HIPAA Update – OCR is Coming... Are You Ready?

Darrell W. Contreras, Esq., LHRM, CHPC, CHC, CHRC
Gregory V. Kerr, CHPC, CHC

Agenda

- Review of OCR Enforcement Activity
  - Proactive v. Reactive Reviews
- OCR Random Audits
  - Background and Overview
  - Results and Findings
  - What’s Next and Recommendations
- OCR Complaint-Driven Investigations
  - Statistics
  - How to prepare
  - Mitigation
- Q & A
OCR Random Audits:

- **Background**
  - Required by the American Recovery and Reinvestment Act of 2009 (Section 13411 of HITECH)
    - Periodic audits
    - Compliance with Privacy, Security and Breach Notification standards
  - KPMG – Awarded $9 million contract to perform the audits
    - Planned 150, completed 115
    - 20 test audits were performed beginning November 2011 and concluding March 2012

Results and Findings

- **Pilot program Summary**
  - 20 pilot audits performed and results analyzed

Analysis of Findings by Rules

Results and Findings

Privacy findings:
- Review process for denials of patient access to records;
- Failure to provide appropriate patient access to records;
- Lack of policies and procedures;
- Uses and disclosures of decedent information;
- Disclosures to personal representatives; and
- Business associate contracts.

Results and Findings

Security findings:
- User activity monitoring;
- Contingency planning;
- Authentication/integrity;
- Media reuse and destruction;
- Risk assessment; and
- Granting and modifying user access.
Results and Findings

OCR Audit protocol:

- First posted on OCR website on June 26, 2012
- Privacy Rule (79):
  1. Notice of privacy practices for PHI
  2. Rights to request privacy protection for PHI
  3. Access of individuals to PHI
  4. Administrative requirements
  5. Uses and disclosures of PHI
  6. Amendment of PHI
  7. Accounting of disclosures.
- Security Rule (81):
  1. Administrative safeguards
  2. Physical safeguards
  3. Technical safeguards
- Breach Notification Rule (10)

Source:  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
What’s Next...

1. Are more audits scheduled?
   Probably latter part of 2013/early 2014
2. Who is eligible for audit?
   Any Covered Entity and Business Associates
3. How much time do you have to respond?
   Upon notice, 10 days to provide requested information
4. Will there be penalties?
   Should be an opportunity to identify and address issues, not an
   enforcement threat unless there is willful neglect.
5. What happens after field work?
   CE given an opportunity to comment on the report after 10 days.
   After 30 days, the report is forwarded to OCR.

Preparing for the Audit

- Prepare now:
- Review policies and procedures
- Training – completed and documented
- Key issues:
  - Security Risk Assessment
  - Protocols for testing technical safeguards
  - Contingency plans
Complaint-Driven Investigations

STATISTICS
Complaints
Investigations

OCR SETTLEMENTS AND PENALTIES

HOW TO PREPARE AND RESPOND TO THE OCR

OCR Complaint Filing Triggers:
- Snooping in a medical record
- Unauthorized disclosure of health information
- PHI placed in the regular trash
- Lost or stolen laptop
- Cell phone or personal camera pictures of patient’s body parts or X-rays

- Top 5 OCR investigation issues with Corrective Action Required:
  1. Impermissible Uses & Disclosures
  2. Safeguards
  3. Access
  4. Minimum Necessary
  5. No NPP (Notice of Privacy Practices)

Source: HHS-OCR Website:
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/top5issues.html
OCR Complaint Statistics
April 2003–December 31, 2012

- Complaints received: 77,190
- Resolved: 70,259 (91%)
- No violation: 8,907 (12%)
- Corrective action required: 18,559 (24%)

The types of covered entities required to take corrective action, in order of frequency:
1. Private Practices;
2. General Hospitals;
3. Outpatient Facilities;
4. Health Plans (group health plans and health insurance issuers); and,
5. Pharmacies.

Source: DHHS/OCR [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html]

Fines, Penalties and Settlement Agreements

- Mass Eye & Ear $1.5M
  - Unencrypted laptop theft
- Alaska DHSS $1.7 M
  - Unencrypted USB stolen from employee’s vehicle
- BCBS TN $1.5 M
  - 57 hard drives stolen; 1M individuals affected
- Cignet Health $4.3M
  - 41 patients-denial of access
  - $3 M failure to cooperate
  - $1.3M denial of access
  - Findings from OCR investigation determined:
    - No P&P
    - No evidence of HIPAA training
    - No monitoring or auditing
    - No safeguards for PHI
    - No security risk analysis

Source: DHHS/OCR [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html]
How to Respond to the OCR

- Notify senior leadership, legal, & compliance
- Designate official to communicate with the OCR
- Contact the OCR Investigator to confirm receipt and establish relationship:
  - Explain that the letter has been received and you will fully cooperate
  - Confirm the deadline established for response to the OCR
    - Can be inconsistent (5 days – 30 days)
- Check for prior investigation of complaint. If no, conduct the investigation immediately.
Data Requests Can Include:

- Submit P&P pertaining to **safeguards** in place to prevent circumstances alleged
- **Any prior complaints** alleging a workforce member was involved in the type of complaint alleged. If so, provide a date of the complaint and how it was resolved
- Provide evidence of **HIPAA training** that occurred prior to the date of the complaint
- Evidence of actions taken to avoid, prevent or **mitigate** the harm from circumstance alleged

Data Requests Can Include (Cont’d)

- Detailed response to allegations including all reports and documentation
- List what evidence you have to support your response:
  - Identify witnesses by name, address and phone number
- Provide a copy of your **risk analysis** pursuant to the HIPAA Security Rule
- Provide copy of your **sanctions policy and access control policies**
Summary

- Prepare early
  - Self-audits, walk through assessments
- Appoint a HIPAA Privacy Officer
- Know your risks
- Find it and fix it!
- Educate
- Communicate
- Update