Release or Not? Patients' Rights to Health Records Becoming Increasingly Complex

By Mary Butler

It is a dark and stormy night at a mid-sized regional trauma center when an EMS team brings in a 30-year-old man who is suffering from a prescription narcotics overdose. The patient is conscious but disoriented when he arrives on a gurney. When he wakes up, his loved ones, dutifully at his side, convince him to voluntarily seek inpatient treatment. As the medical staff prepare his discharge and referral paperwork, the patient, aided by his tech savvy family, requests that none of the claims generated by the hospital visit be sent to his insurance company—they will be paying out of pocket.

The hospital staff calls their chief privacy officer to confirm this is a valid request—and it is. Since September 2013, a HITECH-HIPAA Act modification allows patients to enact a "request for restrictions," allowing them to sequester certain health information from their health record and not release it to an insurer if they pay for a service out of pocket. The privacy officer counsels the patient that he must be diligent about making sure every provider involved in this aspect of his care understands his wishes. While his insurance company isn't alerted about this admission, the privacy officer notes that the encounter will remain in the hospital's records.

Three months later the man is back in the hospital's emergency department, this time for a broken wrist after slipping on ice. Since he has sought treatment for narcotics addiction, he requests that his pain be treated by a non-steroidal anti-inflammatory (NSAID) instead of Vicodin. The attending physician notes this and verifies the request by looking at the patient's prior overdose admission. The patient wants this encounter billed to insurance, but when the nurse asks him for his insurance information, he remembers the wise counsel the privacy officer gave him three months ago. "By the way," he asks, "can you make sure my insurance company doesn't find out why I requested an NSAID?"

The hospital's health information management (HIM) department works painstakingly to redact this information from his claim and the nursing staff sends him on his way.

While this patient was unusually savvy—most patients aren't aware that HITECH revised HIPAA to allow "requests for restrictions" in the release of information (ROI)—patients have received the message that they have more access to their health data than ever before. Thanks to the "meaningful use" Electronic Health Record (EHR) Incentive Program and other federal initiatives, more patients are leaving their doctor's offices and hospitals armed with copies of their visit summaries and access to their patient portal, which has much more clinical information than they are used to getting.

While patients and providers both benefit when patients are more informed about their care, expanded access to health information is putting ROI specialists and HIM professionals in increasingly challenging positions. Knowing whether or not to release information to a patient, their insurance company, or another provider has never been more complicated.

"Consumer access is a huge plus for both the consumer and their health, but whenever healthcare organizations exchange information—digitally, on paper, or verbally—there is a new opportunity for data loss or attack," says David Finn, a health IT officer at Symantec.

HIM professionals are increasingly finding themselves in a shifting privacy landscape thanks to Congress and the Centers for Medicare and Medicaid Services (CMS), which have both recently proposed changes to the HIPAA Privacy Rule (discussed in detail below). And while the ROI rules become more complex, the opportunity for errors to be noticed has also increased. The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) is launching its second round of privacy breach audits aimed at calling out providers found to be restricting patient access to their data.

ROI Under Pressure

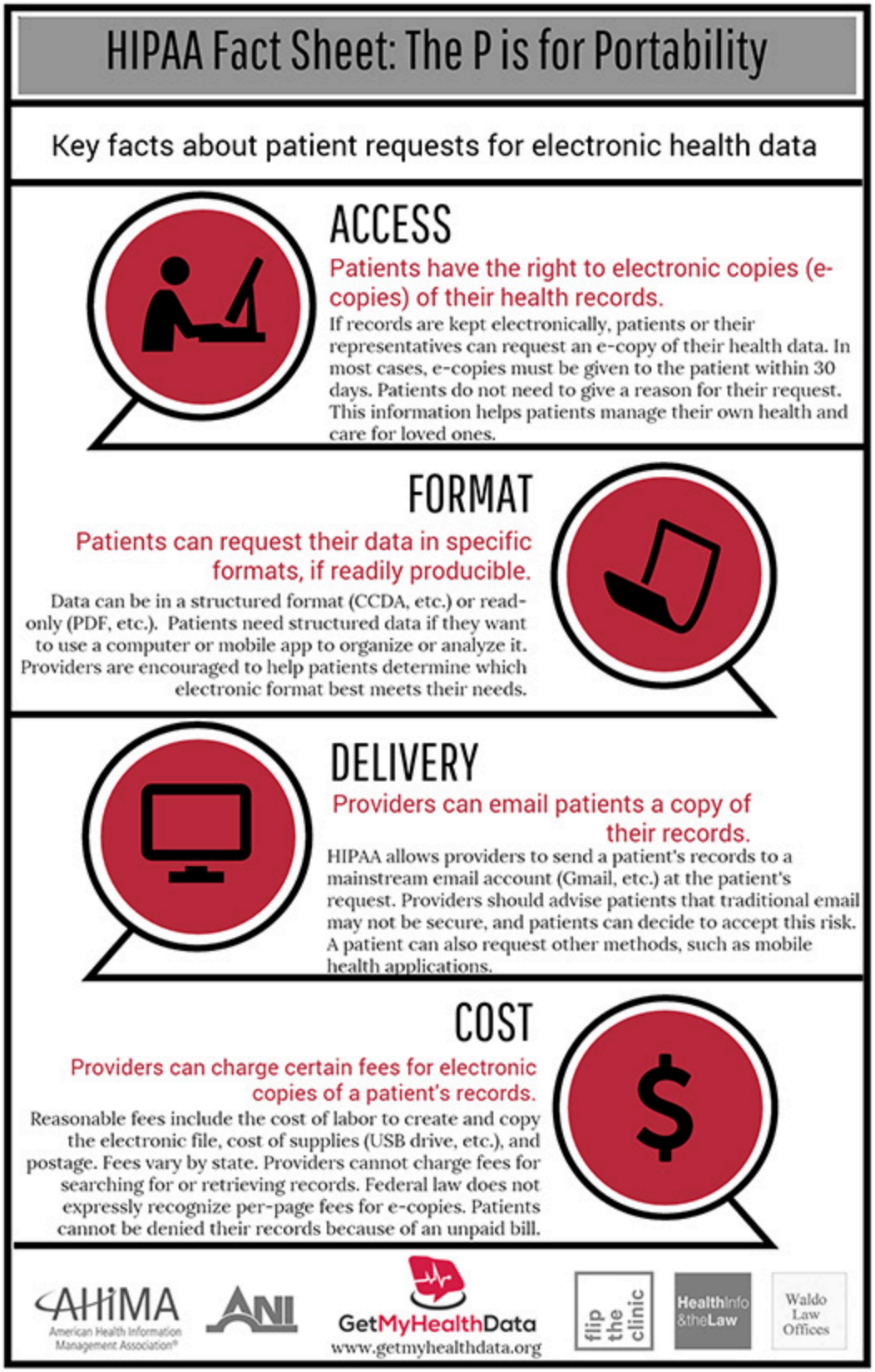
In July 2015, the US House of Representatives passed the 21st Century Cures Act, which would have made significant changes to the de-identification and re-identification of protected health information (PHI) used in research. That legislation was not voted on by the Senate. Instead, the Senate's Health, Education, Labor, and Pensions (HELP) Committee is drafting companion "Innovation" legislation to the House bill, but much of the context was in flux as of press time. It does contain several provisions that focus on data sharing, improving EHR interoperability, and imposing a broad range of fees for patient access to records.

In early February, the Substance Abuse and Mental Health Services Administration, a branch of HHS, issued a proposed rule that would continue to require that a provider obtain a patient's consent for the disclosure or sharing of medical records that would identify, directly or indirectly, an individual who has been diagnosed or treated for a substance abuse disorder. However, it would also let "other health-related information shared by the Part 2 program to be disclosed," without consent, "if permissible, under other applicable laws."

What's more, HIM professionals must also heed new guidance from OCR regarding a patient's right to access their health information (below). The new guidelines: further define what constitutes a "designated record set;" specifies that 30 days is the "outer limit" for turning around a patient's records request; and reinforces that providers cannot require an individual to only request their records in person, among other clarifications.[1] In February, the Office of the National Coordinator for Health IT and OCR started releasing a series of fact sheets to give more visibility to patient's rights under HIPAA.

HIPAA Fact Sheet: Getting Patient Access to Health Data

The following offers key facts about patient requests for electronic health data.



Source: GetMyHealthData campaign

"There is more healthcare information going to more places in more formats than ever before, and that freedom makes centralized control over that information nearly impossible," Finn says. "Clearly, HIM professionals—the people who

understand the data and privacy operations—can't oversee the portals or all the information going in and out. Couple this with limited or no information governance and HIM professionals are fighting an uphill battle."

HIM also finds itself in the middle of another new modification to the HIPAA Privacy Rule that allows some covered entities to report the identities of individuals prohibited from having a firearm for mental health reasons to the Federal Bureau of Investigation's (FBI) National Instant Criminal Background Check System (NICS). The rule only applies to "a small subset" of HIPAA-covered entities that "either make the mental health determinations that disqualify individuals from having a firearm or are designated by their states to report this information to the NICS," said OCR Director Jocelyn Samuels in a blog post on the change.[2]

Debra Primeau, MA, RHIA, FAHIMA, president of Primeau Consulting Group, says this is potentially a tricky area for HIM because behavioral health information carries special protections. HIM professionals not only need to weigh what federal law requires, but what state law requires. In California, where Primeau lives, she has to be mindful of the Confidentiality of Medical Information Act (COMIA) and the Lanterman-Petris-Short Act. Both laws pertain to the authorization and release of medical records tied to short-term and long-term behavioral health admissions or treatment. When making a determination to release a record, HIM professionals must follow the guidelines of the most stringent policy.

"I understand why these laws are necessary, but we're going to have to continue to walk that fine line of providing patient privacy and providing information that is necessary to the intent of the law," Primeau says.

And while there are new changes, many in healthcare and even HIM are still unclear on exactly what HIPAA says and does not say in the first place—one reason why OCR recently issued guidelines for consumers on their rights to health information, mentioned above, after hearing feedback that people are still being denied access to their information. Similar guidance was released by OCR for providers, discussing just what types of information exchanges and releases HIPAA allows in an attempt to foster better interoperability.

The same goes for the privacy changes instituted by the HITECH Act. For example, HITECH changed HIPAA to allow facilities to give family members or caregivers access to patients' records—really anyone involved in the care of a patient during their episode of care—and not just the executor of an individual's estate or formal power of attorney. It is up to the facility to make the decision—though it is well known that gray areas don't sit well in the privacy and ROI world.

Patient Expectations vs. Reality

Advances in EHRs and patient portals, as well as mixed public messaging on what HIPAA actually allows, has resulted in confusion on both sides of the ROI equation. Primeau says patients often expect their online patient portal to contain much more health data than it does.

"I think there was an expectation that with a patient portal, patients would have access to everything, and from what I'm hearing is that's not necessarily the case. There are inconsistencies in the system… I think there's a perception on the patient's end that the information is all shared but the information is still in disparate locations," Primeau says.

Nowhere is this confusion more evident than in the "Tracer Stories" collected by the GetMyHealthData campaign, an alliance of consumer and industry groups, including AHIMA, dedicated to fostering access to digital health information. GetMyHealthData collects the experiences of volunteers—a.k.a. Tracers—who ask their providers for data and report their success or failure back to GetMyHealthData, who then publish the experiences online. The Tracer results have been decidedly mixed. For example:

- One Tracer volunteer reported that her hospital charged her $90 to have some of her medical records transferred to a new doctor.
- A self-described Army wife reported waiting months to get dental records transferred from Washington, DC, to Florida after she moved. The dentist promised an e-mail to speed things along, but it never came.
- Another Tracer volunteer suffered an adverse reaction to a nerve block and wanted to see documentation of the incident so that it wouldn't happen when he had the same procedure repeated later. The provider's HIM director could only send an abstract of his record, which contained no information about the event.
- Other Tracers reported facing a confusing series of authorization forms, phone calls, and missed connections.

The issue of asking individuals to pay for their health data is a controversial one when it comes to ROI because many believe the regulations are too open-ended. HITECH-HIPAA allows providers to charge a "reasonable" fee for the materials and postage required to produce the records, and state law varies as well. The GetMyHealthData campaign has been collecting accounts from individuals who believe the charges may be getting out of hand, especially when it comes to electronic portal access fees.

For example, one Tracer patient reported a case at a suburban Washington, DC, area clinic where patients can pay $125 per year for the "Gold" tier of service, which offers the ability to book appointments online and get access to their immunization history. For $250 per year, or the "Platinum" membership, a patient gets all of the perks of "Basic" and "Gold," as well as three e-visits per year.

While many patient advocates feel all health information should be free, some providers feel justified in charging for access. Reproducing sometimes lengthy health records takes staff time and company resources, as does the cost to launch and maintain an electronic patient portal. Other hospitals outsource ROI to third party vendors, whose business model can in part depend on fees for reproducing records. Also, some hospitals take a nuanced approach, offering one free copy of a medical record but then charging for subsequent copies or for total access to all records.

Coordinators from the GetMyHealthData campaign have met with HHS and CMS officials to discuss issues like portal fees. "While CMS says that it does not believe it is appropriate for patients to be charged fees for portal access, they also note that patient access to data is covered by HIPAA," McKay says. "We think that this message either isn't filtering down to providers given all that's on their plates, or that there is confusion about how HIPAA and meaningful use intersect, leaving some wiggle room."

Empowered Patients Come With a Cost

Elisa Gorton, MAHSM, RHIA, CHPS, director of corporate responsibility and a privacy officer at St. Vincent's Medical Center in Bridgeport, CT, says she's seen an increase in the number of requests by patients to amend information in their health records. Before patient portals her facility would get five to 10 record amendment requests per year—now she can expect four to five per month. Giving patients the opportunity to look for and flag errors in their records is undoubtedly a good thing. But some patients, Gorton says, call HIM to ask for changes that shouldn't be made or to question why aspects of their medical history were mentioned in a recent encounter.

"A common question we get from patients is 'I didn't come in for that [medical issue], why is that on this [visit summary]?'" Gorton says. "Most electronic records have a problem list, which we had to do under meaningful use, and it's pulling information forward every time a patient presents, and patients question it."

Without an intermediary or context, patients can easily misinterpret what they're reading in their health records. "I've seen situations where information is loaded into a portal and seen by the patient before the physician has seen it, and sometimes that's information that a doctor wanted to deliver or explain," Finn says. "When patients look at a single test result without fully understanding the context, they can think they're safe and they're not, or they think something horrible is going on and really nothing really horrible is [going on], but they don't understand that data."

There also is inherent risk in providing patients with a hard copy of their visit and discharge summaries when they leave a facility, Gorton says. "We're finding that when patients get these large chunks of information at discharge, they might just toss it in the garbage can or drop it on the way to their car, and we'll find that in different places. That exposes their PHI to anyone who can come into contact with it," Gorton says.

Tom Walsh, CISSP, the founder and managing partner of tw-Security, says providers can get carried away with well-intended efforts to supply patients with their information. It is standard for many providers to give patients compact discs (CDs) containing PDFs of their health records and imaging results to take to a specialist. Some providers, though, make the mistake of decorating the disk with their logo and branding. Where the marketing department sees opportunity, a privacy officer sees liability—or bait for an identity thief. The data stored on CDs often is not encrypted which makes it easier for patients to share with multiple providers. However, that also means that if it's dropped in a hospital parking lot it's easy for someone else to steal the information. Walsh says he's even seen these CDs given out with the patient's name and date of birth written on the envelope.

What all healthcare professionals ultimately need when dealing with the public's "insatiable desire for data" is the ability to weigh public good versus patient autonomy. In order for patients to make the most of their health data, there needs to be a strong education component on behalf of the provider, says Aviva Halpert, RHIA, CHPS, president of Advize Proactive Consulting. As part of this education, primary care physicians and patient advocates should be educating patients on interpreting portal data. "But they are so overwhelmed with everything else they have to do that it isn't always feasible," she says.

One approach the industry has been using to provide better patient education is to put nurse practitioners and physician assistants in teaching roles when they see patients, but they are overburdened as well, says Halpert.

"Everybody needs to be teaching," she says.

Notes

[1] US Department of Health and Human Services. "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524." www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/.

[2] Samuels, Jocelyn. "Obama Administration Modifies HIPAA to Strengthen the Firearm Background Check System." HHS.gov. January 4, 2016. www.hhs.gov/blog/2016/01/04/obama-administration-modifies-hipaa.html.

Mary Butler (mary.butler@ahima.org) is associate editor at the Journal of AHIMA.

Article citation:
Butler, Mary. "Release or Not? Patients' Rights to Health Records Becoming Increasingly Complex" *Journal of AHIMA* 87, no.4 (April 2016): 14-19.