Health Information Technology Advisory Committee

The Office of the National Coordinator for Health Information Technology

HITAC Annual Report for Fiscal Year 2018

Approved by the HITAC on March 19, 2019

TABLE OF CONTENTS

Executive Summary

The 21st Century Cures Act (Cures Act) requires the Health Information Technology Advisory Committee (HITAC) to develop an annual report to be submitted to the Secretary of Health and Human Services (the Secretary) and to Congress each fiscal year. This report complies with that directive by reviewing fiscal year 2018 (FY18) HITAC activities, describing the landscape of health information technology (IT) infrastructure across priority target areas (interoperability, privacy and security, patient access to information), analyzing infrastructure gaps, and offering recommendations for future HITAC activities.

HITAC Progress in FY18

The Cures Act directs the HITAC to make recommendations to the National Coordinator for Health Information Technology regarding policies, standards, implementation specifications, and certification criteria related to the implementation of a health information technology infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information.

The HITAC began its work in January 2018 and quickly submitted a policy framework to the National Coordinator for Health IT. The full committee, through the work of several subcommittees, developed recommendations to support ONC's work required by the Cures Act. The subcommittees included the:

- Trusted Exchange Framework Task Force
- U.S. Core Data for Interoperability Task Force
- Interoperability Standards Priorities Task Force
- Annual Report Workgroup

Health IT Infrastructure Landscape

The Cures Act specifies three priority target areas within which the HITAC should focus its activities. These priority target areas are an organizing principle for classifying the HITAC's work and organizing this report.

Priority Target Area: Interoperability

While most health care providers now use electronic health records (EHRs), interoperability remains fragmented and uneven. The Cures Act requires HHS to develop regulations in a variety of areas that will significantly impact the current interoperability landscape, such as information blocking and conditions and maintenance of certification requirements. HHS published a proposed rule on March 4, 2019, that addresses these areas. Work is also underway by ONC to develop a trusted exchange framework and common agreement. The HITAC is working to identify priority uses of health information technology and the associated standards and implementation specifications that support such uses.

Priority Target Area: Privacy and Security

Privacy and security of health data are important considerations in advancing and maintaining trust in interoperability. Additionally, poor privacy and security practices heighten the vulnerability of patient information stored in health information systems and on devices, and may lead to events of concern to health care organizations and providers.

Priority Target Area: Patient Access to Information

Continued information and education, as well as improved accessibility to and use of application programming interfaces (APIs), are needed to increase patient awareness of the use of data and health IT resources. Access to health IT can have a positive impact on health, health care, and health equity by supporting shared decision-making between patients and providers, providing personalized self-management tools, and delivering accurate, accessible, and actionable health information.

The HITAC did not identify a need for additional target areas as defined in the Cures Act in FY18. The HITAC will revisit this consideration in the FY19 annual report.

Health IT Infrastructure Gaps, Opportunities, and Recommendations

The Cures Act requires an analysis identifying existing gaps in policies and resources for achieving the ONC FY18 objectives and benchmarks and furthering interoperability throughout the health information technology infrastructure, as well as recommendations for addressing the gaps identified. The HITAC has focused on the following key gaps and opportunities for the health IT industry and has recommended related HITAC activities. In FY19, ONC charged the HITAC to review the proposed rule in support of the HITAC priority target areas, in particular Interoperability and Patient Access to Information.

The following chart summarizes the HITAC's assessment:

Key Gaps	Key Opportunities	Recommended HITAC Activities
Priority Target Area: Interoperability		
Need to increase level of interoperability	Address "reality gap" between the perception of what has been certified for a system and what is truly interoperable in the field	Evaluate whether systems are truly interoperable at both content and transport levels after implementation, especially among smaller practices and by patients to establish measures in the future
Priority Target Area: Privacy and Security		
Implications of emergence of the Internet of Things (IoT)	Consider appropriate polices for the IoT	Identify areas of IoT use that would benefit from guidance and examples of success in the health care industry
Lack of user awareness and education about privacy and security protections	Offer support for and education of technology users regarding privacy and security protections, including for health and other information shared on social media	Identify educational approaches, technological mitigators, and potential regulatory solutions that offer improved privacy and security protections
Variability of information sharing policies across states	Increased uniformity of information sharing policies across states	Review and make recommendations about federal role in setting guidelines for the exchange of data across states
Variability in adoption of cybersecurity framework(s)	Offer support for widespread adoption of cybersecurity framework(s)	Review and make recommendations about the impact of nationwide adoption of cybersecurity framework(s) and delineate cybersecurity accountability for data by role within the health IT infrastructure
Lack of user control to share and disclose information	Consider options for granular levels of consent to share and disclose information	Undertake a review of emerging consent approaches and the technologies that underpin them, and make recommendations for the improvement of current consent approaches
Priority Target Area: Patient Access to Information		
Unmet infrastructure needs for underserved populations	Support infrastructure needs for underserved populations, including exchange costs, the prevalence of electronic equipment, Internet access, pharmacy services, and use of telehealth services	Evaluate impact of monetization of data exchange to establish measures in the future
Accessibility and usability of patient portals and other patient-facing technology continue to need improvement	Consider improvements to accessibility and usability of patient portals and other patient-facing technology	Evaluate patient portal operational effectiveness, patient engagement, and/or patient understanding and use of data to establish measures in the future
Patient awareness and education about health IT resources	Encourage patient and caregiver education about health IT resources	Identify use cases demonstrating the value of patient's data to the patient

Foreword

We are pleased to present the annual report of the Health Information Technology Advisory Committee (HITAC) for FY18.

This report describes the work undertaken by the HITAC during its first year. The HITAC was formed by the 21st Century Cures Act and is governed by the Federal Advisory Committee Act. The HITAC is a federal advisory committee composed of members representing hospitals and health systems, health care providers, health information exchanges, insurers, health IT developers, universities, and federal agencies, as well as patients and consumers. Working together, HITAC members make recommendations about policies, standards, implementation specifications, and certification criteria to the National Coordinator for Health Information Technology within the U.S. Department of Health and Human Services (HHS).

In this report, the HITAC evaluates the health IT infrastructure landscape of the United States for gaps, opportunities, and recommendations. The committee focused its evaluation in three priority target areas: interoperability, privacy and security, and patient access to Information. In addition, this report highlights the work done by the HITAC's Trusted Exchange Framework Task Force, the U.S. Core Data for Interoperability Task Force, and the Interoperability Standards Priorities Task Force. These subcommittees were formed to address particular initiatives identified by Congress as health IT priorities for the Office of the National Coordinator for Health Information Technology (ONC).

We wish to acknowledge and appreciate all the hard work done by committee members and additional members of the public serving on the HITAC subcommittees as well as by committee members participating in the deliberations of the committee as a whole. In addition, we thank the staff of ONC and the other federal agencies who support the HITAC.

It is our privilege to serve as co-chairs for the HITAC. The commitment and diverse expertise of the HITAC members have brought both energy and insight to this evaluation of the U.S. health IT infrastructure. We look forward to another busy year as we continue to seek effective and cost-efficient care delivery using better information and technology to improve the health and well-being of everyone across the United States.

Carolyn Petersen and Robert Wah
Co-Chairs, Health Information Technology Advisory Committee

Overview

Legislative Requirements

In December 2016, Congress passed the 21st Century Cures Act (Cures Act), P.L. 114-255, with a bipartisan majority. The Cures Act created the Health Information Technology Advisory Committee (HITAC) which is governed by the provisions of the Federal Advisory Committee Act (FACA), P.L. 92-463, as amended, 5 U.S.C. App. 2. The HITAC makes recommendations to the National Coordinator about policies, standards, implementation specifications, and certification criteria relating to the implementation of a health information technology infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information. The HITAC replaced the Health Information Technology Policy Committee and the Health Information Technology Standards Committee.

The Cures Act requires the HITAC to develop an annual report to be submitted to the Secretary and to Congress each fiscal year. The annual report must provide:

- Analysis of HITAC progress related to priority target areas;
- Assessment of health IT infrastructure and advancements in the priority target areas;
- Analysis of existing gaps in policies and resources for the priority target areas; and
- Ideas for potential HITAC activities to address the identified gaps.

HITAC Priority Target Areas

Section 4003(e) of the Cures Act established the following priority target areas for the HITAC:

- **Interoperability -** "Achieving a health information technology infrastructure, nationally and locally, that allows for the electronic access, exchange, and use of health information, including through technology that provides accurate patient information for the correct patient, including exchanging such information, and avoids the duplication of patient records."
- **Privacy and Security -** "The promotion and protection of privacy and security of health information in health information technology, including technologies that allow for an accounting of disclosures and protections against disclosures of individually identifiable health information made by a covered entity for purposes of treatment, payment, and health care operations (as such terms are defined for purposes of the regulation promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996), including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care."
- **Patient Access to Information -** "The facilitation of secure access by an individual to such individual's protected health information and access to such information by a family member, caregiver, or guardian acting on behalf of a patient, including due to age-related and other disability, cognitive impairment, or dementia."
- **Any other target area** related to the above target areas that the HITAC identifies as an appropriate target area to be considered.

The HITAC did not identify a need for additional target areas as defined in the Cures Act in FY18. The HITAC will revisit this consideration in the FY19 annual report.

FY18 ONC Objectives and Benchmarks for the HITAC

As required by the Cures Act, ONC established a set of objectives and benchmarks to advance and measure the advancement of the priority target areas during the fiscal year 2018 (FY18) that began on October 1, 2017, and ended on September 30, 2018, outlined in the table below.

FY18 ONC Objectives and Benchmarks for the HITAC		
ONC Objective	**ONC Benchmark***	**Progress in Meeting in FY18**
Publish proposed regulation for implementation of the health IT provisions of the 21st Century Cures Act to drive access to clinical data by: • Advancing proposals related to APIs; and • Identifying behaviors not considered information blocking, which will assist the HHS Office of Inspector General (OIG) in their enforcement of the Cures Act provisions that prohibit information blocking.	Proposed Regulation Covering APIs, Info Blocking, and Other Health IT Topics Published	• Proposed regulation was submitted by ONC to OMB for review on September 17, 2018. The proposed regulation was published in FY19.
Publish the draft Trusted Exchange Framework (TEF) to improve data sharing across disparate health information networks.	Draft Trusted Exchange Framework Published	• Draft Trusted Exchange Framework released on January 5, 2018, for public comment. • HITAC charged with making recommendations and submitted recommendations to the National Coordinator on draft Trusted Exchange Framework and Common Agreement in FY18.
Consider standards and implementation specifications to support priority uses of health IT based on HITAC recommendations, encouraging all stakeholders to implement and use as applicable the specific interoperability needs they seek to address.	Standards and Specifications to Support Priority Uses Considered	• Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process released on January 5, 2018. • HITAC charged with making recommendations to the National Coordinator on USCDI structures and process in FY18. • HITAC charged with making recommendations on priority uses of health IT and associated standards and implementation specifications in FY18.

* For FY18, ONC has defined the HITAC benchmarks as standalone measures rather than comparisons to an established industry standard of excellence. Infrastructure advancements compared to the current state in FY18 will be assessed in future annual reports.

HITAC Progress in FY18

HITAC Meetings

The Cures Act directs the HITAC to make recommendations to the National Coordinator for Health Information Technology regarding policies, standards, implementation specifications, and certification criteria relating to the implementation of a health information technology infrastructure, nationally and locally, that advances the electronic access, exchange, and use of health information.

Accomplishments in FY18

The first meeting of the HITAC took place on January 18, 2018. The HITAC met for a total of seven meetings during FY18, three of which were held in person in Washington, DC. The subcommittees met for a total of twenty-seven meetings.

Policy Framework

The Cures Act directs the HITAC to recommend a policy framework advancing the priority target areas identified under section 3001(c)(3).

Accomplishments in FY18

The HITAC transmitted a recommended policy framework to the National Coordinator for Health IT in February 2018. The policy framework covered a variety of activities ONC should undertake, including:

- Advance the target areas identified in Section 4003 provisions related to:
    - Achieving a health information technology infrastructure that allows for the electronic access, exchange, and use of health information;
    - The promotion and protection of privacy and security of health information in health information technology; and
    - The facilitation of secure access by an individual to such individual's protected health information.
- Align with the Federal Health IT Strategic Plan: 2015-2020 goals, including the enhancement of the nation's health information technology infrastructure.
- Implement provisions in Title IV of the 21st Century Cures Act within its authority, including provisions related to patient access, trusted exchange, interoperability, conditions and maintenance of certification, and information blocking.
- Advance policies, standards, implementation specifications, and certification criteria related to the interoperability of health IT.

Trusted Exchange Framework Task Force

ONC published the draft Trusted Exchange Framework on January 5, 2018. At the HITAC meeting on January 18, 2018, ONC charged the HITAC with developing recommendations to inform the development of the final Trusted Exchange Framework. The HITAC then formed the Trusted Exchange Framework Task Force and charged it with the following:

- *Overarching charge*: The Trusted Exchange Framework Task Force will develop and advance recommendations on Parts A and B of the Draft Trusted Exchange Framework to inform the development of the final Trusted Exchange Framework and Common Agreement.
- *Specific charge*: Make specific recommendations on the language included in the Minimum Required Terms and Conditions in Part B, including—
    - Recognized Coordinating Entity: Are there particular eligibility requirements for the Recognized Coordinating Entity (RCE) that ONC should consider when developing the Cooperative Agreement?
    - Definition and Requirements of Qualified HINs: Recommendations for further clarifying the eligibility requirements for Qualified HINs outlined in Part B.
    - Permitted Uses and Disclosures: Feedback on enhancing or clarifying the six (6) permitted purposes and three (3) use cases identified in Part B.
    - Privacy/Security: Are there standards or technical requirements that ONC should specify for identity proofing and authentication, particularly of individuals?

Accomplishments in FY18

The Trusted Exchange Framework Task Force held nine public meetings to develop recommendations for the HITAC. The HITAC approved and transmitted 26 recommendations to the National Coordinator for Health IT in March 2018.

U.S. Core Data for Interoperability Task Force

ONC published the Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process (draft USCDI) on January 5, 2018. The Cures Act sets an expectation that all of a patient's health information that is stored electronically will be able to be exchanged. The draft USCDI and its proposed expansion process support this goal by specifying a common set of data classes that are required for interoperable exchange and identifying a predictable, transparent, and collaborative process by which the USCDI will be updated and expanded over time.

At the HITAC meeting on January 18, 2018, ONC charged the HITAC with providing feedback on the draft USCDI. The HITAC then formed the USCDI Task Force and charged it with the following:

- *Overarching charge:* Review and provide feedback on the U.S. Core Data for Interoperability (USCDI) structure and process.
- *Specific charge:* Provide recommendations on the following:
    - Mechanisms/approaches to receive stakeholder feedback regarding data class priorities;
    - The proposed categories to which data classes would be promoted and objective characteristics for promotion;
    - How the USCDI would be expanded and by how much; and
    - Any factors associated with the frequency with which it would be published.

Accomplishments in FY18

The USCDI Task Force held nine public meetings to develop recommendations for the HITAC. The HITAC approved and transmitted nine recommendations to the National Coordinator for Health IT in April 2018.

Interoperability Standards Priorities Task Force

The Cures Act requires the HITAC to set priorities for standards adoption. At the HITAC meeting on June 20, 2018, ONC charged the HITAC with providing recommendations to the National Coordinator on standards priorities. The HITAC then formed the Interoperability Standards Priorities (ISP) Task Force and charged the group with the following:

- *Overarching charge*: To make recommendations on priority uses of health information technology and the associated standards and implementation specifications that support such uses.
- *Specific charge*: The ISP Task Force will:
  - Make recommendations on the following:
    - Priority uses of health IT (consistent with the Cures Act's identified priorities);
    - The standards and implementation specifications that best support or may need to be developed for each identified priority; and
    - Subsequent steps for industry and government action.
  - Publish a report summarizing its findings.

Accomplishments in FY18

The ISP Task Force held six public meetings in FY18 and produced an initial list of priority uses for further discussion.[1] In FY18, the ISP Task Force started to work on recommendations for orders and results, which it had determined to be the highest priority area. The ISP Task Force will continue working on recommendations for additional prioritized areas in FY19. These additional areas include medication/pharmacy data, evidence-based care for common chronic conditions, closed loop referrals, social determinants of health (SDOH), and cost transparency.

Annual Report Workgroup

The Cures Act requires the HITAC to develop an annual report to be submitted to the Secretary and to Congress each fiscal year. At the HITAC meeting on June 20, 2018, the HITAC formed the Annual Report Workgroup and charged it with the following:

- *Overarching charge*: The workgroup will inform, contribute to, and review draft and final versions of the HITAC Annual Report to be submitted to the Secretary and to Congress each fiscal year. As part of that report, the workgroup will help track ongoing HITAC progress.
- *Specific charge:* To provide specific feedback on the content of the report as required by the 21st Century Cures Act including:
  - Analysis of HITAC progress related to the priority target areas.
  - Assessment of health IT infrastructure and advancements in the priority target areas.
  - Analysis of existing gaps in policies and resources for the priority target areas.
  - Recommendations for addressing the gaps identified.
  - Identification of additional initiatives potential HITAC activities.

Accomplishments in FY18

The Annual Report Workgroup held three public meetings to discuss the structure and content of the FY18 HITAC Annual Report. The Annual Report Workgroup co-chairs updated the HITAC on September 5, 2018, on its progress and gathered feedback from the full committee.

Health IT Infrastructure Landscape Analysis

Priority Target Area: Interoperability

Background

Over the past decade, hospitals and physician offices have made tremendous gains in shifting their record-keeping from paper to computerized systems. The adoption rate of a basic EHR by non-federal acute care hospitals has increased from 9% in 2008 to 84% in 2015.[2] The adoption rate of a basic EHR by office-based physicians has increased from 17% in 2004 to 64% in 2015.[3] While most health care providers now use EHRs, interoperability remains fragmented and uneven. For example, as of 2017, only 41% of hospitals can find, send, receive, and integrate patient summary of care records from sources outside their health system.[4]

Current State

Much progress has been achieved in increasing the interoperability of health information in recent years, while challenges remain. The following are descriptions of the current state of key topics for which gaps and opportunities have been identified.

Health Information Exchange

Today, there are more than 100 health information exchanges[5] and multiple nationwide organizations that support the electronic exchange of health information. While these organizations have made significant progress and expanded interoperability, connectivity across them has been limited for several reasons, including variations in data use agreements that govern exchange, technical approaches, and the type of exchange supported. The lack of connectivity limits appropriate access to health information by individuals, providers, and payers, unless they join multiple networks. As a result, individuals are burdened by having to access their health information via multiple portals, and health care organizations must create many costly, point-to-point interfaces to send and receive needed data.

The Cures Act requires HHS to develop regulations in a variety of areas that will significantly improve the current interoperability landscape. Rulemaking and initiatives are underway at ONC to advance the interoperability of data related to:

- Secure, Standardized Application Programming Interfaces (APIs);
- Information Blocking;
- Updating the ONC Health IT Certification Program; and
- Price Transparency.

Rulemaking will identify behaviors not considered information blocking which will assist the HHS Office of Inspector General (OIG) in their enforcement of the Cures Act's provisions that prohibit information blocking. The proposed regulation was published on March 4, 2019.

Draft Trusted Exchange Framework

The Cures Act requires ONC to develop or support a trusted exchange framework, including a common agreement among health information networks (HINs) nationwide with the goal of enabling data exchange across disparate HINs. After gathering stakeholder input through public listening sessions and a public comment period, ONC released a draft Trusted Exchange Framework (TEF) in January 2018 for public comment. ONC outlined a number of goals for the TEF including 1) providing a single "on-ramp" to

interoperability for all, 2) supporting nationwide scalability and sustainability, and 3) fostering market competition on data services. The TEF outlines ONC's proposed minimum set of principles, terms, and conditions to support the development of a Common Agreement that will enable a shared set of rules of the road and a technical approach to support data exchange among disparate networks. ONC will select a Recognized Coordinating Entity (RCE) that will help finalize, implement, and update the Common Agreement with stakeholders' input for ONC approval. The Common Agreement will provide the rules of the road for how Qualified HINs (QHINs) connect to one another to enable nationwide data exchange among disparate HINs that represent a variety of networks and participants.

Standards and Implementation Specifications to Support Priority Uses of Health IT

Standards and implementation specifications are critical to achieving interoperability. Accepted standards and accompanying implementation guides support a diverse range of stakeholders. Two initiatives – USCDI and HL7® FHIR® – currently lead this effort.

U.S. Core Data for Interoperability (USCDI)

The Cures Act sets an expectation that all of a patient's health information that is stored electronically should be able to be exchanged. The USCDI and its proposed expansion process aim to achieve this goal by establishing a common initial set of data classes that are required for interoperable exchange and identifying a predictable, transparent, and collaborative process for adding to the initial set over time. ONC released a draft of the USCDI and the expansion process in January 2018. The initial draft of the USCDI built on required data classes included in the Common Clinical Data Set (CCDS) in the ONC 2015 Edition Health IT Certification Criteria (2015 Edition), with the addition of provenance and clinical notes.

USCDI Version 1 Summary of Data Classes[6]
1. Assessment and Plan of Treatment
2. Care Team Members
3. Clinical Notes
4. Goals
5. Health Concerns
6. Immunizations
7. Laboratory
8. Medications
9. Patient Demographics
10. Problems
11. Procedures
12. Provenance
13. Smoking Status
14. Unique Device Identifier(s) for a Patient's Implantable Device(s)
15. Vital signs

HL7® Fast Healthcare Interoperability Resources (FHIR)® Standard

The Health Level Seven (HL7®) FHIR® standard[7] is a representational state transfer (REST)-based standard designed to enable the exchange of information related to health care. This includes clinical data as well as health care-related administrative, public health, and research data. The HL7® FHIR® standard builds on previous data format standards from HL7®. It facilitates interoperability between legacy health IT systems, eases provision of health care information to health care providers and individuals on a wide variety of devices from computers to tablets to cell phones, and allows third-party application developers

to provide medical applications which can be easily integrated into existing systems. HL7® FHIR® provides an alternative to document-centric approaches like the Consolidated-Clinical Document Architecture (C-CDA) by directly exposing discrete data elements as services. For example, basic elements of health care data such as patient identifying information, admissions, diagnostic reports, and medications can be retrieved and manipulated via their own resource URLs.

A number of groups are actively working to use, improve, and refine the HL7® FHIR® standard. The HL7® Argonaut Project is a private sector initiative working to rapidly develop and implement the first-generation HL7® FHIR®-based API to support the 2015 Edition API requirements. The Argonaut Project brings together a variety of health IT developers and provider organizations.[8] HL7® and IHE International recently jointly launched Project Gemini to make more rapid progress in achieving interoperability through HL7® FHIR®.[9] HL7® is also leading the Da Vinci Project to accelerate the adoption of HL7® FHIR® as a standard to support and integrate value-based care data exchange across communities.[10] National interoperability initiatives such as DirectTrust, The Sequoia Project, and CommonWell Health Alliance are all working to advance the use of HL7® FHIR® in their efforts.[11, 12, 13]

Patients' Experience of Health Information Exchange

Patient portals have enhanced the ability of patients to access and share their information. However, patients continue to experience negative impacts on care coordination caused by insufficient health information exchange as they interact with multiple providers and health care systems. Most portals are siloed and tethered to a particular practice or health care system, and vary in usability for patients and providers. In addition, portals often do not contain all of the information in a patient's medical record. For example, about half of individuals who accessed their online medical record reported that it did not include their immunizations (45%) or clinical notes (49%).[14] Health information may also be presented in a way that is not easily used nor understood by patients.[15] Therefore, patients sometimes cannot act as an intermediary in exchanging their health information even when they want to. As a result of insufficient health information exchange, patients are spending more time relaying their medical history than they think they should. Patients spend an average of 8 minutes filling out paperwork at a typical appointment and another 8 minutes explaining their medical history to their doctor while 80% of patients feel they should fill out paperwork only on their first visit to the provider's office.[16] Even more concerning, 90% of patients believe that their lives are at stake when their providers don't have access to their complete medication history.[17]

Priority Target Area: Privacy and Security

Background

As interoperability and access to patient health information expand, the privacy and security of health data are primary concerns for stakeholders. Privacy and security of health data are important considerations in advancing and maintaining trust in interoperability while poor privacy and security practices heighten the vulnerability of patient information stored in health information systems and on devices. Inadequate practices also have the potential to create data management problems for health care organizations via unauthorized and/or unintended disclosure, ransomware, and other avenues.

In 2015, a majority of individuals indicated confidence that their medical records are safe from unauthorized viewing, but had concerns when health information is electronically exchanged.[18] A majority of individuals (74%) were confident their medical records are safe from unauthorized viewing but had

concerns (60%) when health information is electronically exchanged. Ten percent of individuals reported withholding information from their health care provider due to privacy and security concerns regarding their medical record.

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule requires covered health care providers and health plans to provide individuals with access to their health information. HIPAA protects privacy and security by requiring stakeholders with access to protected health information to protect the confidentiality, integrity, and availability of that information.

HHS, via ONC, the Centers for Medicare and Medicaid Services (CMS), and the Office for Civil Rights (OCR), supports privacy and security through a variety of activities.[19] These activities include the Medicare and Medicaid EHR Promoting Interoperability Programs, enforcement of the HIPAA Rules, and the release of educational resources and tools to help providers and hospitals mitigate privacy and security risks in their practices. On December 12, 2018, OCR published a Request for Information (RFI) seeking recommendations and input from the public on how the HIPAA Rules, especially the HIPAA Privacy Rule, could be modified to promote coordinated, value-based health care. A specific area of interest is encouraging information-sharing for treatment and care coordination.[20]

Many states have their own laws and regulations to protect the privacy of health information, and these often have stricter privacy protections and requirements on use and disclosure than the HIPAA Privacy Rule. These statutes and regulations vary from state to state, often narrowly targeting a population, health condition, information collection effort, or specific types of health care organizations. The variation can cause confusion among exchange partners and make it difficult and expensive to harness technology to ensure privacy compliance.[21]

Privacy and security regulations are sometimes cited as a barrier to sharing health information, although many of these concerns have been ameliorated over time, sometimes simply through education about what the law actually requires. Lowering the cost of exchange or increasing financial incentives may boost provider participation more than further reducing legal barriers.[22]

Current State

Much progress has been achieved in increasing the privacy and security of health information in recent years, while challenges remain. The following are descriptions of the current state of key topics for which gaps and opportunities have been identified.

OAuth 2.0 Authorization Protocol and OpenID Connect Authentication Protocol

OAuth 2.0 is a simple authorization protocol that enables a third-party application to securely obtain access to web-enabled services. The OAuth 2.0 specification is useful for conveying use authorization across a network of web-enabled applications and APIs, including for mobile phones and home devices, and is a key component of the HL7® FHIR® standard. [23]

OpenID Connect is a simple identity layer designed to work with OAuth 2.0. It allows applications to verify the identity of the end user based on the authentication performed by an authorization server. It obtains basic profile information about the end user in an interoperable and RESTful manner that supports the use of APIs.[24]

Protections for Patient-Generated Health Data

Patient-generated health data (PGHD) are health-related data created, recorded, or gathered by or from patients (or family members or other caregivers) to help address a health concern.[25] PGHD are an increasingly used data source that requires privacy and security protections, including when de-identified PGHD is monetized.[26] With the shift toward value-based models of health care delivery, there is increasing interest in incorporating PGHD in remote monitoring and telehealth services. While the use of electronically captured PGHD may be relatively new and therefore not yet highly regulated, it may be covered by established laws and regulations for patient health data more generally.[27] As providers gain the ability to receive PGHD, the data may become part of the patient's medical record and existing regulations for data privacy and security, such as HIPAA, would apply.

User-Controlled Mental Health and Behavioral Health Information Sharing

Title 42 of the Code of Federal Regulations, Part 2: Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2) was established to address concerns about the potential use of substance use disorder information in non-treatment-based settings such as criminal or domestic proceedings, e.g., child custody, divorce, or employment. 42 CFR Part 2 is intended to ensure that a patient receiving treatment for a substance use disorder does not face adverse consequences. 42 CFR Part 2 protects the confidentiality of patient records related to a substance use disorder by restricting the circumstances under which federally assisted 42 CFR Part 2 programs can disclose information. Unless an individual provides specific written consent, 42 CFR Part 2 programs are prohibited from disclosing any information that would identify a person as having or having had a substance use disorder. Behavioral health data generated by a non-42 CFR Part 2-covered program is protected by HIPAA and, where applicable, state laws and regulations. The varying disclosure requirements between HIPAA and 42 CFR Part 2 are often cited by stakeholders as a key challenge to integrating behavioral health data into the broader data continuum.

In recent years, the Substance Abuse and Mental Health Services Administration (SAMHSA) has issued a final rule and frequently asked questions (FAQ) list to clarify and simplify the 42 CFR Part 2 consent rules.[28,29] Previously, a patient had to name each individual and organization that could receive their health information.[30] After the final rule, a patient can designate a general entity, such as a HIN and their participants, to receive their health information. While this has eliminated some barriers to the exchange of Part 2-covered health information, gaps remain. Patients still must complete a separate consent for the release of substance use disorder information. HINs and their participants cannot share Part 2-covered health information with a treating provider who is not part of the HIN without again obtaining consent from the patient.[31]

OCR provides specific guidance addressing HIPAA protections, the obligations of covered health care providers, and the circumstances in which covered providers can share information related to mental health and substance use disorder treatment. This guidance includes information about when and how health care providers can share a patient's health information with his or her family members, friends, and legal personal representatives when that patient may be in crisis and incapacitated, such as during an opioid overdose.[32]

Health Information Sharing for Research Purposes

The HIPAA Privacy Rule establishes the conditions under which protected health information may be used or disclosed by covered entities for research purposes. The Privacy Rule defines the means by which

individuals will be informed of uses and disclosures of their medical information for research purposes, and their rights to access information about them held by covered entities. With regard to research, the Privacy Rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct research.

The Privacy Rule does not restrict the use or disclosure of de-identified health information. Traditionally, de-identified health information neither identifies nor provides a reasonable basis to identify an individual. The Privacy Rule permits a covered entity or its business associate to create, use, and disclose information that is not individually identifiable by following the Privacy Rule's de-identification requirements. However, concern is growing that de-identified data can be re-identified using big data sets and machine learning.[33]

Several companies and programs are collecting health information for research using mobile devices and web applications, including Apple's ResearchKit platform, the PatientsLikeMe and 23andMe websites, Epic's Cosmos research database, and the NIH All of Us Research Program.

Direct-to-consumer DNA kits are commonly used by individuals to learn about their ancestry and to assess their potential health risks from genetic illnesses.[34] The collected health information may also be redisclosed for research purposes with informed individual consent. States vary in regulating the collection, retention[35], ownership[36], and redisclosure of this health information for other uses. Several states are passing additional legislation protecting consumers from life, health, and disability insurance coverage discrimination, as well as employment discrimination based on this genetic information.[37]

Patient Matching and Verification

Patient matching is the process of comparing several demographic data elements from different health IT systems to determine if they refer to the same patient. The ability to complete patient matching efficiently, accurately, and at scale has long been identified as a key element for the success of the nation's health IT infrastructure. Accurate patient matching is essential to protecting patient privacy and ensuring patient safety. Incorrect matching can lead to including health information about the wrong person in a patient's record, resulting in both privacy and safety issues. In addition, poor matching can lead to instances where a patient's previous consent decision is not recognized as a new record is created because it is not linked to the previously submitted consent.

Today, accurate patient matching rates vary widely across health care organizations and are difficult to compare as organizations can calculate the rate differently.[38] Most often, organizations use demographic data elements and a matching algorithm to determine if a record should be linked or not. ONC has adopted standards for some demographic data elements used for patient matching in the CCDS, while other elements have no widely adopted format.[39] Organizations treating pediatric patients must take further precautions for identified children with common names, including temporary names such as "baby boy" or "baby girl."[40]

To address this concern, ONC has undertaken a project called Patient Matching, Aggregating and Linking (PMAL). PMAL is focused on the identification and testing of standards for matching patients to their data across and in between clinical and claims data sets, and the identification of algorithms that can be used to reliably perform patient matching in these contexts. PMAL is also working on developing security profiles based on OAuth 2.0, OpenId Connect, and User-Managed Access (UMA) protocols for securing web APIs. These security profiles are being created so that health care APIs can be protected appropriately

while providing necessary access to data. The identified standards and toolsets will safely match patients to their information and make additional clinical data available to providers and researchers in a timely manner.

A recent U.S. Government Accountability Office study noted that many stakeholders believe that no single effort, including a national patient identifier, will solve the patient matching challenge. However, the report states that more steps could be taken by ONC and others to improve patient matching such as requiring demographic data standards for certified EHRs and facilitating the voluntary adoption of such standards.[41]

Disaster Planning for Health IT

The widespread adoption of health IT has significantly improved the health care sector's preparedness for disasters. EHR systems are typically backed up remotely and can remain accessible as a result even in floods or other disasters. However, the advancement of health IT creates new challenges for which health care organizations need to actively plan and prepare. Organizations need to have processes in place to handle unplanned system downtime; for example, when a system becomes unavailable or is compromised in some way due to a natural disaster or malicious attack. With the increased reliance on technology, it is important that organizations both have a process in place and practice using the process so that when system downtime occurs, patient care can continue without risk to patient safety. HHS requires Medicare and Medicaid providers to take steps to plan for a disaster scenario.[42] In addition, HHS has developed a HIPAA Security Risk Assessment tool that contains a series of helpful questions for an organization from a preparedness standpoint to ensure the availability and integrity of electronic health information.[43]

Building interoperable systems across health care will pave the way for communities to better respond to and recover from future disasters. Over the past few years, the California Emergency Medical Services Authority (CalEMSA) has developed the Patient Unified Lookup System for Emergencies (PULSE) to provide selected health care professionals, while volunteering during a disaster, the ability to search and return personal health information about patients they are treating in the field. PULSE, developed by ONC and supported across HHS, proved through an emergency exercise that it was able to successfully integrate the California Trusted Exchange Network (CTEN), California's Disaster Health Care Volunteers (DHV) system, and four health information exchange organizations. Although PULSE is currently operational in parts of California, the vision is to grow PULSE statewide and eventually nationwide in time for the next emergency.[44] This work may function as a model for other states and communities to build upon as needed, modified to meet local conditions.

Priority Target Area: Patient Access to Information

Background

Patients' electronic access and use of their health information will be critical for enabling individuals to better monitor their health as well as manage and coordinate their care.[45] Accessing the data in the most convenient, usable, and accessible ways to the individuals and allowing them to share their information securely with providers and other trusted health partners is important in shifting the industry to a more patient-centric approach to health.

Current State

Much progress has been achieved in increasing patients' access to their health information in recent years, while challenges remain. The following are descriptions of the current state of key topics for which gaps and opportunities have been identified.

Patient-Controlled Data Collection, Access, and Sharing

Availability for patients to access their health information electronically from providers and payers is increasing. According to the 2017 Health Information National Trends Survey, 52% of patients have been offered online access to medical records by a health care provider or health insurer and online access to medical records has grown by 24% since 2014. Patients were more likely to access and use an online medical record when medical providers offered and encouraged use (63%). Of those who were offered access, half accessed their record online. Nearly half of those accessing their records used them to communicate with a health care provider and 14% transmitted data to an outside party, including providers, caregivers, or a service or app.[46]

In addition to clinical data availability, many payers, including Medicare, are improving access to administrative claims data through APIs. The use of APIs can improve individual electronic access to their health information and better support the growing market of patient-facing applications that are designed to allow individuals to access, aggregate, and act on their health information.

The public and private sectors have both made progress in advancing patient access to their health information. MyHealthEData is a government-wide initiative spearheaded by the White House Office of American Innovation, with participation from HHS, including CMS, ONC, and the National Institute of Health (NIH), as well as the Department of Veterans Affairs. The MyHealthEData initiative aims to empower patients by granting the provider of their choice access to their health data, receive copies of their own health data, and share personal health data with anyone they choose, using the device or application of their choice. This effort approaches the issue of health care data access and exchange from the patient's perspective.[47] With full access to their own health information, patients can find providers and health care services to meet their needs, improve understanding of their overall health, and make informed decisions about personal care.

CMS has been working since 2010 to give beneficiaries access to their claims data through the Blue Button project. CMS recently launched Blue Button 2.0, an API that enables Medicare beneficiaries to connect their Medicare claims data to the applications, services, and research programs they choose.[48] Available as part of MyHealthEData, this API gives beneficiaries control over how this data are used and by whom. Blue Button 2.0 uses the HL7® FHIR® standard for beneficiary data and the OAuth 2.0 standard for beneficiary authorization.[49] More than 150 organizations have signed up for the API Developer Preview, a program allowing developers to build integrations to access four years of Medicare Part A, B, and D data for 53 million Medicare beneficiaries.[50]

Similarly, in 2018, the Veterans Health Administration released an app called Mobile Blue Button to help veterans more easily download, store, and share their health record information.[51]

The private sector is also innovating opportunities for patients to access, manage, and share their health data with trusted parties. Apple worked with health systems and health IT developers to allow patients to access and aggregate patient health information. The Apple Health Records EHR data viewer uses the HL7® FHIR® standard to collect patient health data from disparate sources and populate user devices with

clinical information in a consumer-friendly interface. This aggregated view of patients' health records from multiple institutions is presented alongside PGHD, creating a more holistic view of health.[52]

Data Collection Using Mobile/Wearable Devices

The proliferation of consumer health technologies, including smartphones, mobile applications (apps), and wearable devices, has increased the frequency, amount, and types of PGHD available. A report by Research2Guidance in 2017 found that there are more than 325,000 mobile health apps available for download from major app stores.[53] These advances can enable patients and their caregivers to independently and seamlessly capture and share their health data electronically. Providers can use remote monitoring devices, coupled with their deployment of patient portals and secure messaging, to offer innovative ways to connect with patients to strengthen their engagement in managing their health and health care.

However, measurements and data elements, including their structure and format, may vary significantly across devices and apps, posing challenges for combining and comparing PGHD from disparate sources, including clinical data in an EHR. Developers and standards bodies can provide the technical infrastructure and tools required to enable the capture, use, and sharing of PGHD. Increased standardization will help to ensure the functionality of these devices and apps as well as the accuracy and validity of data captured by these tools.[54]

Some consumer devices and apps now communicate with and collect the same health data as medical devices. As a result, questions have arisen about the role of the federal government in regulating and monitoring these capabilities to help balance the benefits and risks to several stakeholder groups. The U.S. Food and Drug Administration (FDA) has established a Digital Health Program to better protect and promote public health and provide continued regulatory clarity. As part of that program, the FDA's Software Precertification (Pre-Cert) Pilot Program intends to "help inform the development of a regulatory model to assess the safety and effectiveness of software technologies without inhibiting patient access to these technologies."[55]

Use and Sharing of Patient-Generated Health Data

PGHD captured and shared in a non-clinical setting can offer real-time insights into a patient's health status and inform progress against a treatment plan, enabling care teams to make timelier, better-informed decisions with patients. Consumer interest in the use of PGHD has increased with the growing prevalence of wearable fitness trackers and mobile health apps as noted above. Many providers and researchers are looking for ways to capitalize on the pervasiveness of these devices and the abundance of data patients are generating.[56]

There are multiple opportunities for PGHD use to help advance value-based payment models, clinical care, telehealth, and research efforts. For example, CMS recently unbundled payment for Current Procedural Terminology (CPT®) code 99091 for remote patient monitoring in the 2018 Medicare physician fee schedule to better support telehealth services.[57] Also in 2018, ONC published a white paper titled "Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024" as well as a practical guide for providers to help identify best practices, gaps, and opportunities for progress in the collection and use of PGHD in care delivery and research.[58]

However, challenges remain for providers such as managing the volume, ensuring data accuracy, tracking data provenance, encouraging exchange, merging PGHD with clinical data, and managing security risks. The use of PGHD may present liability concerns if inaccurate PGHD are used in clinical decisions or if the clinician chooses not to review or act based on the PGHD received. Additionally, barriers to access, low health literacy, and concerns about privacy protections can limit PGHD collection, use, and sharing by patients and caregivers.[59]

Use and Sharing of Social Determinants of Health Data

Social determinants of health are defined as "the conditions in which people are born, grow, work, live, age, and the wider set of forces and systems shaping the conditions of daily life" and are responsible for most health inequalities.[60] Millions of Medicare, Medicaid, and uninsured have high cost, multiple chronic health and social conditions costing at least $850 billion dollars annually.[61] Despite strong evidence linking patients' social circumstances to their health status, the health care system is struggling to address SDOH with patients by identifying patient-specific needs, continuing engagement, and information sharing across health care and community service organizations.

Historically, SDOH data collection approaches generally focused on population-level and policy interventions to address systemic issues hindering health equity and overlooked individual and clinical innovations within health care that can address patients' social circumstances.[62] SDOH integration into clinical care requires 1) collection of patient-level information related to SDOH through assessment and screening tools such as a patient-reported outcomes measures (PROMs) questionnaire, 2) patient access to community resources and ongoing care plan engagement with the care team, and 3) electronic resource identification and communication workflows using standardized data capture across clinical and community settings.

Providers are adopting standard assessment tools, such as the Protocol for Responding to and Assessing Patients' Assets, Risks, and Experiences (PRAPARE) tool,[63, 64] by integrating data collection into EHRs or using stand-alone survey tools. Survey questions using standardized questions can be completed by patients or facilitated by care providers and allow for patient specific data collection on current needs and struggles. These assessments identify the patient's needs and where additional service coordination is needed. Ongoing patient and care team communication is needed to improve access to specialty services for disadvantaged patients promoting care coordination and reducing patient confusion. Access to available community resource information and care coordinators can help patients navigate resources, build meaningful relationships, and foster continued engagement with care and community service providers.

To address patient-specific needs and support interventions, closed-loop clinical to community service referral tools are needed across referral makers to community service providers. Using standardized data capture, such as Logical Observation Identifiers Names and Codes (LOINC), supports uniform representation of SDOH data elements across core domains, improves data capture, facilitates patient access to their health information, and reuse of social and behavioral data for interventions across care and service settings.[65]

Emerging Platforms for Data Sharing by Patients and Caregivers

There are emerging platforms to encourage the exchange and use of health information. These include Apple's Health Records program, which launched at 39 hospitals beginning in March 2018, as well as a Duke Health program using Apple HealthKit and ResearchKit. Additionally, the CARIN Alliance has been

facilitating increased consumer-mediated exchange using mobile health data. This bipartisan collaborative of more than 60 health care and other stakeholders has created a code of conduct for third-party apps to address privacy concerns about health care data collection, use, and sharing.[66]

To assist providers in providing the best care possible, software systems and cloud-based services need to interact with each other to exchange clinical and administrative data to be shared across the care continuum. To advance this goal, provider organizations will need real-time access to patient information to make a unified health record. This will only be possible if the technology is able to combine multiple data sources (e.g., structured data, unstructured clinical notes, medical devices). Standards development organizations such as HL7® and Continua are working to develop device interoperability standards which will help drive interoperability.

Health IT Infrastructure Gap Analysis

The Cures Act requires an analysis identifying existing gaps in policies and resources for achieving the ONC FY18 objectives and benchmarks and furthering interoperability throughout the health information technology infrastructure.

Priority Target Area: Interoperability

Need to Increase Level of Interoperability

Each stage of EHR development, implementation, and use can affect the usability and safety of the technology. Current federal testing criteria address the design and development of EHRs; however, they do not address customized changes made to an EHR as part of the implementation process or afterward.[67] Such changes could impact whether systems are truly interoperable at both content and transport levels after implementation, especially among smaller practices.

Sometimes the electronic exchange of health information creates additional work and burden for providers rather than serving as a tool to assist them in improving patient care.[68] For example, at times, analog communication is still faster for providers than electronic because they can delegate managing a fax to their staff, whereas when data comes in electronically directly to the provider, often the provider must manage it personally. Furthermore, in non-acute settings such as long-term care, providers commonly lack a digital health infrastructure to exchange records electronically, thus leading to a reliance on analog modalities such as fax machines.[69] Increased automation, supported by improved interoperability and usability, is an important step to help reduce provider burden related to the use of health IT systems. To this end, ONC has published the draft report "Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs,"[70] as required by the Cures Act.

Ongoing Efforts Regarding Open APIs, Information Blocking, Trusted Exchange Framework, and Standards and Implementation Specifications

There are more than 100 health information exchanges and multiple national-level organizations that support the electronic exchange of health information. While these organizations have made significant progress and expanded interoperability, connectivity across these networks remains limited due to varying policy and technical requirements. Differing policy requirements are outlined in HINs' data use agreements and policies and procedures. Although some variations are necessary and useful across networks, others present significant challenges to cross-HIN exchange. Examples of variation that create interoperability challenges include varying policies on how data can be used, who can participate in the HIN, the minimum security bar for trust and privacy, and data exchange reciprocity.[71, 72, 73] Varying technical approaches can present challenges to cross-network exchange.[74] Even in instances in which the same standards are used by two HINs, interoperability can be stymied due to lack of specification in the standard and varying implementations across the HINs.[75] Accurate patient matching continues to be a major challenge across interoperability initiatives.[76, 77]

Since the release of the 2015 report on information blocking, HHS has taken a variety of actions to help address the problem including adding attestations to the Medicare and Medicaid Promoting Interoperability Programs and the Merit-Based Incentive Payment System that providers do not block

sharing of information.[78, 79, 80] Even with these actions from HHS, some stakeholders continue to cite information blocking by health IT developers and provider organizations as an ongoing challenge.[81]

Public comments on the draft Trusted Exchange Framework published in January 2018 suggested that implementation of the framework should leverage existing areas of alignment while avoiding disruption or duplication of existing efforts that are successfully enabling data exchange. Enough time should be provided for Health Information Networks (HINs) to implement changes. Commenters also said that the implementation should ensure privacy, security, and patient safety protections. Approaches should ensure flexibility in requirements for use cases and permitted purposes. Additionally, they should accommodate differences in local and state policy, as well as differing business models, technical approaches, and capacities of participating organizations. The implementation should ensure inclusive governance by any coordinating entities. The financial sustainability of approaches should be considered, with attention paid to the financial and technical barriers to participation for small providers. Some commenters suggested piloting approaches first and then scaling up.

Lack of Knowledge about User Experience of Health Information Exchange

While there are numerous process measures assessing the current state of interoperability (i.e., participation rates in HINs and transaction counts), there is little consensus among industry stakeholders and policymakers about what metrics clearly delineate progress.[82] Measures of the user experience of health information exchange for both providers and patients are generally missing. Many stakeholders want to see a shift in the focus of interoperability measurement from process measures to outcome measures so that advancements can be assessed based on both the outcomes and the progress that has been made. ONC, recognizing the gap, commissioned a report from the National Quality Forum (NQF) to develop a measurement framework and measure concepts which can serve as a foundation for addressing the current gaps in the measurement of interoperability, including users' experiences.[83] The measurement framework identified four measurement domains and subdomains that need to be measured to capture interoperability progress, including the usability and application of exchanged information. Work remains to implement this framework and develop a consensus process and outcome measures that industry stakeholders and policymakers agree will demonstrate progress toward increased interoperability.

Unmet Needs of Additional Care Settings and Stakeholder Groups

To successfully move from fee-for-service to alternative payment models, electronic health information must flow when and where it is needed across the entire care continuum, including bringing in new stakeholders such as social service providers. Today, many health care providers that were not eligible to receive incentives payments under the Promoting Interoperability Programs have lower rates of adoption of EHRs and use of health information exchange compared to eligible hospitals and eligible professionals. For example, the following entities can send, find, receive, and integrate patient summary of care records from outside sources: 41% of hospitals[84] (2017), 8.7% of office-based physicians[85] (2015), and 7% of skilled nursing facilities[86] (2016).

The table below outlines the rate of bi-directional exchange between non-federal acute care hospitals and other types of providers including behavioral health and long-term care providers. Previous studies have found a link between the participation in a HIN and the increased ability of a provider to send, find, receive, and use patient health information electronically.[87]

2015 Rates of sending and receiving summary of care records between hospitals and other types of providers[88]				
	Behavioral Health Providers	Long-Term Care Providers	Outside Ambulatory Care Providers	Outside Hospitals
Electronically receive summary of care records from…	23%	23%	37%	40%
Electronically send summary of care records to…	35%	49%	61%	59%

Improving the capability to electronically exchange and use health information of behavioral health and long-term care providers will be an important element of building alternative payment models. Expansion of priority use cases would be a step toward meeting the needs of additional care settings.

Delay in Timeliness between Issuance of Guidelines and Development of Technology

Stakeholders have frequently communicated to ONC and CMS that health IT developers and providers need 18 to 24 months from the issuance of final rules or guidance to be able to safely and efficiently implement required changes into health IT systems and then test and deploy these updated products into the workflow of providers. This lag time, along with delays to the effective date of requirements, can lead to existing regulatory requirements pointing to out-dated versions of a standard and limit health IT developers and providers ability to move to a newer version of a standard.

Need to Improve Data Quality, Provenance, and Usefulness

Data provenance provides the ability to trace and verify who created information and when, how it has been used or moved, and how it is altered throughout its lifecycle. Use of provenance data by health IT systems may assist in the identification of erroneous information.[89] The notification and correction of errors in the process of data collection and exchange may lead to improvements in patient safety and data accuracy. There is an ever-growing need for health data provenance and standardized approaches to capture it due to the widespread adoption of EHRs. Understanding the provenance of the data being exchanged has been identified by stakeholders as a fundamental need to improve its trustworthiness and reliability.[90]

Infrastructure Needs of Stakeholder Groups, Especially Broadband Access

Core infrastructure is essential to the ability of health care organizations to use certain health IT capabilities. For example, broadband access, or high-speed Internet access, is an essential component to support many health IT capabilities including the electronic exchange of health information. According to a Federal Communications Commission (FCC) report, at the end of 2016, 92.3% of the country had access to broadband meeting a speed benchmark of 25 Mbps download/3 Mbps upload. However, more than 24 million individuals still lacked access to broadband, with a higher percentage of these individuals living in rural areas.[91] Lack of broadband availability impacts the ability of providers and patients to participate in telehealth and data exchange efforts.

Priority Target Area: Privacy and Security

Implications of Emergence of the Internet of Things (IoT)

The IoT in health care offers many benefits, including being able to closely monitor patients and using data for analytics.[92] Consumer-specific devices, such as glucose meters, blood pressure cuffs, and other devices designed to record data on patient vital signs, are key areas for medical device integration in the IoT. The IoT enables health care providers to automatically collect information and apply decision support rules to allow for earlier intervention in the treatment process.[93]

With the emergence of the IoT, the flow of health data becomes more dynamic rather than remaining relatively static. For example, health data generated by the IoT could flow bidirectionally between clinical settings and patients' devices, so HIPAA protections of that data would vary as it flows, depending on the context. There are not yet policy frameworks and governance structures in place to address concerns raised by data continually in motion.[94]

As medical devices become more integrated with health IT systems, especially when web-enabled, security risks from malicious hackers, malware, and computer viruses increase. These risks can reduce the device's effectiveness and increase patient safety issues. In response to concerns about the cybersecurity risks of medical devices, the FDA issued formal guidance on how medical device manufacturers should handle reports about cyber vulnerabilities.[95] Further clarification may also be needed around third-party access of IoT data and the privacy and security considerations associated with that access.[96] Health care organizations planning for more integrated systems should consider vulnerabilities by preparing a cybersecurity response and preparedness framework for their EHR, external information sharing, and internal IoT data, thereby ensuring device effectiveness and protecting patient safety.[97]

Lack of User Awareness and Education about Privacy and Security Protections

Users of social media and other technology often lack understanding of the privacy and security protections available, including for health information that they share via social media and other tools. Although social media platforms can enable collaboration, users are also vulnerable to privacy breaches and misuse of their health information. Misunderstandings and overly cautious interpretation of privacy policies cause confusion among health care stakeholders, thereby creating barriers for broader interoperability of health information and behavioral health information. Compounding the confusion are disparate state laws and regulations, as well as consent and disclosure requirements. Further alignment of health data sharing privacy policy is needed, including for secondary or tertiary uses of personally identifiable data and for data available through the IoT, in addition to continued training on what information can be collected, viewed, and disclosed.[98, 99, 100, 101]

Variability of Information Sharing Policies across States

Alignment of state and federal privacy laws is a continuing challenge for advancing interoperability of health information. Most states have their own laws and regulations pertaining to the use, collection and disclosure of health information, which may be stricter than federal requirements governing privacy and access. State law may regulate when a provider may access and disclose personal health information, to whom the information may be disclosed, and for what purpose.[102] The variability in state policies for sharing health information creates perceived and real barriers for sharing information. In addition to differing state policies, policy alignment is needed for health information shared across federal agencies, such as the Department of Veterans Affairs and the Department of Defense.

States also have varying policies regarding patient consent for access, use, and disclosure of information. Patient consent policies typically fall under two categories: 1) opt-out, i.e., patients may be automatically enrolled in a health information exchange (HIE) but are given the opportunity to opt out of having their information stored and/or disclosed by the HIE; and 2) opt-in, i.e., patient consent is required for patient health information to be stored and/or disclosed by the HIE.[103] As of 2016, among 31 states with laws addressing privacy and HIE, 16 followed the opt-out approach, 8 described an opt-in process, and the rest adopted other approaches to HIE participation. Twenty-three states imposed specific confidentiality requirements on HIE users and 5 mentioned confidentiality without providing specific requirements.[104]

Implications of the California Consumer Privacy Act of 2018

Effective January 1, 2020, the California Consumer Privacy Act of 2018 (California Privacy Act) will expand privacy rights of California consumers as well as require businesses to disclose what, why, and how consumers' personal information is being used.[105] Failure to comply with this new law could be costly to businesses due to civil penalties. The law applies to businesses who collect, use, or share personal information of California residents, including those who are outside the state for temporary or transitory purposes (e.g., travelers). California's privacy law does not apply to protected health information regulated by California's Confidentiality of Medical Information Act or by HIPAA's privacy, security, and notification rules, but it does apply to the other personal information held by an organization that meets the criteria above and is doing business in California.[106]

As new consumer data protections grow, the California Privacy Act is an example of aligning policies and offering continuing education for the health care sector and consumers. Other states may establish their own legislation and guidance that are broader or stricter than HIPAA, raising questions about the role of the federal government in coordinating a patchwork of privacy and security protections nationwide, especially when data are shared across state lines.

Variability in Adoption of Cybersecurity Framework(s)

According to many of the senior leaders at health care organizations, HIPAA compliance alone is not enough and implementing a security framework is critical in ensuring a robust security program.[107] There are several cybersecurity frameworks, both paid and publicly available, recommended for improving the security of IT networks. Paid frameworks include the Health Information Trust Alliance (HITRUST) Common Security Framework (CSF). Publicly available frameworks include the International Organization for Standardization (ISO) standards, Center for Internet Security (CIS) Critical Security Controls or Effective Cyber Defense, and National Institute of Standards and Technology (NIST) Cybersecurity Framework. Although most organizations have some sort of security compliance plan, as the threats to networks continue to rise, organizations must update their plans on a regular basis to meet the requirements. The cost and resources needed to adopt cybersecurity frameworks continue to pose challenges in all sectors, including health care and especially for small- to medium-sized organizations. An example of the challenges being faced is health care providers' and systems' concern about being held liable for a breach of data at a vendor over which the organization does not have direct control.

Lack of User Control to Share and Disclose Information

Patients are interested in having more granular control over which types of their health information are shared, with whom, and for what purpose. Patients have differing preferences about sharing data depending on whether the information is sensitive or not.[108] To address this concern, HIPAA-covered entities, e.g., providers, may obtain consent in a manner that limits electronic health information

exchange disclosures on a more granular level. For example, a covered entity could obtain patient consent for disclosures for certain purposes, for disclosures to certain categories of recipients, or for exchanges of certain types of information, such as information that may be considered particularly sensitive. In addition, consent may be obtained either once or on a regular basis.[109] Providing patients with more granular control over their health information has the potential to increase patients' willingness to participate in health information exchange initiatives.[110] The technical capabilities to support granular control can help support the existing variation in state and federal privacy laws.

Efforts such as the Data Segmentation for Privacy (DS4P)[111] and Patient Choice[112] pilots have identified technical approaches that can support more granular patient consent decisions. The DS4P standard allows tagging of a C-CDA document with privacy metadata that express the data classification and disclosure restrictions placed on the data by applicable law. The 2015 Edition includes certification criteria for sending and receiving data using the DS4P standard. [113] There has been limited adoption to date, however, as only 27 modules have certified to one of the criteria out of the 442 modules certified to the 2015 Edition as of September 17, 2018.[114]

Current consent form collection and storage practices are static and setting-specific rather aligned with data in motion that flows across settings. The patient's consent choices should flow with the data regardless of the health care setting. To accomplish this, the design and use of consent forms need to become more user-centered and flexible. Further consideration must also take into account patients who are minors and the varying requirements of state laws for obtaining consent from their legal guardians.[115]

Implications of European Union's General Data Protection Regulation and Privacy Shield

The European Union (EU) issued a regulation in 2016 on data privacy and security protecting personal data. The General Data Protection Regulation (GDPR) set new rules on how companies manage and share personal data. The GDPR is more expansive than HIPAA as it uses a broader definition of personal data and covers any information associated with an "identified or identifiable natural person," including computer IP addresses, photos, and credit card data. The EU law is based on personal rights, whereas HIPAA is focused more on the data itself and who can share it and what can be done with it. [116] GDPR policies include:

- Fines - GDPR requires companies to gain consent for any data collected on EU residents. Organizations that violate the law could face fines up to 4% of their global annual revenue or 20 million Euros -- whichever fine is higher.
- Timeliness and use of resident information - The law mandates that organizations process data requests from EU patients much more quickly than with U.S. standards. Providers will also need to obtain permission to use EU resident information.
- Data erasure and storage - One of the biggest challenges for U.S. providers will likely be the GDPR "right to be forgotten" or sometimes known as the right to erasure. One of the cornerstones of the regulation is strengthening of individual rights, meaning organizations must honor all patient requests to erase personal data. It also places limits on how long data can be stored, covering all data not considered valuable to scientific research under GDPR definition.[117]
- Security - GDPR enhances security requirements to ensure patient data are protected. Methods include implementing the use of pseudonyms for identifying data and redundancy of data, along with routine penetration testing and intrusion detection measures. [118] Additionally, organizations will need to implement a continuous process to evaluate their security measures, including

encryption. Organizations will only have 72 hours to inform EU patients of a breach, whereas HIPAA gives providers 60 days from the time of discovery. [119]

U.S. companies must comply with GDPR if the organization is established in the EU, processes personal data of EU individuals and data for goods and services offered in the EU, and monitors the behavior of EU individuals. [120] Although it seems the GDPR will have little effect on U.S. health care organizations, providers may be affected if their organizations have telehealth relationships with hospitals in the EU or have affiliates in the EU. GDPR will also need to be considered for multi-site, trans-national health care research activities as it relates to human subjects.[121]

Lack of Knowledge about HIPAA and Confidentiality of Substance Use Disorder Patient Records Regulation Implications

Varying privacy laws and policies among states and entities can add complexity and confusion to sensitive health situations when health entities need to share patient information. There are many misunderstandings about how HIPAA's consent rules intersect with other consent laws, including state laws. In 2016, ONC, in cooperation with the National Governors Association (NGA), identified potential steps in a comprehensive roadmap for states to improve interoperability of electronic health information within and among states. Addressing the lack of knowledge or misunderstanding of the confidentiality of substance use disorder patient information must be addressed through training, workflow and business process improvement, policy alignment, and technical capabilities. Technical systems capabilities may not support separating a patient's health information into categories that are in step with current law and policy.[122]

Federal, state, and organizational policy and consent process alignment are needed for secure and efficient exchange of substance use disorder treatment information. Continued education is necessary for understanding when consent is needed for collection, access, and disclosure of health information for varying uses (e.g., treatment, payment, operations, and research) and reducing perceived barriers. Misunderstandings about the type and range of mental health and substance use disorder information that providers can share with others have often resulted in reduced communication among health care providers, patients, and family members, potentially to the detriment of patient care.[123]

Need for Improved Patient Matching When Sharing Data

Patient matching errors can originate from multiple aspects of the patient care experience, such as during patient registration or data sharing among organizations. Matching errors can result in inaccurate record creation, inadvertent merged records, and duplication of patient records. Stakeholders have identified a variety of gaps that could help improve patient matching.

Many stakeholders feel a nationally adopted, unique patient identifier is necessary to enable effective patient matching. [124] Stakeholders have also noted a lack of standardization of the underlying demographic data elements used for patient matching. Some have recommended that health IT developers and health care organizations implement a set of agreed-upon standards that all participants must meet. Standards may include a minimum demographic data set, as well as a strategy for resolving errors when patients are incorrectly matched.[125]

Priority Target Area: Patient Access to Information

Unmet Infrastructure Needs for Underserved Populations

Underserved populations can be identified by geographic access to care, health insurance status, and health professional shortage areas. Underserved populations often have higher rates of cancer, asthma, obesity, behavioral health disorders, and other chronic conditions. Data also show that these populations are more likely to exhibit signs of poor management of chronic disease. Tools such as EHRs, clinical decision support (CDS), patient registries, and consumer health technology improve the quality of patient documentation, access to records, patient engagement, patient safety, and the overall efficiency of the care that providers deliver to underserved patients. Because minority and low-income areas lag behind other areas on EHR adoption, there is concern among health IT experts that increased adoption of health IT among U.S. health care providers overall will exacerbate the digital divide.[126]

ONC has identified the need to customize resources and programs to address the target populations' needs. ONC has also identified barriers to health IT adoption for these populations, such as limited English proficiency, low health literacy, lack of a usual source of medical care, limited access to broadband connectivity, and lack of comfort with technology that impede effective health IT use among some safety-net providers and the underserved patients they treat.[127]

Current infrastructure, such as access to broadband, health IT workforce, and interoperability across organizations, may be inadequate to support underserved patients' and caregivers' access to tools and information. Enabling health IT use in underserved populations requires human resources, technical assistance, and incentives to advance technology use. Such incentives could include reimbursement for alternate care delivery modalities that use health IT such as telehealth virtual visits, home health, and device monitoring. It is also important to understand the needs of the underserved populations by addressing SDOH.

Accessibility and Usability of Patient Portals and Other Patient-Facing Technology Continue to Need Improvement

Patient portals have become more accessible to patients, but most portals are siloed and tethered to a particular hospital or practice. While this approach offers some convenience for patients, they may struggle to manage multiple portals to access their data. Each physician whom a patient sees may have a different portal, and the patient may not have the ability to easily merge information across portals. The technology for patient portals is improving, and many can now be accessed through mobile devices. Some have advanced capabilities, such as telehealth functions, online scheduling options, and the ability to access physician notes, but these more advanced features are not yet widely implemented or adopted. As the technology continues to advance, experts expect portals to evolve beyond the limited functionality they offer today into user-friendly technology that enables access to a patient's aggregated health data available through easy-to-navigate mobile tools.[128]

There are concerns about reimbursement and costs of services offered via patient portals, such as telehealth and text exchanges; these concerns could slow adoption. However, because covered entities can only charge reasonable, cost-based fees for electronic access and the cost of providing electronic access is negligible,[129] access could be provided free of charge. Providers will need to implement workflow changes to fully integrate these services into their practices. Practices will need to establish the types of information that are appropriate to share via portals and what should remain in an office visit.

Patient Awareness and Education about Health IT Resources

Prior ONC research has found that individuals may not realize the value of accessing their online medical record until they have a medical need.[130] Because the patient record request process can take some time, it is of great benefit to be able to access one's data prior to an urgent health need. ONC has taken efforts to reach out to consumers about this concern. For example, ONC's Guide to Getting and Using your Health Records educates individuals and caregivers about the value of online medical records as well as how to access and use their information.[131] ONC also has developed videos and fact sheets to educate consumers about their rights to access their health information under HIPAA.[132] OCR has released education for health care professionals and for patients on patients' rights to access their health information, including the national campaign called "Get It. Check It. Use It."[133]

Continued information and education are needed to increase patient awareness of the use of their data and available health IT resources. The use of health IT to access their data can have a positive impact on health, health care, and health equity by supporting shared decision-making between patients and providers, providing personalized self-management tools, and delivering accurate, accessible, and actionable health information.[134]

Lack of Patient and Caregiver Access to Patient Data

Online access to medical records, such as through patient portals, enables patients and caregivers to view their health information. Although there has been a significant push to expand online access, 72% of individuals either did not view their medical record or were not offered online access to it within the last 12 months.[135] Seventy-six percent of caregivers have not accessed their care recipient's online medical record in the past 12 months. Individuals cited a preference to speak with their health care provider directly (76%), not having a need to use their online medical record (59%), security concerns (25%), and lack of a way to access the online medical record (20%) as the top reasons they did not access it.[136]

While increased availability of patient portals has enabled patients to access more of their health information, gaps remain. Often, only some of a patient's health information is available through a patient portal. In addition, the information available through portals varies across provider organizations.[137] Portals are often siloed and tethered to a particular organization, making it difficult for patients to aggregate and maintain their information.

Use and Sharing of PGHD and Other Data from Mobile Devices

Patients are beginning to use devices and apps to manage their health information and health care. The U.S. Government Accountability Office (GAO) found that as of 2017, one-third of individuals used an electronic device for monitoring their health and one-third of smartphone or tablet owners used their devices to discuss their health with their health care provider. Nearly one in five smartphone, tablet, or electronic monitoring device owners shared health information collected by their devices with a health professional. The GAO also found that of individuals who accessed their medical record online, less than 5% transmitted their health record data to a service or app.[138]

However, patients still face a variety of challenges to sharing their PGHD with their providers. Many provider organizations lack the technical infrastructure, functional workflows, workforce capacity, and training to receive and use the data. Many patients do not understand the value of capturing and sharing PGHD with providers. Some patients have privacy and security concerns that make them to unwilling to share PGHD with their providers.[139] Patient-reported outcomes (PROs), a type of PGHD, are commonly

collected within clinical trials but less commonly in clinical care. However, some providers, oncologists for example, are starting to use PROs in non-research settings to improve clinical care.[140]

Need to Improve Alignment of Timing of Planning Activities with Operational Impact of Technology Development

Frameworks and programs encouraging patient access to information may not align with the development timeline for needed technical capabilities across the industry. Stakeholders have frequently communicated to ONC and CMS that health IT developers and providers need 18 to 24 months from the issuance of final rules or guidance to be able to safely and efficiently implement required changes to health IT systems and then test and deploy these updated products into the workflow of providers.[141] Some changes, such as patient-facing APIs, will require significant new development by health IT developers and providers. In addition, changes to patient access to information can require time for providers to appropriately educate patients about new functionality available to them.

Potential for Lack of Net Neutrality Due to Market Forces

In 2015, the FCC reclassified Internet service providers as "common carriers" similar to phone services, effectively prohibiting them from blocking or slowing down access to particular online content or services. The FCC rule about net neutrality also noted that Internet service providers could not charge service providers or customers more to throttle speeds or block or slow down the flow of specific content.

The rollback of net neutrality protections in 2018 when the FCC regulation was repealed has created an environment of uncertainty in the marketplace for Internet access[142] and stimulated debate about the impact on health care providers and patients. Some stakeholders worry that the change will create an uneven playing field in the health care industry that advantages some health care organizations and developers over others and hinders the ability of new, innovative companies to compete. For example, Internet services providers could charge additional fees to certain companies thereby reducing competition or offer better services to a particular hospital in a region, helping them become the dominant telehealth provider in that region. Higher costs and slower speeds could make it more difficult for health care providers treating underserved populations to be able to exchange data and to make it easily available to patients.[143] The use of telehealth services and the sharing of medical information requiring high bandwidth, such as radiology images, could be negatively affected.[144]

Some state governments are passing laws to encourage continued open access to the Internet[145] but these directives may be in conflict with the new FCC regulation.[146] Some members of Congress are considering taking action to reinstate net neutrality while some technology companies have filed lawsuits.[147]

Recommendations for Addressing Health IT Infrastructure Gaps

The Cures Act requires recommendations for addressing the identified gaps in policies and resources for achieving the ONC FY18 objectives and benchmarks and furthering interoperability throughout the health information technology infrastructure. The HITAC offers the following suggestions for HITAC activities that could result in future recommendations that would be transmitted to the National Coordinator.

Priority Target Area: Interoperability

Opportunity: Address "reality gap" between the perception of what has been certified for a system and what is truly interoperable in the field.

For example, continued mapping of C-CDA data is required when integrating networks and sharing data among smaller providers who may lack resources to upgrade their systems.

> **Recommended HITAC Activity: Evaluate whether systems are truly interoperable at both content and transport levels after implementation, especially among smaller practices and by patients to establish measures in the future.**

Other Opportunities for Further Consideration

- Establish usability metrics for health information exchange.
- Expand priority use cases to meet the needs of additional care settings and stakeholder groups.
- Address alignment of timeliness of guidelines and development of technology.
- Identify incentives across stakeholder groups to improve the level of interoperability and data quality.
- Offer support for increased broadband access across stakeholder groups, especially underserved populations.
- Consider how to improve patient matching when sharing data.

Priority Target Area: Privacy and Security

Opportunity: Consider appropriate policies for the Internet of Things (IoT).

The IoT in health care offers many benefits but further clarification may be needed around third-party access of IoT data.

> **Recommended HITAC Activity: Identify areas of IoT use that would benefit from guidance and examples of success in the health care industry.**

Opportunity: Offer support for and education of technology users regarding privacy and security protections, including for health and other information shared on social media.

Although social media platforms can enable collaboration, users are also vulnerable to privacy breaches and misuse of their health information.

> **Recommended HITAC Activity: Identify educational approaches, technological mitigators, and potential regulatory solutions that offer improved privacy and security protections.**

Opportunity: Increase uniformity of information sharing policies across states.

For example, the California Consumer Privacy Act of 2018 may have nationwide implications as data are exchanged across state lines and if other states pass similar legislation.

> **Recommended HITAC Activity: Review and make recommendations about the federal role in setting guidelines for the exchange of data across states.**

Opportunity: Offer support for widespread adoption of cybersecurity framework(s).

> **Recommended HITAC Activity: Review and make recommendations about the impact of nationwide adoption of cybersecurity framework(s) and delineate cybersecurity accountability for data by role within the health IT infrastructure.**

Opportunity: Consider options for granular levels of consent to share and disclose information.

Current consent form collection and storage practices are static and not aligned with data in motion, i.e., consent should flow with the data. Additionally, the design and use of consent forms need to become more user-centered.

> **Recommended HITAC Activity: Undertake a review of emerging consent approaches and the technologies that underpin them, and make recommendations for the improvement of current consent approaches.**

Other Opportunities for Further Consideration

- Address implications of European Union's General Data Protection Regulation (GDPR) and Privacy Shield.
- Enhance education about HIPAA and Confidentiality of Substance Use Disorder Patient Records (a.k.a. 42 CFR Part 2) regulation implications.
- Consider how to improve patient matching when sharing data.

Priority Target Area: Patient Access to Information

Opportunity: Support infrastructure needs for underserved populations, including exchange costs, prevalence of electronic equipment, Internet access, pharmacy services, and use of telehealth services.

> **Recommended HITAC Activity: Evaluate impact of monetization of data exchange to establish measures in the future.**

Opportunity: Consider improvements to accessibility and usability of patient portals and other patient-facing technology.

> **Recommended HITAC Activity: Evaluate patient portal operational effectiveness, patient engagement, and/or patient understanding and use of data to establish measures in the future.**

Opportunity: Encourage patient and caregiver education about health IT resources.

Recommended HITAC Activity: Identify use cases demonstrating the value of patient's data to the patient.

Other Opportunities for Further Consideration

- Consider workflow and technology improvements to increase use and sharing of PGHD and other data from mobile devices, remote sensors, and other data-generating tools.
    - For example, measure the impact of clinical grade data collected by patients on clinical testing costs.
- Better align the timing of planning activities with operational impact.
- Consider the implications of varying experiences with net neutrality at national, state, and local levels.

Suggestions for Additional HITAC Initiatives

The HITAC did not identify additional HITAC initiatives as defined in the Cures Act in FY18. The HITAC will revisit this opportunity in the FY19 annual report.

Conclusion

Although in FY18 significant progress was made in advancing interoperability, privacy and security, and patient access to information, work remains in these priority target areas to achieve the full potential using health IT tools to help transform the health care sector. In FY19, ONC and the HITAC will continue to focus on advancing the implementation of the health IT provisions of the Cures Act including information blocking, certification enhancements, and the Trusted Exchange Framework and Common Agreement, as well as address emerging issues.

Appendices

Glossary

Application Programming Interface (API) – A set of tools, definitions, and protocols for building and integrating application software. It lets a product or service communicate with other products and services without needing to know how they're implemented.[148]

Common Agreement – A set of terms and conditions for health information exchange between health information networks (HINs) set by the Recognized Coordinating Entity as required by the Cures Act.[149]

Consolidated Clinical Document Architecture (C-CDA) – A document standard for the transmission of structured summary data between providers, and between providers and patients. Transmitted data supports care transitions, referrals and care coordination.[150]

Fast Healthcare Interoperability Resources (FHIR®) Standard – An interface specification that specifies the content of the data exchanged between health care applications, and how the exchange is implemented and managed.[151] The data exchanged includes clinical data as well as health care-related administrative, public health, and research data.

Health Information Exchange (HIE) – Both the act of moving health data electronically between organizations and an organization that facilitates information exchange. HIEs may be statewide, regional, metropolitan, or organization-specific and may be privately owned or publicly funded.[152, 153]

Health Information Network (HIN) – An individual or entity that:

a) Determines, oversees, or administers policies or agreements that define business, operational, technical, or other conditions or requirements for enabling or facilitating access, exchange, or use of Electronic Health Information between or among two or more unaffiliated individuals or entities;
b) Provides, manages, or controls any technology or service that enables or facilitates the exchange of Electronic Health Information between or among two or more unaffiliated individuals or entities; or
c) Exercises substantial influence or control with respect to the access, exchange, or use of Electronic Health Information between or among two or more unaffiliated individuals or entities.[154]

Information Blocking – The Cures Act defines the term 'information blocking' as a practice that:

(A) Is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and
(B) (i) If conducted by a health information technology developer, exchange, or network, such developer, exchange, or network knows, or should know, that such practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information; or

(ii) if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.[155]

Internet of Things – The networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet[156]

Interoperability – The Cures Act defines interoperability, with respect to health information technology, as such health information technology that:

1) Enables the secure exchange of electronic health information with, and use of electronic health information from, other health information technology without special effort on the part of the user;
2) Allows for complete access, exchange, and use of all electronically accessible health information for authorized use under applicable State or Federal law; and
3) Does not constitute information blocking as defined in section 3022(a).[157, 158]

Logical Observation Identifiers Names and Codes (LOINC) – A common language (set of identifiers, names, and codes) for identifying health measurements, observations, and documents[159]

Medical Device – An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease.[160]

Patient-Generated Health Data (PGHD) – Patient-generated health data (PGHD) are health-related data created, recorded, or gathered by or from patients (or family members or other caregivers) to help address a health concern.[161] Patients may also collect data for their own interest.

Qualified Health information Network (QHIN) – A network of organizations working together to share data to implement the Trusted Exchange Framework, having agreed to the Common Agreement.[162]

Recognized Coordinating Entity (RCE) – The RCE will act as a governance body that will operationalize the Trusted Exchange Framework by incorporating it into a single, all-encompassing Common Agreement to which Qualified HINs will agree to abide.

Trusted Exchange Framework (TEF) – A set of principles and minimum required terms and conditions for trusted exchange as required by the Cures Act.[163]

U.S. Core Data for Interoperability (USCDI) – A common set of data classes that are required for interoperable exchange. The USCDI will be expanded over time.[164]

Usability – The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.[165]

Resources

HITAC Materials

HITAC Policy Framework

Trusted Exchange Framework Taskforce Recommendations

U.S. Core Data for Interoperability Task Force recommendations

ONC Publications

2018 Report to Congress: Annual Update on the Adoption of a Nationwide System for the Electronic Use and Exchange of Health Information

Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024: White Paper, Practical Guide, and Infographics

Health IT Data Briefs

The Guide to Getting and Using Your Health Records
Practical tips to help patients access, review, and make the most of their health records

Health IT Playbook

Health IT Privacy and Security Resources for Providers

Health IT Quick-Stats

Interoperability Standards Advisory

Notice of Proposed Rulemaking to Improve the Interoperability of Health Information

Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs (draft)

Trusted Exchange Framework

OCR Publications

HIPAA Security Rule to NIST Cybersecurity Framework Crosswalk

Cybersecurity Guidance

HHS ONC/OCR Security Risk Assessment (SRA) Tool 3.0

Get It. Check It. Use It.
National education campaign about patients' rights to access their health information

NIST Publications

NIST Cybersecurity Framework

NIST Privacy Framework

HITAC Member List

Carolyn Petersen,* Co-Chair, Individual
Robert Wah, Co-Chair, DXC Technology
Michael Adcock, Member, University of Mississippi Medical Center
Christina Caraballo,* Member, Audacious Inquiry
Tina Esposito, Member, Advocate Health Care
Cynthia A. Fisher, Member, WaterRev, LLC
Brad Gescheider, Member, PatientsLikeMe
Valerie Grey, Member, New York eHealth Collaborative
Anil K. Jain, Member, IBM Watson Health
John Kansky, Member, Indiana Health Information Exchange
Kensaku Kawamoto, Member, University of Utah Health
Steven Lane, Member, Sutter Health
Leslie Lenert, Member, Medical University of South Carolina
Arien Malec, Member, Change Healthcare
Denni McColm, Member, Citizens Memorial Healthcare
Clem McDonald, Member, National Library of Medicine
Aaron Miri,* Member, The University of Texas at Austin, Dell Medical School and UT Health Austin
Brett Oliver,* Member, Baptist Health
Terrence O'Malley, Member, Massachusetts General Hospital
Raj Ratwani, Member, MedStar Health
Steve L. Ready, Member, Norton Healthcare
Patrick Soon-Shiong, Member, NantHealth
Sasha TerMaat, Member, Epic
Andrew Truscott, Member, Accenture
Sheryl Turney, Member, Anthem Blue Cross Blue Shield
Denise Webb, Member, Marshfield Clinic Health System
Kate Goodrich, Federal Representative, Centers for Medicare and Medicaid Services (CMS)
Chesley Richards,* Federal Representative, Centers for Disease Control and Prevention
Ram Sriram, Federal Representative, National Institute of Standards and Technology
Lauren Thompson, Federal Representative, DoD/VA Interagency Program Office

* Annual Report Workgroup Member

Acknowledgements

Kory Mertz, Audacious Inquiry
Michelle Murray, ONC
Seth Pazinski, ONC
Lauren Richie, ONC
Kate Ricker-Kiefert, Audacious Inquiry

References

[1] Kawamoto, K. & Lane, S. (2018, September 5). *Interoperability Standards Priorities Task Force Update* [Presentation]. Retrieved from https://www.healthit.gov/sites/default/files/facas/2018-09-05_HITAC_ISP_TaskForce_Presentation_508.pdf
[2] Office of the National Coordinator for Health Information Technology. (2017). *Non-Federal Acute Care Hospital Electronic Health Record Adoption*. Retrieved from https://dashboard.healthit.gov/quickstats/pages/FIG-Hospital-EHR-Adoption.php
[3] Office of the National Coordinator for Health Information Technology. (2016). *Office-Based Physician Electronic Health Record Adoption*. Retrieved from https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php
[4] Rucker, D., & Searcy, T. (2018, October 25). *Acute Care Hospitals Are More Interoperable Than Ever but Challenges Remain*. Retrieved from www.healthit.gov/buzz-blog/interoperability/acute-care-hospitals-are-more-interoperable-than-ever-but-challenges-remain/
[5] Adler-Milstein, J., Sunny C. L., & Ashish K. J. (2016, July). The Number of Health Information Exchange Efforts Is Declining, Leaving The Viability Of Broad Clinical Data Exchange Uncertain. *Health Affairs, 35*(7). Retrieved from www.healthaffairs.org/doi/10.1377/hlthaff.2015.1439
[6] Office of the National Coordinator for Health Information Technology. (n.d.). *U.S. Core Data for Interoperability (USCDI).* Retrieved from https://www.healthit.gov/isa/us-core-data-interoperability-uscdi
[7] HL7 International. (2017). *Welcome to FHIR®. Introduction to HL7 Standards*. Retrieved from www.hl7.org/fhir
[8] HL7 International. (2018). *Argonaut Project Background. HL7 Argonaut Project Wiki.* Retrieved from HL7 wiki: http://argonautwiki.hl7.org/index.php?title=Main_Page%2FBackground
[9] Kubick, W. (2018, September 25). *The Standard: Another Type of Moonshot: Project Gemini.* Retrieved from http://blog.hl7.org/another_type_of_moonshotproject_gemini
[10] HL7 International. (2018). *About the DaVinci Project.* Retrieved from http://www.hl7.org/about/davinci/index.cfm
[11] DirectTrust. (2018, May 21). *Using Direct Trust to Establish a Trusted Exchange Framework for FHIR.* Retrieved from https://directtrust.app.box.com/s/2557qrkhudd3trj1hzkamhkxx5p1ht56
[12] Carequality. (2018, October 10). *FHIR Technical & Policy Workgroups Forming Now* [Blog Post]. Retrieved from *https://*carequality.org/fhir-technical-policy-workgroups-forming-now/
[13] Wright, A. (2018, February 20). *Ready, Aim, FHIR! How CommonWell Is Using FHIR.* Retrieved from www.commonwellalliance.org/blog/how-commonwell-is-using-fhir/
[14] Patel V. & Johnson C. (2018, April). Individuals' use of online medical records and technology for health needs. *ONC Data Brief, no.40.* Office of the National Coordinator for Health Information Technology: Washington DC.
[15] Baldwin, J., Singh, H., Sittig, D., & Giardina, T. (2017, September). Patient portals and health apps: Pitfalls, promises, and what one might learn from the other. *Healthcare 5*(3). doi: 10.1016/j.hjdsi.2016.08.004
[16] Surescripts. (2016). *2016 Connected Care and the Patient Experience*. Retrieved from https://www.slideshare.net/surescripts/2016-connected-care-and-the-patient-experience-70073294
[17] Ibid.
[18] Patel V., Hughes, P., Savage, L., & Barker W. (2015, June). Individuals' Perceptions of the Privacy and Security of Medical Records. *ONC Data Brief, no.27*. Office of the National Coordinator for Health Information Technology: Washington DC
[19] Office of the National Coordinator for Health Information Technology. (2018). *Health IT Privacy and Security Resources for Providers*. Retrieved from www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers
[20] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.) *HIPAA and Care Coordination.* Retrieved from https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/index.html
[21] Office of the National Coordinator for Health Information Technology. (2015). *2015 Update to Congress on the Adoption of Health Information Technology*. Retrieved from https://dashboard.healthit.gov/report-to-congress/2015-update-adoption-health-information-technology-full-text.php
[22] Mello, M., Adler-Milstein, J., Ding, K.., & Savage, L. (2018). Legal Barriers to the Growth of Health Information Exchange-Boulders or Pebbles?. *Milbank Quarterly 96*(1). doi: 10.1111/1468-0009.12313
[23] IETF. (2018, August). *OAuth2.0.* Retrieved from https://oauth.net
[24] OpenID. (n.d.) *Welcome to OpenID Connect.* Retrieved from https://openid.net/connect/
[25] Office of the National Coordinator for Health Information Technology. (2018). *Patient-Generated Health Data*. Retrieved from www.healthit.gov/topic/scientific-initiatives/patient-generated-health-data
[26] Comstock, J. (2016, January 14). *At FTC's PrivacyCon, Concerns About the Monetization of Consumer Health Data.* Retrieved from https://www.mobihealthnews.com/content/ftcs-privacycon-concerns-about-monetization-consumer-health-data
[27] Office of the National Coordinator for Health Information Technology. (2018, January). *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024: Practical Guide*. Retrieved from www.healthit.gov/sites/default/files/onc_pghd_practical_guide.pdf
[28] Substance Abuse and Mental Health Services Administration. (2018, January 3). *Confidentiality of Substance Use Disorder Patient Records*. Retrieved from https://www.federalregister.gov/documents/2018/01/03/2017-28400/confidentiality-of-substance-use-disorder-patient-records
[29] Substance Abuse and Mental Health Services Administration. (2013, July). *Confidentiality Regulations FAQs. Stages of Community Readiness.* Retrieved from www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs
[30] Mello, M., Adler-Milstein, J., Ding, K., & Savage, L. (2018). Legal Barriers to the Growth of Health Information Exchange-Boulders or Pebbles?. *Milbank Quarterly 96*(1). doi: 10.1111/1468-0009.12313
[31] Ibid
[32] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.) *Information Related to Mental and Behavioral Health, including Opioid Overdose.* Retrieved from https://www.hhs.gov/hipaa/for-individuals/mental-health/index.html
[33] Na, L., Yang, C., Lo, C., Zhao, F., Fukuoka, Y., & Aswani, A. (2018, December 21). Feasibility of Reidentifying Individuals in Large National

Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning. *JAMA Network Open. 1*(8):e186040. doi:10.1001/jamanetworkopen.2018.6040

[34] Song, K. (2018, August 4). *4 Risks consumers need to know about DNA testing kit results and buying life insurance.* Retrieved from https://www.cnbc.com/2018/08/04/4--risks-consumer-face-with-dna-testing-and-buying-life-insurance.html

[35] Wyoming, H. B. 119 (2018).

[36] Louisiana, S. B. 442 (2018).

[37] Arizona, Chapter §20-1051 et seq.

[38] The Pew Charitable Trusts. (2018, October). *Enhanced Patient Matching Is Critical to Achieving Full Promise of Digital Health Records*. Retrieved from www.pewtrusts.org/-/media/assets/2018/09/healthit_enhancedpatientmatching_report_final.pdf

[39] Office of the National Coordinator for Health Information Technology. (2018, February 9). *2015 Edition Common Clinical Data Set - 45 CFR 170.102 2015 Edition Certification Companion Guide.* Retrieved from www.healthit.gov/sites/default/files/topiclanding/2018-04/2015Ed_CCG_CCDS.pdf

[40] Dooling, J. & Stambaugh, R. (2018, December 27). *Temporary Newborn Name Compliance: A Focus on Patient Safety* [Blog post]. Retrieved from http://journal.ahima.org/2018/12/27/temporary-newborn-name-compliance-a-focus-on-patient-safety/

[41] United States Government Accountability Office. (2019, January). *Health Information Technology: Approaches and Challenges to Electronically Matching Patients' Records across Providers*. Retrieved from https://www.gao.gov/products/GAO-19-197

[42] Centers for Medicare and Medicaid Services. (2018, July 9). *Emergency Preparedness Rule*. Retrieved from www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Emergency-Prep-Rule.html

[43] Office of the National Coordinator for Health Information Technology. (2018). *Security Risk Assessment Tool*. Retrieved from www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

[44] Gettinger, A. (2017, November 15). *Reflections from a Health IT Perspective on Disaster Response* [Blog post]. Retrieved from https://www.healthit.gov/buzz-blog/uncategorized/reflections-health-perspective-disaster-response

[45] Patel V. & Johnson C. (2018, April). Individuals' use of online medical records and technology for health needs. *ONC Data Brief, no.40.* Office of the National Coordinator for Health Information Technology: Washington DC.

[46] Ibid

[47] Centers for Medicare and Medicaid Services. (2018, March). *Fact Sheet Trump Administration Announces MyHealthEData Initiative at HIMSS18*. Retrieved from www.cms.gov/newsroom/fact-sheets/trump-administration-announces-myhealthedata-initiative-himss18

[48] Centers for Medicare and Medicaid Services. (2018, March). *Trump Administration Announces MyHealthEData Initiative to Put Patients at the Center of the US Healthcare System* [Press release]. Retrieved from www.cms.gov/newsroom/press-releases/trump-administration-announces-myhealthedata-initiative-put-patients-center-us-healthcare-system

[49] Centers for Medicare and Medicaid Services. (2018). *Blue Button 2.0*. Retrieved from https://bluebutton.cms.gov

[50] Centers for Medicare and Medicaid Services. (2018). *Blue Button 2.0, Blue Button API Docs*. Retrieved from https://bluebutton.cms.gov/developers/

[51] U.S. Department of Veterans Affairs. (2018). *Just Released! Mobile Blue Button.* Retrieved from https://mobile.va.gov/content/just-released-mobile-blue-button

[52] Apple, Inc. (n.d.). *Healthcare - Health Records*. Retrieved from https://www.apple.com/healthcare/health-records

[53] Research 2 Guidance. (2017, November). *mHealth App Economics 2017: Current Status and Future Trends in Mobile Health.* Retrieved from https://research2guidance.com/325000-mobile-health-apps-available-in-2017/

[54] Office of the National Coordinator for Heath Information Technology. (2018, January). *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024*. Retrieved from https://www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf

[55] Food and Drug Administration. (n.d.) *Digital Health Software Precertification (Pre-Cert) Program.* Retrieved from https://www.fda.gov/medicaldevices/digitalhealth/digitalhealthprecertprogram/default.htm

[56] Office of the National Coordinator for Health Information Technology. (2018). *Patient-Generated Health Data*. Retrieved from www.healthit.gov/topic/scientific-initiatives/patient-generated-health-data

[57] Robeznieks, A. (2018, June 15*). Key First Steps Taken to Unleash Digital Medicine's Potential.* Retrieved from https://www.ama-assn.org/practice-management/digital/key-first-steps-taken-unleash-digital-medicines-potential

[58] Office of the National Coordinator for Health Information Technology. (2018). *Patient-Generated Health Data*. Retrieved from www.healthit.gov/topic/scientific-initiatives/patient-generated-health-data

[59] Ibid

[60] Daniel, H., Bornstien S., & Kane G. (2018, April). Addressing Social Determinants to Improve Patient Care and Promote Health Equity: An American College of Physicians Position Paper. *Annals of Internal Medicine 168*(8):577-578. doi: 10.7326/M17-2441

[61] NowPow (n.d.). Retrieved from http://www.nowpow.com/

[62] Gottlieb, L., Sandel, M., & Adlers, N. E. B. (2013). Collecting and Applying Data on Social Determinants of Health in Health Care Settings. *JAMA Internal Medicine 173*(11) Retrieved from web.pdx.edu/~nwallace/CRHSP/CollectingSDH.pdf

[63] National Association of Community Health Center. (n.d.). *PRAPARE.* Retrieved from http://www.nachc.org/research-and-data/prapare/

[64] Ibid

[65] LOINC. (n.d.). *Social Determinants of Health.* Retrieved from https://loinc.org/sdh/

[66] Raths, D. (2018, November 28). *CARIN Alliance Creates Code of Conduct for Third-Party Apps. Retrieved* from https://www.healthcare-informatics.com/news-item/carin-alliance-creates-code-conduct-third-party-apps

[67] The Pew Charitable Trusts, American Medical Association, & Medstar Health. (2018, August). *Rigorous Testing and Establishment of Voluntary Criteria Can Protect Patients.* Retrieved from https://www.pewtrusts.org/en/research-and-analysis/reports/2018/08/28/ways-to-improve-electronic-health-record-safety

[68] Pronovost, P., Johns, M., Palmer, S., Bono, R., Fridsma, D., Gettinger, A., et al. (2018). *Procuring Interoperability: Achieving High-Quality, Connected, and Person-Centered Care*. Washington, DC: National Academy of Medicine.
[69] Kruse, C., Mileski, M., Vijaykumar, A., Viswanathan, S., Suskandla, U., & Chidambaram, Y. (2017, September 29). Impact of Electronic Health Records on Long-Term Care Facilities: Systematic Review. *JMIR Medical Informatics 5*(3): e35. doi: 10.2196/medinform.7958
[70] Gettinger, A., & Goodrich, K. (2018, November 28). *Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs: Released for Public Comment* [Blog post]. Retrieved from https://www.healthit.gov/buzz-blog/health-it/strategy-on-reducing-regulatory-and-administrative-burden-relating-to-the-use-of-health-it-and-ehrs-released-for-public-comment
[71] Office of the National Coordinator for Heath Information Technology. (2017, September). *Detailed Analysis of Current Trust Agreements*. Retrieved from www.healthit.gov/sites/default/files/analysis_of_existing_trust_arrangements_printable.pdf
[72] Office of the National Coordinator for Heath Information Technology. (2016, September). *State HIE Consent Policies: Opt-In or Opt-Out*. Retrieved from www.healthit.gov/sites/default/files/State%20HIE%20Opt-In%20vs%20Opt-Out%20Policy%20Research_09-30-16_Final.pdf
[73] Office of the National Coordinator for Heath Information Technology. (2016, September). *State-Sponsored Health Information Exchange (HIE) Organizations' Consent Policies: Opt-In or Opt-Out.* Retrieved from www.healthit.gov/sites/default/files/Individual%20State%20HIE%20Organizations%20Consent%20Policy_20160930_FINAL.PDF
[74] Office of the National Coordinator for Heath Information Technology. (2017, September). *Detailed Analysis of Current Trust Agreements*. Retrieved from www.healthit.gov/sites/default/files/analysis_of_existing_trust_arrangements_printable.pdf
[75] U.S. Government Accountability Office. (2015, September). *Nonfederal Efforts to Help Achieve Health Information Interoperability*. Retrieved from www.gao.gov/assets/680/672585.pdf
[76] Torkzadeh, R. (2018). Advancing a Nationwide Patient Matching Strategy. *Journal of AHIMA 89*(7), 30-35. Retrieved from bok.ahima.org/doc?oid=302539#.W5_CDOhKjIU
[77] U.S. Government Accountability Office. (2015, September). *Nonfederal Efforts to Help Achieve Health Information Interoperability*. Retrieved from www.gao.gov/assets/680/672585.pdf
[78] Office of the National Coordinator for Health Information Technology. (2015, April). *Report to Congress: Report on Health Information Blocking*. Retrieved from www.healthit.gov/sites/default/files/reports/info_blocking_040915.pdf
[79] Centers for Medicare and Medicaid Services. (2017). *The Merit-Based Incentive Payment System (MIPS) Advancing Care Information Prevention of Information Blocking Attestation: Making Sure EHR Information Is Shared*. Retrieved from www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/MACRA-MIPS-and-APMs/ACI-Information-Blocking-fact-sheet.pdf
[80] Centers for Medicare and Medicaid Services. (2017, November). *The Medicare and Medicaid Promoting Interoperability Programs Prevention of Information Blocking Attestation Fact Sheet*. Retrieved from www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_InformationBlockingFact-Sheet20171106.pdf
[81] Monica, K. (2017, March). *Health Information Exchanges Report Information Blocking.* Retrieved from https://ehrintelligence.com/news/health-information-exchanges-report-information-blocking
[82] Devine E., Totten A., Gorman P., Eden K., Kassakian S., Woods, S., et al. (2017). Health Information Exchange Use (1990-2015): A Systematic Review. *eGEMs*. (1):27. DOI: http://doi.org/10.5334/egems.249
[83] National Quality Forum. (2017, September). *Interoperability 2016-2017 Final Report*. Retrieved from www.qualityforum.org/Publications/2017/09/Interoperability_2016-2017_Final_Report.aspx
[84] Pylypchuk Y., Johnson C., Henry J., & Ciricean, D. (2018, November). Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2017. *ONC Data Brief, no.42.* Office of the National Coordinator for Health Information Technology: Washington DC.
[85] Jamoom, E.W. & Yang, N. (2016, October). *State Variation in Electronic Sharing of Information in Physician Offices: United States, 2015*. NCHS data brief, no 261. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/27805548
[86] Alvarado, C. S., Zook, K., & Henry, J. (2017, September). Electronic Health Record Adoption and Interoperability among U.S. Skilled Nursing Facilities in 2016. *ONC Data Brief, no. 39.* Office of the National Coordinator for Health Information Technology: Washington, DC.
[87] Patel V., Pylypchuk Y., Henry J., & Searcy T. (2016, July) Variation in Interoperability among U.S. Non-federal Acute Care Hospitals in 2015. *ONC Data Brief, no.37*. Office of the National Coordinator for Health Information Technology: Washington DC.
[88] Ibid
[89] National Institute of Standards and Technology. (2018, June). NIST Big Data Interoperability Framework: Volume 4, Security and Privacy. *Special Publication 1500-4rl*. Retrieved from https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-4r1.pdf
[90] Office of the National Coordinator for Health Information Technology. (2018, January). *Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process*. Retrieved from https://www.healthit.gov/sites/default/files/draft-uscdi.pdf
[91] Federal Communications Commission. (2018, February). *2018 Broadband Deployment Report*. Retrieved from www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report
[92] Chacko, A., Hayajneh, T. (2018, July 23). Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology. (4)14 http://doi.org/10.4108/eai.13-7-2018.155079.
[93] Ibid
[94] National Committee on Vital and Health Statistics. (2017, December 13*). Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges.* Retrieved from https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf
[95] Food and Drug Administration, Center for Devices and Radiological Health. (2018). *Digital Health - Cybersecurity*. Retrieved from www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm
[96] Collaboration of the Health IT Policy and Standards Committees, API Task Force. (2016, May 12*). Application Programming Interface (API) Task Force Recommendations.* Retrieved from https://www.healthit.gov/sites/default/files/facas/HITJC_APITF_Recommendations.pdf
[97] Connolly, J. L., Christey, S. M., Daldos, R., Zuk, M., & Chase, M. P. (2018, October*). Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*. Retrieved from https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

[98] Davis, J. (2018, November). *AMIA Calls for Federal Alignment of Health Data Privacy Policies.* Retrieved from https://healthitsecurity.com/news/amia-calls-for-federal-alignment-of-health-data-privacy-policies
[99] Hollis, K. (2016, July 20). To Share or Not to Share: Ethical Acquisition and Use of Medical Data. *AMIA Joint Summits on Translational Science Proceedings. 2016:* 420–427. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5001759/
[100] Tanner, A. (2017, January 10). Strengthening Protection of Patient Medical Data. Retrieved from https://tcf.org/content/report/strengthening-protection-patient-medical-data/
[101] Voas, J., Kuhn, R., Laplante, P., & Applebaum, S. (2018, October 17). Internet of Things (IOT) Concerns. *National Institute of Standards and Technology Cybersecurity White Paper.* Retrieved from https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft
[102] Milken Institute School of Public Health. (2012*). Health Information & the Law: States*. Retrieved from www.healthinfolaw.org/state
[103] Office of the National Coordinator for Heath Information Technology. (2016, September). *State HIE Consent Policies: Opt-In or Opt-Out*. Retrieved from www.healthit.gov/sites/default/files/State%20HIE%20Opt-In%20vs%20Opt-Out%20Policy%20Research_09-30-16_Final.pdf
[104] Mello, M., Adler-Milstein, J., Ding, K., and Savage, L. (2018). Legal Barriers to the Growth of Health Information Exchange-Boulders or Pebbles?. *Milbank Quarterly 96*(1). doi: https://doi.org/10.1111/1468-0009.12313
[105] Wagner, P., & Kim, D. (2018, July). How Will the New California Consumer Privacy Act of 2018 Will Affect Your Business?. *The National Law Review*. Retrieved from www.natlawreview.com/article/how-will-new-california-consumer-privacy-act-2018-will-affect-your-business
[106] Ibid
[107] HIMSS. (2018). *2017 HIMSS Cybersecurity Survey*. Retrieved from www.himss.org/sites/himssorg/files/2017-HIMSS-Cybersecurity-Survey-Final-Report.pdf
[108] Caine, K. & Hanania, R. (2012). Patients want granular privacy control over health information in electronic medical records. *Journal of American Medical Informatics Association 20(1)*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555326/
[109] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment: Individual Choice.* Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/individualchoice.pdf
[110] Caine, K. & Hanania, R. (2012). Patients want granular privacy control over health information in electronic medical records. *Journal of American Medical Informatics Association 20(1)*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555326/
[111] Office of the National Coordinator for Health Information Technology. (n.d.). *2015 Edition Final Rule: Data Segmentation for Privacy (DS4P).* Retrieved from www.healthit.gov/sites/default/files/2015editionehrcertificationcriteriads4p_10615.pdf
[112] Office of the National Coordinator for Health Information Technology. (2018, October). *The Patient Choice Technical Project Homepage*. Retrieved from https://oncprojectracking.healthit.gov/wiki/display/PATCH/The+Patient+Choice+Technical+Project+Homepage
[113] Office of the National Coordinator for Health Information Technology. (n.d.). *2015 Edition Final Rule: Data Segmentation for Privacy (DS4P).* Retrieved from www.healthit.gov/sites/default/files/2015editionehrcertificationcriteriads4p_10615.pdf
[114] Office of the National Coordinator for Health Information Technology. (2018). [Data file]. Retrieved from https://chpl.healthit.gov
[115] U.S. Department of Health and Human Services, Office for Civil Rights. (2017, September 12). *Can a minor child's doctor talk to the child's parent about the patient's mental health status and needs?.* Retrieved from https://www.hhs.gov/hipaa/for-professionals/faq/2092/can-minor-childs-doctor-talk-childs-parent-about-patients-mental-health-status-and-needs.html
[116] Davis, J. (2018, March). *Europe's GDPR Privacy Law Is Coming: Here's What US Health Orgs Need to Know.* Retrieved from www.healthcarefinancenews.com/news/europes-gdpr-privacy-law-coming-heres-what-us-health-orgs-need-know
[117] Ibid
[118] Ibid
[119] Ibid
[120] Armstrong, J. P., & Bywater, A. (2017). *What Healthcare Organizations Should Know About the GDPR*. Retrieved from https://whitepapers.em360tech.com/wp-content/uploads/GDPR-Implications-of-the-GDPR-in-Healthcare-042717-d1.pdf
[121] U.S. Department of Health and Human Services, Office for Human Research Protections. (2018, March 13). *Attachment B – European Union's General Data Protection Regulations.* Retrieved from https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-b-implementation-of-the-european-unions-general-data-protection-regulation-and-its-impact-on-human-subjects-research/index.html
[122] Savage, J. & Isaac, P. (2016, December 9). Office of the National Coordinator for Health Information Technology. *A Road Map for States: Addressing Privacy and Policy Barriers to the Availability and Flow of Electronic Health Information.* Retrieved from www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/roadmap-states-addressing-privacy-policy-barriers-availability-flow-electronic-health-information
[123] National Alliance on Mental Illness. (2014, April 15*). Understanding What HIPAA Means For Mental Illness*. Retrieved from www.nami.org/About-NAMI/NAMI-News/Understanding-What-HIPAA-Means-for-Mental-Illness
[124] Accreditation Council for Pharmacy Education, America's Health Insurance Plans, American Health Information Management Association, American Medical Association, American Medical Informatics Association, Association of Clinicians for the Underserved, et al. (2018, May 9*). Letter to Encourage Language That Ends Patient Safety Issues Related to Patient Matching*. Retrieved from http://Bok.ahima.org/PdfView?Oid=302512
[125] Monica, K. (2018, July). *How to Create a Standardized Nationwide Patient Matching Strategy.* Retrieved from https://ehrintelligence.com/news/how-to-create-a-standardized-nationwide-patient-matching-strategy
[126] Office of the National Coordinator for Health Information Technology. (2013, May). *Understanding the Impact of Health IT Undeserved Communities and Those with Health Disparities*. Retrieved from www.healthit.gov/sites/default/files/hit_disparities_report_050713.pdf
[127] Ibid
[128] Pratt, M. (2018, July). *The Future of Patient Portals.* Retrieved from www.medicaleconomics.com/business/future-patient-portals
[129][129] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.) *Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524.* Retrieved at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html#newlyreleasedfaqs

[130] Office of the National Coordinator for Health Information Technology. (2017). *Improving the Health Records Request Process for Patients*. Retrieved from www.healthit.gov/sites/default/files/onc_records-request-research-report_2017-06-01.pdf
[131] Office of the National Coordinator for Health Information Technology. (2018, April). *The ONC Guide to Getting and Using Your Health Records*. Retrieved from www.healthit.gov/sites/default/files/facas/2018-04-18_HITAC_ConsumerGuide_Presentation-508.pdf
[132] Office of the National Coordinator for Health Information Technology. (2017*). Your Health Information Rights*. Retrieved from www.healthit.gov/topic/privacy-security/your-health-information-rights
[133] U.S. Department of Health and Human Services, Office for Civil Rights. (2017, September 7). *Get it. Check it. Use It.* Retrieved from https://www.hhs.gov/hipaa/for-individuals/right-to-access/index.html
[134] Office of Disease Prevention and Health Promotion. (n.d.). *Health Communication and Health Information Technology*. Retrieved from www.healthypeople.gov/2020/topics-objectives/topic/health-communication-and-health-information-technology
[135] Patel, V. & Johnson, C. (2018, April). Individuals' use of online medical records and technology for health needs. *ONC Data Brief, no.40.* Office of the National Coordinator for Health Information Technology: Washington DC.
[136] Ibid
[137] U.S. Government Accountability Office. (2017, March). *HHS Should Assess the Effectiveness of Its Efforts to Enhance Patient Access to and Use of Electronic Health Information*. Retrieved from https://www.gao.gov/assets/690/683388.pdf
[138] Ibid
[139] Office of the National Coordinator for Heath Information Technology. (2018, January). *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024*. Retrieved from https://www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf
[140] Olsen, K. (2018, May 31). Utilizing Patient-reported Outcomes in Cancer Clinical Trials [Blog post]. Retrieved from https://blog.aacr.org/utilizing-patient-reported-outcomes-in-cancer-clinical-trials/
[141] Zehel, J. (2017, September 6) *Healthcare Accelerators for Startups* [Blog post]. Retrieved from https://www.redoxengine.com/blog/healthcare-accelerators-for-startups/
[142] Vincent, B. & Abbruzzese, J. (2018, December 8). *Net neutrality could get a reprieve once Democrats take control of the House.* Retrieved from https://www.nbcnews.com/tech/tech-news/net-neutrality-could-get-reprieve-once-democrats-take-control-house-n945501
[143] Gaynor, M., Lenert, L., Wilson, K., & Bradner, S. (2017, May 31). Telecommunication Policies May Have Unintended Health Care Consequences [Blog post]. Retrieved from www.healthaffairs.org/do/10.1377/hblog20170531.060342/full/
[144] Ibid
[145] National Conference of State Legislatures. (2018, October 1). *Net Neutrality Legislation in States.* Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-legislation-in-states.aspx
[146] Campbell, F. (2018, August 13). *State Net Neutrality Regulations Are An Exercise in Futility*. Retrieved from https://www.forbes.com/sites/fredcampbell/2018/08/13/state-net-neutrality-regulations-are-an-exercise-in-futility/#1288923d4742
[147] Ibid
[148] Red Hat Inc. (n.d.). *What are APIs?.* Retrieved from. https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces
[149] Office of the National Coordinator for Health Information Technology. (2018, January). *Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process*. Retrieved from https://www.healthit.gov/sites/default/files/draft-uscdi.pdf
[150] HIMSS Interoperability & Standards Practices Task Force. (2014, November 13*). C-CDA Review*. Retrieved from https://www.himss.org/c-cda-review
[151] HL7 International. (2018). *FHIR Exchange Module.* Retrieved from http://www.hl7.org/fhir/exchange-module.html
[152] Terry, K. (2016, January 11). *Health IT Glossary.* Retrieved from https://www.cio.com/article/2985044/healthcare/health-it-glossary.html?page=3
[153] American Medical Informatics Association. (2013, April 7). *Glossary of Acronyms and Terms Commonly Used in Informatics.* Retrieved from https://www.amia.org/glossary
[154] Office of the National Coordinator for Heath Information Technology. (2018, January 5). *Draft Trusted Exchange Framework.* Retrieved from https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf
[155] 21st Century Cures Act, Pub. L. 114-255, 130 Stat. 1033, codified as amended at §§300jj–52.
[156] Merriam-Webster. (n.d.). *Definition of Internet of Things.* Retrieved from https://www.merriam-webster.com/dictionary/Internet%20of%20Things
[157] 21st Century Cures Act, Pub. L. 114-255, 130 Stat. 1033, codified as amended at §§300jj–19a.
[158] Anthony, E.S. % Morris, G. (2018, January 8). *21st Century Cures Act Overview for States*. Retrieved from https://www.healthit.gov/sites/default/files/curesactlearningsession_1_v6_10818.pdf
[159] LOINC. (n.d.). *What LOINC Is.* Retrieved from https://loinc.org/get-started/what-loinc-is/
[160] Food and Drug Administration. (n.d.). *Medical Device Overview.* Retrieved from https://www.fda.gov/forindustry/importprogram/importbasics/regulatedproducts/ucm510630.htm
[161] Office of the National Coordinator for Heath Information Technology. (2018, January 19). *What are patient-generated health data?* Retrieved from https://www.healthit.gov/topic/otherhot-topics/what-are-patient-generated-health-data
[162] Office of the National Coordinator for Heath Information Technology. (2018, January 5). *Draft Trusted Exchange Framework.* Retrieved from https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf
[163] Ibid
[164] Office of the National Coordinator for Health Information Technology. (2018, January). *Draft U.S. Core Data for Interoperability (USCDI) and Proposed Expansion Process*. Retrieved from https://www.healthit.gov/sites/default/files/draft-uscdi.pdf
[165] National Institute of Standards and Technology. *Health IT Usability.* (2017, August 9). Retrieved from https://www.nist.gov/programs-projects/health-it-usability