Part B Insider (Multispecialty) Coding Alert

HIPAA Compliance: Don't Let HIPAA Worries Plague Your Small Practice

Know these compliance basics to avoid HIPAA audits for smaller practices.

Since every practice is different, there is no one-size-fits-all plan for addressing HIPAA compliance. Now that Phase 2 of the HIPAA audits courtesy of the Office of Civil Rights (OCR) are hot and heavy, even small practices should be wary of their patient interactions, as these random desk audits will continue through Dec. 2016.

If the news coming from both the OCR and OIG is any indication, every practice is vulnerable to an audit, and the HHS and its subsidiaries are tired of excuses for the lack of office HIPAA plans. Sole proprietors and small groups need to be especially watchful, particularly as they still manage a heavy load of paper documentation and forms that need to be copied, faxed, and mailed, which is where common HIPAA violations occur. For these specific reasons, it is crucial that every Medicare provider and staff member appreciate the magnitude of HIPAA and revere the policies in place to protect patients and their PHI at your practice□no matter the size.

Respond to Verifications

"A covered entity is required to comply with HIPAA, regardless of its size," explains **Michael D. Bossenbroek, Esq.**, of Wachler & Associates, P.C. in Royal Oak, Michigan. "Compliance includes written policies and procedures. If a practice has to report a breach, is selected for an audit, or is the subject of the complaint, and OCR investigates, OCR likely will expect to see the entity's compliance policies."

Verification. If you or your business partners received an Audit Entity Contact Verification form over the past few months, don't panic. This important form is meant to verify the contact information of the covered entities at the practice, so it is wise to respond to it to avoid confusion down the road.

"The OCR has stated that if an entity doesn't respond, it does not mean the entity will avoid an audit," says Bossenbroek. "And, being asked to provide contact verification information does not mean you will be selected for an audit."

After verifying your contact information, the OCR will send you a questionnaire regarding the size, type, and operations of your organization. You'll also need to identify each of your business associates. It will then use this information to put together its pool of potential auditees.

Remember the rules. Be aware of the audit timelines for addressing OCR concerns. If you do find yourself at the center of a desk audit, you'll have ten business days to submit the requested data via an online portal to the OCR for review, suggests the OCR's guidance on 2016 desk audits. Once the digital information is checked, you'll receive an email with the results, which you must weigh in on within ten business days. After your commentary is researched, the auditor follows up with the final audit report within 30 business days of your response.

Partners count too. Business partners of covered entities will also be part of the audit process, the OCR guidance indicates, and they will be privy to the same basic principles of investigation that the covered entities have succumbed to, including the desk reviews and a copy of the final audit report.

Once the final reports and reviews are said and done, you may still be chosen for an onsite audit. After you get the alert via email, the auditors will perform a more detailed in-house audit, lasting approximately three to five business days. If

their findings show a serious breach on your part, you may be subject to the typical notifications and punishments related to a HIPAA breach. For a legal review of what's involved in both a desk and onsite audit and the repercussions for both covered entities and their business associates, take a look at this link http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when.

Put Your Policies in Place Now

Even a small practice can make an impact with HIPAA protocols by stopping breaches before they start and setting up business agreements that are compliant, but the initial task of creating resources and office compliance codes can be a daunting task for a limited staff to undertake.

"It is a real challenge for smaller practices with limited resources to comply with HIPAA," explains Bossenbroek. "And, I think the challenge comes more with Security Rule compliance than Privacy Rule compliance. However, there is what I would refer to as 'low hanging fruit' or basic HIPAA compliance issues that OCR has repeatedly identified and that a practice could address without much difficulty."

Go to the source. Some of the best advice devoted to both HIPAA privacy and security issues comes from the HHS, OCR, and ONC. As these government organizations are setting up the rules, they also offer the most comprehensive ideas on how to avoid the pitfalls. You can look at your run-of-the-mill online search engines for set-up ideas, but remember these aren't necessarily giving you the complete picture of what to include, ignore, and avoid.

"While I would not recommend pulling policies and procedures off of a simple Google search, there are trustworthy online resources, particularly the HHS website, where practices can turn for help," Bossenbroek mentions.

The HHS website offers a "HIPAA for Professionals" overview, which gives a complete outline of the rules, the Phase 2 HIPAA audits, timelines, and more. With Advancing Care Information (ACI) around the corner, the ONC has been amassing electronic compliance and EHR resources while revising its site and offering more HIPAA-forward tools and ideas. It's Guide to Privacy and Security of Electronic Health Information has a plethora of data for practices of all shapes and sizes. (https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information.)

Support groups. If you can't afford to engage a HIPAA-compliance vendor or law firm, there are other organizations that can offer insight. For example, don't overlook the professional organizations you are involved with, suggests Bossenbroek.

"I would suggest a practice consult with professional organizations where providers might have memberships (like a physician organization) and see if they offer HIPAA resources and tools," he says. "It is my experience that medical societies have collaborated on HIPAA compliance, such as offering presentations and materials."

Tip. Utilize your available resources and continue to educate yourself and your staff on HIPAA's best practices. With a thorough understanding of the dimensions of the rules, setting up a plan is doable for even the sole-provider practice. As value-based care continues to be at the heart of the upcoming MACRA initiatives, protecting and preserving patients' information should be a primary focus for all clinicians and their associates.

"Ignoring or failing to have policies will only hurt the practice, and may provide added justification for OCR to be more severe if it seeks to impose penalties or negotiate a settlement," says Bossenbroek.