Health Information Compliance Alert

HIPAA: Take These 8 Steps To Information Security Compliance

Check to see how compliant your organization is.

If you've become complacent about reducing the risk of privacy breaches in your practice, you're playing with fire: The feds are enforcing penalties right and left and practices are liable for these fines. By taking these eight steps recommended by **Ester Horowitz, CMC, CITRMS, CIISA,** to prevent protected health information breaches, you'll be well on the way to compliance.

1. Adopt a culture of privacy thinking and expect others to adhere to the same. Facilities and practices need to understand that it is actually more expensive to fix a breach than to prevent it. Checking to see who sees which information as well as how it is moved and used would be a good starting point, Horowitz stressed in her March 22 audio presentation "Identity Theft and HIPAA: What You Don't Know DOES Hurt You" sponsored by The Coding Institute's Audio-Educator. Create data encryption policies to safeguard information during transfer of records, create military-grade firewalls and cyber security guidelines. "Establish guidelines, policies, and procedures [that detail] how you will secure that information and expect others to support it," she said. While this might necessitate hiring a computer techie and/or purchasing the requisite software and hardware, the long-term impact and saving in penalty payouts would be significant, pointed out Horowitz.

2. Conduct education on an on-going basis and expect your staff to stay up to speed on security rules. It is critical for a facility/practice to keep abreast of changes in governmental policy, rules and regulations, and edits to existing legislation to remain compliant. Just as newer methods of protection for privacy are found on a regular basis, newer ways to breach information security measures are found by those who do so for reasons of identity theft and/or fraud. So you need to learn just how breaches occur. "You should be aware of the potential for breach risk in the organization based upon how information moves within the organization," stressed Horowitz.

3. Designate a high-level official who can be entrusted with the responsibility to implement policies, procedures, and maintain vigilance. "Raising the security awareness of your workforce is your best defense against having a breach incident," said **David Holtzman**, health information privacy specialist at the Department of Health and Human Services' Office for Civil Rights, which enforces the HITECH Act breach notification rule. His comments came at a conference, "Safeguarding Health Information: Building Assurance Through HIPAA Security," co-sponsored by the OCR and the National Institute of Standards and Technology.

4. Detect the potential for exposure and take corrective action. Vulnerability in privacy matters should never be taken lightly. Physical protection of data is as important as encryption added Horowitz. "Do not neglect physical safeguards for areas where paper records are stored and used," warned Holtzman. Files, papers and devices like laptops that anybody can pick up or which lie unprotected in cars or on the top of a desk or even on the seat of train or at the airport are potential breach points, he added. A case in point is the reported loss of documents by an employee of Mass General while commuting to work which cost the facility a hefty $1 million fine.

5. "Create clear and well-documented administrative and physical safeguards for storage devices and removable media (that store protected health information) ... Those organizations that have good foundations of policies and procedures respond better to incidents," pointed out Holtzman. Healthcare service providers need to do business with others that support the same. These may include business associate agreements, client privacy statements, internet security policies, etc. "HIPAA states that a covered entity (healthcare provider or health plan) may only provide protected health information to those Business Associates from whom it has received assurances that the information will be safeguarded as required by HIPAA (HITECH has supplemented these provisions)," says **Kenneth N. Rashbaum, Esq.** of Rashbaum Associates, LLC, New York, NY in an exclusive **Eli** interview.

6. Monitor routinely to avoid obsolescence and reduce new exposures to threats suggested Horowitz at the same audioconference. There is no such thing as failsafe, but "good practices" reduce potential for loss andliability for the business years later. "Identify methods to evaluate security protocols you put in place and adjust accordingly over time," she said. Audits to monitor the potential of others to breach data security and hotlines and ombudsman programs are some of the other methods suggested by Horowitz to reduce the potential for data breaches and consequent liability. "There are requirements for appropriate processes for breach response, notification, investigation, and remediation. We recommend a hotline to facilitate response time," says Rashbaum.

7. Mitigate the impact of breaches. Advances in technology have meant that healthcare facilities and service providers need to be doubly wary about protecting patient privacy points out Rashbaum. Breaches of privacy can help those who steal medical identities warned Horowitz. Records indicate that over 11 million identities have been reported to have been stolen. Stolen healthcare records and medical identities may be even more valuable to the bad guys than stolen credit or debit card information because the medical information can pave the way for free healthcare. "A breach may comprise loss if [it involves] information beyond personal identifying information (trade secrets, financial data, company data, etc.)," points out Rashbaum. Keep a contingency plan in hand to respond to unforeseen breaches advises Horowitz.

8. Enforce the rules. Facilities and practices should prove their willingness to enforce information security compliance by taking stern action against snoopers the way University Medical Center in Tucson did against staff who viewed confidential health records after a Jan. 8 shooting incident in Tucson, Arizona. Three people were fired as they had violated a "zero tolerance policy on patient privacy violations," according to a statement released by the hospital on Jan. 12. However, the administrators announced that they believed none of the patients' confidential information had been made public, according to the Arizona Daily Star. Healthcare service providers should be willing to reprimand, dismiss and even refuse to do business with any entities who may not be willing to comply with information security measures stressed Horowitz. "Employees can and have been suspended or, in some cases, dismissed for viewing patient information they had no business reason to access," reminds Rashbaum.