Bitter ROI Irony: Former ONC HIPAA Rights Advocate Faced Same Frustrating Record Access Challenges as Other Patients

By Lucia Savage, JD

One hallmark of my work as chief privacy officer at the Office of the National Coordinator for Health IT (ONC) was reminding everyone about the individual's right to get a copy of their own protected health information (PHI) and, since 2009, to download or transmit it directly from a certified electronic health record (EHR) system.

In my last few months at ONC in late 2016, and continuing into 2017, I had two occasions to exercise this right myself. This essay describes my release of information (ROI) experiences in an annotated context. It also suggests ways Health Insurance Portability and Accountability Act (HIPAA)-covered entities and their business associates, including specialized document handling companies, can improve the ROI experience for everyone.

AHIMA's members are familiar with this right of an individual to get their own PHI (I will refer to this as the Access Rule). The Office for Civil Rights (OCR) and ONC have excellent materials on the rule available for review.[1] The original regulation was finalized in 2000 as 45 CFR 164.524.[2] In section 13242 of the Health Information Technology for Economic and Clinical Health Act (HITECH), Congress interpreted that regulation to require, in statute, that it also included an individual's right to transmit the PHI "directly from an electronic health record" system.[3] In 2013, OCR updated the Access Rule in light of HITECH.[4] These rules underlie the work I did with ONC. Finally, in December 2016, Congress passed and President Obama signed the 21st Century Cures Act (Cures), which adds requirements that EHR vendors and healthcare providers not "block" an individual's ability to compile a longitudinal record of their health history—a record that could be compiled relatively easily if the Access Rule really worked as written.[5] My own experience is just one of thousands of experiences that illustrate it doesn't work as written, and that we have a lot of work to do.

On a business trip in 2016 it became clear that I needed some dental work. As it turned out, a 41-year-old filling had failed. I saw my dentist July 6, 2016. He removed the old silver and drilled out the rot, leaving a 2mm hole in my tooth, which required a crown. He started that work and I paid $1,965. He submitted a request to the insurance company for reimbursement. On August 9, the insurance company denied benefits, claiming that a crown was unnecessary. On September 26, 2016 the dentist filed an appeal. In the appeal, the dentist included his complete notes and the digital photos from several angles of the 2mm hole in the tooth. He also opined that the hole was too large to be filled with a traditional filling.

On October 3, 2016 I also filed a detailed written appeal, as I had paid my dentist in full. In that appeal, I requested a copy of any PHI used to decide my benefits claim that my dentist had not supplied. I also requested an estimate of the copying costs for such PHI, not knowing what was in their files.

The Access Rule's preamble from 2000 explains that one reason for the rule is an individual's right under federal law to know the evidence used to make an adverse benefit determination against them.[6] In the case of PHI, this evidence is contained in a "designated record set," which is PHI "used by a covered entity to make decisions" such as benefit denials "about the individual."[7] Note that my request was in writing, the data was clearly identified, and there was no question about my identity. I received no answer. Then, the following saga unfolded:

- On November 9, 2016 the insurance company sent me a denial letter identical to the prior denial letter, but with a new date. They did not respond in any way to my request for my PHI. I complained to the insurance regulator, the District of Columbia Department of Health.
- By December 26, 2016 I still had not received my PHI. On December 27, nearly three months after my first request, I filed a complaint with OCR using its online tool. I uploaded my October 3, 2016 letter which included the request for PHI.

- On December 30, 2016 I called the insurance carrier. After first being disconnected when I escalated to a supervisor, I finally found a person who promised me I would get a response in seven to 10 days. I never got a response.
- On January 25, 2017, I received a nice letter from OCR saying it had informally contacted my insurance company, and explained in detail my rights. But it did not say how much longer I would wait for my PHI.
- On February 14, I called OCR. I spoke to an OCR analyst who told me to wait *another* 30 days for my PHI. She also told me that the insurance company's privacy officer had called OCR in response to OCR's letter, but that the privacy officer had never heard of nor seen my request for my PHI. I told the OCR analyst that the company's poor internal processes did not excuse the failure to supply my PHI. I then continued to wait.
- On February 25, I filed a second complaint with OCR because I had not received my PHI.
- On March 3, I received a letter from the insurance company's chief compliance officer that included printed versions of the relevant PHI from the designated record set. Needless to say, the only medical information the carrier had about my tooth was what my dentist had submitted.
- Shortly after March 3, I wrote to the compliance officer and pointed out that the only evidence they had was that a crown was necessary. The carrier's own coverage documents stated that it was required to give full credence to clinical evidence from an individual's treating professional unless there was countervailing evidence. There being no countervailing evidence about my tooth, I asked for my benefits to be paid. Shortly thereafter, I received a check for $300. Yes, that is 16 cents on the dollar that I paid my dentist. A pyrrhic victory to be sure, but it felt good nonetheless.

Some things the insurance company could have done better in this situation are included in the sidebar above. I also think OCR's letter, while quite informative about the Access Rule, could have been more consumer-friendly. A person with enough savvy to file an Access Rule complaint with OCR has some knowledge of their rights already. What would have been helpful was to know was:

1. Who did OCR talk to at the covered entity?
2. When should the consumer expect to get their PHI?
3. What were next steps the consumer should take to get their PHI?

ROI Fail Postmortem #1: What This Dental Insurance Company Could Have Done Better

1. The Appeals Unit that in October 2016 received my appeal along with my Access Rule request seemed to have just ignored it. At best, the unit did not know how to respond to the request. Internal consciousness raising and a consumer-centric philosophy could fix this. Ignoring the request resulted in a federal complaint.
2. The facility privacy officer could have contacted me once she heard from OCR. I am a chief privacy officer now, and have the responsibility of dealing directly with inquiries from individuals. I would contact the upset individual if OCR contacted me about an Access Rule request.
3. Six months passed between October 2016 and March 2017. Even if the privacy officer got a letter from OCR on approximately January 25, why did it take until March 3 to reproduce 12 pages of materials that my dentist had already submitted?
4. The privacy officer, to mitigate risk to their employer, could have thought about *why* I requested my PHI. What if someone at the insurance company had just said: "Oh, Ms. Savage, we do not have any information other than what you submitted, let me see if I can't get someone to look at your claim again."

After that ordeal, I thought I was done with the bitter taste of ROI irony, but not so. In March 2017, I enrolled my family in my new employer's life insurance. To effectuate my life insurance choice, my husband and I each needed to complete the medical evaluation, which meant getting my PHI from our current physician. We see different physicians at the same medical group.

I thought it would be easy. I thought I could just upload the signed life insurance company release of information authorization form through my doctor's EHR portal, once I securely logged in with my two-factor authentication from a recognized device. (My physician is a stage 2 participant in the "meaningful use" EHR Incentive Program with a full EHR.) That would certainly have been compliant with HIPAA. But it did not happen.

My physician's office staff told me through the portal that they are not authorized to handle requests for PHI from individuals. I was told to call a phone number in Baltimore, MD and request the forms from the provider organization. My husband was undertaking the same process for his life insurance with my employer, so he called to obtain authorization forms, since our physician's organization does not accept authorization forms that they did not draft. We got the right forms by mail about seven days later, some drafted by the physician organization and others with the branding of a large well-known health information record handling company. The forms all had been photocopied so many times they were grey, not black.

My husband and I filled out each of the three pieces of paper relevant to our individual requests. I called the Baltimore document office to see if I could email the forms. I was told only faxing or mailing was allowed. Not only is emailing forms by individuals perfectly lawful, but I don't have a fax. So, I stapled my husband's forms together and my forms together, put them in a single envelope and mailed them to Baltimore. I waited. Two weeks passed. We eventually received photocopies of my husband's medical records, but not mine.

I called the Baltimore office. They referred me to the health information records handler. I called them. They were very nice, but had no record of my authorization, even though it was in the same envelope as my husband's authorization. Clearly, the envelope had been received because my husband's forms were received and processed. The service representative told me to resubmit the forms, and that I would have to re-sign them so that the date was accurate, because they would not accept my photocopy of the forms they had misplaced. I was also told it was illegal for me to send them via email (not true, see above). They also told me that it was illegal for them to send me my PHI by email (also not true; they could use appropriately secured email, for example with one of many encryption programs, or I could waive a secure transmission). I had a deadline from the life insurance company which would not accommodate starting the process over again.

I escalated to a supervisor. I spent about an hour on the phone. I begged and pleaded because it was not my fault that her customer, the physician's medical group, lost my forms. Finally, she agreed to allow me to email her a scanned copy of the forms I had previously sent with my husband's forms. I received my records by mail about 10 days later.

But it wasn't over. The life insurance company requested that I get a more recent physical before it would approve my application. This necessitated another document request. I checked with the life insurer, which advised that if I just printed what was in my Summary Care Record on my physician's EHR portal, and submitted a recent lab result, they would have what they needed.

At my physical, I requested a lab order. At the lab, I asked the lab staff to send the results directly to me as is my right under the Clinical Laboratory Improvement Act (CLIA) so that I would have the results in hand, and not have to depend on my physician's office records process.[8]

Following the physical, I printed my visit summary from the EHR portal, scanned the lab results and visit summary to a PDF, and emailed the documents to the life insurer's secure fax server. (Note, by scanning my lab report, I eliminated its ability to be used as structured data. This was probably not particularly relevant for life insurance. For patient-mediated exchange for care, however, scanning would at the minimum cause re-keying at the receiving physician's office, and at the worst generate redundant lab tests to obtain the structured data.) I bypassed entirely my physician's record office in Baltimore, and its document contractor.

However, it turned out the life insurer needed my physician's notes from the physical. My physician does not use OpenNotes, and notes are not legally required to be posted in the portals of Certified EHRs, so I could not automatically download them.[9] Securely logging into my physician's EHR portal, I asked my physician to cut and paste their notes into a message so I could securely retrieve and print them. That was not allowed, I was told. I could, however, request the notes through the document office and its formal authorization process—that did not work the first time around.

I called the Baltimore document office twice over the course of three days, and left voicemails both times, but my calls were never returned. Desperate because the medical group's document office was not responsive, I messaged my physician, begging her to print the notes, put them in a sealed envelope and leave them with the office receptionist, where I would pick them up using my photo ID. Thankfully, this worked. I submitted the notes to my life insurer, and my life insurance was approved.

Based on my experience and knowledge, printing the notes and leaving them at the receptionist desk where I picked them up with a photo ID is no different under the HIPAA Privacy or Security Rules than pasting them into the secure messaging

feature of the portal. But I am glad that my physician agreed to this bypass method.

Now working as the chief privacy officer for a covered entity, I am sympathetic to the need to keep track of what PHI is going out the door, to whom, and for what purpose. In 2017, however, there are so many better ways to do that without wasted time, stamps, mail, faded paper forms, and lost correspondence. I took a photo of the paper generated by these two requests for PHI (see above). The stack is 3.5 cm high. Imagine what this process would look like if we actually used 2017 technology like secure messaging through portals, web-design, or even email with attached PDFs of forms. Imagine what it is like for caretakers of the profoundly ill trying to manage daily life while endlessly navigating the typical ROI quagmire.

We can do better.

ROI Fail Postmortem #2: What the Physician Practice Could Have Done Better

Here are some things the physician's practice could have done differently to provide the PHI I requested for my life insurer, without any special software installations, upgrading their EHR to a 2015 Edition certified version with that infamous open-application program interface (API), or having to deal with an app I chose.[10]

1. **You don't have to use a form.** First, while HIPAA regulations say a covered entity may use a form to confirm an individual's request for their own PHI is legitimate, a form is not required. Rather, what is required is a reasonable inquiry into the legitimacy of the request and confirmation of the identity of the requestor.[11] A state-required form that interferes with an individual's rights to health information under the Access Rule may be preempted.[12]
2. **Recognize and take action on messages and PHI requests sent through authentic portal log-ons.** Here, my first request for my PHI was through a two-factor log-in to a messaging portal. As my electronic credentials were reliable, nothing more by way of permission paperwork was legally required. My physician may have needed clarity about which records I requested, but those questions could have been asked in a follow-up message or a phone call to me. By the way, eSignatures instead of ink are valid under federal law.[13]
3. **Empower local office staff to ensure PHI requests are routed correctly and responded to**. Here, I sent a valid signed "request for information" document from my life insurer. I wouldn't have even minded if my physician's office referred this submission to their document office, where knowledgeable follow up could have been made. Instead, the request was categorically rejected.
4. **Accept any piece of paper that is legitimately signed, no matter who drafted it.** As AHIMA's standardized Patient Request for Health Information Model Form becomes adopted, organizations should not create barriers by requiring their branded forms be used. Lawyers, this note is for you. (For details on AHIMA's release of information form, visit www.ahima.org/modelform.)
5. **Demand easy-to-install technology from your EHR vendor or your document management vendor.** If this were almost any other business setting, the portal itself would include the ability to request records through a simple drop-down available after a person authenticated their identity through the log-in process. Or, an EHR portal could link to an online tool developed by the covered entity's document management company.
6. **Be an early adopter of the e-version of AHIMA's Patient Request for Health Information Form.** Maybe if, as is planned, AHIMA's standard form is widely used and soon turned into a standard set of software data points, an app will be developed, as is envisioned in ONC's 2015 Edition of Certified Health Information Technology rule and recent OCR/ONC videos on patient access.[14]

Note: None of the examples described in Postmortems 1 and 2 depend on an organization adopting the open API described in ONC's 2015 Edition of Certified Health Information Technology rule. Nor do any of these examples require an organization to allow an individual to use an app for collecting their PHI (though those features would be awesome).

Notes

[1] Department of Health and Human Services. "Your Rights Under HIPAA." HHS.gov. February 1, 2017.

[2] Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information: 45 CFR Parts 160 and 164." *Federal Register* 65, no. 250 (December 28, 2000).

[3] Department of Health and Human Services. "H.R. 1-112. Title XIII—Health Information Technology (HITECH Act)." HealthIT.gov. February 19, 2009.

[4] Department of Health and Human Services. "Pages 5253–5706." *Federal Register* 178, no. 17 (January 25, 2013).

[5] Congress.gov. "H.R. 34 – 21st Century Cures Act: Section 4006." December 13, 2016.

[6] Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information: 45 CFR Parts 160 through 164, preamble." *Federal Register* 65, no. 250 (December 28, 2000): 82,547.

[7] Department of Health and Human Services. "Standards for Privacy of Individually Identifiable Health Information: 45 CFR 164.50." *Federal Register* 65, no. 250 (December 28, 2000): 82,489.

[8] Department of Health and Human Services. "42 CFR 493: Office of the Secretary; 45 CFR Part 164: CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports." *Federal Register* 79, no. 25 (February 6, 2014): 7,290.

[9] OpenNotes. Home page.

[10] Department of Health and Human Services. "2015 Edition Certification Companion Guide. Application Access – All Data Request – 45 CFR 170.315(g)(9)." HealthIT.gov. October 30, 2015.

[11] Department of Health and Human Services. "45 CFR Parts 160 and 164: Standards for Privacy of Individually Identifiable Health Information; Final Rule." *Federal Register* 65, no. 250 (December 28, 2000): 82,462, 82,547.

[12] Department of Health and Human Services. "Does the HIPAA Privacy Rule preempt state laws?" HHS.gov. July 26, 2013.

[13] House.gov. "15 USC Ch. 96: Electronic Signatures in Global and National Commerce." June 30, 2000.

[14] Department of Health and Human Services. "Access."

Lucia Savage (lucia.savage@omadahealth.com) is the chief privacy and regulatory officer at Omada Health, based in San Francisco, CA. From October 2014 to January 2017 Savage served as the chief privacy officer at the Office of the National Coordinator for Health IT.

Article citation:
Savage, Lucia. "Bitter ROI Irony: Former ONC HIPAA Rights Advocate Faced Same Frustrating Record Access Challenges as Other Patients" *Journal of AHIMA* 88, no.11 (November 2017): 30-34.