Bloomberg BNA

Health IT Law & Industry Report™

VOL. 8, NO. 4 JANUARY 25, 2016

BNA INSIGHTS

Making a Patient's Right of Access Effective for Digital Health

By Jodi Daniel

There are very few types of information that people have difficulty obtaining in the digital age. Today, we access information on every possible topic and from all corners of the globe at the click of a button. We routinely combine information in new and creative ways to manage our own affairs and learn from the unique combinations of data we can collect. However, when it comes to the most fundamental and personal type of information that impact our lives—data that are held by entities with which we have relationships—we rarely do any of these things. This is the story of health information in the United States and how we can get patients real access to their health data.

There are many discussions about the value of patients having access to their health information for care coordination, treatment and self-care, and the federal government has worked hard to promote it. As we move toward ubiquitous adoption by health care providers of electronic health records (EHRs), focusing payment on health outcomes, and developing innovative tools that enable individuals to capture their own information through wearable sensors and mobile health applications, why is it that patients are not exercising their right to access their clinical health information? What more needs to happen to support the use of this health information in ways that benefit consumers? To realize

Jodi Daniel is a partner in Crowell & Moring's Washington office and a member of the firm's health care group, where she provides strategic advice to clients navigating the legal and regulatory environments related to technology in the health care sector. Daniel is the former director of the Office of Policy in the Office of the National Coordinator for Health Information Technology. She can be reached at jdaniel@crowell.com.

 ISSN 2151-2876

the benefits of patient engagement in health that are available through digital health tools, we must overcome these challenges.

What actions have been taken in the past?

Patients have had a right to access their health information from most health care providers and payers since April 14, 2003, the date the HIPAA Privacy Rule[1] took effect. The rules limit disclosures of ''protected health information'' but also *require* disclosure to the individual upon request. This right is quite broad. It applies to all information in a ''designated record set,'' which is all information used in whole or in part to make decisions about individuals, not just information in their official medical record. This was a bold change at the time.

Access to records has been a concern since the policy was adopted. Complaints to the Office for Civil Rights (OCR) at HHS for not being able to access data have been among the top three HIPAA complaints for ten of the last twelve years. Generally, these complaints have been resolved by OCR working with covered entities toward voluntary compliance, rather than OCR imposing fines.

There have been a few modifications to the access right over the years to grant individuals greater rights of access. Specifically, OCR has modified its regulations to expand the right of access to:

- include protected health information (PHI) held by labs;
- provide that an individual has a right to direct a covered entity to transmit PHI to a third party; and
- provide that a covered entity that holds PHI electronically must provide the information in the electronic form and format requested by the individual, if readily producible.

HHS has also supported patient access to their data through other regulations and programs. Specifically, the Office of the National Coordinator for Health Information Technology (ONC) has included provisions in its certification regulations for certified EHR technology to enable an individual to ''view, download, and transmit'' their data from an EHR.

The Centers for Medicare & Medicaid Services (CMS) has included in the EHR Incentive Program requirements for providers to make health information accessible to patients and to show that a percentage of their patients actually have accessed the data. This last issue, holding providers accountable for patients accessing their data, has been a controversial policy but one that HHS implemented because there was limited use of the access provisions by patients.[2] HHS changed the requirement for Meaningful Use Stage 2 to only require providers to demonstrate that one patient access her health information. These requirements ramp up to 10 percent of patients by 2018.[3]

The federal government also promoted the Blue Button Initiative. Blue Button is a simple-to-use, secure method for patients to get their health information electronically. ONC worked to enhance the technical standards for Blue Button and created a Blue Button Pledge Program,[4] for organizations to commit to making personal health data available to Americans.

So why hasn't behavior changed?

With all of the policy changes and requirements, why have we not seen the level of access that would reflect the value of this data and the trends in data access more broadly?[5] The primary reasons may lie in the culture of our health care delivery system.

First, some doctors would rather not share this information. When the HIPAA Privacy Rule was first published, I presented to a group of doctors, including a discussion of the patient right of access. I was interrupted, yelled at, and personally criticized for being involved in setting policy that undermined doctors' rights to ''their'' medical records and their ''personal notes.'' Some providers see medical records as assets of their business and sharing them would enable another provider to take their patients. While this sentiment has changed over time, many patients continue to face barriers to accessing their records.[6]

Second, even if health care providers are willing to share medical records, these requests take time and resources in an environment where there are many other competing demands. Providers also may lack sufficient understanding of how to comply with the patient access requirements and may be concerned if they give information inappropriately or without proper procedures that they may violate the HIPAA Privacy Rule and be subject to OCR oversight and penalties. This may make providers more inclined to establish procedures or fees that discourage requests by patients for their data.

Third, patients often do not ask for their health information. Sometimes it is because they do not understand the value of the information.[7]

---

[1] Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191; 45 CFR Part 160 and Part 164, Subparts A and E.

[2] CMS asserted that ''patient access to their health information is an important aspect of patient care and engagement'' and that providers ''are in a unique position to strongly influence the technologies patients use to improve their own care, including viewing, downloading, and transmitting their health information online.'' CMS, Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. 53968, 53976-77 and 54009 (Sept. 4, 2012).

[3] CMS, Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Modifications to Meaningful Use in 2015 Through 2017, 80 Fed. Reg. 62762, 62951 (October 16, 2015).

[4] https://www.healthit.gov/patients-families/pledge-info.

[5] In a 2014 survey of health care providers on HIPAA compliance, respondents were asked whether their organization experienced an increase in the number of patient requests for medical records since the HIPAA Omnibus Rule began requiring organizations to provide patients access to electronic copies of their records. More than half of respondents (57 percent) had not noticed an increase and did not anticipate one. *Compliance After the Omnibus Rule; 2015 HIPAA Benchmarking Report*, Medical Records Briefing (Vol. 30, No. 4), April 1, 2015.

[6] *Understanding Individuals' Right under HIPAA to Access their Health Information*, Jocelyn Samuels, Director, Office for Civil Rights, January 7, 2016, *available at* http://www.hhs.gov/blog/2016/01/07/understanding-individuals-right-under-hipaa-access-their.html].

[7] Niam Yaraghi and Joshua Bleiberg, *Your Medical Data: You Don't Own It, But You Can Have It*, Brookings TechTank, April 28, 2015, *available at* http://www.brookings.edu/blogs/techtank/posts/2015/04/28-health-record-copying-fees.

  HITR ISSN 2151-2876

Other times, it may be due to cultural issues in our health care system. There is a power differential between doctors and patients, and individuals may fear being labeled as ''difficult'' or having their request for their health information negatively impact the care they receive as a patient.[8]

While there are many things that interfere with a patient's right of access, we know that the more frequently a patient accesses his information, the more it motivates him to take action to improve his health.[9] We also know that when patients have access to their health information, they can improve the quality of the information in their health records by providing more accurate and up-to-date information to providers.[10]

What is in the new OCR guidance?

OCR released guidance on January 7, 2016, explaining the HIPAA Privacy Rule right of access. The guidance walks through all the access provisions, including the latest revisions under the HIPAA Omnibus Rule (45 CFR Parts 160 and 164), and many lingering misperceptions.

It addresses some critical issues that relate to digital health and the patients' ability to access electronic health information, such as:

■ *General Right to Access:* HIPAA access to health information is broad and includes all information used to make decisions about individuals, which is significantly more information than is generally available to patients through certified EHR technology. Access includes the right to transmit a copy to a third party designated by the individual.

■ *Requests for Access:* A covered entity may impose certain requirements on the way the individual makes a request. For example, a covered entity may require that the access request is in writing, including the use of specific forms.

■ *Verification:* The requirement for verification may not create barriers or unreasonably delay an individual's access to PHI. Unreasonable measures include requiring a person to physically come into the office, use a web portal, or use paper mail to make such a request.

■ *Form and format:* If the request for an electronic copy relates to a document maintained electronically, the entity must produce it electronically. It must be in the electronic form and format requested by the individual if it is readily producible in that form and format (even if the covered entity would prefer to provide access in a different electronic form and format).

■ *Manner of Access:* Individuals generally have a right to receive copies of their PHI by mail or email. Covered entities are not expected to take on unacceptable security risks to their system in providing access (e.g., using external portable media provided by the individual) and are not responsible for a disclosure of PHI while in transmission to the individual.

■ *Timeliness:* Access must be provided within 30 calendar days; however, the guidance also asserts that covered entities that already use health information technology in daily operations should be able to respond much faster as the 30 days is an outer limit.

■ *Fees:* Covered entities may impose a cost-based fee for providing access to PHI. Generally, fees may *only* include the cost of labor for copying the PHI, supplies for creating the copy, and postage. The fee cannot include any other costs, even if other costs are authorized by state law.

■ *Denial of Access:* There are very limited circumstances for denying access to PHI. A covered entity may **not** require an individual to provide a reason for requested access and may not be denied access based on a rationale if it is provided.

The guidance explains the relationship between HIPAA and the CMS EHR Incentive Program. The requirements of the CMS EHR Incentive Program overlap with HIPAA but differ in important respects. Specifically, the EHR Incentive Program applies to a smaller set of health information, a ''common clinical data set,''[11] while the HIPAA Privacy Rule applies to all information in a ''designated record set,'' a much broader set of data.

In addition, the EHR Incentive Program requires health information to be available much more quickly, within days, whereas the HIPAA Privacy Rule allows for up to 30 days to make health information available. Ultimately, if an entity participates in the EHR Incentive Program and is covered by HIPAA, the entity must comply with *both* the EHR Incentive Program requirements and the HIPAA Privacy Rule.

The guidance also discusses access through a mobile application or other device. Specifically, it references the requirements in the EHR Incentive Program that certified EHR technology must enable application programming interface (API) functionality to allow patients to use the application of their choice to access their data. The guidance does not, however, assert that use of APIs is required under HIPAA.

Guidance is helpful, but more is needed.

The OCR guidance clarifies misperceptions of the patients' right to access their health information. It explains that many of the barriers, such as significant fees for copies of records and requirements to obtain copies of records in person, may be unlawful. It also clarifies the misperception that a covered entity cannot email health information to the patient, and in fact, states the contrary—that a covered entity is *required* to do so if the patient requests email transmission after understanding the security risks.

The guidance supports the availability of health information in the form and format requested by the individual, if available, and requires that it be available electronically if it is maintained electronically. The guid-

[8] Dominick Frosch, et al., *Authoritarian Physicians and Patients' Fear of Being Labeled ''Difficult'' Among Key Obstacles to Shared Decision Making''* Health Affairs, 31, no.5 (2012): 1030-1038.

[9] *Engaging Patients and Families: How Consumers Value and Use Health IT*, National Partnership for Women and Families, December 2014, *available at* http://www.nationalpartnership.org/research-library/health-care/HIT/engaging-patients-and-families.pdf.

[10] *Demonstrating the Effectiveness of Patient Feedback in Improving the Accuracy of Medical Records*, NORC, June 2014, *available at*https://www.healthit.gov/sites/default/. . ./20120831_odrfinalreport508.pdf.

[11] 45 CFR § 170.102, 80 Fed. Reg. 62602, 62742 - 62743 (Oct. 16, 2015).

ance also clarifies the limited ability to deny patients' access to their data and reiterates the requirement that patients be able to direct that their information be sent to a third party, which would include a digital health product that they use to manage their information.

In a digital health environment, the HIPAA right of access alone does not ensure that health information will be readily available to patients where and when they need it and in a form that is useful.

However, in a digital health environment, the HIPAA right of access alone does not ensure that health information will be readily available to patients where and when they need it and in a form that is useful.

Assuming this guidance improves patient access to health information, some practical obstacles and limitations remain:

■ *Process requirements*: Providers can require that the request be in writing, and in the case of directing health information to a third party, they must do so.

■ *Timeliness:* Providers are only required to provide access within 30 days and may extend to 60 days.

■ *Verification requirements:* Providers are required to verify the identity and authority of the person requesting PHI (no technical requirements specified). While this can be accomplished electronically, covered entities may establish widely diverging processes.

■ *Form and Completeness:* HIPAA requires disclosure of all PHI in a designated record set, but the EHR system might only support electronic access to a common clinical data set. The patient only has the right to specify the format in which his or her PHI is provided if the PHI is ''readily producible'' by the provider in such format. This might effectively render a significant portion of the requested data inaccessible for consumption by digital health tools.

■ *Regularity:* The HIPAA right of access requires a request by the patient. The patient does not have the right to require the provider to send regular updates of their PHI, but may be required to make repeated requests for access every time new records are created.

■ *Practical Challenges:* The guidance mentions the availability of API functionality to support patient access through a mobile application or other digital tool of their choosing, but it suggests that security risks may limit a covered entity's use of API functionality.

While many of these issues would require a regulatory change, some can be addressed with guidance. For example, guidance and practical solutions would support providers making PHI available through innovative tools that rely on API functionality.

If a provider is using Certified EHR Technology (2015 Edition), and a patient requests access through a mobile application that is using API functionality, the HIPAA Privacy Rule should require the provider to grant this request from the individual because the form and format requested is ''readily producible.''

HHS could clarify that security concerns should be addressed but should not be an excuse for patient access when access through API functionality is readily available.

HHS could also support development of best practices that build on existing uses of API functionality in other sectors to help providers address security appropriately.

While many of these issues would require a regulatory change, some can be addressed with guidance.

Perhaps the most significant barrier to patient access to health information is beyond current regulatory authority to address: the uneven protection of health information in the United States. HIPAA protects most health information that is held within the health care system, but once that information is shared with the individual for her use, in most cases there are few—if any—privacy protections. Individuals may forgo use of tools that consolidate or otherwise allow them to effectively use their own health information out of concern that taking the information outside the protected health sector will allow it to be used in ways that they do not expect or desire.

Conclusion

Existing laws designed for a non-networked world do not assure a patient's convenient and timely access to all of her health information in a single location. This leaves many innovators stuck at the starting line, and patient self-management and communication with providers behind the times.

Therefore, it is crucial to examine practices that may interfere with the appropriate flow of information to consumers. The new OCR guidance addresses many of these challenges to the degree possible under existing policies. This is a positive step, but the policies themselves need to go further and, in some cases, modifications to the HIPAA Privacy Rule should be considered.

Best practices are needed to address practical challenges—first and foremost, the security and technical challenges for use of APIs.

The legal structure of health information protections needs to be reconsidered in light of the changing sources and uses of health information, to ensure protection of health information outside the health care system.

Beyond changes to the rules, the legal structure of health information protections needs to be reconsid-

   ISSN 2151-2876

ered in light of the changing sources and uses of health information, to ensure protection of health information outside the health care system. When considering the lack of protections of patient health information once it is released outside the health care setting and the explosion of data created outside the scope of HIPAA, it is easy to see that we have a set of policies that are not matched with our new reality. It is imperative that we address the uneven protection of health information.

The government took the important first step of creating the right and the expectation that individuals have access to their health information. Innovators are creating a new generation of tools to leverage that information.

To unleash the improvements digital health and health data can bring to health care, self-care, coordination of care, and informed decision-making, it is time to create a new approach and a new set of expectations. This approach must guarantee comprehensive access to health information, and protection of health information, regardless of where it originates from or where it is maintained.