Strafford

Presenting a live 90-minute webinar with interactive Q&A

HIPAA Audits: Preparing for Phase 2 Audits for Covered Entities and Business Associates

Developing, Ensuring and Documenting HIPAA and HITECH Privacy and Security Compliance

WEDNESDAY, AUGUST 19, 2015

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Dianne J. Bourque, Member, **Mintz Levin Cohn Ferris Glovsky and Popeo**, Boston

Ryan S. Higgins, **McDermott Will & Emery**, Chicago

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-755-4350** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about CLE credit processing call us at 1-800-926-7926 ext. 35.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

HITECH Audits Phase I – What Have We Learned?

Presented by: Dianne J. Bourque, Esq.

August 19, 2014

Strafford Webinars

Dianne J. Bourque, Esq.
dbourque@mintz.com

Mintz Levin. **Not your standard practice.**

The HITECH Audit Program

- The HITECH Act Section 13411 requires HHS to perform periodic audits of covered entity and business associate HIPAA compliance.
- In 2011, OCR established a pilot audit program, developed an audit protocol and used the protocol to evaluate the HIPAA compliance efforts of 115 covered entities.
- OCR also conducted a formal, audit evaluation to measure the effectiveness of the pilot audit.

The First Round of Audits

- In November and December of 2011, OCR and KPMG notified the first 20 covered entities of their selection for audit.
- The notification letter included a request for documents and information to for scheduling the onsite review by the KPMG audit team.
- On-site reviews began in January, 2012 and ended in March 2012.

Initial 20 Entities Selected for Audit

Type of Entity	Entity Location
Medicaid Plan	-
Allopathic & Osteopathic Physicians	NY
Hospital	NJ
Group Health Plan	PA
Group Health Plan	DC
Healthcare Clearinghouse	-
Nursing & Custodial Care Facilities	MD
Pharmacy	PA
SCHIP	-
Allopathic & Osteopathic Physicians	NC
Allopathic & Osteopathic Physicians	AL
Hospital	KY
Group Health Plan	TN
Healthcare Clearinghouse	OK
Health Insurance Issuer	NM
Hospital	TX
Health Insurance Issuer	MO
Dentist	CO
Health Insurance Issuer	ND
Laboratory	SD

The Audit Protocol

The OCR HIPAA Audit Protocol contains the privacy, security and breach notification elements to be assessed

- Privacy: Notice of privacy practices, rights to request privacy protection for PHI, access to PHI, administrative requirements, uses and disclosures of PHI, amendment and accounting of disclosures.
- Security: Administrative, physical and technical safeguards
- Breach Notification: Breach notification.

For each HIPAA standard, there is a regulatory reference, testing procedures (such as interview Privacy Officer or management, review documentation or forms)

The audit protocol is available here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Audit Findings

- Only 13 out of 115 entities had no findings or observations (11%) – 2 providers, 9 health plans and 2 clearinghouses.
- Security accounted for 60% of the findings, which is far more frequent than privacy and breach notification findings
- Providers had a greater proportion of findings and observations (65%) but only constituted 53% of the entities reviewed.
- Smaller entities struggled with everything

Privacy Findings

- Notice
- Right to request privacy restrictions
- Access
- Administrative requirements
- Uses and Disclosures of PHI

Security Findings

- Risk Assessment (!)
  - Two thirds of the entities audited had no complete and accurate risk assessment.
- Addressable implementation specifications
  - Almost every entity *without* security findings had fully implemented the "addressable" standards
- Other problem areas: access management, security incident procedures, contingency planning and backup, workstation security, media movement and destruction, encryption, audit controls and monitoring
- Providers had more security findings

Breach Notification Findings

- Notification to individuals was the problem area
  - Timeliness, method of notification, and the burden of proof (whether or not notification is necessary)

Reasons for Findings

- Most common across all entities: entity unaware of the requirement
  - 39% of privacy findings
  - 27% of security findings
  - 12% of breach notification findings
- Other Causes
  - Lack of application of sufficient resources
  - Incomplete implementation
  - Complete disregard

Privacy

Entities most commonly unaware of:

- Notice requirement
- Access requirement
- Minimum necessary requirement
- Authorization requirement

Security

Entities most commonly unaware of:

- Risk analysis requirement
- Media movement and disposal requirement
- Audit controls and monitoring requirement

Informal OCR Comments

- Business Associates to be targeted in the second round of audits
- Group health plans of interest due to lack of complaints
- Audits will lead to enforcement

What Have We Learned?

- Don't wait until you get an audit letter to think about compliance
- Use the audit protocol to assess existing compliance measures
- Use the risk assessment, training and other tools that OCR has developed
- Use all available tools if you are a small provider
- Risk assessment and access are a big deal
- Addressable security standards are important – especially encryption
- A binder of policies and procedures is not sufficient

McDermott Will & Emery

Preparing for Phase 2 Audits

Ryan Higgins, Esq.

Associate

rshiggins@mwe.com

312-984-2052

Agenda

McDermott Will & Emery

- Scope of Phase 2 Audits
- Selection of Phase 2 Audit Recipients
- Phase 2 Audit Program Process
  - Audit Procedures and Methods
  - Navigation of Audit Process
- Preparation for Phase 2 Audits

Scope of Phase 2 Audits

McDermott Will & Emery

- OCR will prioritize areas of greater risk to the security of PHI and on pervasive non-compliance based on Phase 1 Audits (rather than a comprehensive review of all HIPAA Standards).
- Unlike the Phase 1 Audit Program, which focused on Covered Entities (CEs), OCR will conduct Phase 2 Audits of both CEs and Business Associates (BAs).
- Based on prior statements from OCR, 350 CEs and 50 Bas will be selected for Phase 2 Audits.
- Phase 2 Audits are expected to take place over 3 years.

Selection of Phase 2 Audit Recipients - CEs

McDermott Will & Emery

- OCR sent pre-audit screening surveys in spring 2015 to a pool of CEs that may be selected for Phase 2 Audits. Surveys request organization and contact information.
- OCR had originally planned to issue these screening surveys in the summer of 2014.
- Based on prior statements from OCR, OCR randomly selected 550 to 800 CEs through the NPI database and other external sources.
- OCR has said based on the survey responses, it will select approximately 350 CEs, 232 health care providers, 109 health plans, and 9 health care clearinghouses.

Selection of Phase 2 Audit Recipients - BAs

McDermott Will & Emery

- Data requests will ask the CEs to identify and provide contact information for their BAs.
- OCR will select 50 BAs for Phase 2 Audits from this pool: 35 IT-related and 15 non-IT related (*e.g.*, TPAs).
- OCR has previously indicated that compliance audits of BAs would begin in 2015 and continue into 2016, but this timeframe will likely be pushed back based on delay in the Phase 2 Audits of CEs.

Preparation for Phase 2 Audits

McDermott Will & Emery

- CEs and BAs should focus on correcting common Phase I Audit violations and preparing for auditor's document and information requests.
- OCR will make its Phase 2 Audit protocol available on its website to facilitate self-audits.

OCR Phase 2 Audit Priorities

McDermott Will & Emery

- Based on prior statements from OCR, OCR will audit approximately 150 of the selected CEs and 50 of the selected BAs for compliance with the Security Standards.
- 100 of the selected CEs for compliance with the Privacy Standards.
- 100 of the selected CEs for compliance with the Breach Notification Standards.

OCR Phase 2 Audit Priorities (cont'd)

McDermott Will & Emery

- 2016 Projected Priorities
  - Security Rule—Encryption and Decryption
  - Security Rule—Physical Facility Access Controls
  - Breach Rule—Breach Reports
  - Privacy Rule—Complaints
  - Other areas of high risk based on 2015 Phase 2 Audit findings

Address OCR Priority Items

McDermott Will & Emery

OCR Priority Item	CE/BA Action Step
Administrative Safeguard: Risk Analysis and Risk Management (§164.308(a)(1))	• Confirm periodic completion of a thorough security risk assessment of all information systems (IS) • Confirm that recommendations resulting from risk assessment were addressed or on reasonable timeline
Physical Safeguard: Device and Media Controls (§164.310(d))	• Implement electronic media sanitization policy (See NIST Special 800-88, Guidelines for Media Sanitization) to address disposal and re-use of electronic media • Implement an inventory of IS assets, including mobile devices, to track physical movement of EPHI

Address OCR Priority Items (cont'd)

McDermott Will & Emery

OCR Priority Item	CE/BA Action Step
Technical Safeguard: Transmission Security (§164.312(e))	• Review security measures to guard against unauthorized access to EPHI transmitted over Internet/networks • Implement encrypted email and/or text messaging applications
Technical Safeguard: Encryption and Decryption (§164.312(a)(2)(iv)) (2016 Audit Priority Item)	• Confirm that IS assets and software that transmit EPHI either employ encryption or written risk analysis supports absence of encryption
Physical Safeguard: Facility Access Control (§164.312(e)) (2016 Audit Priority Item)	• Confirm adoption of a location-specific physical security plan for each physical location with access to PHI; not merely a security policy that requires a physical security plan

Address OCR Priority Items (cont'd)

McDermott Will & Emery

OCR Priority Item	CE/BA Action Step
Breach Notice Content and Timeliness of Notice by CE to Individuals (§164.404)	Confirm breach notification policy reflects Breach Notification Rule's content and timeliness requirements for breach notification to individuals
Breach Reporting by BA to CE (§164.410)	BA should confirm that breach notification policy reflects Breach Notification Rule's content and timeliness requirements for breach reporting by BA to CE

Address OCR Priority Items (cont'd)

McDermott Will & Emery

OCR Priority Item	CE Action Item
Access of Individual to PHI (§164.524)	Confirm that CE has an appropriate written policy addressing individual's right to access PHI, including appropriate limitations on fees
Notice of Privacy Practices (NPP) (§164.520)	• CE should review NPP to confirm that it meets Privacy Rule's content requirements • Website privacy policy is not sufficient • CE must post NPP on its website

Address OCR Priority Items (cont'd)

McDermott Will & Emery

OCR Priority Item	CE/BA Action Item
Reasonable Safeguards (§164.530(c))	• Ensure that CE/BA has reasonable and appropriate safeguards in place for PHI in any medium, including paper PHI (e.g., shredding machines for paper PHI)
Training on Policies and Procedures (§164.530(b))	• Confirm training materials are consistent with final omnibus rule • Implement system to track Workforce members' completion of training • Review system records to confirm that all Workforce members have been trained as needed for job duties

Other Preparatory Steps

McDermott Will & Emery

- Ensure that CE/BA has a complete list of BAs with current contact information and an associated inventory of signed, upstream and downstream BA agreements for Phase 2 Audit data request.
- If CE/BA has not implemented any of the Security Rule's' addressable implementation standards for any information system or facility, confirm that it has documented:
  - why the implementation specification was not reasonable and appropriate; and
  - the alternative security measures implemented.

Compliance Resources and Tools

McDermott Will & Emery

- OCR's security risk analysis tool for small providers: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
- McDermott offers a security risk assessment and gap analysis tool and model privacy security and breach notification policies and procedures for CEs (providers, insurers and group health plans) and Bas, including those with cloud-based IT
- OCR and NIST Guidance on Security Rule, including links to relevant NIST publications: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

OCR Data Request and CE/BA Response

McDermott Will & Emery

- CEs and BAs will have two weeks to respond to data request.
- Data request will specify the content, file names and other documentation requirements.
- OCR auditors will consider documentation submitted on time and will not request clarifications or additional information so it is critical that CE/BA provide a complete response.
- OCR will consider documentation that is current as of the time of the request.
- Failure to respond to a request could lead to a referral to the applicable OCR Regional Office for a compliance review.

OCR Desk Reviews

McDermott Will & Emery

- OCR previously stated that the Phase 2 Audits would be conducted as “desk audits” rather than onsite visits.
- In more recent statements, OCR stated that while most Phase 2 Audits will be desk audits, OCR will so conduct some onsite, comprehensive audits.
- Auditors will only consider timely submitted documentation and information.

OCR Audit Report

McDermott Will & Emery

- OCR will present CE/BA with a draft audit report to allow management to comment before report is finalized.
- Develop an analytical response that advocates for CE/BA with a respectful tone that communicates commitment to compliance.
- OCR will take into account management's response and issue a final report.
- Audits are intended to be educational, but could result in a referral to the applicable OCR Regional Office.