ComplyAssistant

Webinar Summer Series #1

Attorneys at Oscislawski LLC

OCR HIPAA Audits Have Begun

Are You Prepared?

presented by

Helen Oscislawski, Esq.

June 22 2016

Attorneys at
Oscislawski LLC

Presenter Background

- Gerry Blass brings 35+ years of experience in healthcare information technology. Prior to ComplyAssistant, Mr. Blass was the Chief Information Security Officer (CISO) for a major healthcare system in New Jersey.
- In 2002 Gerry founded ComplyAssistant to provide software and service solutions for HIPAA and IT strategic planning Today, ComplyAssistant provides software and service solutions to over 100 healthcare organizations with a focus on HIPAA-HITECH-OMNIBUS, PCI, HITRUST, Meaningful Use, Accreditation, OIG (federal and state), Conflict of Interest, and other federal and state healthcare regulations.
- Gerry is an active member of HIMSS and participates in national and various chapter events and actively shares content in HIPAA 411, a LinkedIn group he co-founded, along with many other related LinkedIn groups Gerry is an active member and presents at industry association events, including HIMSS, HFMA, AITP, NCHICA, and HCCA.

Gerry Blass
President and CEO
ComplyAssistant

Presenter Background

- Helen founded Oscislawski LLC to pursue her vision and desire to create a truly client-centric, modern-day law practice that responds to the changing needs of her predominant healthcare client base. She is known to many as a "go to" attorney for legal guidance on HIPAA, HITECH, state privacy laws, and electronic health information exchange (HIE).

Helen Oscislawski
Founder of
Attorneys at Oscislawski

HIPAA Audit (Phase 2) Overview

Director of Office of Civil Rights

HHS.gov U.S. Department of Health & Human Services

About HHS | Programs & Services | Grants & Contracts | Laws & Regulations

- Leadership
  - HHS Secretary
    - Biography & Portrait
    - Blog Posts
    - Speeches
    - Videos
    - Testimony
    - Op-eds
    - Contact Information
- Budget & Performance

Jocelyn Samuels

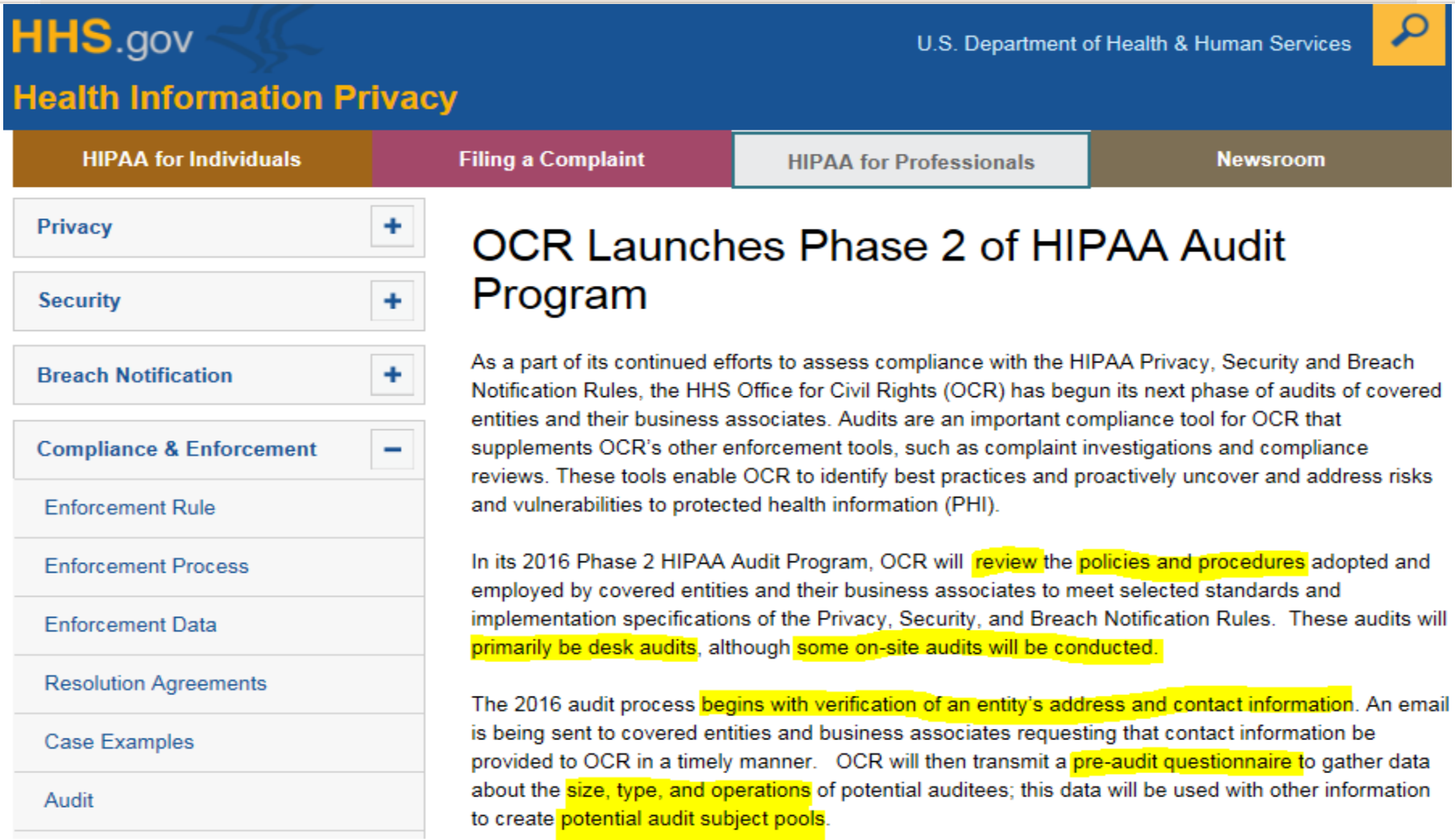
Director, Office for Civil Rights (OCR)

Jocelyn Samuels is the Director of the HHS Office for Civil Rights, where she leads that Office's work to enforce federal laws that help to ensure non-discrimination and equity in federally funded health and human services. She also spearheads enforcement of federal laws that protect the privacy and security of medical information and the rights of individuals to their health records.

Ms. Samuels was previously the Acting Assistant Attorney General for Civil Rights at the United States Department of Justice, where she managed the operations of the Civil Rights Division. Highlights of her tenure included leading the Division in landmark efforts to protect the right of citizens to access the franchise under the Voting Rights Act of 1965; advancing systemic reform of city police departments across the country; working to provide individuals with developmental disabilities the opportunity to live and work in their communities; promoting student diversity; overseeing the prosecution of hate crimes under the Matthew Shepard and James Byrd, Jr. Hate Crimes Prevention Act; and preventing housing, lending, and employment discrimination.

HIPAA Audits (phase 2) is Underway

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html



HHS.gov

U.S. Department of Health & Human Services

Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

- Privacy +
- Security +
- Breach Notification +
- Compliance & Enforcement –
  - Enforcement Rule
  - Enforcement Process
  - Enforcement Data
  - Resolution Agreements
  - Case Examples
  - Audit

OCR Launches Phase 2 of HIPAA Audit Program

As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the HHS Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates. Audits are an important compliance tool for OCR that supplements OCR's other enforcement tools, such as complaint investigations and compliance reviews. These tools enable OCR to identify best practices and proactively uncover and address risks and vulnerabilities to protected health information (PHI).

In its 2016 Phase 2 HIPAA Audit Program, OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted.

The 2016 audit process begins with verification of an entity's address and contact information. An email is being sent to covered entities and business associates requesting that contact information be provided to OCR in a timely manner. OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees; this data will be used with other information to create potential audit subject pools.

Who Will Be Audited?

- Covered Entities
- Business Associates
- Individuals & Organizations
- Large & Small
- Entities "*all sizes and functions*"

How Will OCR Pick?

- Want a ***broad spectrum*** of candidates. Entities of all sizes and functions.
- OCR has an algorithm with ***sampling criteria***.
  - Size
  - Type
  - Operations
  - Affiliation/relationship with other healthcare organizations
  - Public/Private
  - Geography
- No entities that have current open complaint investigation or undergoing a compliance review by OCR.

The Selection Process

- Contact Info **Verification Letter** (*or e-mail*)
- **Pre-Screening Questionnaire** sent to gather additional data about your size, type and operations
- **Identification of Business Associates** (*spreadsheet*)
- OCR will select Entity for HIPAA Audit through **random sampling.** Selected auditees will be **notified** of their participation

DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

DATE

Contact Person's Name
CE/BA Name
Address
City, State ZIP

"Communications from OCR will be sent via email and may be incorrectly classified as spam. If your entity's spam filtering and virus protection are automatically enabled, we expect you to check your junk or spam email folder for emails from OCR"

If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr

Pre-Screening Questionnaire

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html

- Is your entity public or private?
- Single location or multi-location delivery sites
- Is your organization part of, "affiliated with" or otherwise owned or controlled by another organization?
  - If yes, describe the nature of the relationship
  - Name of the other organization(s)
- Are you a HIPAA covered entity?
- How many patient visits, beds, clinicians on staff?
- Do you maintain or transmit PHI in electronic format?
- Do you use EMRs?
- What is your total revenue?
- Other specific questions for Health Plans, Clearinghouses and Business Associates.
- Also questions about your OHCAs and Affiliated Covered Entities.

Pre-Screening Questionnaire (*con't*)

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html

Also questions about OHCAs and Affiliated Covered Entities:

- **Question 26:** Identify whether any of the covered entity(ies) for which you provide business associate functions are Organized Health Care Arrangements (OHCA) or Affiliated Covered Entities (ACE) (choose all that apply).
- **Question 27:** Identify the approximate number of each type of covered entity for which you provide business associate functions: (please indicate a number for each option selected): NOTE: If you provide business associate functions for OHCA's or ACE's, please add the component covered entities separately into the totals below. For example, if you are a business associate to an OCHA comprised of 10 covered providers, add 10 to the covered provider total option below)
- **Question 28:** Do your business associate activities involve maintaining or transmitting protected health information in electronic form?
- **Question 29:** Do you perform business associate functions in more than one state?

Business Associate Information

- **Business Associate Name**
- **Type of Service(s) provided**
- **Website URL**
- **First Point of Contact**
  - Title
  - First Name
  - Last Name
  - Contact Address
  - City
  - State
  - Zip
  - Phone
  - Phone Extension
  - Fax
  - Email
- **Second Point of Contact**
  - Title
  - First Name
  - Last Name
  - Contact Address
  - City
  - State
  - Zip
  - Phone
  - Phone Extension
  - Fax
  - Email

What If an Entity Doesn't Respond to OCR's Requests for Information?

If an entity does not respond to requests for information from OCR, including address verification, the pre-screening audit questionnaire and the document request of those selected entities, OCR will use publically available information about the entity to create its audit pool.

IF YOU DO NOT respond to OCR's initial communications, **YOUR ORGANIZATION MAY STILL BE SELECTED FOR A HIPAA AUDIT or BE SUBJECT TO A COMPLIANCE REVIEW.**

How Will the HIPAA Audits Work?

- **Desk audits** (*mostly*)
  - Round 1 = Covered Entities
  - Round 2 = Business Associates
  - Privacy Rule, Security Rule & Breach Notification (they will tell you in the letter what you are being audited for)
  - Will be finished by December 2016
- **Onsite audits** – Round 3.
  - Examine a broader scope of requirements
- Auditee will be required to submit a broad range of documentation via an "**new secure audit portal**". OCR will share results of findings.

Timelines for Audits

- After Letter is received, have **10 business days** from the date of the information request **to submit** all information via secure portal.
- After OCR receives all the information, auditors have **10 business days** to **review and return** written comments.
- OCR auditor will complete a **final audit report** within **30 days** after the auditee's response. You will get a copy of the final report.
- If you are selected for an on-site audit, it will take **3-5 days** depending on size of the entity.

What Happens After the Audit?

- Primarily a **compliance improvement** activity.
- OCR *will* ***use information*** gathered to develop compliance **tools** and technical **assistance**, and what corrective action would be most helpful.
- Should the audit reveal a "***serious compliance issue***":
  - OCR may initiate a compliance review to further
  - OCR reserves right to assess penalties.
- There will be **NO LIST** posted of which entities are selected or have been audited

OCR Protocol for HIPAA Audits

Audit Protocol: General Instructions

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

- "***Management***" means the appropriate privacy, security, and breach notification **official(s)** or **person(s)** designated by the CE or BA for the implementation of P&Ps and other standards;
- Must **provide only the specified documents**, **not** compendiums of all entity policies of procedures. The auditor will not search for relevant documentation that may be contained within such compilations
- Unless otherwise specified, all document requests are for **versions in use as of the date of the audit** notification and document request
- Unless otherwise specified, selected entities should submit documents via **OCR's secure online web** portal in **PDF, MS Word or MS Excel**
- If the requested number of documentations of implementation is not available, the entity must provide instances from equivalent previous time periods to complete the sample. If no documentation is available, the entity must provide a statement to that effect
- **Workforce members** include entity employees, on-site contractors, students, and volunteers
- **Information systems** include hardware, software, information, data, applications, communications, and people

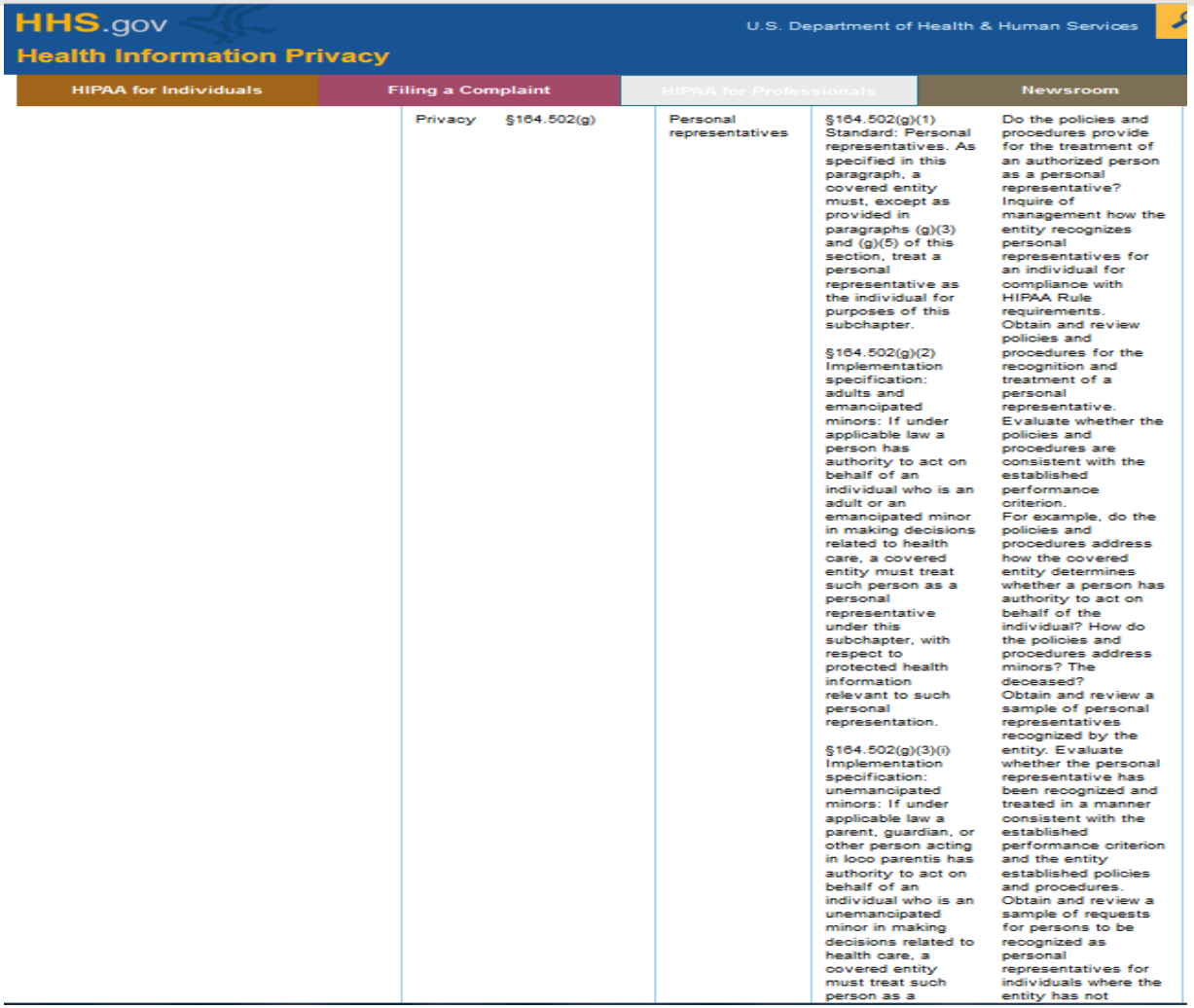
Audit Protocol: Scope

- Privacy Rule
- Security Rule
- Breach Notification Rule

Audit Protocol: Privacy Rule

- Notice of privacy practices for PHI
- Rights to request privacy protection for PHI
- Access of individuals to PHI
- Administrative requirements
- Uses and Disclosures of PHI
- Amendment of PHI
- Accounting of Disclosures

Audit Protocol: Privacy Rule



HHS.gov
U.S. Department of Health & Human Services
Health Information Privacy

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

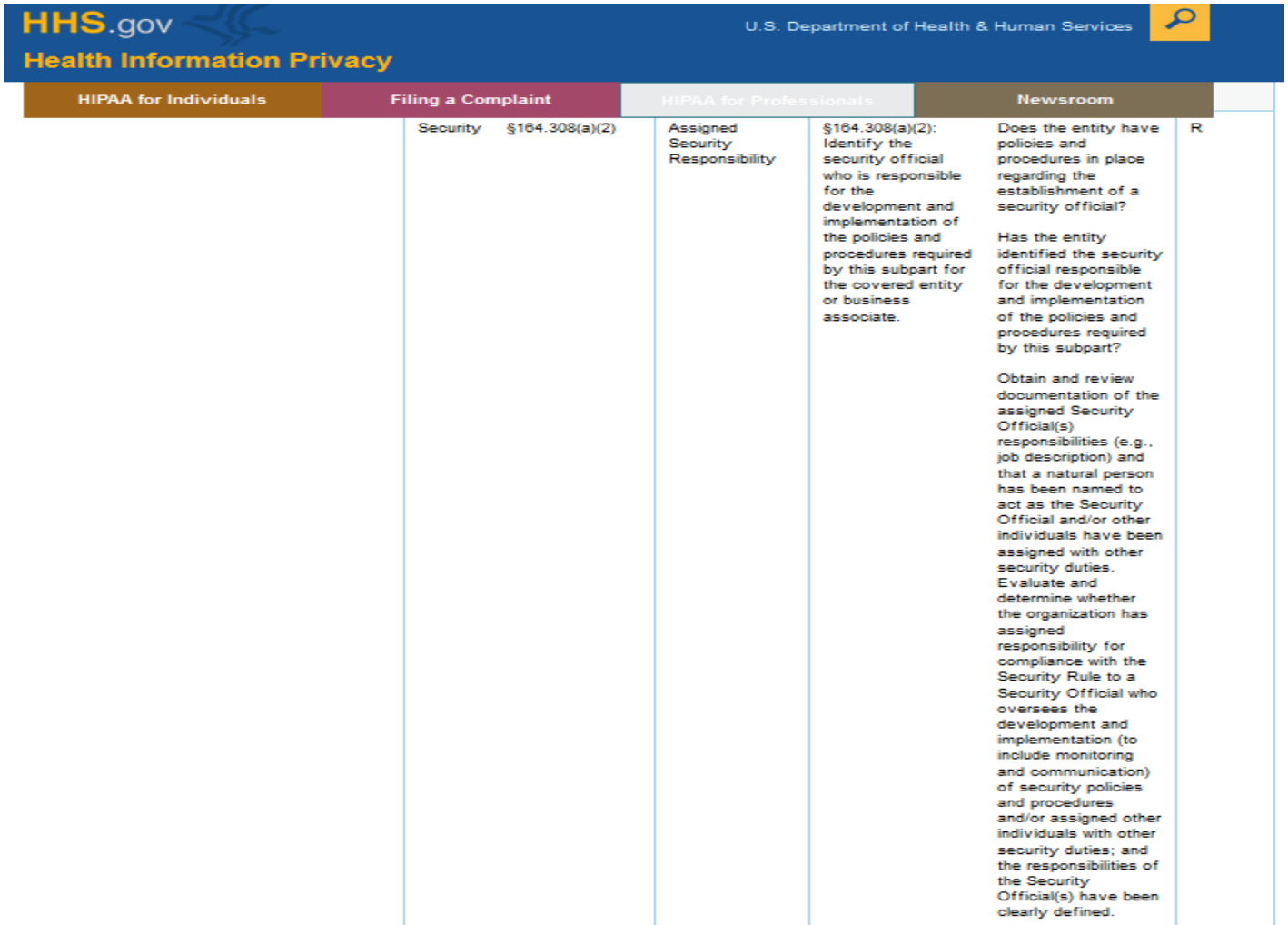
	Privacy	§164.502(g)	Personal representatives	§164.502(g)(1) Standard: Personal representatives. As specified in this paragraph, a covered entity must, except as provided in paragraphs (g)(3) and (g)(5) of this section, treat a personal representative as the individual for purposes of this subchapter. §164.502(g)(2) Implementation specification: adults and emancipated minors: If under applicable law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, a covered entity must treat such person as a personal representative under this subchapter, with respect to protected health information relevant to such personal representation. §164.502(g)(3)(i) Implementation specification: unemancipated minors: If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, a covered entity must treat such person as a	Do the policies and procedures provide for the treatment of an authorized person as a personal representative? Inquire of management how the entity recognizes personal representatives for an individual for compliance with HIPAA Rule requirements. Obtain and review policies and procedures for the recognition and treatment of a personal representative. Evaluate whether the policies and procedures are consistent with the established performance criterion. For example, do the policies and procedures address how the covered entity determines whether a person has authority to act on behalf of the individual? How do the policies and procedures address minors? The deceased? Obtain and review a sample of personal representatives recognized by the entity. Evaluate whether the personal representative has been recognized and treated in a manner consistent with the established performance criterion and the entity established policies and procedures. Obtain and review a sample of requests for persons to be recognized as personal representatives for individuals where the entity has not

Audit Protocol: Security Rule

- Administrative
- Technical
- Physical

- Completed Risk Analysis?

Audit Protocol: Security Rule



HHS.gov
Health Information Privacy

U.S. Department of Health & Human Services

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

Security	§164.308(a)(2)	Assigned Security Responsibility	§164.308(a)(2): Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Does the entity have policies and procedures in place regarding the establishment of a security official? Has the entity identified the security official responsible for the development and implementation of the policies and procedures required by this subpart? Obtain and review documentation of the assigned Security Official(s) responsibilities (e.g., job description) and that a natural person has been named to act as the Security Official and/or other individuals have been assigned with other security duties. Evaluate and determine whether the organization has assigned responsibility for compliance with the Security Rule to a Security Official who oversees the development and implementation (to include monitoring and communication) of security policies and procedures and/or assigned other individuals with other security duties; and the responsibilities of the Security Official(s) have been clearly defined.	R

Audit Protocol: Breach Notification

- Administrative Requirements
- Training
- Complaints
- Sanctions
- Refraining from Retaliatory Acts
- Waiver of Rights
- Policies and Procedures
- Documentation
- Breach Risk Assessment + Exceptions
- Notices Required (individuals, media, HHS or CE (if BA)) plus timing, content & method
- Burden of Proof

Audit Protocol: Breach Notification

HHS.gov
Health Information Privacy

U.S. Department of Health & Human Services

HIPAA for Individuals | Filing a Complaint | HIPAA for Professionals | Newsroom

				agency).	
Breach	§164.404(b)	Timeliness of Notification	§164.404(b) Timeliness of Notifications. Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	§164.404(b) Timeliness of Notifications Were individuals notified of breaches within the required time period? Inquire of management. Obtain and review the policies and procedures for notifying individuals of breaches and determine whether such policies and procedures are consistent with §164.404, including providing notification without unreasonable delay and in no case later than within 60 days of discovery of a breach. Obtain and review a list of breaches, if any, in the specified period and documentation indicating the date individuals were notified, the date the covered entity discovered the breach, and the reason, if any, for delay in notification to determine whether all individuals were notified consistent with §164.404(a), (b).

Enforcement Focus Areas

Triple S Management Corp

November 30, 2015 - $3.5M and 1 YR CAP

- Facts: Triple S, a parent company for health insurance subsidiaries, reported numerous breaches over a 5-year period. Nov 2010 breach involved **failure to terminate access credentials** of former employees who proceeded to access PHI after termination. Multiple reports of sending data through vendor **without a BAA** in place (reportable?) and one report of employee **copying CD with e-PHI and downloading** it to computer of new employer. Finally, after receiving multiple breach reports, OCR launched an investigation. Found "**widespread [HIPAA] non-compliance throughout the various subsidiaries of Triple-S**"

- OCR Findings:
  - Enterprise-wide Risk Analysis must be conducted for all entities under "control" of parent
  - Implementation of P&Ps for all areas that Triple-S fell short on

Univ of Washington Medicine

December 14, 2015 - $750,000 and 1 YR CAP

- Facts: UWM reported a breach after **employee down loaded an e-mail with attachment that contained malicious malware** which compromised IT system and affected 90,000+ patients' data. OCR investigated and found that UWM comprised of 12 affiliated entities, but noone was making sure that the affiliated entities are HIPAA compliant. Risk Analysis did not include the external affiliated entities!

- OCR Findings:
  - Risk Analysis must be conducted for **all affiliated entities**, and updated annually or as necessary "in response to environmental or operational changes that affect the security if ePHI.
  - Employees must be **trained** on **phishing** and **malware**

Feinstein Institute for Medical Research

March 17, 2016 - $3.9M Settlement & 3YR CAP

- Facts: September 14, 2012 OCR received breach notification from Feinstein Institute that **unencrypted laptop** wa[illegible] n[illegible]
- C[illegible] to
  - Failed to implement P&P on **removal of devices in and out of the facility**
  - **Failed to encrypt**, or document why encryption was not reasonable and appropriate and implement an alternative

"This case demonstrates OCR's commitment to promoting the privacy and security protections so critical to build and maintain trust . . . For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure."

- OCR Director, Jocelyn Samuels

North Memorial Health Care

March 16, 2016 - $1.5M Settlement & 2YR CAP

Facts: **September 27, 2011**, North Memorial reported to OCR that on **July 25, 2011** an unencrypted laptop containing ePHI of 6,697 individuals was stolen from Accretive Health's employee's car. **Accretive was North Memorial's Business Associate.**

OCR Findings:

- North Memorial **failed to enter into a BA Agreement** with Accretive and began providing them with ePHI as of March 21, 2011 and failed to enter into a BAA until Oct 14, 2011.

- As a result, North Memorial **impermissibly disclosed** ePHI between March 21, 2011 through October 13, 2011without obtaining satisfactory assurances form Accretive.

- Remember: HITECH did not make BAs directly subject to compliance until **September 23, 2013**

Pool & Land Physical Therapy

February 16, 2016 - $25,000 Settlement & 1 YR CAP

- Facts: August 8 2012, OCR received a complaint from patients that Pool & Land PT was **posting patient testimonials** with **facial images** on **website** without patients' authorization

- OCR Findings:
  - **Marketing purposes** requires HIPAA Authorization
  - Failed to develop and implement **P&Ps** that addresses posting PHI to **internet** and **social media** requires a signed HIPAA Authorization
  - Required removal of all PHI from its website AND ***best efforts*** to **remove all cached versions from the Internet**!!

Additional Contact Information

Full URL for the information form:

https://complyassistant.com/contact

Or you can email or call:

Gerry Blass: gerry@complyassistant.com

800-609-3414 Ext.700

Helen Oscislawski: helen@oscislaw.com

609-385-0833

References

- OCR Phase 2 Audit Protocols:
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
- Business Associate Template:
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/batemplate/index.html
- Pre-Screening Questionnaire:
  - http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/index.html
- Encryption standards:
  - http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html