Bloomberg BNA

BNA's
Health Law Reporter™

Phase 2 HIPAA Audits: Compliance and Audit Response Tips for Covered Entities and Business Associates



TAMMY WARD WOFFENDEN, JENNIFER L. RANGEL AND LAUREN M. FINCHER

On March 21, 2016, the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced the second phase of its Health Insurance Portability and Accountability Act (HIPAA) compliance audit program ("Phase 2 Audits"). The much anticipated Phase 2 Audits are the sequel to OCR's 2011-2012 pilot audit program that assessed HIPAA controls and processes implemented by 115 covered entities. The new Phase 2 Audits are expected to focus on a larger pool of covered entities and their business associates and, while expected to consist primarily of desk audits, are also expected to include some on-site audits. Every covered entity and business associate is potentially subject to an audit and therefore should be prepared to provide evidence of policies and procedures adopted and employed to meet standards and implementation specifications of HIPAA's Privacy, Security and Breach Notification Rules.

Although it does not appear that OCR plans to initiate widespread enforcement activity resulting from audit findings, covered entities and business associates should be aware that, if OCR identifies a serious compliance issue during an audit, a full review and enforcement action may ensue. Developing an understanding of the audit process as well as OCR's historical enforcement actions, previous HIPAA compliance guidance and best practices for audit response will help organizations prepare for an audit and avoid pitfalls that could lead to more aggressive enforcement by OCR.

Tammy Ward Woffenden and Jennifer L. Rangel are partners, and Lauren Fincher is an associate, in the Austin, Texas, office of Locke Lord LLP. They focus on regulatory, transactional and administrative health law issues. Tammy can be reached at twoffenden@lockelord.com or 512-305-4776. Jennifer can be reached at jrangel@lockelord.com or 512-305-4745. Lauren can be reached at lfincher@lockelord.com or 512-305-4843.

Phase 2 Audit Basics

Phase 2 Audits will begin with desk audits of covered entities followed by a second round of desk audits of business associates.[1] OCR has started sending e-mails to covered entities and business associates requesting confirmation of the entities' contact information. Once this information is obtained, OCR will transmit a pre-audit questionnaire to gather information about entities potentially subject to audits. As part of the pre-audit screening questionnaire, OCR is asking that covered entities identify their business associates. If an entity does not verify its contact information or submit the pre-audit questionnaire, OCR will use publicly available information about the entity to create the audit subject pool. Consequently, an organization may still be selected for an audit, even if it fails to respond to OCR's initial communication. The final audit pool will be selected based on pre-audit questionnaire responses with

[1] *See* U.S. Dept. of Health and Human Servs., *HIPAA Privacy, Security, and Breach Notification Audit Program* (March 21, 2016), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.*

 ISSN 1064-2137

consideration of the size, type and operations of the entity.

Once OCR identifies participants in the audit pool, it will notify them that they are subject to a desk audit. OCR's notification letter will introduce the audit team, explain the audit process and communicate OCR's expectations in more detail. The letter will also include initial requests for documentation. OCR expects documentation to be submitted through OCR's secure online portal within 10 business days of the date of the request. The documents will be reviewed and the organization will subsequently receive OCR's draft findings. Audited organizations will have ten business days to review the draft findings and return written comments to the auditor. The auditor will then complete a final audit report within 30 business days after the organization's response. The final audit reports will generally describe how the audit was conducted, discuss any findings and contain organization responses to the draft findings.

All desk audits in this phase will be completed by the end of December 2016. After completion of covered entity and business associate desk audits, OCR will conduct a round of on-site audits. The on-site audits will examine a broader scope of requirements than the desk audits. On-site audits are expected to focus on a new group of audit subjects, though some organizations that have been the subject of a desk audit may also be subject to a subsequent on-site audit.

How to Prepare

Heading into the first round of Phase 2 Audits, covered entities and business associates should consider the following preparatory steps:

- **Confirm National Provider Identifier (NPI) Contact Information**: Because OCR may use NPI information to identify initial contact information of covered entities, any authorized officials or contacts and respective e-mail addresses listed with the National Plan & Provider Enumeration System (NPPES) should be current.
- **Monitor e-mail filters**: Communications from OCR will be sent via e-mail and may be incorrectly classified as spam. If an organization's spam filtering and virus protection are automatically enabled, OCR expects organizations to check junk or spam e-mail folders for e-mails from OCR. Authorized officials and contacts on file with NPPES should be aware of potential e-mail traffic from OCR.
- **Inventory Business Associate Arrangements:** Covered entities should prepare and update lists of business associates, including contact information, and confirm that business associate agreements are in place. Business associates should do the same with regard to their subcontractors that qualify as business associates.
- **Review Current HIPAA Compliance Practices:** Covered entities and business associates should take a number of steps to prepare for desk audits, including: updating security risk assessments if one has not recently been performed; reviewing and updating privacy, security and breach notification policies and procedures; updating workforce training and security reminders as indicated; reviewing and updating Notices of Privacy Practices; and completing an inventory of business associates and business associate agreements (including confirming that such agreements comply with the Health Information Technology for Economic and Clinical Health (HITECH) Act). Covered entities and business associates also should consult OCR's audit protocol, which contains the requirements that OCR will assess during an audit, for additional insight into OCR's expectations concerning HIPAA compliance.[2] Organizations that receive a pre-audit questionnaire from OCR should confirm that documents relating to HIPAA compliance are readily available.

Audit Response Practices

Once a covered entity or business associate knows of an impending desk or on-site audit, implementing effective audit response practices will help the organization efficiently gather relevant information, track the progress of the audit, predict potential concerns arising from the audit process and effectively respond to audit findings. Best practices include:

- All responses should be provided within the timeframes prescribed by OCR. In the event an entity needs additional time, the auditors should be immediately contacted to request a formal extension. If approved, it is advisable that such extensions are documented in writing.
- Upon notice of an audit or investigation, an organization should put a hold on routine destruction of documents relating to HIPAA compliance (such as records of accounting of disclosures) and put relevant parties on notice of hold obligations to avoid routine destruction.
- During an audit, representatives of the organization should remain friendly and cooperative. The organization should carefully read document requests and provide complete responses to the auditor. If OCR requests specific policies and procedures, it is not advisable to inundate OCR with every policy and procedure ever adopted by the organization.
- If the auditor is on-site, the organization should assign an employee to be with the auditor(s) at all times and to make notes regarding the audit activities. Such notes should include the types of records requested, general demeanor and interactions with the auditor and any supplemental requests made by the auditor. The organization should try to keep a complete copy of materials provided to the auditors (whether provided on-site or through the OCR online portal). Following the audit, the organization should conduct an internal review of the records and locate anything that may

[2] U.S. Dept. of Health and Human Servs., *Audit Protocol – Current*, *available at* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html.

  HLR ISSN 1064-2137

have been missing and not provided during the audit.

- Organizations should take advantage of the opportunity to respond to draft findings and, to the extent possible and appropriate, respond to all deficiencies noted in draft findings and address any legal and factual responses to the findings.

- If an on-site audit is conducted, the organization should be prepared to demonstrate proper facility access controls, including requesting visitor identification and sign-in procedures. Workplace security measures, such as protecting inadvertent viewing of protected health information (PHI) by visitors and the public, should be evaluated prior to the site visit. Proper placement of computer monitors and secure filing systems (such as locked cabinets) should be considered.

Avoiding Pitfalls

OCR plans to use audit findings to help develop additional tools and guidance to assist the industry with compliance, self- evaluation and breach prevention. However, if OCR identifies a serious compliance issue during an audit, further compliance review and investigation may follow. Covered entities and business associates should confirm that their practices do not fall into certain traps that could lead to more aggressive enforcement. Past mistakes resulting in significant settlements with OCR have included:

- **Failure to enter into Business Associate Agreements:** Although the HITECH Act extended direct liability for certain Privacy Rule requirements and the HIPAA Security Rule to business associates, covered entities must continue to track their business associates and enter into HIPAA compliant business associate agreements. OCR has recently reported two large settlements involving the failure to enter into business associate agreements. In March 2016, OCR announced a $1.55 million settlement with a Minnesota health-care system following investigation of a breach report that indicated that an unencrypted, password-protected laptop was stolen from a business associate's workforce member's locked vehicle, impacting the electronic PHI of 9,497 individuals.[3] OCR expressed concern that the system failed to enter into a business associate agreement with a major contractor and failed to institute an organization-wide risk analysis to address the risks and vulnerabilities to its patient information. OCR concluded that a risk assessment should have covered all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes. In November 2015, OCR entered into a $3.5 million settlement involving similar allegations against an insurance holding company in San Juan, Puerto Rico.[4]

- **Unauthorized Disclosures on Websites and Social Media:** Covered entities and business associates should consider incorporating use of social media into HIPAA compliance training. Organizations with a presence on social media should consider adopting a social media policy along with a specific HIPAA compliant authorization form relating to the use of individual images and videos. In February 2016, a small physical therapy practice entered into a $25,000 settlement with OCR following an investigation of a complaint that the practice posted patient testimonials, including full names and full face photographic images, to its website without obtaining valid, HIPAA-compliant authorizations. In addition to finding that the practice failed to reasonably safeguard PHI and made impermissible disclosures on its website, OCR found that the practice failed to implement policies and procedures with respect to PHI that were designed to comply with HIPAA's requirements regarding authorization.[5]

- **Loss or Theft of Unencrypted Laptops and Other Devices:** Covered entities and business associates that permit their workforce to use, and travel with, laptops containing PHI should address risks associated with laptop use in policies and procedures, ongoing security risk assessments and workforce training. Furthermore, based on the number of enforcement actions and fines assessed for loss and theft of unencrypted laptops containing PHI, OCR has communicated little tolerance for the failure to encrypt mobile devices. As recently as last month, OCR announced a $3.9 million settlement with a biomedical research institute in New York after an investigation involving a laptop computer containing the ePHI of approximately 13,000 patients and research participants that was stolen from an employee's car.[6] Although encryption of ePHI is an ''addressable'' standard under the HIPAA Security Rule, OCR has consistently taken the position that ''[c]overed entities and business associates must understand that mobile device security is their obligation, . . . [and OCR's] message to these organizations is simple: encryption is your best defense against these incidents.''[7] Covered entities and

[3] U.S. Dept. of Health and Human Servs., *$1.55 million settlement underscores the importance of executing HIPAA business associate agreements* (March 16, 2016), *available at http://src.bna.com/ecW*.

[4] U.S. Dept. of Health and Human Servs., *Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement* (Nov. 30, 2015), *available at http://src.bna.com/ecY*.

[5] U.S. Dept. of Health and Human Servs., *Physical therapy provider settles violations that it impermissibly disclosed patient information* (Feb. 16, 2016), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/complete-pt/index.html*.

[6] U.S. Dept. of Health and Human Servs., *Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement* (March 17, 2016), *available at http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html*.

[7] U.S. Dept. of Health and Human Servs., *Stolen laptops lead to important HIPAA settlements* (April 22, 2014), *available at http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html*.

business associates should maintain an inventory of any mobile devices that contain PHI.

- **Losing PHI:** Covered entities, such as home health-care and hospice providers, whose workforce has a legitimate business purpose for taking PHI outside of the workplace should have policies and procedures in place to train their workforce regarding traveling with PHI and have mechanisms in place to confirm that records are returned to the entity. Over the years, OCR has fined covered entities for losing records in public, having records stolen and failing to ensure that records are properly returned after an employee's termination.

- **Improper Disposal of PHI:** OCR also has brought actions against entities that fail to properly discard PHI.[8] Covered entities and business associates should have document destruction policies and procedures requiring secure disposal of PHI and should train their workforce on proper disposal of PHI.[9] With regard to electronic PHI, organizations should confirm that practices are in place for secure disposal or recycling of equipment—including servers, laptops and photocopiers—containing PHI.

- **Using Insecure Applications and Software:** OCR has expressed concern and brought actions against covered entities for using unsecured internet-based document storage and share sites;[10] failing to update IT resources with available patches and running outdated, unsupported software;[11] disabling firewalls;[12] and inadvertently permitting public online access to PHI or not having proper controls securing online access to PHI.[13] OCR has consistently communicated that covered entities and business associates must carefully consider the security of IT resources, ensure that PHI available through online access is secured through access controls, and that an enterprise-wide security risk assessment is conducted routinely. Organizations must also adopt—and follow—HIPAA security policies and procedures and risk management policies that effectively identify and mitigate risks related to electronic PHI.

- **Failure to Perform Complete and Accurate Security Risk Assessments:** The HIPAA Security Rule requires all covered entities and business associates to conduct accurate and thorough risk assessments to help prevent, detect, contain and correct security violations.[14] An overarching theme seen in most OCR enforcement actions is the failure to conduct ongoing and routine risk assessments or incomplete, inadequate or infrequent risk assessments that fail to address or identify common vulnerabilities such as laptop security, maintenance of proper IT resources, and facility and access controls. Covered entities and business associates should confirm that they have a current and thorough security risk assessment on file and that any potential vulnerabilities noted in the risk assessment have been addressed with a documented response. If applicable, organizations should also confirm that they have a documented justification explaining why any safeguards regarded as addressable implementation standards under the Security Rule have not been adopted. The failure to perform a risk assessment is possibly the most common reason for the assessment of penalties.

- **Failure to Maintain Effective Policies and Procedures:** Another common theme seen in many OCR enforcement actions involves failure to adopt and follow effective and comprehensive HIPAA policies and procedures that address HIPAA Privacy, Security and Breach Notification requirements. Covered entities and business associates should confirm that day-to-day practices are consistent with such policies and procedures. Furthermore, policies and procedures should be instructive and practical for workforce implementation and not simply restate language in the rules. Organizations should be prepared to provide OCR with copies of their policies and procedures and evidence of related workforce training and attendance.

Conclusion

In addition to moving toward a permanent audit program, OCR will continue to investigate complaints, tips, media reports and breach notifications. OCR also is enhancing its internal tracking systems to identify entities

[8] U.S. Dept. of Health and Human Servs., *HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records* (April 30, 2015), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cornell/index.html*.

[9] U.S. Dept. of Health and Human Servs., *$800,000 HIPAA Settlement in Medical Records Dumping Case* (June 23, 2014), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/parkview-health-system/index.html*.

[10] U.S. Dept. of Health and Human Servs., *HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications* (July 10, 2015), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/semc/index.html*.

[11] U.S. Dept. of Health and Human Servs., *HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software* (Dec. 2, 2014), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/acmhs/index.html*.

[12] U.S. Dept. of Health and Human Servs., *Data breach results in $4.8 million HIPAA settlements* (May 7, 2014), *available at http://www.hhs.gov/about/news/2014/05/07/data-breach-results-48-million-hipaa-settlements.html*; *Idaho State University Settles HIPAA Security Case for $400,000* (May 21, 2013), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/idaho-state-university/isu-agreement/index.html*.

[13] U.S. Dept. of Health and Human Servs., *County Government Settles Potential HIPAA Violations* (March 7, 2014), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/skagit-county/index.html*; *WellPoint pays HHS $1.7 million for leaving information accessible over Internet* (July 11, 2013), *available at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/wellpoint/index.html*; *HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards* (April 7, 2012), *available at https://wayback.archive-it.org/3926/20150121155453/http://www.hhs.gov/news/press/2012pres/04/20120417a.html*.

[14] 45 C.F.R. § 164.308.

  HLR ISSN 1064-2137

that have systematic problems with HIPAA compliance, as evidenced by multiple breach reports.[15] As OCR further refines its investigative and auditing procedures, additional guidance is anticipated but many also expect more enforcement activity and penalties.

[15] *See* Dept. of Health and Human Servs., Office of Inspector General, OEI-09-10-00510, *OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards*, (2015); OEI-09-10-00511, *OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities* (2015).