Top HITECH-HIPAA Compliance Obstacles Emerge: Analyzing lessons learned from six months of Omnibus Privacy Rule implementation efforts

By Mary Butler

Have a spare 32.8 million hours? The US Department of Health and Human Services (HHS) sure hopes so.

As noted in the *Federal Register*, that figure is the total number of hours the HHS Office for Civil Rights (OCR) estimated it would take all HIPAA-covered entities combined to enact the landmark privacy and security changes brought on by the HITECH-HIPAA Ominbus Final Rule.

Ahead of the September 23, 2013 compliance date of the HITECH-HIPAA Omnibus Final Rule, media outlets were clucking over the total number of hours OCR federal regulators estimated it would take to comply with the law.

Break that number down and things start to seem slightly more manageable: 125,000 hours for covered entities to establish or modify business associate agreements; 350,000 hours to document security procedures; and 167 hours to revise the language of privacy notices.

While it may make for sensational discussion, the health information management (HIM) professionals actually doing all this legwork haven't had time to wring their hands over man-hour estimates. They had to dive in and put new plans in motion. On the whole, with proper planning, providers and consultants say they've had adequate time to become compliant with the Omnibus Rule updates.

The final Omnibus Rule went into effect in March 2013, with a final compliance date of September 23, 2013. However, many healthcare experts remain particularly concerned about the extent to which providers and other HIPAA-covered entities are truly compliant. It's easy for many covered entities, especially small ones, to fly under the radar until a breach incident or some other HIPAA violation occurs.

The degree of optimism and pessimism swirling around HIPAA compliance often depends on a provider's resources, training, and system-wide communication. With that in mind, just over a year since the Omnibus Final Rule was released, it's important to examine just where covered entities are in their compliance efforts, as well as evaluate OCR's ability to enforce the rules—a matter that has raised concerns from federal watchdogs.

Mary Poulson, MA, RHIT, CHC, CHPC, former co-chair of AHIMA's Privacy and Security Council, consults with small office-based physician practices on Omnibus Final Rule compliance, and agrees that this segment of covered entities are most at risk for privacy breaches and noncompliance. They're busy getting ready for ICD-10-CM/PCS, implementing electronic health record systems (EHRs) and attesting to the "meaningful use" EHR Incentive Program—while also trying to find time to implement the HITECH-HIPAA Omnibus Final Rule.

"I think office-based practices do the best they can with the tools they have to work with. A lot is expected of them," Poulson says. "[However] I would venture to say that many private physician groups aren't even aware that the final rule became final and that there were changes to HIPAA."

While HIPAA compliance can vary among providers, there are some provisions of the Omnibus Rule that have proven harder to comply with than others—and have become obstacles in the path to compliance for many providers.

Obstacle #1—Restriction Requests for Out-of-Pocket Services

Easily one of the most buzzed about provisions of the Omnibus Final Rule among HIM professionals is the right for patients to sequester information from their health record if they pay for the related service out-of-pocket.

The provision is intended to help consumers with sensitive conditions, or who have sought treatments that they don't want their health plan to know about, such as plastic surgery, mental health conditions and treatments, or diagnoses such as HIV.

Vickie Patterson, CPA, CIA, CRMA, CAC, national compliance lead for Protiviti, consults with providers on HIPAA compliance. She says that because the provision is so new, and consumers aren't aware of it, many providers have not yet been put to the test. Covered entities must update and distribute their Notice of Privacy Practices (NPP) to reflect the changes. This will start to get the word out.

"I noticed in all the organizations I worked with, they made the appropriate revisions, they've been distributing it, and pointing out to patients that there have been changes and they need to read it [the NPP]," Patterson says.

But the NPP is just one of the adjustments providers must make. The hard part of complying with this rule is changing the workflow and operations to accept these requests and ensure it is handled properly and the information is not shared with payers.

Once the Omnibus Rule was published, Protiviti started building privacy reviews and gap assessments for this provision even before the enforcement date. Patterson has found that providers are really thinking the health information restriction workflow and process through. But vendors play a role in designing EHRs that help users accommodate patient requests. In many cases, Patterson says the technology doesn't support what the regulations are requiring, particularly when it comes to requests for restrictions.

Some providers, such as Baylor Health System, based in Texas, are actively working with their EHR vendors on restriction functionality. Baylor's chief compliance officer, Robert Michalski, CHC, CHPC, says fine tuning the restriction process will be ongoing, internally and with vendors. Some vendors have been proactive in creating EHR systems that can handle sequestering information, Patterson says. "I think for the most part what I've seen is, most of the vendors that I've dealt with have the ability to go in and have the private folders for things like HIV testing and psychotherapy notes," Patterson says.

Nancy Davis, MS, RHIA, CHPS, system director of privacy at Ministry Health Care, based in Door County, Wisconsin, says her organization has devised a procedure for a series of triggers in the EHR in the event a patient requests a restriction. But like many providers, her organization's system hasn't yet been tested. While she has confidence in it, she remains skeptical about whether it will become a frequently utilized service.

"One of the biggest things in this economy, I think very few people feel comfortable saying 'I'll pay out-of-pocket,'" Davis says.

She says that if someone was going to be tested for a sexually transmitted disease, or seek treatment for a mental illness, it would be easier to hide that information by going to a new provider altogether.

"I think it's very, very difficult to not have that information permeate your record," Davis says. "So, here's the thing, if you're trying to hide something, it's probably going to come out one way or another. If you're trying to hide an HIV or diabetes status, diagnoses like that, even if [you] go in for a sprained ankle, the fact that [you're] HIV [positive] or diabetic is a co-morbidity."

Obstacle #2—Business Associate Agreements Get a Reboot

One of the most dramatic changes to HIPAA enacted by the Omnibus Final Rule was that it said all healthcare business associates and their subcontractors would now also be covered under the HIPAA Privacy Rule. The final rule also increased the number of entities considered business associates by expanding the definition to include subcontractors that create, receive, maintain, or transmit protected health information (PHI) on behalf of another business associate. Additionally, business associates are now responsible and liable to the covered entity for the activities of their subcontractors who have entered into a business associate agreement with them. The definition of the term business associate was also expanded to include:

- Health information organizations
- E-prescribing gateways

- A person that provides data transmission services for protected health information (PHI) exchange on behalf of a covered entity and requires access to such information on a routine basis

Personal health record (PHR) vendors Business associate agreement (BAA) compliance dates vary as follows:

- If there is an existing agreement between a covered entity and its business associate that has been signed prior to January 25, 2013 (the date of publication of the Omnibus Final Rule) and does not need to be renewed by March 26, 2013 or September 23, 2013, then the agreement can remain valid until September 23, 2014. This effectively created a transition period of one year from the compliance date of September 23, 2013.
- If the BAA was executed after January 25, 2013, then it must be compliant with the Omnibus Rule by September 23, 2013.

For Michalski, updating his organization's BAAs has been his number one concern since the rule was finalized. Michalski estimates that his organization has several thousand business associates, so identifying every one and updating their BAAs is a work in progress, he says.

Michalski says that prior to the Omnibus Final Rule, his organization didn't have a comprehensive BAA repository, though it had a contract database. However not every contract made its way into the database. The process of going through and identifying all of the organization's business associates, evaluating whether they fit the new definitions of a business associate, and then updating their agreements has been a tremendous endeavor, Michalski says.

Complicating the matter is the tug of war the organizations and business associates are in between whose agreement to use. "There are some very large companies and associations and surveyors that take the position that 'if you want to use our services, you have to use our business associate agreement,'" Michalski says. "It's kind of a dance that we do between our legal departments to evaluate whose business associate agreement is really going to win at the end of the day, and which terms within them may prevail."

Daniel Shay, JD, an attorney for Alice G. Gosfield and Associates, specializes in helping healthcare organizations comply with HIPAA. The dance that covered entities must do with their business associates is something he sees a lot. Often, Shay says, it's a matter of contractual leverage.

"If you're a giant hospital system, and the vendor really wants your business, you can hand the vendor your business associate agreement and say 'Sign this or we walk.' And the vendors will sometimes [do] that," Shay says. "But if you're dealing with one of the larger EHR companies, or some of them now provide free EHRs, they're going to say 'Sign our business associate agreement or find another health record.' So what ends up happening is you have this patchwork of different BAAs."

Patterson is confident that a majority of providers will be able to get their contracts up to speed by the final September 2014 enforcement date. As mentioned above, certain covered entities were granted an extra year, beyond the September 2013 compliance date, to review and renegotiate their BAAs. Again, smaller practices are at a bit of a disadvantage.

"Some of the larger ones, even though there's more contracts and more amendments to get done, I think that they actually have a little bit more of an advantage if they have the additional staff and have more people focused on different activities going on," Patterson says. "They've had probably close to 18 months now, or will have before their deadline."

OCR Responds to Criticism of Lax HIPAA Enforcement Efforts

In recent months, the Office for Civil Rights (OCR) has been the subject of criticism from HHS's Office of Inspector General (OIG) for falling behind on HIPAA enforcement. A December report from OIG criticized OCR for not being in compliance with the National Institute of Standards and Technology's Risk Management framework for its information systems used to process and store investigation data, because the agency chose to focus on operability rather than system and data security.

"For example, OCR did not obtain HHS authorizations to operate the three systems used to oversee and enforce the Security Rule," the report stated. "In addition, it did not complete privacy impact assessments, risk analyses,

or system security plans for two of the three systems. Exploitation of system vulnerabilities, normally identified through the Risk Management process, could impair OCR's ability to perform functions vital to its mission."

In response to the criticism, Rachel Seeger, OCR's senior health information privacy outreach specialist, says "the industry can expect that we [OCR] will continue enforcing rules." In a statement to the *Journal of AHIMA*, OCR noted that the agency corrected administrative and information system documentation deficiencies, which were highlighted in the report, prior to the final report's publication.

"The major recommendation by the OIG was that OCR should implement an audit or audit-type function rather than rely solely on complaints as a means of assessing compliance with the HIPAA Security Rule," OCR officials stated. "OCR is in total agreement with the recommendation of the OIG, and in our response documented for the OIG all the steps we have been taking to pilot and implement an audit program since the conclusion of the OIG field work in 2011. Even without an appropriation, OCR is committed to maintaining a permanent audit program."

Additionally, Seeger says the agency is undertaking huge outreach and education programs to help patients become aware of their new rights under the HITECH-HIPAA Omnibus Final Rule, and help providers—particularly small organizations—become compliant. "We have been trying very hard to address the importance of leadership in our press releases and in our education efforts. It is so important for individuals who are in leadership positions to take accountability and compliance starts with them," Seeger says.

Indeed, the Omnibus Final Rule includes changes to increase patient engagement with their health records and protected health information (PHI). The rule also removes HIPAA privacy protections from records pertaining to an individual deceased for more than 50 years; establishes new limitations on the use and disclosure of PHI for marketing and fundraising purposes; and prohibits the sale of PHI without appropriate authorization, among other measures.

Seeger says it's still too early to speculate as to how enforcement efforts are going, or how many fines have been levied enforcing the new protections. "Just like with any other rulemaking, the industry has to have some time to come into compliance," Seeger notes.

OCR is being aggressive in its patient engagement efforts, posting videos on its website and establishing educational partnerships with organizations such as Medscape.net. Through Medscape, OCR is offering continuing education credits for providers who learn about the new law, calling it a "one-stop shop" for small physician practices.

Obstacle #3—Redefining HIPAA's Breach Definition

Another major change to HIPAA guidelines under the Omnibus Final Rule is the definition of what constitutes a breach. The rule changed the "harm threshold," a measurement called for in the interim rule to determine if patient harm was created from a breach and therefore warrants a breach notification, to the need for covered entities to conduct a risk assessment when a breach occurs. This has caused confusion about whether and when covered entities need to send out breach notifications.

The Omnibus Final Rule, published on January 25, 2013, included final modifications to the Breach Notification Rule, which replaced the interim final rule originally published in 2009. The definition of "breach" in 45 CFR 164.402 is now defined as "the acquisition, access, use, or disclosure of protected health information in a manner which compromises the security or privacy of the protected health information."

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. As a result, breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

Again, smaller providers could struggle more with this change, Davis says. "It really depends on maybe the level of compliance and sophistication of these small practices," she says. "I know that when I talk to colleagues and other areas, they don't worry about any of this until they get a breach. And then they say 'What should I do?' and I say 'Did you have this covered in your Notice of Privacy Practices?' And they say 'No, I'm supposed to do that?'"

The new rule demanded a change in the way HIPAA training is conducted, Davis says. She admits that her new training efforts were meant to scare employees "a little," but she says she was tired of hearing "I didn't know that," or "Nobody told me that," when it came to reporting breaches.

Davis says her old training plans were more academic, focusing on the history of HIPAA, compliance, and fines. "And that was all well and good, but it wasn't really applied practically. So last year, especially as we migrated into more and more systems with the EHRs, we took a look at it and we did two things," Davis says.

First, Davis surveyed her organization's privacy officers and asked what they'd like to see redesigned in training and education around privacy and security. Then she went through three years of privacy and security logs to see which areas needed the most attention.

"We sort of dumped the academics and we focused on real case scenarios," Davis says. "We just went through where we were having problems, and then we focused on consequences."

"I don't think we've been strong enough. We've always focused on consequences for the patient, but now we're focusing on consequences for the employees… corrective action. 'You could lose your job or your license,'" Davis says.

Baylor's Michalski says that under the new guidelines, there has been an increase in the number of reportable breach disclosures at his facility.

"In terms of handling the breach scenarios… the effort on our part hasn't really changed," Michalski says. "The end analysis has somewhat increased our disclosures though."

Michalski says he's witnessed a phenomenon that other privacy and security experts have raised alarm bells about—consumer breach fatigue. He says that in the past, and even before he came to Baylor, he used to see a bigger consumer response when security breaches were front page news.

"Even in the last year or two, where we've had to send out letters like that, we're just getting less and less responses back. People aren't calling and asking as many questions about those," Michalski says.

Read More
Performing a Breach Risk Assessment

www.ahima.org
For more information on breach risk assessments, read this September 2013 *Journal of AHIMA* Practice Brief located in the AHIMA HIM Body of Knowledge.

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

Article citation:
Butler, Mary. "Top HITECH-HIPAA Compliance Obstacles Emerge: Analyzing lessons learned from six months of Omnibus Privacy Rule implementation efforts" *Journal of AHIMA* 85, no.4 (April 2014): 20-24.