HealthIT.gov

Individuals' Access to Their Own Health Information

ONC Policy Brief

Date: June 3, 2012
Author: Jamie Skipper, R.N., Ph.D.
Acknowledgements: Jodi Daniel, Mary Jo Deering, Erin Poetter, Lygeia Ricciardi

Table of Contents

What's the Issue?

Individuals who engage in their health care achieve better health outcomes and benefit from lower health care costs.[1] Having ready access to health information held by health care providers and health plans allows patients to be better managers of their health and care by, for example, making more informed treatment decisions, adopting healthy behaviors related to diet and exercise, or taking medications as advised by their providers.[2]

Having ready access to health information held by health care providers and health plans allows patients to be better managers of their health.

Providers are able to more easily and quickly share health information with their patients when health records are in electronic form, as this enables communication and information sharing through electronic health portals or electronic transmissions to a web-based personal health record (PHR).

Multiple barriers still remain to providing individuals access to their health information. Some health care providers do not store health information in electronic form, and patients must wait until physical copies are made and mailed to them. Additionally, many individuals are unaware of their legal right to ask for a copy of their health information from their providers. There are also cultural and operational challenges that may prevent individuals from asking for and receiving a copy of their records, such as limited time during office visits, an unwillingness to be viewed as challenging their doctor, or non-standardized provider processes to support the individual's request for a copy of his or her records.

[1] Hibbard J and Cunningham, PJ. *How Engaged are Consumers in Their Health and Health Care, and Why Does It Matter?* Washington, DC: Center for Studying Health System Change. Research Brief No. 8, October 2008.

[2] Hibbard, Judith H., et al., "Do Increases in Patient Activation Result in Improved Self-Management Behaviors?" *Health Services Research*, Vol. 42, No. 4 (2007).; Becker, Edmund R., and Douglas Roblin, "Survey of Health and Healthy Behaviors Among Working Age Kaiser Permanente Adults in 2005," presented at the Annual Research Meeting of AcademyHealth, Orlando Fla., (June 2007); Becker and Roblin (2008).

The Office of the National Coordinator for Health Information Technology has been working with federal, state and private partners to leverage current legislation and regulations to design health IT policies and programs that enhance individuals' electronic access to their information.

The Office of the National Coordinator for Health Information Technology (ONC) has been working with federal, state, and private partners to leverage current legislation and regulations to design health IT policies and programs that enhance individuals' electronic access to their information in a secure and timely manner.

This brief will review how legislative milestones and federal and private industry efforts, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, Health Information Technology for Economic and Clinical Health Act (HITECH), and the federal electronic health records (EHR) incentive programs, have been major driving forces to realizing the goal of individuals having access to electronic copies of their health information. In addition, this brief will highlight other related efforts by the U.S. Department of Health and Human Services (HHS) and other federal agencies that are currently underway, such as Blue Button, ONC's Consumer e-Health Program, and Standards and Interoperability initiatives that aim to bolster individuals' access to their records. Lastly, this brief will identify some of the remaining challenges that continue to be hurdles for individuals in accessing their health information in a secure and timely manner.

What Has Happened So Far?

HIPAA and HITECH

The HIPAA Privacy Rule gives individuals the right to get a copy of their health information from most doctors, hospitals, and other health care providers.

The Standards for Privacy of Individually Identifiable Health Information (the HIPAA Privacy Rule) established, for the first time, a set of national standards for the protection of certain health information. The Secretary of HHS issued the HIPAA Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HIPAA Privacy Rule gives individuals the right to get a copy of their health

information from most doctors, hospitals, and other health care providers as well as health plans and, in certain circumstances, health care clearinghouses (collectively called "covered entities").[3] The HIPAA Privacy Rule also establishes minimum attributes of the process for providing access, denying access, and documenting actions taken. Generally, covered entities must provide individuals with a copy of their health information, including their medical record, billing record, and other records used to make decisions about them, within 30 days of their request (45 CFR § 164.524(b)(2)). They must provide the copy in the form or format requested by the individual if it is readily available, such as in PDF format or on a CD or thumb drive. If the individual's preferred form or format is not available, the covered entity must provide the copy in a readable hardcopy format or whatever form or format agreed to by the covered entity and the individual, which can be either paper or electronic. In addition, the rule permits covered entities to charge individuals no more than a reasonable, cost-based fee for a copy of their health information.[4]

In 2009, the HITECH Act, enacted as part of the American Recovery and Reinvestment Act, instructed the Secretary of HHS to strengthen individuals' access rights in a number of important ways. First, it instructs HHS to clarify individuals' access rights under HIPAA by expressly requiring covered entities to provide individuals access to their information in electronic format if the covered entity has adopted electronic health record technology. In addition, HITECH specifies that if individuals so

In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) instructed the Secretary of Health and Human Services to strengthen individuals' access rights in a number of important ways.

[3] The Administrative Simplification standards adopted by HHS under HIPAA apply to any entity that is:

- A health care provider that conducts certain transactions in electronic form (called here a "covered health care provider"
- A health care clearinghouse
- A health plan

An entity that is one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations. (http://www.cms.gov/HIPAAGenInfo/06_AreYouaCoveredEntity.asp)

[4] Many states have defined a reasonable fee to range from around $2.00 to $0.10 for the first 10-25 pages. In most states, the maximum allowable fee for the remaining pages will be less than the first set of pages and is usually based on a sliding scale. In addition, states allow other additional charges such as handling fees and postage fees. For example, in Louisiana, a reasonable charge for medical records not to exceed:

- $1.00 per page for first 25 pages
- $0.50 per page for pages 26-500
- $0.25 per page thereafter
- Plus handling charge of $15.00
- Plus actual postage

Regardless of the state fee structure, HIPAA covered entities must base their fees are their actual costs, and the fee may only include the cost of copying (including supplies and labor) and postage. It cannot include the cost of retrieving the information. Cost for copies of x-rays, microfilm, electronic, and imaging media are allowed to be higher to cover the actual cost of reproducing these non-paper records. (http://www.legis.state.la.us/lss/lss.asp?doc=97291)

choose, they may direct the covered entity to transmit a copy of their record to a person or entity they designate (a provision that would permit individuals to direct their information to a web-based personal health record).

In addition, HITECH provided for the adoption of security and privacy requirements for entities that use and disclose protected health information (PHI)[5] in the performance of a covered function or activity on behalf of a covered entity (i.e., "business associates" as defined at 45 CFR 160.103). As a result, business associates who are contracted by covered entities to respond to individuals' requests for their health information will be required to follow these rules on the compliance date provided in the final rule issued to implement the requirements. For example, a hospital that is a member of a Health Information Organization (HIO) currently must have a business associate agreement with the HIO to transmit electronic health information to it for storage and exchange purposes. As part of that business associate agreement, the HIO may be required to directly receive and respond to patient requests for their health information. Under the July 2010 proposed rule for implementing the HITECH modifications to HIPAA, the HIO would be required to adhere to the new requirement for providing the information in electronic format within 30 days of the patient's request, subject to certain exceptions. While the hospital would continue to be responsible under HIPAA for ensuring that the HIO follows its business associate agreement, if the final rule follows the proposed rule, the HIO would also be liable for penalties if it failed to meet such requirements.

HITECH does not dictate what electronic media (Web portal, CD, email, thumb drive) must be used to supply the individual with an electronic copy of his or her health information. HITECH also does not require covered entities to furnish electronic copies if the information is only stored in paper format. HITECH leaves in place many of the other requirements of the HIPAA Rules, such as requiring the copy be provided in a readable format if requested by the individual, and allowing a reasonable, cost-based fee.

National Quality Strategy

In 2011, HHS released the "National Strategy for Quality Improvement in Health Care," required by the Patient Protection and Affordable Care Act of 2010 (ACA). This strategy highlighted the importance of "patient access to understandable information and

[5] The Privacy Rule defines PHI as individually identifiable health information, held or maintained by a covered entity or its business associates acting for the covered entity, that is transmitted or maintained in any form or medium.

decision-support tools that help patients manage their health and navigate the health care delivery system" in order to foster better individual and family-centered care[6] as envisioned in the ACA.[7]

EHR Incentive Programs

The EHR Incentive Program requires certain eligible health care providers and eligible hospitals to demonstrate meaningful use of certified EHR technology in order for them to receive incentive payments.

In July 2010, the HHS Centers for Medicare & Medicaid Services (CMS), in coordination with ONC, released the Final Rule pertaining to Stage 1 of the Medicare and Medicaid EHR Incentive Programs. The EHR Incentive Programs, authorized through HITECH, require certain eligible health care providers and eligible hospitals to demonstrate meaningful use of certified EHR technology in order for them to receive incentive payments.

For Stage 1 incentives, the definition of meaningful use includes criteria that focus on enhancing individual access to their health information, such as providing patients online access to their health information as well as an electronic copy of their:

- Health information upon request
- Discharge instructions after a hospital visit[8]
- Clinical care summary[9] after each office visit

ONC is working with CMS to create Stage 2 Meaningful Use requirements that continue

[6] The Institute of Patient and Family Centered Care defines family-centered care as "an approach to the planning, delivery, and evaluation of health care that is grounded in mutually beneficial partnerships among health care providers, patients, and families. It focuses on respect and dignity, information sharing, participation, and collaboration between health providers, patients, and their families." (http://www.ipfcc.org/faq.html)

[7] http://www.healthcare.gov/center/reports/quality03212011a.html

[8] CMS defines discharge instructions as follows: Any directions that the patient must follow after discharge to attend to any residual conditions that need to be addressed personally by the patient, home care attendants, and other clinicians on an outpatient basis. (https://www.cms.gov/ehrincentiveprograms/30_Meaningful_Use.asp)

[9] CMS defines a clinical-care summary as follows: An after-visit summary that provides a patient with relevant and actionable information and instructions containing the patient name, provider's office contact information, date and location of visit, an updated medication list, updated vitals, reason(s) for visit, procedures, and other instructions based on clinical discussions that took place during the office visit, any updates to a problem list, immunizations or medications administered during visit, summary of topics covered/considered during visit, time and location of next appointment/testing if scheduled, or a recommended appointment time if not scheduled, list of other appointments and tests that the patient needs to schedule with contact information, recommended patient decision aids, laboratory and other diagnostic test orders, test/laboratory results (if received before 24 hours after visit), and symptoms. (https://www.cms.gov/ehrincentiveprograms/30_Meaningful_Use.asp)

to advance individuals' access to their health information. For instance, the draft regulations for Stage 2 include a requirement that providers offer patients the ability to view, download, and transmit their health information. This includes the ability to direct that their information be sent to a third party, such as a personal health record.

Federal Health IT Strategic Plan

The Federal HIT Strategic Plan 2011-2015 includes a goal to empower individuals with health IT to improve their health and the health care system and specific objectives to strengthen individuals' access to their health information and their ability to communicate electronically with their health care providers. These objectives include:

- Encouraging providers, through Medicare and Medicaid EHR Incentive Programs, to give individuals access to their health information in an electronic format.

The Federal HIT Strategic Plan 2011-2015 includes a goal to empower individuals with health IT.

- Increasing EHR adoption that will lead to an increase in the number of providers who have patient records stored in an electronic format, thus increasing the number of individuals who have access to a copy of their records in electronic format.

- Having federal agencies that deliver or pay for health care act as a model for sharing information with individuals, and making tools available to do so.

- Establishing public policies, such as Meaningful Use requirements, that foster individual and caregiver access to their health information while protecting privacy and security.

- Supporting the development of standards and tools that make EHR technology capable of interacting with consumer health IT and building these requirements for the use of adopted standards and tools into EHR certification.

Consumer e-Health Program

ONC released educational tools on its website (www.healthit.gov) to help consumers understand how they can get their health information more easily.

Numerous policy and programmatic activities are already underway to help boost individuals' engagement in their own health and with health care providers. For example, ONC released educational tools on its website (www.healthit.gov/) to help consumers understand how they can get their health information more easily. These tools include, among others, a patient access checklist that explains step-by-step how to request health information from health care providers or their business associates and how individuals can use this information to improve their care.

On June 8, 2011, ONC announced the launch of the Investing in Innovation (i2) Initiative, a new program designed to challenge innovations in health IT. Of these "challenge" grants, Ensuring Safe Transitions from Hospital to Home is challenging software developers to create easy-to-use tools to help patients and caregivers access the information and materials they need to answer questions about their condition, their medications and medical equipment, and their post-discharge plans and then share this information with doctors, pharmacists, nurses and other professionals in their next care setting (e.g., home, nursing home, hospice).

In September 2011, ONC also began a consumer engagement program through which various health care stakeholders (both those that hold and do not hold personal health information) are able to make a pledge to raise the bar on how they help individuals access their health information. Information holders pledge to make it easier for individuals and their caregivers to have secure, timely, and electronic access to their health information. Non-information holders pledge to engage and empower individuals to be partners in their health through information technology. ONC accepted pledges through March 2012 and created www.healthit.gov/pledge to display pledgees and offer further information on the pledge program. ONC will continue to support and learn from the community of participating organizations in the months ahead, and will highlight some of their successes in a

ONC also began a consumer engagement program through which various health care stakeholders are able to make a pledge to raise the bar on how they help individuals access their health information.

consumer track of the Health Data Initiative Forum "Health Datapalooza" meeting in June 2012.

CLIA and Access to Laboratory Data

In September 2011, HHS proposed amending aspects of two existing rules, the Clinical Laboratory Improvement Amendments of 1988 (CLIA) and the HIPAA Privacy Rule to further expand individuals' access to their health information. The proposed changes would provide individuals with the right to receive their test reports directly from laboratories, a right which is currently limited in many states.

Privacy and Security Guidance and Tools

Web-based PHRs are a useful tool for individuals to review and share their health information. However, individuals may be reluctant to use a web-based PHR if it is unclear how a PHR company may handle an individual's health information in their PHR. To address this, ONC released a PHR Model Privacy Notice that can be used by PHR companies to communicate their privacy and security policies and data sharing practices to individuals in a uniform and easy-to-understand manner.

Web-based personal health records are a useful tool for individuals to review and share their health information.

The PHR Model Privacy Notice is meant to be similar to other consumer oriented "labels" that have been developed for other industries, such as the nutrition facts label for food. As more individuals obtain access to their electronic health information and use PHRs to manage this information, it is important for them to be aware of PHR companies' privacy and security policies and data-sharing practices.

In 2008, ONC highlighted the individuals' right to access their health information as one of the eight fundamental principles in its *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*. ONC created this framework to serve as a guide for public and private-sector entities that hold or exchange electronic individually identifiable health information (IIHI) and for the development of any compliance and enforcement approaches, including industry self-regulation. The framework states that persons and entities that participate in a network for the purpose of electronic exchange of IIHI should provide individuals with "a simple

and timely means to access and obtain their IIHI in a readable form and format."

Access Through Clickable Download Tools

Other federal agencies have also taken steps to promote individuals' access to their health information. For example, in 2010, the Veterans Administration (VA), in collaboration with CMS, the Department of Defense (DoD), and the Markle Foundation, introduced the "Blue Button" capability that allows individuals to download their personal health information from specific sources.

Other federal agencies have also taken steps to promote individuals' access to their health information.

The DoD's Blue Button feature allows veterans to access and download their information from their My Health***e***Vet Personal Health Record account online into a very simple text file (or an enhanced PDF) without the need for additional software. This text file is available to be read, printed, or saved on any computer. The download can include all their health information or can be broken out by class of information, or by date range. VA Health***e***Vet users can also add personal information into that record through the website. DoD's new TRICARE Online also provides the Blue Button download feature to enable patients to safely and securely access, print or save their demographic information, allergy and medication profiles.

CMS provides Medicare beneficiaries the ability to access their claims data on www.mymedicare.gov, where Medicare beneficiaries can then create and print a report called the "On-the-Go report" to share with their caregivers and providers.

Many private-sector health care information holders are now making pledges within the ONC consumer engagement campaign to offer Blue Button-type capabilities very soon.

Standards and Interoperability

The Direct Project, launched in March 2010 as a part of the Nationwide Health Information Network, was created to specify a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. The Direct Project focuses on the technical standards and services necessary to securely push content from a sender to a receiver. Though initial efforts have been focused on messages between providers, subsequent

efforts have been expanded to include message transport between health organizations and an individual's personal health record.

In October 2011, ONC also launched the Data Segmentation Initiative through the Standards and Interoperability Framework to enable the implementation and management of varying disclosure policies in an electronic health information exchange environment in an interoperable manner. The Initiative aims to produce a pilot to test the ability of providers to share portions of an electronic health record while not sharing others, for example, information that has heightened protection under the law such as substance abuse treatment records. In the absence of standards for data segmentation and exchange of sensitive health information, some organizations have chosen simply to exclude entire categories of health information from exchange.[10] This excluded data includes information that originates from federally funded health centers that is protected under 42 CFR Part 2 or from care that has been fully paid for out-of-pocket by the individual. Initial functional and data set requirements for the Data Segmentation Initiative will encompass metadata tagging of privacy attributes in clinical and policy records in order to promote the appropriate sharing of these types of sensitive information while preventing its improper disclosure.

What Are the Open Issues?

Further developments in policies and programs can help extend and enhance individual's access to their health information. The opportunities and challenges include:

- **Removing the social barriers to individuals asking their health care providers for a copy of their health information:** Although the HIPAA Rules and the HITECH Act emphasize an individual's right to a copy of his or her health information, some providers are still either unaware or unclear of the extent to which individuals have the right to inspect and to obtain a copy of their health information. This has resulted in instances where individuals do not feel empowered to request a copy of their health information or do not receive a copy of their records when they exercise their right of access.

[10] Goldstein M and Rein A. Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis, Prepared for the Office of the National Coordinator, DHHS, September 2010

- **Getting individuals their health information in a reasonable time with a reasonable level of readability:** The only federal law governing timely responses to requests for records is HIPAA, which requires responses within 30 days with a possible 30-day extension. Also, HIPAA and HITECH do not define what "readable" means in terms of electronic copies. Therefore, there may be a wide variation among covered entities and business associates on how "readable" is defined. Normally, providers know this to mean that health information must be in human-readable format instead of a machine-readable format. However, neither HIPAA nor HITECH establish criteria on how easy it is for an individual to understand the information within his or her health record.

- **Most PHRs cannot download health information directly from EHRs:** The lack of this capability has forced individuals who want their information electronically to rely on external devices (such as CDs and thumb drives) to manually transfer information from the EHR to their PHR. The concern of damaging or losing the external information device raises security and usability issues. However, privacy and security concerns also remain prime barriers to opening EHRs to direct PHR access. Though efforts within the Blue Button initiative and the Direct Project are making headway in creating a more efficient and safe transport environment for health information, much work lies ahead before all PHRs can quickly and securely communicate with EHRs.

- **Making automatic updates available to PHRs and the concerns involved in such a feature:** Current legislation and proposed regulations require that a covered entity transmit a copy of an individual's health information to an entity or person designated by the individual, which may include a PHR. The onus of keeping an updated PHR rests solely on the individual at the present. The transmittal of updated health information to an individual's PHR is not a natural by-product of receiving care.

- **Portability of individuals' health information:** Though individuals have a right to an electronic copy of their health records, not all providers have digitized all their patients' health records. Many health organizations still do not have EHRs and some still function fully on paper. Some institutions have EHRs that provide individuals with electric portals to access their information. However, most patient portals are limited to the information collected by the institution providing the portal. PHRs provide an avenue for individuals to collect, store, and manage their health information in one place and can travel with an individual. However, as

explained above, PHRs still have many unresolved issues that prevent the full portability of health information.

- **Privacy issues of PHRs:** HIPAA and HITECH dictate a "floor" of privacy and security measures for a PHR associated with an entity covered under those laws. However, PHRs offered by entities not covered by HIPAA or HITECH are currently not subject to any national privacy and security standards. Some PHR vendors offer privacy policy statements, the adherence to which may be enforced by the Federal Trade Commission. However, PHRs offered by entities not covered by HIPAA are not required to post privacy policy statements, and to the extent they do, the information within these statements varies greatly. Consumers of PHRs have a difficult task determining whether PHR vendors release their PHR data (information within their PHR), to whom they release PHR data, and if the PHR vendor has security measures in place to protect their PHR data. ONC's PHR Model Privacy Notice is a step forward in addressing this issue. However, this notice is a communication tool that is policy neutral and does not address the lack of national privacy and security standards for PHRs.

- **Determining reasonable costs that providers can impose on individuals and the effects of these associated costs:** Under HIPAA and HITECH, individuals can be charged for the costs of obtaining a copy of their health information. However, this cost must be reasonable and cannot be greater than the entity's labor, supplies, and postage costs in responding to the request for the copy, and cannot include retrieval fees. HIPAA does not preempt state law with regard to costs, as long as the costs are reasonable and do not include retrieval fees. Most states have set further regulations on maximum allowable costs. Some states have specified a cost ceiling for labor, supply, and postage separately. However, most of these state cost ceilings currently reflect the cost of providing access to paper copies, not electronic.

- **Patient ID proofing:** National patient authentication standards do not exist for providers to ensure that personal health information is transmitted to the correct individual or individual's PHR. Authentication standards would allow providers to better ensure that the person or organization they are sending health information to is who they represent. With an increase in patient engagement, providers may receive more requests to transmit updated health information to, for example, an individual's PHR. Some of these requests for health information may come from an individual through his or her PHR. Proper authentication protocols can reduce

the risk of transmitting protected health information to the wrong individual. However, patient authentication standards must be balanced with usability standards that prevent authentication protocols from making it too difficult for individuals to obtain a copy of the health information from their provider. The White House has begun an initiative, called The National Strategy for Trusted Identities in Cyberspace, to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. The strategy calls for the development of interoperable technology standards and policies — an "Identity Ecosystem"—where individuals, organizations, and underlying infrastructure—such as routers and servers—can be authoritatively authenticated.

- **Granting proxy access to the individual's caregiver or another designee:** The HIPAA Privacy Rule generally requires covered entities to grant access and other rights to any person (such as a caregiver) who is the patient's "personal representative" (i.e., a person with authority to make health care decisions for that patient). However, sufficient national guidance does not exist to specify a process by which individuals can securely and efficiently grant their caregivers access to their health information. Caregiver access is often essential to ensuring continuity of care for individuals who cannot advocate for themselves. This access must be balanced with proper authentication criteria to safeguard an individual's health information from a person to whom caregiver status has not been granted by the individual. In addition, health providers should have and be educated on caregiver access protocols to remove unnecessary barriers to the continuity of care for the individual.

ONC is continuing to work with federal, state, and private stakeholders to determine the proper policy solutions and standards for the issues outlined above. This includes working with the Health Information Technology Policy and Standards Committees, working with the Federal Trade Commission and other governmental agencies on protecting PHR data, and launching pilots and grants to test these newly developed policy solutions and standards. Our work is highlighted on our website: www.healthit.gov.

HealthIT.gov