HIPAA Regulatory Alert

Supplement to *Healthcare Risk Management* and *Hospital Access Management*

HIPAA compliance audits begin with a pilot program

You should prepare now — Documents are due 10 days after notice

As promised by the Department of Health and Human Services' Office for Civil Rights (OCR) and mandated by the HITECH Act, HIPAA compliance audits have begun, and 20 organizations were visited during the pilot phase of the program.

"Hospitals selected for the audit have to provide a lot of documentation in a short timeframe," explains **Adam Greene**, partner at the Washington, DC, law firm of Davis Wright Tremaine and a former OCR official. In addition to the expected policies and procedures related to privacy and security, auditors want to see current risk analyses and documentation related to improvement of data protection, he adds. *(See related story on documentation tips, p. 2.)* "Be aware that the audit's scope extends past electronic health records and covers privacy and security of data in clinical, research, and billing departments, as well as employee use of email and text messaging."

From the time of notification of an audit, you have 10 calendar days to provide all of the documents requested, says **Mac McMillan**, chief executive officer of CynergisTek, an information technology security consulting company. McMillan advised a Texas hospital included in the initial audit.

Because initial documents requested also include non-HIPAA specific items such as demographic information about a hospital's market and patient population, and an organizational chart, prepare ahead of time by knowing where these documents are located, he suggests.

The audit is scheduled between 30 and 90 days from the date of the notice, but OCR does give five days' notice before auditors arrive, says McMillan. "Actually, my client got eight days' notice, which helped us make sure everyone who was likely to be interviewed by auditors, or involved in the audit, was onsite during those days." OCR estimates audits to take 3-10 days, depending on the organization being audited. McMillan says his hospital client's audit was one week long. *(Learn what to expect during an audit, p. 3.)*

Because you do not have a lot of time to educate people who may be involved in the onsite audit, set up your audit team now, suggests **Chris Apgar**, CISSP, president of Apgar & Associates, a Portland, OR-based consulting firm. "This will make preparation for the audit easier because everyone will understand their role." *(See how to set up an audit team, p. 3.)*

Results of the 20 audits conducted during the pilot program will be used to evaluate the audit tool as well as the audit process, and to make changes if needed before the remaining 130 audits scheduled for 2012 are conducted after the pilot program's completion in the spring, says Apgar. Although larger organizations such as health plans, claims clearinghouses, and larger hospitals expected to be audited earlier rather than later in the process, the pilot program included a dental office, a long-term care facility, and a pharmacy. "I am sure these smaller organizations were surprised at their inclusion, but it is important to smaller providers that the pilot included them," he says.

EXECUTIVE SUMMARY

At press time, results of the HIPAA compliance audit pilot program and any resulting changes in the process or the audit tool were expected to be finalized in the spring. Lessons learned by organizations in the pilot phase of the program include:

- Identify and locate key HIPAA policies, procedures, and documentation. Develop a system that ensures quick access before you receive the 10-day notice to provide information.
- Have an up-to-date risk analysis related to privacy and security rules.
- Evaluate your business associate program to ensure you have documented your management of those relationships.
- Establish your HIPAA compliance audit team, and assign specific responsibilities before your receive an audit notice.

OCR auditors and staff members will be able to ensure that the audit tool is practical for smaller as well as larger organizations, which will help small hospitals, specialty hospitals, and freestanding surgery centers, he adds.

Prepare now

Although there is no way to know if your organization will be one of the 130 additional audits conducted in 2012 or in upcoming years, you can take steps now to prepare, suggests McMillan.

"Even if you don't know exactly what documents will be requested in your initial notice, there are a number of items that can be expected," he says. "Ten calendar days is not a lot of time to gather documents, so the first step is to know where everything is located."

Apgar says, "You don't have to centralize all policies and documentation related to HIPAA privacy and security issues, but you do need to have a way to quickly access them."

Assigning the responsibility to one or two people and creating an index of all documents that might be requested is a good start, he says. Identify the documents, their location, and contact information for the people who can access them easily.

Be sure you have a current risk analysis, says Apgar. "The rule does not specify how often a provider must conduct a risk analysis, but a good guideline is annually or whenever there is a change that might affect security risk levels," he points out. Adding a new business associate or introduction of a new system such as electronic health records are points at which a risk analysis should be done, he says.

Along with the documentation of the risk analysis, auditors will want to see corrective action plans and data to show progress in remediation of areas that were identified as non-compliant, says Greene. "This is very important if the hospital is aware of a potential weakness in compliance," he says. "Demonstrate to auditors that you are aware of the issue, have identified steps to correct it, and are making progress."

McMillan says, "Pay close attention to how you manage your business associate relationships, and document your efforts to carefully control information released to them. This requires more than showing a copy of an agreement. Document due diligence related to flow of information, procedure for termination, and process to jointly handle breaches." *(For information about business associates and HIPAA, see "Data breaches attributed to business associates increase,"* HIPAA Regulatory Alert, *March 2012, p. 1.)*

Set up an audit team

"OCR has hinted that there will be no hesitance to levy fines on non-compliant organizations identified in the audits," says Apgar. These fines will be used to support the audit program, so although it was originally described as a non-punitive program, it is important to take the process seriously to avoid potential fines, he adds.

Because the HITECH Act has given OCR the ability to assess significant financial fines, this is not the time to play the odds, warns Greene. "Although your chance of being one of the 130 organizations audited this year is small, look at this as a way to get your house in order," he says. "Perform a thorough assessment, make sure your HIPAA training programs are effective, and even if you prepare for an audit that doesn't happen, your hospital and your patients benefit."

SOURCES

For more information about preparation for HIPAA compliance audits, contact:

- **Chris Apgar**, CISSP, President and CEO, Apgar & Associates, 11000 SW Barbur Blvd., Suite 201, Portland, OR 97219. Telephone: (502) 384-2538. Fax: (503) 384-2539. Email: capgar@apgarandassoc.com.
- **Adam Greene**, Partner, Davis Wright Tremaine, Suite 800, 1919 Pennsylvania Ave. NW, Washington, DC 20006-3401. Telephone: (202) 973-4213. Fax: (202) 973-4413. Email: adamgreene@dwt.com.
- **Mac McMillan**, Chief Executive Officer, CynergisTek, 8303 N. MoPac Expressway, Suite 128B, Austin, TX 78759. Phone: (512) 402-8555. Email: mac.mcmillan@cynergistek.com. ■

Get these documents ready for an audit

Although there is no way to know exactly what documents you will be asked to provide in the initial HIPAA compliance audit notice from the Department of Health and Human Services' Office for Civil Rights (OCR) there are some items you can expect to see on the list, according to experts interviewed by HIPAA Regulatory Alert:

- **all policies related to compliance with HITECH privacy and security requirements;**
- **documentation of risk analysis for the organizations;**
- **business associate agreements and documentation of provider management;**
- **HIPAA training program for employees;**
- **names of compliance officers along with organizational chart for the provider;**
- **demographic information about the hospital, the patient population, and the medical staff.**

Some of the documents you should also be prepared to provide include:

• **List of terminated employees as well as new hires.**

"This list will be used by the auditors to see how well you disable access for terminated employees and control access to protected health information for new employees," explains **Mac McMillan**, chief executive officer of CynergisTek, an information technology security consulting company, who advised a Texas hospital included in the initial audits. Although you might have a policy that describes the process, this list will give auditors an opportunity to see if your actual practice follows the policy.

• **Proof of employee training on privacy and security requirements.**

Having a HIPAA training program and proving that employees receive the training are different things, points out **Adam Greene**, partner at the Washington, DC, law firm of Davis Wright Tremaine. Your documentation should describe the content of the training program, who provides the training, and how you ensure that all employees are trained, he adds.

• **List of complaints related to privacy.**

Be prepared to share a list of complaints you've received from patients, family members, or employees about data privacy or security issues, says Greene. Documentation should include the complaint, who handled it, how it was handled, and how it was resolved.

There are also some documents you should choose to include, suggests Greene.

• **Description of your best practices.**

"The audit contract calls for identification of best practices, so if you know you have an effective poster campaign or HIPAA hotline, provide documentation of the program's success," suggests Greene.

• **Improvement plans related to privacy and security.**

Almost all risk analyses result in identification of areas that can be improved, points out Greene. "If you know you have a weakness, don't try to hide it and hope the auditors don't notice," he says. "Provide documentation of a plan to address a non-compliant area, show that you have prioritized the issues, and provide the results of evaluations of your efforts to come into compliance." ■

What can you expect when auditors arrive?

The initial notice of audit from the Department of Health and Human Services' Office for Civil Rights (OCR) asks for a significant amount of documentation and information to be submitted within 10 days of the notice date, but that will not be the end of information for which you'll be asked, says **Mac McMillan**, chief executive officer of CynergisTek, an information technology security consulting company, who advised a Texas hospital included in the initial audits.

"A pre-audit conference call is made a minimum of five days before the visit," explains McMillan. His client's audit occurred six weeks after the initial notice, but it could have been scheduled anytime during a 30-90 day period from the date of the notice, he says. During the conference call, additional documentation and a list of people with whom the auditors want to meet is provided. "The call is helpful because you can make sure your key people are onsite when the auditors arrive and prepared to meet with them," McMillan adds.

His client provided a conference room for the auditors to use during the visit and gave them guest privileges on the hospital's wireless network, he says. "The privacy and security officers cleared their schedules so they were available to the audit team the entire week," he explains. In addition to the privacy and security officers, make sure other administrative and medical staff leaders are aware of the audit and are prepared to meet with auditors, he suggests.

Auditors did walk around the facility, says McMillan. "Let your entire staff know the auditors will be onsite and that they may talk with employees at any time," he says. The walking tour and talks with employees are two ways the auditors can check to see if the hospital policies are communicated and understood by all employees.

Remember that an auditor's job is to uncover weaknesses, points out McMillan. "After you submit your initial documentation, you don't know if the auditors are going to audit your entire program or focus on specific areas," he says. They have the option of conducting the audit either way, he adds.

Immediately following the onsite visit, the hospital received an outline of audit results along with specific areas in the privacy and security rules in which the hospital was deficient, says McMillan. "This outline gives hospital leaders a good idea of what the final report will include," he says. "The hospital had 10 days to respond to the final report and provide any additional documentation that demonstrated compliance." ■

Do now: Set up in-house audit team

A well-prepared team that understands roles and responsibilities when a notice of a HIPAA compliance audit is received is essential for every organization and should be established long before a notice is received, suggests **Chris Apgar**, CISSP, president of Apgar & Associates, a Portland, OR-based consulting firm. Educate them about the purpose of the audit, and give each person specific responsibilities, he says.

"Define who the caretakers of the auditors will be when they are onsite, and make sure they understand their role in the audit," Apgar says.

One way to test your documentation index and the effects of your audit team's education is to conduct a "fire drill," recommends **Adam Greene**, partner at Davis Wright Tremaine, Washington, DC. Deliver a mock audit notice to the administrative offices. If plans go well, the chief executive officer is immediately notified that the letter has arrived and requests for information are disseminated quickly. "Making sure the letter doesn't sit unopened on someone's desk is important," Greene points out.

Set a deadline of gathering all requested documents in 6-7 days from the date of the notice so you have time to identify missing items.

In addition to testing your ability to respond to the audit notice in 10 days, conduct a mock HIPAA compliance audit throughout your organization, suggests Apgar. Don't focus only on policies and procedures, or the information technology department, he says. "Auditors are likely to walk throughout your facility, in multiple departments, so take your own walk through the hospital," he says. "Look for shared computers that have passwords on notes taped to the monitor or screens that can be easily read by members of the public," he says.

Mac McMillan, chief executive officer of CynergisTek, an information technology security consulting company, says, "Make sure all employees understand your privacy and security policies and the purpose of the audit. The greatest risk in a HIPAA compliance audit is not your information technology staff; it is other employees." ■

Proposed rules published for stage 2 meaningful use

Comment period ends May 7, 2012

The Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare and Medicaid Services (CMS) have issue Notices of Proposed Rulemaking that are open for comment until May 7, 2012.

The CMS proposed rule applies to stage two of the "Meaningful Use" rule and new requirements that participants in the Electronic Health Record (EHR) Incentive Programs will have to meet to demonstrate meaningful use in the program. The companion ONC rule discusses the certification capabilities and standards and tests that Certified EHR Technology (CEHRT) would have to do. Although the two rules overlap some, they are different.

A few of the items included in the proposed rule include:

- Nearly all of the Stage 1 meaningful use core and menu objectives would be retained for Stage 2 meaningful use.
- "Provide patients with an electronic copy of their health information" objective would be removed because it would be replaced by an electronic/online access" core objective.
- For eligible hospitals and CAHs, the set of CQMs beginning in 2014 would align with the Hospital Inpatient Quality Reporting (HIQR) and The Joint Commission's hospital quality measures.

The proposed rule for Stage 2 Meaningful Use also includes a minor delay of the implementation of the onset of Stage 2 criteria from the current 2013 implementation date to 2014.

To access the CMS proposed rule, "Medicare and Medicaid Programs: Electronic Health Record Incentive Program-Stage 2 Meaningful Use," go to federalregister.gov/a/2012-4443.

To access the ONC proposed rule, "Health Information Technology; Implementation Specifications, and Certification Criteria: Electronic Health Record Technology, 2014 Edition," go to federalregister.gov/a/2012-4430. ■

Consumer privacy is subject of FTC report

The Federal Trade Commission (FTC) has issued a final report outlining best practices for businesses to protect the privacy of American consumers and give them greater control over the collection and use of their personal data.

The report proposes a privacy framework that would have no legal effect on HIPAA-covered entities. However, some of the practices proposed in the report, such as automated mechanisms to track access of information and restoration of patient consent to sharing information, might be considered as the Department of Health and Human Services updates the HIPAA privacy rule to incorporate more stringent privacy protections.

To see a copy of the report, go to http://1.usa.gov/H3LgcC. ■