Health IT Leadership Roundtable:

Future of Interoperability and Secure Consumer Access to Health Care Data

Health IT Leadership Roundtable: Future of Interoperability and Secure Consumer Access to Health Care Data

Executive Summary

Health care clinicians, hospitals, health plans, and consumer advocates all agree – patients should have access to meaningful and actionable health information.

Patients' health information may include medical history, tests performed, family history, and diagnoses and services rendered – information that is critical to enabling more informed patient and clinician health care decision-making, thereby improving quality of care and health outcomes.

However, patients and their clinicians often face challenges in accessing timely and meaningful information that they can use, while also maintaining the privacy and security of this information.

With this in mind, in January 2020, a wide range of organizations representing clinicians, hospitals, health plans, technology companies, and consumer advocates joined together to jointly host a *Leadership Roundtable on the Future of Interoperability and Secure Consumer Access to Health Data* (the Roundtable).[1]

Health IT Leadership Roundtable Host Committee
AMERICAN ACADEMY OF FAMILY PHYSICIANS
AMERICAN COLLEGE OF PHYSICIANS
AMERICAN HEALTH INFORMATION MANAGEMENT ASSOCIATION
AMERICAN HEART ASSOCIATION
AMERICAN HOSPITAL ASSOCIATION
AMERICAN MEDICAL INFORMATICS ASSOCIATION
BLUE CROSS BLUE SHIELD ASSOCIATION
COLLEGE OF HEALTHCARE INFORMATION MANAGEMENT EXECUTIVES
CONSUMER TECHNOLOGY ASSOCIATION
FEDERATION OF AMERICAN HOSPITALS
NATIONAL PARTNERSHIP FOR WOMEN & FAMILIES
PREMIER HEALTHCARE ALLIANCE

The Roundtable sought to provide an opportunity for a diverse set of patients, policymakers, and organizations to find common ground in identifying ongoing patient health information access and interoperability challenges and solutions to those challenges.

This White Paper seeks to summarize many of the key conversations and perspectives raised during the Roundtable event, and recommendations for moving forward. The White Paper: (1) describes the current consumer health information access environment, including recent regulatory efforts to advance consumer access to personal health information through third party applications; (2) highlights efforts to standardize and make available meaningful and actionable health care data; and (3) outlines legislative and regulatory barriers to information sharing in the health care system as identified by the Roundtable.

Key recommendations resulting from the Roundtable discussions include:

- *Education and Engagement*
  - *Administrative, Private Sector* - Create materials to help clinicians and patients better understand the Health Information Portability and Accountability Act (HIPAA), including the Privacy Rule, the delineation between HIPAA and non-HIPAA-covered entities, and notice and consent policies.

- *Privacy and Security*
  - *Administrative* - Establish a public-private partnership to review privacy and security policies for third-party apps and create a Star-rating, or some other indicator, of their commitment to privacy and security of patients' information.

- o *Legislative* - Establish a data privacy structure that ensures health data is protected regardless of whether it is covered by HIPAA, aligning privacy and security rules where possible.
  - o *Legislative* - Create stronger compliance and government enforcement mechanisms for entities not subject to HIPAA and adequate funding for such mechanisms.

- **Data Sharing and Interoperability**
  - o *Private-Sector* – Support for bidirectional information sharing built on a foundation of robust data integrity that would allow patients to add to their health record.
  - o *Legislative/Administrative* – Strengthen consumer discrimination protections related to downstream or secondary uses of data.
  - o *Legislative/Administrative* – Dedicate funding to support standards development by the private-sector for priority data elements and use cases.

Introduction

The health care system is rapidly evolving. New medical innovations, treatments, and technologies – as well as reforms to health care payment and delivery systems – are changing the ways consumers interact with their clinicians and receive care.

The health care system is increasingly reliant on the exchange and transfer of data, allowing researchers to better understand the effectiveness of new treatments or medical devices; clinicians to obtain greater insight into a patient's medical history and to consult with other clinicians on a clinical care team; researchers to access and analyze data to address increasingly complex issues; and for patients to gain access to their health care information to facilitate decision-making and engagement in their health.

Such information interchanges seem simple and logical. However, the laws and standards governing the exchange and transfer of information, and siloed and disaggregated technology and systems underpinning such transfers, are anything but. (*See Appendix for a brief overview.*) The complex rules related to privacy, security, disclosure, and right of access of health care information serve a vital purpose but are not well understood by many in the health care system. They were also largely developed prior to technological advancement and the Internet and when paper medical records were the norm. Meanwhile, the disjointed evolution of information systems and electronic health record (EHR) technology often limits the seamless exchange of information across, within and outside of systems. Finally, our growing understanding of what constitutes 'health information' means that large amounts of health-related information is increasingly captured outside of HIPAA's requirements and patient protections. Thus, many have called for changes or additions to existing regulations to promote greater information sharing.

Most importantly, there is a need to ensure that patients, their providers and their clinicians can understand their health information access rights and responsibilities, have access to meaningful and actionable health information, and that privacy and security is foundational.

To achieve a future world where seamless exchange of health information can help drive health care decision-making and accelerate research and cures, we must bolster patient trust both within in the health care system, as well as with non-traditional actors who touch health information. Patients must trust that only minimally necessary information is collected; that the information provided to their clinicians and other care team members, or shared with third parties, will be kept secure; and that their information will not be inappropriately shared with others, used against them, or used for purposes other than the intended purpose. Further, consumers should be informed about how their health information may be used by those outside the health system. In acknowledging these goals, organizations and entities within the health care system remain committed to assuring and maintaining patients' trust and reflecting

patient choices regarding the privacy and security of their health information while also advancing interoperability.

Below, we describe some of the opportunities and ongoing challenges in ensuring interoperability and patient access to their health care information today.

Advancing Consumer Access to Health Care Information

Health care clinicians, hospitals, health plans, technology companies, and consumer advocates all agree – patients should have access to meaningful and actionable health information. The access, exchange, and use of health information is essential for patients to manage their health care needs and to share information with their clinicians and caregivers.

Providing patients with access is also expected to help individuals to better understand and manage their information and increase their participation in and contribution to clinical research. Studies also have found that when patients have access to their clinician's clinical visit notes, they are more informed about their care, remember what to discuss during doctor visits, feel more in control of their care, and take their medications as prescribed.[2] Other studies show that patients' use of health information is associated with improved patient engagement, satisfaction, and convenience.[3]

Consumer Access and Use of Electronic Medical Records

Today HIPAA-covered entities and business associates must provide patients, upon request, with access to their protected health information (PHI), in the form and format of their choosing. While patients may request hard copies of their records, online access to medical records is often provided through patient portals, release of information services, or through other devices connected to a clinician's EHR system. The current push to enable patient access to their health care information through open access application programming interfaces (APIs) – driven in part by advancements in technology and increasing consumer use of mobile devices to manage all facets of life – is expected to greatly expand opportunities for patients to access and engage with their health care information compared to today.

According to a 2019 report from the Office of the National Coordinator for Health IT (ONC) on access, viewing and use of online medical records, 51 percent of individuals were offered access to their online medical records in 2018.[4] Of the patients offered access to their online medical records, 58 percent viewed their record at least once in the past year.

ONC also found that 75 percent of patients surveyed were encouraged by their clinicians to use online medical records and that those who were encouraged to use their online medical record were almost twice as likely to access it.[5]

According to ONC, of individuals who were offered and viewed their record in 2018, 24 percent said they used their health information to help make a decision about how to treat an illness or condition. Eighty-three percent said their online medical record is useful for monitoring health.[6] In 2017, 85 percent of patients who accessed their medical records did so to view their test results, 62 percent did to perform health-related tasks, 39 percent used to inform their treatment plan, and 14 percent transmitted their record to another entity.[7]

However, several studies have discussed challenges in patient access and use of their online records, citing cumbersome or difficult to use tools, incorrect information with little ability to modify, and inconsistent access to information – as well as concerns about privacy and security of information.[8,9] Surveys have also found that patients are interested in more robust functionality and features of online access.[10] Although ONC found that only three percent of patients who accessed their online medical records in 2017 transmitted their health record information to a service or app,[11] many believe that open-access APIs will encourage the development of many more choices and tools for patients to access and engage with their health care information via mobile applications (apps).

Privacy and Security Concerns

Third party apps, wearable fitness trackers, and social media platforms have become a common part of modern life. In 2018, half of smartphone or tablet owners had health or wellness apps, such as Apple Health or Google Fit, which were commonly used to track progress towards a health-related goal.[12] Consumers are also beginning to take advantage of apps to download and transport their medical records.[13]

Apps and other digital tools provide consumers with convenient, informative and innovative tools to track, store, and share their health care information. But such tools also present a new challenge in protecting patient data privacy. Most apps are not covered by HIPAA, and therefore do not have to abide by the same privacy and security rules as covered entities such as health plans, clinicians, and hospitals. Health information collected by a non-covered app, as well as HIPAA-protected PHI shared by a covered entity with a non-covered app at a patient's direction, may not be protected once the information has been transmitted or a non-covered app on a consumer device.

While some clinicians and hospitals already provide patients with access to their health care information through mobile health apps, the interoperability, patient access and information blocking rules proposed by ONC and the Centers for Medicare & Medicaid Services (CMS) are poised to greatly expand consumer access and convenience in accessing their information through a mobile health app or tool of their choice. The regulations have the potential to revolutionize the way that consumers access their information, but also raise concerns about issues such as privacy and security, consumer literacy and education, data standardization and transparency regarding use of data shared by patients.

62% of consumers want their data and privacy protected, even if it means foregoing access to their information

Recent media stories have pointed to some of the potential consequences, noting instances where apps have shared information with third parties for advertising and other purposes, often without disclosure to or consent from individuals using the apps.[14] Meanwhile, advances in technology such as machine learning have demonstrated the ability to re-identify significant portions of deidentified data,[15] underscoring the challenges of balancing patient access and information sharing while simultaneously protecting privacy.

Data also points to consumer concern with privacy and security. A 2018 poll found that 49 percent of U.S. adults are extremely or very concerned about their health care data security,[16] and a recent AHIP survey found that 90 percent of consumers want technology companies held to the same high standard and scrutiny as health insurance providers when it comes to protecting their information. Sixty-two percent of respondents said that they want their data and privacy protected, even if it means foregoing easier access to their health information.[17]

The HHS Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) are responsible for ensuring that companies comply with HIPAA and the FTC Act, which prohibits companies from engaging in

deceptive or unfair acts or practices in or affecting commerce.[18] Others have suggested the use of a framework called OAuth 2.0 will help to verify that a consumer has authorized the disclosure of their information.[19] While many at the Roundtable agreed that these mechanisms could be a starting point, additional government enforcement power, transparency, and oversight of non-HIPAA-covered entities is needed to help support and enable the goals of patient access while maintaining the trusted relationship between patients and their clinicians.

For instance, several Roundtable participants noted that privacy policies included in terms and conditions for third party apps reviewed during consent processes average 9,600 words and are written at a college reading level. Additionally, there is no current federal requirement for a third-party app to clearly notify a patient that when information is disclosed to a non-HIPAA covered entity the protections of HIPAA no longer apply, or when the third-party app has elected to re-share information with other downstream entities. The current consent process is often an all or nothing approach, meaning, unless a consumer consents to an entity's privacy policy they are not able to use the product. This take it or leave it approach does not allow for informed patient consent to information sharing, nor does it allow for a patient to revisit his or her consent at a later point.

As we move to enable better patient access to health care information, clear guardrails and more transparent, plain-language privacy and security policies are needed to help enable and maintain patient and clinician trust and to allow for sanctioned, and seamless exchange of health information.

Next Steps in Enabling Patient Access
The CMS and ONC interoperability, information blocking and patient access rules will open up new ways for consumers to gain access to and to act on their health care information, alleviating many of the challenges they may currently face and giving consumers the benefit of being able to access their information where and when they want to.

However, we must do more than just enable access to information. To fully realize a vision of an engaged and informed consumer, the health care system must concurrently work to provide consumer education and engagement, so that patients understand their access rights and what trusted tools are at their disposal to access and make use of their information. Most importantly, we need to provide consumers with information about how to keep their health care information private and secure, including when sharing with third parties, so that they can make informed choices.

We must also provide clinicians and others within the health care system with seamless and easy access to guidance about health information access and privacy, so that they are better informed of and able to exercise their rights and responsibilities under HIPAA. Providing clinicians with better information and tools will help them to more easily provide assistance and guidance to patients as part of their normal workflow, and to feel more comfortable that sharing their patients' sensitive health information at their direction will not cause harm. This will help to foster patient-clinician trust, allow for more time for patient care, and ensure that the burden of information sharing does not solely fall on the patient.

Data Standardization to Support Consumer Access and Use
According to the Transparency Policy Project, an interdisciplinary group based at the Harvard Kennedy School, for consumers to meaningfully act on information, it needs to be understandable and available where and when consumers make their choices.[20] This concept applies directly to the use of health data.

Development of Data Standards

Data standardization efforts help to promote the exchange of usable and actionable information for patients, providers, clinicians, and other stakeholders in the health care system. Data and interoperability standards offer health IT developers, EHR vendors, and health care entities a foundation to exchange data successfully. According to ONC, "standards are agreed-upon methods for connecting systems together. Standards may pertain to security, data transport, data format or structure, or the meanings of codes or terms."[21] Without consistent standards and a common vocabulary, or rules-of-the-road, data shared from one organization to another is meaningless. Additionally, standards need to be implemented consistently to leverage the benefits of their use.

Health IT standards are defined, updated, and maintained by standards development organizations (SDOs) through collaborative processes. Examples of SDOs include Health Level 7 (HL7), Direct Trust, Integrating the Healthcare Enterprise (IHE), and Digital Imaging and Communications in Medicine (DICOM).[22]

ONC also publishes a dynamic compendium of standards, called the Interoperability Standards Advisory (ISA) to "recognize interoperability standards and implementation specifications for industry use to fulfill specific clinical health IT interoperability needs." ONC recently released the 2020 version of the ISA,[23] which includes additional social, behavioral, and psychological interoperability needs, and new subsections on care coordination for referrals and for clinical notes, among others.[24]

One of the more widely known and increasingly used set of standards is called Fast Healthcare Interoperability Resources (FHIR), and is developed and maintained by HL7. The FHIR standard is an iterative standard, expanding codes as new use cases are developed. Other organizations and efforts have developed around the FHIR standard, such as the Da Vinci Project[25] and the Argonaut Project[26], to create guidelines on how organizations can use FHIR to exchange data in a consistent manner given specific use cases.

CMS uses the FHIR standard for its Blue Button API, which enables Medicare beneficiaries to connect their claims data to applications and tools of their choice.[27] Apple Health also uses FHIR to allow consumers to connect to their providers' and clinicians' EHRs, if available, to collect their health records on their phone. According to Apple, supported data types include allergies, conditions, immunizations, lab results, medications, procedures, and vitals.[28] Notably, both CMS and Apple use the OAuth 2.0 framework for user authentication, which verifies that a request for information was authorized by the user, but does not necessarily imply informed consent.
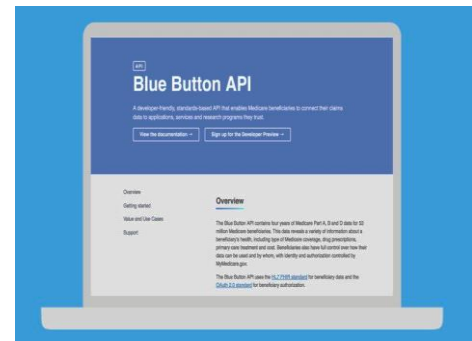
Additionally, CMS and ONC are proposing to advance their broader goals of interoperability and patient access through FHIR-based APIs. ONC is proposing to require Certified EHR Technology (CEHRT) to include a FHIR-based API that will enable access to the U.S. Core Data for Interoperability (USCDI),[29] while CMS is proposing to require health plans to use FHIR-based APIs to make patient claims and other health information available to patients through apps.[30]

Gaps and Challenges in Standards Development

While FHIR-based or other standards-based APIs will help to accelerate health care information sharing, other challenges persist in developing, standardizing, integrating, and translating data so that it is meaningful and actionable.

For instance, while there are many mechanisms in place to design new use cases and standards, the process for developing, testing, and scaling standards takes time and resources. Several Roundtable panelists noted concern that unless there is a sufficient business case and funding to develop use cases in a timely manner, there may be gaps in interoperability of information.

Another challenge raised during the Roundtable was the applicability of interoperability and data sharing across the continuum of care and outside of the health care setting. It is important to close gaps in care not only through real time clinical data access and exchange at the point of care by integrating claims, clinical, lab, and pharmacy data, and also to ensure that post-acute and other types of settings beyond acute and ambulatory ones are able to appropriately contribute to and access patient health information.

Additionally, it would be helpful to be able to include non-clinical data that might inform health care and treatment that is collected by health apps or other tools, or housed in other systems. One panelist called this idea a "Life Record" – essentially, a longitudinal record of clinical and non-clinical data that can be used to inform decision-making related to an individual's health.

"Patients don't just want data, they want the systems and the insights around the data. The current infrastructure doesn't do that, since EHR vendors' customers are not patients,"

Use and Translation of Meaningful Data

To achieve widespread interoperability and patient access to health care information, we need both a shared set of comprehensive and adopted standards, as well as tools that will interpret data and present them to consumers, providers and clinicians in ways that are meaningful and actionable. Consumers make more informed choices and demonstrate greater comprehension when health care information is presented in less complex ways.[31] And, according to a recent survey, 82 percent of adults want their health care information delivered in a way that is more concise and simpler to understand.[32]

As one panelist mentioned during the Roundtable, "patients don't just want data, they want the systems and the insights around the data. The current infrastructure doesn't do that, since [EHR vendors'] customers are not patients."

As the new CMS and ONC rules accelerate a future that is more centered on the consumer, we need to ensure that there are tools in place to identify the key data points and translate them for the consumer and the clinician, while also providing for other use cases where the entirety of a patients' EHR is useful. This includes ensuring that the appropriate standards have been developed and tested, and are ready to scale nationally.

For example, it would be helpful if prior to seeing a patient, a clinical decision support tool could flag identified pieces of the patient's record for a clinician to discuss with a patient, and similarly, if a consumer

were better able to understand any gaps in care and use that to speak with their clinicians. Additionally, Roundtable participants spoke about insights that artificial intelligence (AI) and advanced analytics might produce both for patients and clinicians, and in clinical and biomedical research.

In sum, participants noted that in a future world, it would be ideal to be able to seamlessly aggregate, link, triage, and transform data in ways that are useful and insightful.

Legislative and Regulatory Barriers to Information Sharing in the Health Care System

Ideally, the seamless access, exchange, and use of EHI would allow consumers to more easily manage their health care needs and to share their information with their clinicians and caregivers, and improve health care delivery and the experience of care. Moreover, promoting interoperability and better sharing of health information would drive innovative improvements in care delivery and payment models, human-centered design approaches, and groundbreaking research and development.

However, as noted above, today there are often challenges in ensuring that patients have access to meaningful and actionable information, our current patchwork of privacy and data sharing laws make information sharing difficult to navigate, and data systems and standards are not yet fully integrated and compatible across the health care system.

The proposed rules from CMS and ONC seek to promote greater interoperability and patient access to health information by requiring health care entities to incorporate open access APIs and implementing penalties for entities that fail to share information when appropriately requested by the patient. But these proposed rules represent just one piece of the puzzle.

HHS is also expected to release regulations updating HIPAA to provide greater clarity on how it applies to care coordination efforts. The Administration is simultaneously continuing other efforts to promote access to and use of information and to enforce HIPAA through OCR. Meanwhile, there is a larger ongoing discussion about data privacy beyond the health care arena, with Congress and the Administration raising concerns about how and to what extent Big Tech is accessing, exchanging and using all sorts of personal and/or identifiable information – not just health information.

In addition to the Administration's current work, continued policymaking and coordination across the health and non-health sectors is needed to fully address the underlying health information privacy and access challenges. As we move forward, we will also need to continually assess the consequences of the choices we are making and course-correct in ways that limit friction between health information technology vendors, EHR vendors, clinicians, hospitals and patients while maintaining trusted relationships and not increasing burdens on these groups. Facilitating patient access is a shared responsibility and will require stakeholders from across the health care system to do their part to achieve our shared goals.

Below, we outline several shared goals to help guide policymaking efforts for patient access to health information, as well as some of the commonly suggested next steps for ensuring such access.

Shared Patient Access Goals

- Provide consumers with access to their health care information and allow them to share their information as they wish.
- Increase patient access to meaningful and actionable information that patients and clinicians can use to make health care decisions.

- Expand patient education and engagement so that consumers understand their health information access rights, how to access their information, what tools they can use to access their information, and what it means to share their information with non-HIPAA-covered entities.
- Educate clinicians, administrative staff, and other stakeholders about patient health information access and sharing rights and responsibilities.
- Provide patients and clinicians with more transparent information about apps' privacy and security policies and functions and require meaningful, informed consent.
- Ensure any new requirements maintain the trusted relationship between the patients and their clinician and/or health plan and minimize administrative burdens on these groups.

Common Suggestions for Expanding Patient Access to Health Information

- Ensure patients have education and resources available to make informed decisions with their health care information, especially when it comes to third party apps (e.g., consumer health IT literacy).
- Give clinicians clear guidance and a cross-walk outlining how HIPAA and state privacy laws will interact with the new interoperability and information blocking rules.
- Establish a data privacy structure that ensures health data is protected regardless of whether it is covered by HIPAA, aligning privacy and security rules where possible and requiring privacy and security policies to be transparent and easy to understand.
- Promote clear, readable, and streamlined consent policies, with the ability for consumers to renegotiate the terms and scope of their consent at the time of consent and in the future.
- Ensure new information sharing requirements are aligned with HIPAA (e.g., they do not create duplicative or conflicting requirements that confuse patients, clinicians, etc.).
- Provide for appropriate government enforcement to ensure consumers and clinicians are protected.
- Encourage and promote the timely development and testing of comprehensive data standards that can be implemented at scale to enable successful data exchange across entities and care settings.

Key Recommendations

During the Health IT Roundtable, several common themes and recommendations aimed at improving patient access to their health care information were raised.

- *Education and Engagement*

  o *Administrative, Private Sector* - Create materials to help clinicians and patients better understand HIPAA and the Privacy Rule, the delineation between HIPAA and non-HIPAA-covered entities, and notice and consent policies.

- *Privacy and Security*

  o *Administrative* - Establish a public-private partnership to review privacy and security policies for third-party apps and create a Star-rating, or some other indicator, of their commitment to privacy and security of patients' information.
  o *Legislative* - Establish a data privacy structure that better aligns privacy and security rules inside and outside of HIPAA.
  o *Legislative* - Create stronger compliance and government enforcement mechanisms for entities not subject to HIPAA and appropriate adequate funding for such mechanisms.

- *Data Sharing and Interoperability*

    - *Administrative/Private-Sector* – Support for bidirectional information sharing built on a foundation of robust data integrity that would allow patients to add to their health record.
    - *Legislative/Administrative* – Strengthen consumer discrimination protections related to downstream or secondary uses of data.
    - *Legislative/Administrative* – Dedicate funding to support standards development by the private-sector for priority data elements and use cases.

APPENDIX A

**Health IT Leadership Roundtable: Future of Interoperability and
Secure Consumer Access to Healthcare Data**

January 30, 2020

AGENDA

8:30 a.m.	**Welcome & Housekeeping** Kristen McGovern, Partner, Sirona Strategies; former Chief of Staff at the HHS Office of the National Coordinator for Health IT
8:35 a.m.	**Opening Remarks** Justine Handelman, Senior Vice President, Office of Policy and Representation, Blue Cross Blue Shield Association
8:40 a.m.	**Keynote Remarks** Dr. Don Rucker, National Coordinator for Health IT, HHS Office of the National Coordinator for Health IT
9:30 a.m.	**Congressional Perspectives on Health IT** Senator Bill Cassidy, U.S. Senator, Member of the Senate Finance Committee and Senate HELP Committee
9:50 a.m.	**Panel: Advancing Consumer Access to Health Data** Description: Panelists will highlight innovative ways that they are engaging patients and their caregivers with health care data today. As we look to a future world where increasing amounts of health care data are shared electronically, what, if any, new protections and/or education initiatives are needed to ensure patients understand how and what their data will be used for? What considerations are top of mind for providers and plans when they share information with third parties at the patient's direction? What use cases are most important for patients? Panelists: • Aaron Miri, Chief Information Officer, Dell Medical School & UT Health Austin, The University of Texas at Austin • Lina Walker, Vice President of Health Security, AARP Public Policy Institute • Dr. Edward Juhn, Sr. Medical Director, Care Innovation and Technology Integration, Blue Shield of California • Laura Hoffman, Assistant Director, Federal Affairs, American Medical Association
10:50 a.m.	**Panel: Data Standardization to Support Consumer Access** Description: It is not enough to simply share health care data; providers and consumers need actionable information that supports clinical decision making. This

	panel will highlight private sector work to standardize health care data to support innovation and drive behavior change where appropriate. Panelists: • Karen Wilding, Senior Director, Quality & Value Based Care, the University of Maryland Medical System; Compliance Officer, UM Quality Care Network & Transform Health MD; Member of the College of Healthcare Information Management Executives (CHIME); Past President, Board of Directors, Maryland HIMSS • Laurent Rotival, SVP Strategic Technology Solutions, Chief Information Officer, Cambia Health Solutions • Dr. Zeshan Rajput, MD, MS; Physician Informaticist and Principal, The MITRE Corporation • Sherri Zink, SVP, Chief Data Officer, BlueCross BlueShield of Tennessee
11:50 a.m.	**Lunch Break**
12:30 p.m.	**Research Spotlight: Overview of NPWF/AARP Roundtable Report** • Lina Walker, Vice President of Health Security, AARP Public Policy Institute • Erin Mackay, Associate Director, Health Information Technology Programs, National Partnership for Women & Families
1:00 p.m.	**Panel: Legislative and Regulatory Barriers to Information Sharing in the Healthcare System of the Future** Description: This panel will highlight ongoing barriers to consumer access and interoperability, opportunities for Congress and the Administration to take additional action to advance information sharing with patients and appropriate third parties where directed by the patient. Panelists: • Justine Handelman, Senior Vice President, Office of Policy and Representation, Blue Cross Blue Shield Association • Steven Waldren, Vice President, Chief Medical Informatics Officer, American Academy of Family Physicians • Erin Mackay, Associate Director, Health Information Technology Programs, National Partnership for Women & Families • Erin Richardson, Vice President & Associate General Counsel, Federation of American Hospitals
2:00 p.m.	**Closing Remarks/Call to Action**

APPENDIX B
Health Information Interoperability and Patient Access Laws and Regulations

Health Insurance Portability and Accountability Act

The ***Health Insurance Portability and Accountability Act*** (HIPAA) was enacted in 1996.[33] Among other provisions, the law included a requirement that the Secretary of HHS publicize standards for the electronic exchange, privacy, and security of health information. In 2002, HHS released final, amended regulations establishing Standards for Privacy of Individually Identifiable Information (Privacy Rule). The Privacy Rule was intended to ensure proper protection of individuals' health information while also allowing for the flow of health information between organizations subject to the Privacy Rule, called "covered entities." Covered entities include health plans, health care providers, health care clearinghouses, and their business associates.

The ***Privacy Rule*** protects all "Individually Identifiable Health Information" held or transmitted by a "covered entity" or its business associate, in any form or media, whether electronic, paper, or oral – this is referred to as "protected health information" (PHI). This includes information that relates to (1) the individual's past, present, or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present, or future payment for the provision of health care to the individual; (4) and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.[34]

Through the Privacy Rule, individuals have a ***right to access*** their PHI maintained by a covered entity, or by a business associate on behalf of a covered entity in a "designated record set," which comprises the (1) medical records and billing records about individuals maintained by or for a covered health care provider; (2) enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a health plans; or (3) other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals."[35]

This right of access also includes the right to direct the covered entity to transmit a copy of the PHI to a designated person or entity of the individual's choice – often referred to as a third party – which could be a caregiver, a third party application (app), an organization, or other type of entity. An individual's personal representative also has the right to access PHI about the individual in a designated record set and to direct the data to a third party.

The Privacy Rule also defines and limits the circumstances in which an individual's PHI may be used or ***disclosed by covered entities***. A covered entity is *required* to disclose information only if an individual or their personal representative specifically requests access to, or an accounting of disclosures of, their PHI, and to HHS when complying with a review or enforcement action.

Additionally, a covered entity is *permitted*, but not required, to use and disclose PHI without individual authorization under certain circumstances, including (1) to the individual; (2) for treatment, payment, and health care operations; (3) if given the opportunity to agree or object; (4) if the disclosure is incident to an otherwise permitted use and disclosure; (5) for public interest and benefit activities; and (6) if it is within a limited data set for the purposes of research, public health, or health care operations. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

Health Information Technology for Economic and Clinical Health Act

Congress then enacted the ***Health Information Technology for Economic and Clinical Health*** (HITECH) Act in 2009 to promote the adoption and meaningful use of health IT, including through incentive payments

to encourage hospitals and other health care clinicians to adopt electronic health records (EHRs). The Act significantly increased the rate of adoption of EHRs in hospitals and in clinician offices.

Importantly, HITECH also included provisions related to privacy and security of health information transmitted electronically. HITECH updated HIPAA's right of access standard to allow individuals to obtain a copy of their health information in electronic format.

21st Century Cures Act

In 2016, Congress passed the *21st Century Cures Act* (Cures Act), which aimed, among many other provisions, to promote the adoption of new interoperability standards and to define and mitigate instances of 'information blocking.'

The Cures Act defined information blocking as practices that are likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information. The Cures Act also established new enforcement authority and penalties to discourage certain entities from blocking the exchange and use of electronic health information.

The HHS National Coordinator for Health IT (ONC) and the Centers for Medicare and Medicaid Services (CMS) issued proposed regulations in early 2019 that would implement the provisions of the Cures Act. According to HHS, the rules would "increase choice and competition while fostering innovation that promotes patient access to and control over their health information."[36] While these rules have yet to be finalized, a list of some of the key provisions in the proposed rules follows, along with several other key Administration initiatives to promote greater sharing of and access to health information.

CMS and ONC Proposed Interoperability, Information Blocking, & Patient Access Rules
CMS Proposed Rule

- Proposes to require Medicare Advantage (MA) organizations, state Medicaid and CHIP fee-for-service (FFS) programs, Medicaid managed care plans (MCOs), CHIP managed care entities, and qualified health plan (QHP) issuers in federally-facilitated exchanges (FFEs) to implement, test, and monitor an openly-published Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR)-based APIs to make patient claims and other health information available to patients through third-party applications and developers.
- Proposes to require MA organizations, MCOs, CHIP managed care entities, and QHP issuers in the FFEs to support electronic exchange of data for transitions of care as patients move between these plan types.
- Proposes that payers in CMS programs be able to participate in a trusted exchange network.
- Proposes to make publicly available whether an individual clinician, hospital, or critical access hospital submitted a "no" response to any of the three attestation statements regarding information blocking in the Promoting Interoperability Programs. [37]

ONC Rule

- Proposes updates to the 2015 Edition EHR Certification Criteria, including removed, updated, revised, and new criteria. Importantly, ONC proposes to remove the current Common Clinical Data Set definition and replace it with the United States Core Data for Interoperability (USCDI) standard, which will increase the minimum baseline of data classes that must be commonly available for interoperable exchange. ONC also proposes to adopt a new API criterion which would require the use of HL7 FHIR standards and several implementation specifications.
- Proposes to establish new conditions and maintenance of certification requirements for Health IT modules, as well as a new process for enforcing compliance with such standards.

- Proposes definitions related to the practice of information blocking, as well as seven categories of reasonable and necessary practices that would not be considered to constitute information blocking: (1) promoting the privacy of EHI, (2) preventing harm, (3) promoting the security of EHI, (4) recovering costs reasonably incurred, (5) responding to requests that are infeasible, (6) licensing of interoperability elements on reasonable and non-discriminatory terms, and (7) maintaining and improving health IT performance.

Other Administration Initiatives to Promote Patient Access to Health Information

Additionally, beyond the CMS and ONC proposed patient access and interoperability rules, the Administration has spearheaded several other key initiatives to promote greater sharing of and access to health care information.

- **MyHealthEData** – An overarching initiative that intends "empower patients by ensuring access and use of their health care data while keeping it safe and secure. Having timely electronic access to health information makes it easier for people to make more informed decisions about their health care needs."[38]
- **Blue Button 2.0** – Launched as part of the MyHealthEData Initiative, Blue Button is an API that contains four years of Medicare Part A, B, and D information for 53 million Medicare beneficiaries.[39]
- **Beneficiary Claims Data API** - The Beneficiary Claims Data API (BCDA) enables Accountable Care Organizations (ACOs) participating in the Shared Savings Program to retrieve Medicare Part A, Part B, and Part D claims data for their prospectively assigned or assignable beneficiaries. This includes Medicare claims data for instances in which beneficiaries receive care outside of the ACO, allowing a full picture of patient care.[40]
- **Data at the Point of Care Pilot** - Data at the Point of Care is a pilot API program that enables healthcare providers to deliver high quality care directly to Medicare beneficiaries by making a patient's Medicare claims data available to the provider for treatment needs. The information can be accessed in the existing workflow and without logging into another application or portal.[41]
- **Trusted Exchange Framework and Common Agreement** – The 21st Century Cures Act also required HHS to establish a national framework and common agreement for the trusted exchange of health information. ONC is currently in the process of implementation.[42]
- **OCR Patient Access Initiative** - HHS Office of Civil Rights (OCR), which has enforcement authority over HIPAA, launched a new "Right of Access Initiative" in 2019, through which it intends to "vigorously enforce the rights of patients to receive copies of their medical records promptly and without being overcharged." Since announcing the initiative in September 2019, OCR has issued two enforcement actions and settlements.[43],[44]

---

[1] See Appendix A for the agenda for the *Health IT Leadership Roundtable: Future of Interoperability and Secure Consumer Access to Health Care Data.*

[2] Peacock S, Reddy A, Leveille SG, et al. (2016). "Patient Portals and Personal Health Information Online: Perception, Access, and Use by U.S. Adults." Journal of the American Medical Informatics Association, 24(e1), Available here: http://bit.ly/2RYizaa

[3] Kruse CS, Bolton K, Freriks G. (2015). "The Effect of Patient Portals on Quality Outcomes and its Implications on Meaningful Use: A Systematic Review." J Med Internet Res. 17(2):e44

[4] ONC, (2019). "Trends in Individuals' Access, Viewing, and Use of Online Medical Records and Other Technology for Health Needs: 2017-2018." Available here: http://bit.ly/2G4DOAn

[5] ONC (2018), "Individuals' Use of Online Medical Records and Technology for Health Needs." Available here: http://bit.ly/2O8xbkP

[6] ONC, (2019). "Trends in Individuals' Access, Viewing, and Use of Online Medical Records and Other Technology for Health Needs: 2017-2018." Available here: http://bit.ly/2G4DOAn

[7] ONC (2018) Individuals' Use of Online Medical Records and Technology for Health Needs.: Available here: http://bit.ly/2vkzafC

[8] GAO, (2017). "Health information technology: HHS should assess the effectiveness of its efforts to enhance patient access to and use of electronic health information." Available here: http://bit.ly/31x9yrF

[9] Anthony DL, Campos-Castillo C, Lim PS, (2018). "Who isn't Using Patient Portals and Why? Evidence and Implications from a National Sample of US Adults." Health Affairs, (37)12. Available here: http://bit.ly/36Z4VYk

[10] National Partnership for Women and Families, (2014). "Engaging Patients and Families: How Consumers Value and Use Health IT." Available here: http://bit.ly/38mFIIU

[11] ONC (2018), "Individuals' Use of Online Medical Records and Technology for Health Needs." Available here: http://bit.ly/2vkzafC

[12] ONC (2019), "Electronic Capabilities for Patient Engagement among U.S. Non-Federal Acute Care Hospitals: 2013-2017." Available here: http://bit.ly/313d8tx

[13] ONC (2018), "Individuals' Use of Online Medical Records and Technology for Health Needs." Available here: http://bit.ly/2vkzafC

[14] New York Times, "When Apps Get Your Medical Data, Your Privacy May Go With IT," September 3, 2019. See also Washington Post, "Smoking and Depression Apps Are Selling Your Data to Google and Facebook, Study Finds," April 22, 2019.

[15] Liangyuan N, Yang C, Lo C, et al. (2018). "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 Netw Open, Available here: http://bit.ly/2ZYdPU8

[16] Scout Poll, (July 25, 2018), Available here: http://bit.ly/31u7LUr

[17] AHIP and Morning Consult, 2020 Available here: http://bit.ly/2SIbdYG

[18] Federal Trade Commission, (2016). "Sharing Consumer Health Information? Look to HIPAA and the FTC Act." Available here: http://bit.ly/3a8kX4j

[19] Blog Post by Dr. Don Rucker, National Coordinator for Health IT, U.S. Department of Health and Human Services, "ONC's Proposed Rule Will Connect People to Their Care," (February 11, 2019). Available here: https://bit.ly/391qTMa

[20] Fagotto E, Fung A. (2017). "Can Transparency and Technology Make Us Healthier?" Available here: http://bit.ly/380LVdB

[21] ONC, (2020), "Health IT Standards." Available here: http://bit.ly/2S89N9F

[22] For more information about these and other standards development organizations, see American Medical Informatics Association, "Standards Development Organizations." Available here: https://bit.ly/3c9UtBp

[23] ONC, (2020), "2020 Interoperability Standards Advisory." Available here: http://bit.ly/2UxRgFo

[24] ONC, (2020). "Top Six Changes in the ISA 2020 Reference Edition." Available here: http://bit.ly/2vX0KQc

[25] HL7, "About the Da Vinci Project." Available here: https://bit.ly/3cbbOJZ

[26] HL7, "Welcome to the Argonaut Project." Available here: https://bit.ly/37Y93sc

[27] CMS, (2020). "Blue Button 2.0." Available here: http://bit.ly/375Eoc6

[28] Apple Health. Available here: https://apple.co/3757eJF

[29] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, Notice of Proposed Rulemaking, 84 Fed. Reg. 7424-7610, March 4, 2019

[30] Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans in the Federally-Facilitated Exchanges and Health Care Providers, 84 Fed. Reg. 7610-7680, March 4, 2019

[31] Kutzman ET, Greene J. (2016). "Effective Presentation of Health Care Performance Information for Consumer Decision Making: A Systematic Review." Available here: http://bit.ly/2H03b6V

[32] AHIP and Morning Consult, (2020). "Pricing Transparency Polling Presentation." Available here: http://bit.ly/31q6OfK

[33] P.L. 104-191

[34] U.S. Department of Health and Human Services (HHS), Office of Civil Rights, "OCR Privacy Brief: Summary of the HIPAA Privacy Rule." Available here: http://bit.ly/35hDzvL

[35] HHS, "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524." Available here: http://bit.ly/36vKhjo

[36] HHS, "HHS Proposes New Rules to Improve the Interoperability of Electronic Health Information." Available here: http://bit.ly/2sSgsLg

[37] Centers for Medicare and Medicaid Services (CMS), "CMS Interoperability and Patient Access Proposed Rule: CMS-9115-P." Available here: http://bit.ly/2N37Atd

[38] CMS, "MyHealthEData." Available here: https://go.cms.gov/2x07gGe

[39] CMS, "Blue Button 2.0." Available here: http://bit.ly/375Eoc6

[40] CMS, "Beneficiary Claims Data API." Available here: http://bit.ly/38mxXBW

[41] CMS, "Data at the Point of Care." Available here: http://bit.ly/2Yg5VrM

[42] ONC, "Trusted Exchange Framework and Common Agreement." Available here: http://bit.ly/2UI2XdP

[43] HHS, "OCR Settles First Case in HIPAA Right of Access Initiative." Available here: http://bit.ly/306Bbr3

[44] HHS, "OCR Settles Second Case in HIPAA Right of Access Initiative." Available here: http://bit.ly/39N4WBi