Segal Consulting

update

Public Sector Benefits Compliance News

April 21, 2016

New HIPAA Privacy and Security Audit Program Announced

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently announced that it has begun the next phase of its audits of covered entities and their business associates under the Health Insurance Portability and Accountability Act (HIPAA): Phase 2 HIPAA Audit Program.[1] These audits will assess compliance by health plans and their business associates with the HIPAA Privacy and Security Rules and the breach notification rules under the Health Information Technology for Economic and Clinical Health Act (HITECH).[2]

Background on Covered Entities

Employer-sponsored health plans are covered entities under HIPAA's Privacy and Security rules. These plans have the obligation to comply with the HIPAA and HITECH rules, which includes assuring that any service providers who use and disclose their participants' protected health information (PHI) execute business associate agreements that require them to protect that information. These business associates would include administrators, consultants, and any other entities that use or disclose PHI on behalf of the plan.

Background on the OCR's Phase 1 Audits, a Pilot Program

In 2011 and 2012, the OCR conducted Phase 1 audits of 115 covered entities. During that audit process, covered entities received both a site visit and an audit report. The process allowed the covered entity to discuss concerns and undertake corrective actions. Any violations found were addressed by the OCR outside the audit process. The OCR studied the results of the Phase 1 pilot program before implementing Phase 2, which will audit both covered entities and business associates.

Phase 2 Audits

During Phase 2, the OCR will conduct audits of approximately 200 covered entities and business associates. Most of the audits will be desk audits of covered entities, such as health plans and health care providers, followed by a second round of desk audits of business associates. Desk audits will be completed by the end of December 2016.

Health Compliance News Highlights:

- HHS will conduct more than 200 audits in the Phase 2 HIPAA Audit Program.
- Plan sponsors should conduct security assessments every two to three years, and when new electronic uses are adopted.
- A HIPAA/HITECH audit should include review of policies, training and operations.

[1] Phase 2 was announced on March 21, 2016. Information about OCR's HIPAA Privacy, Security, and Breach Notification Audit Program is available on the HHS website.

[2] HITECH, enacted in 2009, requires HHS to conduct periodic audits of covered entities and business associates to ensure compliance with the HIPAA Privacy and Security Rules and the HITECH breach notification rules. For background, see Segal's September 2009 *Bulletin*, "Final Regulations on HITECH Security Breach Notification for HIPAA Protected Health Information."

Covered entities and business associates will be notified of the scope of their desk audit in a document request letter. A third set of audits will be conducted on site. Those on-site audits will be broader in scope than the desk audits.

What Criteria Will the OCR Consider When Deciding Which Entities to Audit?

The selection criteria for an audit will include the following:

- Size of the entity,
- Affiliation with other health care organizations,
- The type of entity and its relationship to individuals,
- Whether an organization is public or private,
- Geographic factors, and
- Present enforcement activity with the OCR.

The OCR will *not* audit entities that have an open complaint investigation or that are currently undergoing a compliance review.

How Will the OCR Notify Entities Selected for an Audit?

Covered entities selected for an audit will be notified via email. The first email contact will be to verify contact information to identify covered entities and business associates. The OCR advises covered entities with a spam filter to check their junk or spam email folder for email from the OCR (OSOCRAudit@hhs.gov).

After contact has been established, entities selected for an audit will be sent an email notification of their selection and will be asked to provide information in response to a document request letter. Entities will also be asked to provide contact information for their business associates. Documents and other requested data will be submitted by the covered entity online via a new secure audit portal on the OCR's website within 10 business days of the date on the information request. The OCR will perform a desk audit and share draft findings with the entity. The audited entity will be able to respond to the draft findings and the response will be included in a final audit report. On-site audits may be conducted of selected covered entities and business associates.

What Will the OCR Do with the Audit Results?

Audit results will be used by the OCR for several purposes. The OCR plans to use Phase 2 of the audit process to identify best practices and discover risks and vulnerabilities to PHI. The OCR also intends to develop tools and guidance to assist the health care industry in self-evaluation and preventing data breaches. It will share best practices identified in the audit process, and will provide guidance on compliance challenges.

However, if a serious compliance issue arises during a Phase 2 audit, the OCR may conduct a compliance review and further investigation. The OCR will not publish a list of audited entities or findings of an individual audit.

"If a serious compliance issue arises during a Phase 2 audit, the OCR may conduct a compliance review and further investigation."

New Focus on Electronic Health Apps

The OCR recently issued guidance on how the HIPAA Privacy and Security rules apply to health information that a participant creates through the use of an electronic health app.[3] These apps are used by health insurers, plan administrators, and other service providers, such as wellness companies, to provide a handy interface to participants who want to file claims, check benefits or track healthy behaviors on their smartphone or tablet. The guidance is part of an initiative from the OCR to adapt the HIPAA and HITECH rules to innovative health information technology.

[3] In February 2016, the OCR issued guidance on how the HIPAA Privacy and Security rules apply to health information that a patient creates, manages or organizes through the use of an electronic health app: Health App Use Scenarios & HIPAA. The guidance is part of an initiative from the OCR to develop technical assistance related to the relationship of innovative health information technology, HIPAA and HITECH.

Plan sponsors that wish to develop their own apps, or that retain companies with health apps, should review the guidance so that they understand their obligations with respect to the apps. For example, if an employer plan hires an app developer to create an app for plan participants, the app developer would be a business associate and a business associate agreement would be required.

Implications for Plan Sponsors

Regardless of this new round of audits, plan sponsors and their business associates have significant obligations with regard to HIPAA and HITECH compliance. Policies should be updated, staff should be trained, and technology should be reviewed annually. In addition to the chance of audit, plan sponsors are under increased legal scrutiny with regard to these issues, as highlighted in the text below.

"Higher penalties mean that there is significant muscle behind the OCR's efforts."

HITECH increased the penalties for HIPAA violations up to $1.5 million for each criteria violated. These higher penalties mean that there is significant muscle behind the OCR's efforts. Enforcement history from the OCR's website shows that HITECH breach reporting and follow up enforcement actions have been taken against large and small entities, and result in hefty fines.

The OCR frequently seeks and obtains Resolution Agreements from covered entities and business associates that have experienced a privacy or security breach. A Resolution Agreement is a settlement agreement between the OCR and the entity that requires both a financial payment and a Corrective Action Plan (CAP). The CAPs generally have a list of tasks that the entity must complete and require frequent reports back to OCR about the status of compliance with the CAP. Tasks may include completing a security risk assessment, training workforce employees, preparing policies and procedures, and assuring that all business associates are identified and have current business associate agreements.

Increased Enforcement Activity: Recent Examples

In the last three months, OCR enforcement activity includes the following:

- A research institute paid a settlement of $3.9 million after OCR found multiple violations. A stolen laptop was unencrypted, so a breach report was made to OCR by the institute. While investigating the breach, OCR found that the institute had failed to conduct a risk assessment, not adopted policies and procedures to safeguard PHI, failed to implement policies and procedures governing receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and failed to implement a mechanism to encrypt ePHI or, alternatively, document why it was not reasonable.
- A physical therapy provider paid a settlement of $25,000 for posting testimonials from patients on its website without obtaining proper HIPAA written authorizations.
- A health care center paid a $1.55 million settlement after a business associate employee's unencrypted laptop was stolen, and further investigation revealed that the center did not prepare a risk assessment or business associate agreements.
- A university medical center paid a $750,000 settlement after its systems were infected with malware when an employee downloaded an email. Further investigation revealed that the university medical center did not conduct a comprehensive security risk assessment of all of its affiliated entities.

What Can Plan Sponsors Do to Ensure Compliance?

The best way to ensure compliance is to conduct an audit to identify whether the plan's HIPAA and HITECH policies and procedures are up to date. The first step is to look at the following compliance requirements:

- ***Security-Risk Assessment*** Is there a HIPAA security-risk assessment? Has it been updated periodically (ideally every two to three years) and also whenever new electronic technology or use of PHI is introduced?
- ***Privacy and Security Officers*** Are the entity's privacy and security Officers well trained on HIPAA and is there a process for reporting potential breaches and assessing whether they must be reported to HHS and/or the participant?
- ***Staff Training*** Are staff who handle PHI trained on the HIPAA and HITECH rules, as well as the entity's policies and procedures? Is refresher training repeated regularly? Are new employees trained prior to being allowed to handle PHI?
- ***Privacy Notices*** Have plan participants received a HIPAA Privacy Notice, and reminders at least every three years? Is the Notice on the plan's website?
- ***Business Associates*** Does the entity review whether each service provider is a business associate? Does the entity have contact information for all business associates? Are all business associate agreements readily available?
- ***Inventory of Technology that Can Store PHI*** Is there an inventory of all electronic devices, including computers, mobile devices (*e.g.*, laptops, phones and tablets) and copiers/scanners?
- ***Written Policies and Procedures for Safeguarding PHI*** Are HIPAA Privacy and Security policies and procedures in writing? Have they been updated since 2009, when HITECH was enacted? Are there policies and procedures for safeguarding *electronic* PHI, including policies for all electronic devices and policies for securing information through regular password changes and timely software updates?
- ***Encryption*** Has encryption been implemented for data in motion and at rest, and, if not, is a reasonable reason not to use encryption documented in a risk assessment?
- ***Disposal*** Is there a policy in place that addresses the destruction of drives, disks, removable storage devices and **other** media? Is PHI irretrievably wiped from these devices according to HIPAA and HITECH rules?
- ***Security Protections for Web or Mobile Applications*** If the entity has developed new web or mobile applications, is the app developer a business associate and are appropriate security protections in place for the apps, particularly during transition from one platform to another?

"The best way to ensure compliance is to conduct an assessment."

"Plan sponsors that are not confident of the answers to these questions should take steps to review their HIPAA compliance and conduct a current risk assessment."

Plan sponsors that are not confident of the answers to these questions should take steps to review their HIPAA compliance and conduct a current risk assessment.

What Else Can Plan Sponsors Do?

The potential scope of the HIPAA audits, the possibility of a resolution agreement and/or penalties all suggest that plan sponsors should review their fiduciary liability insurance to make sure it is current. Sponsors of plans that are audited may want to file a circumstance notice with their carriers alerting them to an incident that may give rise to a claim.

How Segal Can Help

Segal assists plan sponsors and their attorneys with compliance issues, including conducting HIPAA security-risk assessments, reviewing and updating HIPAA Security Policies and Procedures and providing staff training. Segal Select Insurance Services, whose core products include fiduciary liability insurance and cyber liability insurance, can review existing professional liability insurance policies and advise what HIPAA and other cyber-related coverages may be available to transfer risk and help protect plan assets.

Questions?

For more information about how these new rules may affect your plan, please contact your Segal consultant or the Segal office nearest you.

Segal Consulting

Segal Consulting is a member of The Segal Group.

To receive *Update* and other Segal publications, join our email list.