Be e-Prepared: Tips for Tackling Ever-changing Electronic Audits, e-Discovery, and e-Measures

By Mary Butler

Don’t let the quiet before the storm fool you. Regulators might be hushed now, but compliance activity is expected to keep health information management (HIM) professionals on their toes throughout 2015. As electronic health record (EHR) implementation becomes more pervasive, so too does the ever-evolving role of keeping EHRs compliant with a myriad of new regulations that have been—or soon will be—implemented in the coming months.

Major legislation that went into effect in 2013 and 2014, such as the HITECH-HIPAA Omnibus Final Rule and the e-measures accompanying the “meaningful use” EHR Incentive Program, have allowed healthcare providers time to come into compliance. But representatives from the US Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR) have indicated that aggressive enforcement of HITECH-HIPAA is on the horizon.

Congress put off ICD-10-CM/PCS compliance for another year until 2015, but clinical documentation improvement (CDI) training should not be delayed since claims submitted to federal and commercial payers are being scrutinized more than ever. Recovery Audit Contractors (RACs) and Medicare Audit Contractors (MACs) are also expected to return with a vengeance soon, meaning CDI efforts must continue.

Potential changes to the Federal Rules of Civil Procedure (FRCP) demand that providers make protected health information (PHI)—including data from EHRs, mobile devices, and social networks—available for e-discovery requests. HIM professionals must be up to the task as patients and consumers grow more fearful about the security of their PHI. In August, Chinese hackers stole non-medical information from 4.5 million patients in a breach involving Community Health Systems. Then, in another high-profile case in August, hackers breached Apple’s iCloud and stole files from many celebrities in a breach that renewed concerns about cloud systems and the EHRs that rely on them.

More and more EHRs and other data are being used to meet or prove compliance with regulations and quality programs. Because of this, HIM professionals should follow suit with the Boy Scouts and Girl Scouts of America and “Be e-Prepared,” collecting merit badges (or peace of mind) by using their skills to ensure their organization meets the various forms of necessary healthcare compliance.

As HIM directors and compliance officers prepare for the year ahead, experts offer the following tips for ensuring e-preparedness.

RACs and MACs Bite Back

The impending implementation of ICD-10 isn’t the only reason providers need to have CDI programs in place—the resumption of the Centers for Medicare and Medicaid Services (CMS) RAC program, even in its limited capacity, should keep HIM professionals on alert. In February 2014, CMS announced it would be temporarily suspending the much-feared audit program due to a backlog of appealed cases and the re-awarding of contracts. In August, however, CMS announced that RACs would resume with limited review.

Ostensibly, RACs and other fraud chasing contractors such as MACs, Zone Program Integrity Contractors (ZPICs), and Comprehensive Error Rate Testing (CERT) Contractors, are intended to help the government and commercial payers recover overpayments by reviewing submitted claims for medical necessity. And according to figures released by CMS, the contractors are doing a good job. In 2013, CMS claimed RACs recovered $2.3 billion, according to the American Hospital Association’s (AHA) RacTrac website. According to the AHA, however, as of March 2014, 64 percent of providers who appealed RAC decisions were successful, with a total of $263 million returned to providers.

Jordan R. Viehman, MHA, RHIA, government audit coordinator for Cone Health, says that while the state of RAC investigations were up in the air, MACs picked up the slack, raking providers over the coals on their Medicare claims. Complicating the matter is the "two midnight" rule, which CMS issued in the spring of 2014. The rule attempts to clarify what Medicare considers to be criteria justifying an inpatient stay. According to the rule, a patient who stays in the hospital for two midnights meets the standard. The rule requires physicians to certify, supported by documentation, why a patient needs to be admitted for an inpatient stay rather than an observation stay. But CMS put a lot of stipulations on the definition, causing chaos among auditors and providers alike. Coders were caught in the middle having to figure out whether to code cases as observation or inpatient stays.

Viehman says the volume of audits that many providers face, and the record requests that come with them, can be overwhelming, forcing some hospitals and clinics—large and small, urban and rural—to shut their doors or suffer huge hits to revenue. Additionally, appealing RAC and MAC audits is costly in terms of the staff needed to respond to denials and the tracking software needed to monitor the process.

HHS' Office of the Inspector General (OIG) is also scrutinizing claims, especially those for short inpatient stays, Viehman says. To cope with all the audits, she recommends that HIM departments make sure to respond to auditor requests for records in a timely fashion and as completely as possible.

"You've got to make sure that on the front end you have good quality review processes in place when you're getting these observation cases looked at. [Get] these short stays for inpatient cases looked at, and make sure the documentation tells the whole story," Viehman says. "Look at it from the auditor's perspective. They have to be able to piece together the patient's story and that hospital stay, and if you look at it and you're unable to piece that story together, chances are they're not going to be able to."

Viehman says there's a lot of talk in Washington, DC about redesigning the audit process, and that CMS is holding hearings on the appropriateness of the audits. "To be honest, the appeal process is so backlogged right now because of these inappropriate audits. There's a big question on how are we going to clean this up going forward. And what can we do going forward to prevent this crisis," she says.

In response to the appeals backlog, CMS has offered affected providers a settlement, or "administrative agreement mechanism," under which they would pay hospitals 68 percent of all medical claims appealed by those providers. The majority of those claims are from short inpatient stays that RACs claim should be billed at outpatient rates. Viehman says the offer is "all or nothing" because providers can't pick and choose which appeals they feel the settlement should apply to.

"In other words, if you have a claim that is an inpatient-only account that was denied, and you take the appeals settlement, you are essentially settling for 68 percent of something that should have been paid at 100 percent," Viehman notes. "It not only will entice physicians to pay more attention to these audits and their documentation—an opportunity for CDI to shine—but it is also going to impact those providers who may own physician groups."

Achieving Meaningful e-Compliance and EHRs

With stage 2 of the meaningful use program in full swing, eligible providers are still struggling to comply with a number of requirements to obtain their incentive payments from CMS.

Mac McMillan, chair of the HIMSS Privacy and Security Policy Task Force and CEO of CynergisTek, says providers are wrestling with the encryption requirement. Under meaningful use, eligible providers need to encrypt data stored within EHRs as well as consider encryption technologies for health information on mobile devices, laptops, and removable USB devices, as well as data exchanged between patients and providers.

Additionally, McMillan says, meaningful use-required risk assessments "continue to be an issue for some people. We hear from people in their 12th hour of attestation and they're saying 'Oh, I forgot I had to do a risk assessment,'" he says.

The coordination of care elements of meaningful use are a trouble spot, too, due to a general lack of interoperable systems across the continuum of healthcare, McMillan says. "What's interesting, we've done some audits around stage 2. In a couple cases, they were actually meeting the [coordination of care] requirement, they just weren't documenting it properly," McMillan says.

Sandra Joe, MJ, RHIA, director of corporate compliance at Northwest Community Healthcare, is overseeing the rollout of a new EHR system. Tracking meaningful use compliance and having protocols in place for MAC or RAC audits are top of mind for Joe, she says. She is also being proactive to keep clinicians and HIM professionals aware of the perils of copying and pasting in EHRs—which can lead to inappropriate documentation, degradation of a record's reliability, and possible fraud investigations. Joe says she'd like to see regulators be more aggressive in enforcing policies against copy and paste.

"You should not be allowed to copy and paste. That should be a standard. So software companies that sell EHRs should disable the ability to cut and paste," Joe says. "That's what I believe from a compliance perspective. We need to have people really support that, because of the liability."

Joe has been working in work groups with physician champions of the EHR rollout to reinforce the message that copy and paste shouldn't be going on.

"When a person is requesting a record, an attorney from the outside, they can start seeing that there's a lot of copy and paste in the record," Joe says. "It's a liability to the organization, but it also impacts patient care."

Eyes on HIPAA Compliance

OCR will be under pressure this coming year to step up enforcement of the HITECH-HIPAA Omnibus Final Rule requirements. Part of the increased urgency stems from an OIG report that found OCR has not demonstrated adequate oversight and enforcement of HIPAA. OIG recommended—among other things—that OCR conduct more periodic audits of covered entities.

This summer, in speaking at an American Bar Association conference, HHS attorney Jerome B. Meites, JD, said that OCR's last 12 months of enforcement activity will "pale in comparison to the next 12 months," according to the June 13, 2014 article "HHS Attorney: Major HIPAA Fines and Enforcement Coming" in *Data Privacy Monitor.*

That means providers and privacy officers had better make sure their business associate agreements are in order, that encryption, risk assessments, and mitigation processes are in place, and that protocols for dealing with a privacy and security breach notification are ready to go.

McMillan and his company are getting a lot of requests from providers for help in preparing for risk assessments and putting programs in place. He also helps providers prepare for e-discovery requests.

"A lot [of organizations] are getting a lot smarter in wanting to have the tools to better identify the information that's relevant to a claim—so that what they provide lawyers with, to use and process a claim, is information that they know is related to the incident," McMillan says. "As opposed to what they used to do, which is download their database and turn it over to the lawyers to process. That was extremely costly to them, and risky, because it exposed a lot more information to those lawyers than what was necessary."

But McMillan, like many other security experts, remains concerned about providers' ability to respond to new and existing threats, both internal and external.

"We have a lot of organizations that are not managing their environments effectively from a security perspective. They're not patching as diligently as they should be. They're not hardening systems before they put them in production," McMillan says.

This can get even riskier for organizations that are in a merger-and-acquisition-centric field like healthcare. "There's a lot of risk around these smaller ones [organizations] that don't have the same level of privacy and security as the bigger ones do. And when they don't address that early on, it basically introduces risk into their environment when they connect," McMillan says.

Some providers, however, could see a brief reprieve in HIPAA audits. Even though Meites warned OCR's HIPAA enforcement would be accelerating, in September OCR said it would be delaying the second phase of the HIPAA audit program. The delay will last until OCR is able to roll out new software that allows audited organizations to submit data through a web portal, according to the publication *Healthcare Info Security.*

In speaking at a Healthcare Information and Management Systems Society event in September, Linda Sanches, OCR's health information privacy senior advisor, noted there is no solid timeframe as to when OCR will resume audits. But she did provide specifics on how audits will be conducted and how many providers and business associates will be involved.

For instance, Sanches said OCR had originally planned to conduct 400 desk audits. With the new technology changes, they plan only to do fewer than 200 targeted audits. Auditors will be looking for evidence that providers and business associates are conducting risk analyses, and take a comprehensive look at sanction processes, Sanches told *Health IT Security*. Additionally, OCR will be asking providers for a complete list of their business associates.

e-Compliance and Federal Rules of Civil Procedure

Upcoming amendments to the Federal Rules of Civil Procedure, if approved by Congress in 2015, should cause providers to look at their record preservation policies for critical electronic health information—specifically, the proposed rules that govern electronically stored information (ESI) and e-discovery requests, a function handled in healthcare settings by HIM professionals.

As Ron Hedges, JD, noted in the August 2014 *Journal of AHIMA* article "Federal Changes Proposed for eDiscovery Litigation Rules," to remain compliant with e-discovery laws under the FRCP providers must demonstrate a reasonable effort to develop "a defensible records retention policy, perhaps within an overall information governance structure, that anticipates the imposition of a duty to preserve." This is vital for all HIM departments, Hedges wrote, and staff must "document that policy, implement it, and monitor it."

Kris Vann, product marketing manager for Actiance Inc., a healthcare compliance consultant, says the FRCP amendments are also intended to help keep providers from hoarding patient data to the point where it becomes detrimental and a liability to the organization. For many years, providers have kept records out of fear of falling out of compliance and being hit with a sanction. The clarification of the rules will be welcome news to healthcare professionals.

"The congressional changes are meant to alleviate that somewhat and say 'Hey, you're not going to get a spoliation sanction if it's not willful or gross negligence.' If you're in good faith, trying to protect against this, you shouldn't be hoarding," Vann says. "I think in the beginning people were doing a knee-jerk reaction. And now they know we need to clean up health."

Electronic Communication Threatens HIPAA Compliance

To stay compliant with HIPAA and respond effectively to e-discovery requests, healthcare organizations increasingly need to monitor employee use of social media, e-mail communications, instant messaging, and text messaging.

Joanna Belbey, social media and compliance specialist for Actiance, advises providers to treat new forms of communication as they would paper-based and verbal communications in their efforts to prevent data leakage.

"The thing about social media in healthcare is just that there are no real new rules and procedures. It's taking your existing procedures and applying them to a new media," Belbey says. "It's just common sense—[but] it requires additional effort."

According to Belbey, federal regulators are going to start asking providers to prove that they're monitoring employees' behavior on social media for HIPAA compliance. "For example, if you're going to allow those people [employees] to use social media, for whatever reason, you need to have good policies in place and make sure they understand the guidance, and then you have to supervise it and prove to regulators that you're doing spot checks, reviewing communications to make sure there are no violations," Belbey says.

To do this effectively, providers need to have thoughtful training programs and accessible best practices. They should also consider third-party monitoring of all electronic communications. In today's healthcare environment, clinicians "channel hop" when discussing patient care. Doctors, for example, may discuss a patient over the phone, and then continue the conversation later over a secured instant or text messaging platform, or even via Skype or Google Hangout. All of these channels should be monitored since they could be subject to e-discovery. It's critically important to know how providers, and HIM departments, capture this information.

"When you do e-discovery, you need to be able to reconstruct that conversation so it makes sense—keep the structure of social media in place so that you understand who said what to whom, and who saw that correspondence," Belbey says. "And that, unless you've set your system up to capture it in that way, is a very time consuming process. And can cost many thousands of dollars of lawyers going through documents and e-communications."

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

Article citation:
Butler, Mary. "Be e-Prepared: Tips for Tackling Ever-changing Electronic Audits, e-Discovery, and e-Measures" *Journal of AHIMA* 85, no.11 (November 2014): 22-25.