the PDD was the development of Information Sharing and Analysis Centers (ISACs) for each critical infrastructure sector. ISACs are, "privately led sector-specific organizations advancing physical and cyber security critical infrastructure protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners."[97]

One of the goals of an ISAC is to promote and enhance the bi-directional sharing about cyber threats and vulnerabilities within its sector-specific organizations and the federal government. This information sharing advances resilience, which is the ability to prepare for and respond to threats and vulnerabilities within a specific industry. ISACs are currently established for critical infrastructure sectors such as financial services, electricity and water. The National Health ISAC (NH-ISAC) is a non-profit industry-led effort to address the cyber security threats to healthcare and public health. In 2003, the Department of Homeland Security's *Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*, designated HHS as the Sector-Specific Agency responsible for ensuring the integrity of the health system.[98] A subsequent Presidential Policy Directive identified healthcare and public health (HPH) as a critical infrastructure sector.[99] Despite being identified as critical infrastructure for the nation, healthcare is one of the industry sectors least prepared for a cyber-attack, as it is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures, much less against more advanced persistent threats.[100]

There are various factors within healthcare that contribute to the aforementioned cybersecurity challenge. The health IT ecosystem is composed of multiple systems that are interconnected, including EHRs, laboratory systems, patient portals, medical devices and many other systems. Consequently, the ecosystem is incredibly complex, with these systems being managed across an exponential number of

[96] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22, 1998. http://www.fas.org/irp/offdocs/paper598.htm

[97] NIST Cybersecurity Framework

[98] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection. December 17, 2003. http://www.dhs.gov/homeland-security-presidential-directive-7

[99] Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[100] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

organizations. As all of these health IT systems become connected to each other, the cyber threats increase at a significant rate, as an intrusion in one system could allow intrusions in multiple other systems. Additionally, there is high variability in the capabilities and resources healthcare organizations have at their disposal to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cybersecurity; however, small and mid-sized organizations may not have these resources and may not be able to afford them. Finally, there is a significant behavioral and cultural change necessary in the industry regarding the relevance of cybersecurity risks. Many in the industry do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks.

There are increasing cyber-attacks on electronic health information, particularly large stores of information. Despite being identified as critical infrastructure for the nation, the healthcare system could do more to prepare for a cyber-attack.[101] There are various factors within healthcare that contribute to this aforementioned cybersecurity challenge. The health IT ecosystem is composed of multiple systems that are interconnected, including a wide variety of inputs that need security controls such as EKG machines, EHRs, robots and many other systems. Consequently, the ecosystem is incredibly complex, with these systems being managed across an exponential number of organizations. As all of these health IT systems become connected to each other, security risk can rise, as an intrusion in one system could allow intrusions in multiple other systems.

Additionally, there is high variability in the capabilities and resources that healthcare organizations have deployed to prevent cyber-attacks. Large organizations have the resources and expertise to have a dedicated information security team to address cybersecurity; however, small and mid-sized organizations may not have these resources and some may not be able to afford them. Finally, significant behavioral and cultural changes are necessary in the industry regarding the relevance of cybersecurity risks. Many in healthcare do not realize the significant risk to their systems and do not understand the importance and urgency of implementing security best practices to prevent cyber-attacks.

Encryption

Encryption of data both at rest and in transit is another component of a ubiquitous, secure network infrastructure. Encryption is a method of scrambling or encoding data so that it cannot be read without the appropriate key to unscramble the content. Two common ways encryption is used or applied are to send messages (particularly over networks that are not secure otherwise, like the Internet) and store data. These are sometimes referred to as information in transit and information at rest, respectively. In both cases, the core mechanism is the same. A program takes a piece of information (a string of data bytes) and changes it into another piece of information (a different string of bytes, and not necessarily

[101] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

the same number of bytes). The original piece of information is commonly referred to as being in the clear and the piece of information into which it is changed is referred to as encrypted. For encryption to work, it must be possible for another program (or possibly another algorithm in the same program) to reverse the process and change the encrypted information back into the information in the clear. This is called decrypting. Another constraint is that the algorithm to decrypt should not be obvious; otherwise, unwanted recipients would be able to recover the original information.

Encryption of data at rest is in some aspects simpler than encryption of data in transit. Data at rest is encrypted and decrypted through capabilities of most major database management systems, most laptop operating systems and at least some mobile operating systems. Encryption of data in transit, however, may require appropriate software compatibility across a learning health system's technology as well as effective management of a public/private key environment.

Encryption technology is not being fully utilized in health care. OCR, in promulgating the breach notification regulations, created a safe harbor for electronic health data that was encrypted such that if that data was accessed, used, or disclosed while encrypted, it did not result in a reportable, remediable breach of ePHI. Despite this safe harbor, health IT systems have been slow to adopt encryption technology, both of data at rest and in transit and the result is that 35% of 2013 breaches reported to HHS were the result of a theft or loss of an unencrypted device containing protected health information.[102]

[102] Breach Report 2013: Protected Health Information (PHI). Redspin. February 2014. https://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf