Morgan Lewis

OCR LAUNCHES THE HIPAA PHASE 2 AUDITS: ARE YOU PREPARED?

Morgan Lewis Webinar

W. Reece Hirsch, CIPP, Partner
Nicole R. Sadler, CIPP, Associate

April 5, 2016

Preparing for Phase 2

- On March 21, the Dept. of Health and Human Services Office for Civil Rights (OCR) announced the second phase of audits of compliance with the HIPAA privacy, security and breach notification rules
  - As required by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act)
  - Announcement was made by OCR Director Jocelyn Samuels at the HIPAA Summit conference in Washington
- Healthcare industry has been expecting Phase 2 for more than a year and a half

A New Era of HIPAA Enforcement

- Phase 2 audits mark the beginning of a new era in HIPAA enforcement
- This is the perfect time for HIPAA covered entities and business associates to review their HIPAA compliance programs -- even if you’re lucky enough to avoid audit
- Phase 2 and future HIPAA enforcement should be viewed in the context of September 2015 report from the HHS Office of Inspector General, charging that OCR wasn’t
  - Investigating enough small data breaches
  - Keeping track of all healthcare organizations found to have violated HIPAA

Focus on Desk Audits

- Phase 2 will consist of more than 200 desk and on-site audits
  - Original plan for Phase 2 was 350 covered entities and 50 business associates audited
  - Desk audits focus on review of documents and do not involve on-site auditing
  - Majority of Phase 2 audits will be desk audits but there will be some on-site audits
- First round of desk audits will focus on covered entities (health plans, health care providers and health care clearinghouses)
- Second round will focus on business associates

Audit Schedule

- The first two rounds of desk audits are expected to be completed by December 2016
- Third round of audits will be on-site and will begin later in the year
- An entity that is subject to a desk audit may also have to undergo an on-site audit

Address Verification

- OCR is now sending emails to covered entities and business associates asking them to verify their contact information
- These entities will receive a “pre-audit questionnaire” requesting details about their business size, type and operations
- OCR will create a pool of audit targets that represent a wide and representative sampling of covered entities and business associates

Factors in Selection

- OCR will consider the following factors in selecting audit subjects:
  - Size of the entity
  - Affiliation with other healthcare organizations
  - Type of entity and its relationship to individuals
  - Whether organization is public or private
  - Geographic factors
  - Present enforcement activity with OCR
- OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review

Does a Security Breach Make You an Audit Target?

- OCR’s Linda Sanches said at a Healthcare Compliance Association Compliance Institute that OCR is not selecting entities for the audit program based upon whether they’ve reported a breach to OCR
  - Goal of Phase 2 is to have a somewhat random but representative sample
- Of course, a significant breach can lead to an OCR investigation

Audit Protocols

- Protocols for the Phase 2 audits will be posted on the OCR website soon, according to Director Samuels
- The protocol for the Phase 1 audits was widely considered to be very burdensome
- Phase 2 audit protocols are designed to work with a broad range of covered entities and business associates
  - But application may vary depending on the size and complexity of the audited organization

Desk Audit Process

- Entities selected for a desk audit will be notified by email and will be asked to provide documents and other data
- Unlike the Phase 1 audits, the desk audits will not address all HIPAA standards
- Focus will be on particular provisions of the HIPAA Privacy, Security and Breach Notification Rules, such as
  - Security risk analysis and risk management
  - Notices of privacy practices (for CEs)
  - Response to requests for access to PHI
  - Content and timeliness of breach notifications

Timing of Audit Responses

- Audit subjects will have 10 business days to submit the requested information through an audit-specific portal on OCR’s website
  - Delays in commencement of Phase 2 were attributed to the time needed to develop the audit portal
- OCR will then review the documentation and develop draft findings
- Auditors will share their findings with audited entities, allowing them 10 business days to respond
- Entity’s written responses will be included in the final audit report, which will also be shared with the audited entity

On-Site Audits

- Similarly, entities will be notified by email of their selection for an on-site audit
- On-site audits will be conducted over 3-5 days (depending on the size of the entity)
- Will be more comprehensive and have a broader focus on HIPAA requirements
  - Similar to Phase 1 audits
- As in the desk audits, entities will have 10 business days to review the draft findings and provide written comments to the auditor
- OCR will share a copy of the final audit report with the entity

Enforcement Actions to Follow?

- OCR stated that the audits are intended to help the agency get out in front of potential compliance issues and better direct its guidance to the industry
- Samuels: “We don’t intend it to be a punitive mechanism”
- However, audits that uncover “serious” issues may trigger an OCR compliance review in addition to the audit
- What qualifies as “serious”?
  - The absence of a HIPAA security risk analysis?
    - That has been a basis for OCR enforcement actions arising out of a security breach or other incident

How Serious is “Serious”?

- Phase 1 audits were intended to assess level of covered entity compliance with a wide range of HIPAA standards
- Now that more time has passed since HIPAA effective dates, will clear noncompliance with any single Privacy, Security or Breach Notification Rule standard be deemed a “serious” issue?
- That seems to be the attitude that OCR has taken in recent enforcement actions, which are typically prompted by a reported security breach or patient complaint

Engaging Legal Counsel

- Engaging legal counsel may be advisable to ensure that an audit response does not make unnecessary admissions that could be damaging in a subsequent enforcement action
- When timeliness of breach notification is being reviewed, need to make sure that breach investigation report tells the full story, explains factors that influenced timing
- Because desk audits are document-intensive, want to make sure that you’re putting your best foot forward
  - If you’re submitting a document that poses a compliance risk, you need to be sure you know that BEFORE you deliver it to OCR
- Once deficient policies and procedures or other documentation is provided to OCR, it may be difficult to “unring the bell”

No “Wall of Shame”

- OCR will not post a list of audited entities or the findings of an individual audit that clearly identifies the audited entity
- However, under the Freedom of Information Act (FOIA), OCR may be required to release audit notification letters and other information about the audits
- Unlike OCR’s “Wall of Shame” that publicly posts information regarding covered entities that have experienced breaches involving more than 500 individuals

Phase 1 Audit Findings

- OCR conducted pilot HIPAA audits during 2011 and 2012 (Phase 1 Audits), focusing on covered entities
  - Phase 2 will also audit business associates
- Phase 1 involved 115 covered entities, and the results were not very encouraging
  - No findings or observations for only 11% of the covered entities audited
  - Despite representing 53% of the audited entities, health care providers were responsible for 65% of the total findings and observations

Phase 1 Audit Findings (cont.)

- The smallest covered entities were found to struggle with compliance under all three of the HIPAA standards
- More than 60% of the findings or observations were Security Rule violations
  - 58 of 59 audited health care provider covered entities had at least one Security Rule finding or observation
  - Even though the Security Rule represented only 28% of the total audit items
- Security Rule compliance is clearly a problem area

Phase 1 Audit Findings (cont.)

- More than 39% of the findings and observations related to the Privacy Rule were attributed to a lack of awareness of the applicable Privacy Rule requirement
- Only 10% of the findings and observations were attributable to a lack of compliance with the Breach Notification Rule
- Phase 1 audits were labor intensive
  - Assessing compliance with 169 requirements
  - Typically 3-4 weeks of active audit response work
  - Phase 2 will take a lighter, more targeted approach

What Are the Likely Areas of Focus?

- Security risk analysis and risk management
- Notices of privacy practices (for CEs)
- Response to requests for access to PHI
- Content and timeliness of breach notifications
- These areas were cited by OCR’s Samuels in her announcement
- Phase 2 will NOT extend beyond the HIPAA Privacy, Security and Breach Notification Rules
  - No review of state medical privacy and security law compliance

Other Possible Audit Areas for Covered Entities

- When the Phase 2 audits were anticipated in 2015, OCR stated that audits of covered entities would also focus on:
  - Device and media controls (Security Rule)
  - Transmission security (Security Rule)
  - Safeguards (Privacy Rule)
  - Training on policies and procedures (Privacy Rule)

Likely Audit Areas for Business Associates

- When audits were expected in 2015, audits of business associates were to focus on
  - Risk analysis and risk management (Security Rule)
  - Breach reporting to the covered entity (Breach Notification Rule)
- Areas such as Notice of Privacy Practices and access to patient requests for PHI are more relevant to covered entity operations

The New OCR Portal

- New OCR portal technology is expected to ease the human workload in the audit process by collecting, collating and analyzing audit data
- New portal will be used to conduct pre-audit survey screening and will also allow entities to enter audit data
- All documents submitted in response to the audit must be in digital form and submitted electronically through the portal
- The portal technology is intended to save OCR time and allow them to conduct more audits

Staffing the Audits

- Audits were originally to be conducted by OCR regional investigators
  - Unlike Phase 1 audits, which were performed by contractor KPMG
- Phase 2 audits are now to be conducted by FCi Federal
  - Government services provider based in Ashburn, VA
  - Awarded the contract in October 2015

Feeling Lucky?

- Given the relatively small sample size, the chances that a particular organization will be selected for audit are fairly low
- But preparation for audit will help an organization avoid sanctions in the event of an investigation – which could be triggered by any breach reported to HHS
- Phase 2 audits are likely to be the beginning of an ongoing audit program
  - More sustainable for OCR because using internal staff and new web portal

Preparing for Phase 2: List Your Business Associates

- OCR will ask for a list of business associates as part of the pre-audit screening questionnaire
  - Those lists will be the source of the business associates chosen to be audited in the second round of Phase 2
- Covered entities should prepare a list of business associates in advance, including
  - Contact information
  - The nature of the service that the business associate provides
  - Can be challenging for organizations with hundreds (or thousands) of business associate relationships

Ensure that OCR's Emails Don't End Up in Your Spam Folder!

- OCR stated that it will be sending audit-related emails from OSOCRAudit@hhs.gov
- OCR expects covered entities and business associates to check their spam and junk mail folders for correspondence from the agency
- If you don't respond to an address verification email, OCR will use publicly available contact information
  - You will still be in the audit pool

OCR Has Provided a Roadmap – Use It!

- OCR has done the healthcare industry a favor by highlighting its areas of focus for the Phase 2 audits
  - Make sure that your HIPAA compliance program thoroughly addresses those risk areas
- When the Phase 2 audit protocol is issued, convene your audit response team and carefully review your compliance with the identified HIPAA standards

Other Likely Phase 2 Risk Areas

- Do you have a compliant Notice of Privacy Practices (reflecting Final Rule tweaks)?
  - Not just a website privacy notice
- Have you encrypted laptops containing PHI and other devices? If you don't encrypt, does your risk analysis explain how you reached that decision?
- Do you have an inventory of information system assets, such as mobile devices?
  - Even if you've adopted a Bring Your Own Device policy
- Does your organization have a facility security plan for each physical location that maintains PHI?

More Likely Phase 2 Risk Areas

- Has your workforce been properly trained to comply with your HIPAA privacy, security and breach notification policies? How recently?
  - Has that training been documented?
- Somewhat surprisingly, patient access to PHI has also proven to be an area where many organizations are deficient
  - Ensure that personnel responding to records requests are aware of HIPAA timing requirements

Identify Your Audit Response Team; Conduct a Mock Audit

- Covered entities and business associates will only have 10 business days to respond to a request for a documentation and 10 business days to review the auditor’s draft findings
- Identify your audit response team now to ensure they will be prepared to respond promptly and within required timeframes
- Performing a mock audit can be helpful
  - See what documentation can be produced in 10 business days with respect to key risk areas (risk analysis, breach response, etc.)
  - Identify the point person for coordinating the audit response

Do the Documents Tell Your Story?

- In a desk audit, your policies, procedures and other documentation must tell your story
  - You won’t have the opportunity to provide supplemental explanations as in an on-site audit
- Desk audits favor organizations that take a rigorous, formal, documented approach to compliance
  - If your organization does not fit that description, now is the time to improve your documentation
- Have your policies been thoroughly updated to reflect the HIPAA Final Rule?

Check the Dates

- Make sure that policies and procedures have been approved, implemented and updated on a regular basis, which is an indicator of an active HIPAA compliance program
  - Updating the security risk analysis is particularly critical because system configurations and threats inevitably change
  - If more than 2 years have passed since your last HIPAA risk analysis, this area should be carefully reviewed
- If the date on a requested document is after the date of the audit request, then OCR will not consider the entity compliant

Dotting the I’s

- Make sure that your HIPAA policies are approved, signed and dated
  - Failure to sign a policy can create a presumption of noncompliance
- Best practice is to have your policies and procedures fully implemented and documented today
- However, if you receive a pre-audit questionnaire, you may still scramble to improve documentation before being selected for audit – but it’s not optimal

Map Your Data Flows

- OCR’s Sanches has recommended that covered entities prepare for audits by identifying the location of PHI within an organization and tracking data flows
  - within the organization ***and*** with third parties
- A data mapping exercise can help identify weak points in a HIPAA compliance program that may require
  - Enhanced policies and procedures
  - Additional workforce training

Physical Access Controls

- An OCR representative has highlighted physical access as an area of focus, saying:
  - Theft accounts for 50% of all breaches
  - Despite focus on digital safeguards, 21% of breaches involve paper records
  - Cited Parkview Health case, in which nonprofit health system agreed to pay $800,000 and adopt a corrective action plan
  - Parkview employees left 71 cardboard boxes of medical records on the driveway of a retiring physician’s home

Phase 2’s Focus on the Security Rule

- In preparing for an audit, a focus on Security Rule standards is advisable
- Confirm that all action items reflected in your risk analysis have been completed or are on a reasonable schedule for completion
- If you have chosen not to implement any of the Security Rule’s addressable implementation standards, then clear documentation should be available explaining and justifying that decision

Security Risk Analysis

- Recent OCR enforcement actions involving North Memorial Healthcare of Minnesota (March 16, 2016) and University of Washington Medicine (December 2015) focused on the absence of adequate risk analysis
  - Covered entities and business associates should be able to show OCR auditors that they have performed a comprehensive security risk analysis that takes into account the current landscape of security risks
  - An inadequate risk analysis can call into question a host of security policies and procedures
  - In Phase 1 audits, 2/3 of entities audited lacked a complete and accurate risk analysis

Raising the HIPAA Security Rule Compliance Bar

- The cornerstone of HIPAA Security Rule compliance is the risk analysis
  - "An ***accurate and thorough assessment*** of potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI"
    - 45 CFR § 164.308(a)(1)(ii)(A)
  - In order to accurately and thoroughly assess current security risks, healthcare organizations must familiarize themselves with current cyber threats
  - In the Ponemon Institute's 2105 Study on Privacy and Data Security of Healthcare Data, 70% of respondents said greatest security threat was employee negligence, which does not appear to be accurate
  - An organization that misunderstands its primary security threats is likely to misallocate its security resources
  - If your organization does not have internal IT and security staff who have their finger on the pulse of current cyber threats, then need to consider engaging external resources

Encryption Is A HIPAA Enforcement Priority

- September 2015: NIST and OCR co-hosted annual security conference
  - OCR emphasized the importance of encryption
  - If an organization chooses not to encrypt ePHI, its risk analysis must:
    - Address the decision
    - Demonstrate that compensating controls have been implemented to protect unencrypted ePHI
    - Encryption remains “addressable” rather than required, but larger healthcare organizations with greater resources will be held to a higher standard

Incident Response Plans

- Incident response plans are a focus for both covered entities and business associates under the Phase 2 audits
- Documenting and implementing a comprehensive incident response plan is one of the best things that an organization can do to improve its HIPAA compliance posture
  - Reduces risk of investigation
  - Likely responsive to Phase 2 audits
  - Mitigates substantial damages that may arise from a significant and poorly managed breach

Security Breach Incident Response Plan

- Typically developed as a stand-alone module distinct from security policies and procedures
  - More than just a technical, systems document, requires input from legal, compliance and others
  - Includes employee-facing components

Incident Response Plans

- An effective incident response plan should:
  - Establish an incident response team with representatives from key areas of the organization
  - Identify necessary external resources in advance (forensic IT consultant, mailing vendor, call center operator, credit monitoring service)
  - Provide for training of rank-and-file personnel to recognize and report security breaches
  - Outline media relations strategy and point person

The Incident Response Team Leader

- There should be an incident team leader
  - Often an attorney or Chief Privacy Officer
  - Manages overall response
  - Acts as liaison between management and incident response team members
  - Coordinates responsibilities of team members
  - Develops project budgets
  - Ensures that systemic issues brought to light by a breach are addressed going forward

The Incident Response Team

- Because of the far-reaching impact of a significant breach, the Incident Response Team should include representatives from
  - Management
  - IT & Security
  - Legal
  - Compliance/Privacy
  - Public relations
  - Customer care
  - Investor relations (for public companies)
  - Human resources
  - External legal counsel (as appropriate)
  - Data breach resolution provider (as appropriate)

Meet During Peacetime

- No incident response team should be forced to learn their roles on the fly during a breach
  - Meet in peacetime
  - Understand the steps outlined in the breach response plan and each team member's role and responsibility
  - Run scenarios in advance
    - What does your company's worst-case scenario look like?
    - Is your company protected from potential breach liabilities through indemnification? Cyberliability insurance?
    - How likely is it that breach damages might exceed contractual limitations of liability? Insurance liability limits?

Training

- Incident response plan should include a module that is shorter and directed to employees
  - Can form the basis for regular training (once a year is advisable)
  - Employees should be able to identify the significance of a breach when it occurs and report it promptly to supervisors
- Discovery of a breach by an employee may be imputed to the organization
  - Clock begins ticking for notification of affected individuals
  - HIPAA recognizes this form of constructive knowledge

Spotting the Signs

- The employee-facing portion of an incident response plan should help employees spot the many possible signs of a security breach, such as:
  - Suspicious entries in system or network logs
  - Unsuccessful logon attempts
  - Unusually poor system performance
  - "Doorknob rattling," such as social engineering attempts
  - System alarms or other indications from intrusion detection systems
  - Recent CEO spoofing scams directed at obtaining employee data for tax fraud

The Time to Prepare for Phase 2 Is Now

- Since Phase 2 will be completed during 2016, the time to prepare for a HIPAA Phase 2 audit is now
- Even though only approximately 200 organizations will be audited in Phase 2, preparing for Phase 2 will help a covered entity or business associate
  - Ensure that it's HIPAA compliance program has addressed the areas of greatest compliance concern for OCR
  - Positioned the organization in case it is the target of a HIPAA investigation (as opposed to an audit) or a post-Phase 2 HIPAA audit
  - Reduce its general exposure to a damaging security breach

Questions?

Speaker Contact Information:

Reece Hirsch

reece.hirsch@morganlewis.com

415.442.1422

⌘

Nicole Sadler

nicole.sadler@morganlewis.com

415.442.1372

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing
Boston
Brussels
Chicago
Dallas
Dubai
Frankfurt
Hartford
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis