HIPAA omnibus rule compliance tips for small practices, medical groups

This is the first of a two-part series of tips on preparing for the HIPAA omnibus rule to go into effect. The first part covers how to identify your organization's greatest risk in advance of the rule's enforcement.

The HIPAA omnibus rule went into effect in early 2013, and federal enforcement was set to begin this fall after a 180-day grace period expires Sept. 23. With this in mind, Jaime Dupuis, practice consultant for the Regional Extension Center of New Hampshire (RECNH) offered a checklist of compliance tasks for attendees of a recent webinar, some of whom were smaller physician practices and medical groups:

- Update your Notice of Privacy Practices (NPP). Dupuis gave examples from the Affairs, Beth Harris County Hospital District Texas and Stanford as recently updated NPPs that might inspire your organization's next draft.
- Rework business associate agreements (BAAs) to reflect the fact that they are now directly liable for HIPAA compliance as well as subject to new breach notification rules.
- Make risk analysis an ongoing process that includes at minimum: defining and assembling a risk analysis team; evaluating the likelihood and impact of potential risks to protected health information (PHI); listing the findings (including the policy or security gaps) in the assessment; develop a work plan and timeline for mitigating risks; implement appropriate security measures to address identified risks; develop and refine written policies and procedures to fully comply with regulations; and, finally, have the team meet regularly to ensure continuous, reasonable and appropriate security protections.
- Work on highest-risk vulnerabilities first. Risk assessments are a big part of meaningful use attestation and HIPAA compliance moving forward. While only your own risk assessment reveals your own punch list of breach possibilities, HHS's Office of Civil Rights pegs physical theft of patient records the number-one cause of HIPAA violations (55%), followed by disclosure of PHI without patient consent (20%) and data lost/not accounted for (12%).
- Confirm that risk analyses cover the following topics: physical security of hardware and devices; password management and role-based security access; portable and mobile device policies; data encryption and network security. Administrative safeguards such as data backup and employee termination policies that also cut off former employees' network access should be covered as well.
- Strengthen your employee password policy and require employees to regularly change passwords. Get more advice on this topic -- and the whys behind it -- here.
- Employ a network firewall; install and regularly update antivirus software. While these two pieces of "data security 101" advice might not sound particularly earth-shattering, they bear repeating as many offices still aren't employing these basics.

PHI security, mobile protection part of HIPAA omnibus compliance

This is the second of a set of two tips from Jaime Dupuis, practice consultant for the Regional Extension Center of New Hampshire (RECNH). The first tip covered why it's important to conduct organizational risk assessments. Here, Jaime details how to establish a culture of PHI security in order to be compliant with the upcoming HIPAA omnibus rule.

Don't fall for the fallacy that a meaningful use certified EHR vendor has created HIPAA compliance for you merely through the certification process.

- Protect mobile devices. This includes, but isn't limited to the following: Use passwords or other user authentication to access the devices; install and enable data encryption; do not install (or if they're present, disable) file-sharing applications; secure Wi-Fi networks delivering protected health information (PHI) to mobile devices and create a guest network for non-employees; store no patient data on mobile devices if possible; and employ remote-wiping systems in case of mobile device loss or theft.
- Remember, the omnibus rule states that providers can't send information on a particular patient procedure back to the patient's health plan pocket for that care. Set up a process to honor such requests among billing and coding staff.
- Control physical access to your facilities, as well as to your PHI. Consider the following questions: Who handles your backups? Where do they take them? How is data destroyed once paper, hard drives or thumb drives, and tapes leave your organization's possession? Be sure to monitor and audit these issues.
- Speaking of audit logs, remember that the systems that have been set up to record who's logged into your EHR and other systems, when they log in, and which data files they access there are useless unless you review them periodically, take action when discrepancies or potential privacy violations are found, and document those actions.
- Plan for the unexpected. Have data backup and disaster contingency plans in place to ensure continuity of access to patient data.
- Establish and foster a culture of PHI security through training, refreshers and reminders to change passwords, update antivirus software, etc. Empower users to deal with breaches the right way by designing a breach reporting process and training employees to understand what is reportable, how to report it, and how investigations will proceed.

Lastly, don't fall for the fallacy that a meaningful use certified EHR vendor has created HIPAA compliance for you merely through the certification process. This fallacy is one that small providers might be tempted to believe.

"I hear [this] a lot: 'My EHR vendor took care of everything I need to do about privacy and security -- I'm on a certified system, isn't that enough?'" said Dupuis, whose RECNH is a division of the Massachusetts eHealth Collaborative. "As you can see, there are things aside from the technical aspects that need to be controlled when looking at privacy and security. There are many parts to this."