Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 31, 2016

Patient Access to Health Information in the Digital Age

In 2000, the Health Information Portability and Accountability Act (HIPAA) Privacy Rule established a set of federal standards for the use and disclosure of personal health information. The Privacy Rule also gave individuals the right of access to their health information. In the years since the Privacy Rule took effect, individuals have often complained that health care providers place undue restrictions on that access, in violation of HIPAA.

At the time the Privacy Rule was issued, most health information was recorded and stored on paper. Today, the widespread adoption of electronic health record (EHR) systems makes it easier for individuals to access their medical data. Under the Medicare and Medicaid EHR incentive program, which has paid $35 billion to hospitals and physicians that demonstrate meaningful use of EHR technology, patients must be given timely online access to information maintained in an EHR.

New requirements for the EHR incentive program will enable individuals to access their health information in real time using software applications (apps) on their smart phones and other mobile devices. Many health policy analysts see this as a potential game changer. Instead of hospitals and physicians controlling their health data, patients will be able to take charge and more easily use and share the data to make informed choices about their health.

However, analysts caution that expanding electronic access to health information faces a number of obstacles—cultural, economic, legal, and technical—that must be addressed.

HIPAA's Right of Access

The Privacy Rule gives individuals the right of access to inspect and obtain a copy of their protected health information (PHI). This is a legally enforceable right, not a privilege. Covered entities may deny access only in a very few circumstances.

The Health Information Technology for Economic and Clinical Health (HITECH) Act expanded the HIPAA right of access for electronic PHI (ePHI) maintained in an EHR. The act gave individuals the right to direct health care providers, health plans, and others subject to HIPAA—collectively known as covered entities—to transmit a copy of their ePHI to a third party of their choosing, such as a caregiver or another provider (see **Figure 1**).

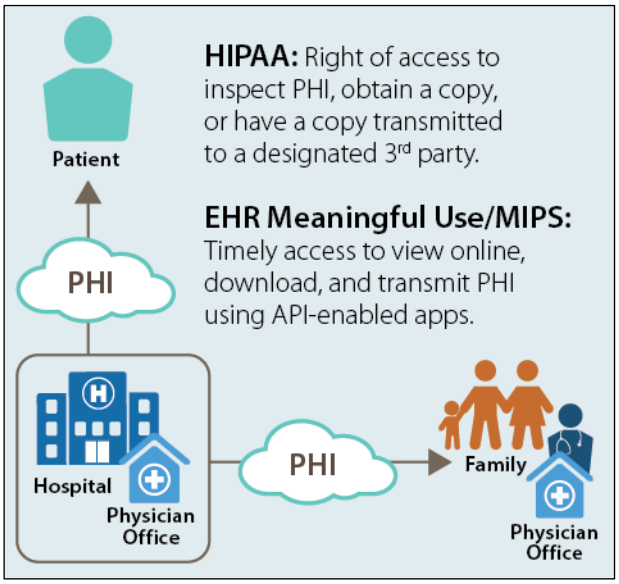
If an individual requests an electronic copy of information contained in his or her EHR, the covered entity generally must provide it in the format requested if it has the capability to produce the information in that format.

The right of access covers clinical information, insurance information, billing and payment records, wellness and disease management program records, and other information used by covered entities to make health care decisions about individuals.

Individuals seeking access to their health information sometimes find that providers are reluctant or slow to release it. Patient data is a valuable economic asset, and physicians and hospitals likely do not want their competitors gaining access to it. People stay with their doctors in part because their information resides with them, and obtaining and sharing health records with other doctors has traditionally been a challenge. The easier information moves, the easier it may be for patients to switch providers. In light of these factors, some health providers may worry that releasing patients' health information will cause them to lose patients.

Moreover, some health care providers mistakenly believe that they own the information and are under no obligation to share it.

Figure 1. Patient Access to Health Information



Source: Prepared by CRS

Electronic Access: View, Download, Transmit

Physicians and hospitals must meet a series of meaningful use criteria under the EHR incentive program to receive a Medicare and/or Medicaid incentive payment and avoid Medicare payment adjustments (i.e., penalties). One of the requirements for successfully demonstrating meaningful use supports the HIPAA right of access. Providers must give patients timely online access to view, download, and transmit (VDT) to a designated third party certain core data maintained in an EHR (see **Figure 1**).

A nationally representative survey sponsored by the Office of the National Coordinator for Health IT (ONC), within the Department of Health and Human Services (HHS), found that the proportion of individuals offered online access to their electronic medical records increased from 28% in 2013 to 38% in 2014, which was the first year that VDT became a meaningful use requirement. Typically, access is provided via a proprietary online patient portal.

As part of its testing protocol, the national health IT certification program tests EHR systems to ensure that they have a secure online VDT capability that encrypts and protects the data in accordance with IT security standards.

API-Enabled Access to Electronic Health Data

The next stage of meaningful use adds an important component to the VDT requirement—the use of application programming interfaces, or APIs.

An API is a set of programming instructions and standards that allows one software program to access the services of another. If a software developer makes an API publicly available, other developers can use it to design apps that communicate with that software. For example, many apps use the Google Maps API to request, retrieve, and display customized Google Maps.

The most recent set of regulations for the national certification program require EHR vendors to make their APIs and accompanying documentation public (i.e., open APIs) as a condition of maintaining product certification. Using these open APIs, software developers are then able to design apps that interface with EHR systems.

Beginning in 2017, hospitals and physicians—most of whom will be participating in the new Medicare Merit-based Incentive Payment System (MIPS)—must ensure that patients have the ability to view, download, and transmit data from an EHR using an API-enabled app of their choice (see **Figure 1**).

These apps must provide sufficient information to uniquely identify the patient and allow the patient access to (1) view and download some or all of the data elements from a common set of clinical data maintained in his or her EHR, and (2) transmit the data to a designated third party using either a secure (encrypted) method of electronic transmission or unencrypted email, if the individual chooses to accept the risk.

Unlocking the Potential of Health Care APIs

API-enabled apps will give patients and their caregivers easier access to ePHI and allow them to control its use and exchange (i.e., consumer-directed health information exchange). Open APIs will make it easier for developers to create apps that patients and caregivers can use to retrieve ePHI from multiple EHRs and consolidate it in a single location. For providers having difficulty using their EHR systems, open APIs will allow them to build customized interfaces in-house or shop around for an interface better than the one that came standard with their EHR system.

However, to ensure the widespread use of open APIs for accessing ePHI, important issues need to be addressed. First, patients and providers need to be educated about their rights and responsibilities under HIPAA and the HITECH Act. The HHS Office for Civil Rights (OCR) continues to receive complaints from patients having difficulty accessing their information. This year, OCR and ONC have released new guidance, a set of answers to frequently asked questions, and a series of short educational videos (in English and Spanish) to help individuals better understand their right to access their health information.

ONC also has developed an online patient engagement playbook for health care providers, based on best practices and real-world solutions, to help providers use health IT to inform and engage their patients.

Second, the widespread use of open APIs raises privacy and security concerns. Some experts worry that open APIs could lead to the unauthorized use and disclosure of patient information unless adequate privacy and security safeguards are in place.

To address these concerns, ONC last fall established an API Task Force. In May 2016, the Task Force released a report that generally supported the use of open APIs, provided they are properly managed, and appropriate standards and infrastructure are in place. The report made a series of recommendations on such topics as app registration and certification, patient authorization, identity proofing, user authentication, and auditing and accounting of disclosures.

Third, open APIs must be standardized, with transparent terms of use, policies, and developer fees. Proprietary APIs and a lack of transparency regarding the costs and policies associated with their use pose a challenge for start-ups seeking to partner with EHR vendors and develop new apps. While a single standard is not yet in place, an industry-led, market-driven effort—Project Argonaut—is working to accelerate the adoption of a standard that can be applied to web-based mobile apps for EHR data sharing.

In February 2016, the nation's largest EHR vendors and private health care systems, and more than a dozen leading professional associations and stakeholder groups, pledged to use standardized APIs so that mobile medical apps that are compatible with one another can easily be developed and marketed. Also, ONC is offering cash prizes for innovative and user-friendly apps for consumers and providers that use open, standardized APIs.

Finally, health policy experts question whether the current payment environment provides sufficient financial incentive for providers to engage and share information with patients. As already noted, health care providers will soon be subject to payment adjustments under the EHR incentive program (hospitals) and MIPS (physicians) if they fail to provide VDT access using API-enabled apps and are not actively engaged with patients.

C. Stephen Redhead, Specialist in Health Policy

IF10461

Disclaimer