Zip It!

Feds, State Strengthen Privacy Protection

TexasMedicine

Practice Management Feature – July 2012

Tex Med. 2012;108(7):33-37.

By Crystal Conde
Associate Editor

When it comes to enforcing HIPAA data security and privacy standards, the federal government means business. In fact, the government is conducting a national pilot program to audit 150 physicians and others that HIPAA covers as the first phase of a concerted effort to crack down on HIPAA violations.

Health law attorney Ana Cowan, an attorney with the Austin office of Brown McCarroll, says the audit pilot program, coupled with a new Texas electronic health record (EHR) privacy law that exceeds HIPAA requirements and takes effect on Sept. 1, should grab physicians' attention. (See "Texas Raises the Privacy Stakes.")

"Texas is progressive about patient privacy, and starting Sept. 1, physicians need to consider additional state requirements. Failure to comply with state and federal law exposes physicians to additional scrutiny and civil penalties. Now is the time to make sure physicians are in compliance with both federal and state privacy requirements. They need to take this seriously," she said.

The Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) hired the accounting firm KPMG LLP to conduct the audits, authorized by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act. The audits began in November and are scheduled to be completed by December. At press time, OCR was examining 20 covered entities, none of them in Texas. The government has not said how it picks audit targets, saying only the selections are "designed to provide a broad assessment of a complex and diverse health care industry."

Violating HIPAA rules can be costly. In April, an Arizona cardiology practice paid $100,000 and agreed to a corrective action plan after HHS received a complaint the practice posted clinical and surgical patient appointments on a publicly accessible Internet-based calendar. HHS said the investigation found the practice had few policies and procedures to comply with HIPAA, had limited safeguards to protect patients' electronic protected health information (PHI), did not document that it trained any employees on HIPAA policies, and did not identify a security official or conduct a risk analysis.

When OCR selects a practice for an audit, investigators interview key practice staff, inspect office privacy and security protocols, and assess the practice's compliance with federal regulations and policies.

Post-audit reports include recommendations for correcting compliance problems. While the audits can identify best practices and areas for improvement, KPMG will turn serious HIPAA violations over to OCR, which could then open a separate investigation and take enforcement action.

That's why it's important for all physicians to make sure they comply with the law and prepare for a possible audit, says Deborah Hiser, who also is with Brown McCarroll.

"HIPAA is evolving in terms of enforcement. There is a definite move away from the complaint-driven agency we saw in the past to an agency that is feeling congressional pressure to impose civil penalties," she said.

Martin Garza, MD, an Edinburg solo pediatrician and a member of TMA's Council on Practice Management Services, says the Texas Medical Association's *Policies & Procedures: A Guide for Medical Practices* is a useful HIPAA compliance tool that will help with any OCR audit.

"The HIPAA and HITECH manuals in the guide are extremely detailed and provide sample forms we've modified to fit the practice. We update the information regularly, and the manuals are available electronically so the whole staff can access them at any time," he said.

Ms. Hiser and Ms. Cowan wrote the HIPAA and HITECH privacy and security manuals for the guide. The manuals include updated details on Texas' new EHR privacy law as well as template policies and forms for:

- Staff training on the HITECH Act requirements,
- Business associate agreements that incorporate the HITECH amendments,
- Breach risk assessments, and
- Use of email with patients.

"TMA has worked with experts in crafting its policy and procedure guide. I feel more confident in my HIPAA compliance because I know the information comes from a trustworthy, reliable physician advocate," Dr. Garza said.

A hard copy of the guide, including details on Texas' new EHR privacy law, with customizable CD is $295 for members and $395 for nonmembers. The customizable CD alone is $255 for members and $355 for nonmembers. TMA also offers a downloadable update on Texas' new EHR privacy law for physicians who previously purchased the policy and procedure guide.

To order the guide and to inquire about the update download, call the TMA Knowledge Center at (800) 880-7955, or email knowledge@texmed.org.

Get Ready

A survey performed by HCPro Inc. – a Massachusetts-based health care regulation and compliance education, training, and consulting firm – indicates a majority of health care entities aren't ready for HIPAA compliance audits. Of the 400-plus survey respondents, including health information management directors and compliance officers, only 17 percent said they are fully prepared, and 70 percent said they were somewhat prepared. A lack of commitment by senior management to HIPAA compliance was among the reasons they cited for not being fully prepared for compliance audits.

Ms. Cowan agrees with Ms. Hiser that physicians need to be ready if the auditors come calling.

"At this point, all physicians must have all policies and procedures required by the HIPAA privacy, breach notice, and security rules finalized and regulator-ready. If OCR selects you for an audit, contact your legal counsel, and be prepared to cooperate as necessary during the onsite visit," she said.

Additional preparatory steps to consider include:

- Adopt comprehensive privacy policies and procedures that are up to date and specific to the practice. Be certain you have updated, signed business associate agreements with all business associates.
- Conduct a risk assessment of the practice. If you haven't done one within the past year, do it now. Focus on successful implementation of policies and procedures.
- Identify "high-impact" vulnerabilities, such as the method used for disposing of PHI.
- Train everyone on staff according to policies and procedures. Train regularly and have staff take tests. Document all training. The privacy officer should retain all training materials.

TMA and Brown McCarroll have other resources to help physicians comply with HIPAA and prepare for a possible OCR audit. TMA's webinar "HIPAA and the HITECH Act," presented by Ms. Hiser, guides physicians in preparing and implementing policies to comply with the regulations. The webinar, which offers an hour of ethics continuing medical education, details who must comply, what the federal government considers a breach, and how to conduct a risk assessment.

For more information, call the TMA Knowledge Center at (800) 880-7955, or visit the TMA Education Center.

Brown McCarroll developed a webinar titled "HIPAA Audits: What They Are Looking For and What You Can Do to Prepare" in case KPMG comes calling. The free webinar discusses:

- Who may be subject to an audit,
- The audit process and timeline,
- How to prepare for an audit,
- What the auditors are looking for, and
- The ramifications of failing an audit.

For more information, call (512) 479-9776.

What to Expect

Ms. Hiser and Ms. Cowan previously represented physicians the OCR investigated for alleged HIPAA violations.

"Thus far, we have been successful in working with the agency to deal with such allegations. To date, none of our clients have been sanctioned or have been required to enter into corrective action plans subject to OCR oversight," Ms. Hiser said.

She says OCR scrutinized their clients for inadvertently disclosing PHI such as mailing a bill to a wrong address, failing to verify a person's identity, not having appropriate breach policies and procedures, and having computers containing PHI lost or stolen – to name a few.

Physicians who get an audit letter from OCR have only 10 business days to respond to a request for documentation. Ms. Hiser says OCR likely will request extensive records that could include, but are not limited to, risk assessments, training and incident reports, vendor information, access rights, and management security procedures.

OCR gives 30 to 90 business days notice before an onsite audit. During site visits, KPMG auditors ask employees what they understand about the practice's HIPAA policies and procedures and observe processes and operations to help determine compliance. Based on their findings, auditors develop and share a draft report with physicians, who then have 10 business days to review it and to submit written comments.

"It is wise to consult with an attorney to assist in legal arguments regarding the scope and application of the rules and justification of your approach to implementation," Ms. Hiser said.

Ms. Cowan also notes that OCR expects physicians and their staff to know who is responsible for recording and examining activity in information systems that contain PHI. They also should have a list of all information systems that house electronic PHI data, as well as network diagrams, including all hardware and software used to collect, store, process, or transmit the information. Finally, she encourages practices to designate staff members to take the lead in the event of an audit.

Ms. Cowan says violations that may warrant OCR opening a separate compliance review include:

- Willful and inappropriate sale of PHI;
- Inappropriate disclosure of sensitive information, such as sexually transmitted diseases or mental health records;
- Failure to safeguard electronic media containing large amounts of patient information;
- Consistent failure to implement HIPAA, such as not training personnel or not having policies and procedures; and
- Failure to cooperate with OCR.

Ms. Hiser says OCR fined Cignet Health $4.3 million last year for not providing medical records and not complying with the agency's requests for documentation during an investigation. She says OCR enforcement typically requires practices to sign three-year corrective action plans, to send periodic updates to the agency, and to develop policies approved by the agency.

Increased penalties under the HITECH Act and enforcement actions by federal government and states' attorneys general have serious implications for physicians who fail to comply with the rules. Ms. Hiser says it's important that physicians comply with the encryption and destruction requirements under HITECH, audit electronic systems to detect security incidents and violations, and notify patients quickly in the event of a breach, especially identity theft.

HHS defines a breach as "an impermissible use or disclosure under the [HIPAA] Privacy Rule that compromises the security or privacy of the protected health information" and poses a significant risk of "financial, reputational, or other harm" to the patient.

Ms. Hiser says physicians would be smart not only to have a system to detect PHI breaches but also to encrypt all confidential patient information. The reason: Physicians and business associates must provide the required notification only if the breach involves unsecured PHI.

HHS has information on ways to render unsecured PHI unusable, unreadable, or indecipherable on its website.

Civil penalties for unintentional HIPAA violations range from $100 to $50,000 per violation. Criminal penalties for fraud include a minimum $100,000 fine and up to five years imprisonment. Individuals who violate HIPAA with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm face a maximum $250,000 fine and 10 years imprisonment. (Read "Mum's the Word," August 2010 *Texas Medicine*, pages 49-53, or visit www.texmed.org/Template.aspx?id=16452.)

For more information about penalties, consult Section 13410 of the HITECH Act.

Crystal Conde can be reached by telephone at (800) 880-1300, ext. 1385, or (512) 370-1385; by fax at (512) 370-1629; or by email.

RELATED STORY

Texas Raises the Privacy Stakes

Starting Sept. 1, Texas physicians and other covered entities using electronic health records (EHRs) must comply with a state privacy law that imposes requirements more stringent than HIPAA.

For example, while HIPAA has always required physicians to train their employees, the new state law mandates training specific to the staff members' scope of employment, to occur within 60 days after they are hired. In addition, training must be provided at least once every two years, says Austin health care attorney Deborah Hiser.

Another significant difference is the Texas law directs physicians to notify patients their health information is subject to electronic disclosure, says Austin health care attorney Ana Cowan.

"Notice must be posted in the physician's place of business. If the electronic disclosure is not related to certain activities like treatment, payment, or health care operations, the physician must actually obtain patient authorization in order to engage in the electronic disclosure."

Both attorneys urge physicians to begin updating their HIPAA manuals to include the additional requirements imposed by the state law. Under the law, the Texas attorney general may ask HHS to audit covered entities for compliance, and anyone who accesses, reads, scans, stores, or transfers protected health information electronically and without authorization may face felony charges.

Fort Worth emergency physician Matt Murray, MD, vice chair of the Texas Medical Association Ad Hoc Committee on Health Information Technology, says it's especially important for physicians to become well-versed in cyber liability risk and Texas' new EHR privacy law.

For instance, under the new state law, physicians using EHRs must give patients their electronic records within 15 business days of a written request (just like physicians have been required to do for paper records under state law). The state law is more stringent than the 30 days HIPAA allows. Physicians may provide the record in another format if the patient agrees.

The new law also allows for assessment of civil penalties up to:

- $5,000 per each negligent violation in one year;
- $25,000 per each intentional violation in one year;
- $250,000 for a violation committed knowingly and intentionally that involves using PHI for financial gain; and
- $1.5 million if a court finds "the violations have occurred with a frequency as to constitute a pattern or practice."

To avoid violating the law and facing steep penalties, Dr. Murray advises physicians to contact an attorney to ensure compliance with the new regulations and to consult their area regional extension center (REC) for assistance with security risk analysis and management. Dr. Murray is chair of the North Texas REC board of directors.

For more information on the RECs, visit TMA's REC Resource Center.

SIDEBAR

TMA ADVANTAGE
July 24 TMA Webinar Outlines Cyber Security

Matt Murray, MD, a Fort Worth pediatric emergency physician and vice chair of TMA's Ad Hoc Committee on Health Information Technology, will conduct a webinar on cyber liability on July 24.

He will discuss privacy, security, and patient consent concerns; Texas' new privacy law; HITECH changes to HIPAA; physician accountability and financial penalties for privacy breaches; problems that can impede safe use of electronic health records and electronic exchange of records; risk assessment tools; and encryption.

To register, visit the TMA Education Center.

Back to article

RELATED STORY

TMLT's Cyber Liability Coverage

Because medical practices are vulnerable to computer hacking, viruses, and identity theft due to the amount of sensitive information they collect, the Texas Medical Liability Trust (TMLT) offers cyber liability coverage.

It is available to physicians, medical groups, or to physicians and entities combined, and it's included with a policy at no additional cost. The policy covers what TMLT considers the four most important data breach and privacy liability exposures:

- Network security and privacy coverage for third-party claims from electronic and physical information breaches, virus attacks, hacks, identity theft, and defense costs for regulatory proceedings;
- Regulatory insurance that covers administrative fines and penalties stemming from an investigation by a federal, state, or local government agency resulting from a privacy breach;
- Patient notification and credit-monitoring costs coverage that includes all necessary legal, information technology forensic, public relations, advertising, call center, and postage expenses to notify third parties about the breach of information;
- Data recovery costs insurance that includes all reasonable and necessary costs to recover and/or replace compromised, damaged, lost, erased, or corrupted data.

For more information, call TMLT at (800) 580-8658.

July 2012 Texas Medicine Contents
Texas Medicine Main Page

Published: 6/19/2012 3:16:45 PM