Getting Your HIPAA House In Order

Cybersecurity + Breaches
AGENDA

✓ Types of Enforcement
✓ 2016 OCR Enforcement
✓ Effective Compliance Program
✓ Cyber$ecurity Insurance
✓ 2016 Happenings ... already !!
✓ Questions
Types of Enforcement

- Complaint
- Investigation
- Criminal
- Audit
The Office for Civil Rights [OCR]

– Writes HIPAA Security, Privacy and Breach Notification Regulations
– Enforces HIPAA Security, Privacy and Breach Notification Regulations
– Keeps the penalties and fines imposed

– Legal Authority:
  • The laws: HIPAA, the HITECH Act
  • The related regulations
    – Notice of Proposed Rule Making [NPRM]
    – Final Rule [FR]
  • The regulations’ preambles
  • OCR Guidance Documents
  • OCR FAQs
QUIZ
Complaints

Complaints to the Secretary - in the original 1996 Law and related regulations:

- 45 CFR 160.306
- http://www.hhs.gov/ocr/privacy/hipaa/complaints/

Complaint Requirements - Your complaint must:

1. Be filed in writing...
2. Name the covered entity...
3. Be filed within 180 days occurrence...
Complaints to the Secretary

✧ ANYONE CAN FILE!
✧ HIPAA PROHIBITS RETALIATION
✧ HOW TO SUBMIT YOUR COMPLAINT

To submit a complaint, please use one of the following methods:

√ File your complaint electronically via the OCR Complaint Portal at
  https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf
√ File A Complaint Using Our Health Information Privacy Complaint
  Package at
  http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf
√ File A Complaint Without Using Our Health Information Privacy
  Complaint Package at
  http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html#no
  package
√ File A Security Rule Complaint at
  https://ocrportal.hhs.gov/ocr/cp/complaint_frontpage.jsf;jsessioni
d=E68436962D0B81F547503C5016113B55.ajp13w
Investigation

Investigations - from the original 1996 HIPAA Law and related regulations:

Results in:

- Resolution Agreements
- Corrective Action Plans
- Penalties and Fines
<table>
<thead>
<tr>
<th>Violations</th>
<th>Amount per Violation</th>
<th>Violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable cause</td>
<td>$1000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect - corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect – not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
HIPAA Criminal Enforcement

- **Complaint**
  - Possible Criminal Violation
  - Accepted by DOJ
  - DOJ declines case & refers back to OCR

- **Intake & Review**
  - Possible Privacy or Security Rule Violation

- **Investigation**

- **Resolution**
  - OCR finds no violation
  - OCR obtains voluntary compliance, corrective action, or other agreement
  - OCR issues formal finding of violation

- **Resolution**
  - The violation did not occur after April 14, 2003
  - Entity is not covered by the Privacy Rule
  - Complaint was not filed within 180 days and an extension was not granted
  - The incident described in the complaint does not violate the Privacy Rule
Phase 2 Audits


- The 2016 Phase 2 HIPAA Audit Program 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

Can grow into an investigation and Result in:

- Resolution Agreements
- Corrective Action Plans
- Penalties and Fines
Phase 2 Audits

- When will the next round of audit commence?
- Who will be audited?
- On what basis will auditees be selected?
- How will the selection process work?
- What if an entity does not respond to OCR’s requests for information?
- What is the general time line for an audit?
- What happens after an audit?
- How will consumers be affected?
- Will audits differ depending on the size and type of participants?
- Will auditors look at state-specific privacy + security rules in addition to HIPAA’s privacy, security, and breach notification rules?
- Who is responsible for paying the on-site auditors?
2016 OCR Enforcement

• 2nd CMP Case
• Small Providers
• All Case Examples: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html
2nd CMP Case

- Administrative Law Judge rules in favor of OCR enforcement, requiring Lincare, Inc. to pay $239,800
- A U.S. Department of Health and Human Services Administrative Law Judge (ALJ) has ruled that Lincare, Inc. (Lincare) violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and granted summary judgment to the Office for Civil Rights (OCR) on all issues, requiring Lincare to pay $239,800 in civil money penalties (CMPs) imposed by OCR.
- Lincare is a provider of respiratory care, infusion therapy, and medical equipment to in-home patients, with more than 850 branch locations in 48 states.
- OCR’s investigation of Lincare began after an individual complained that a Lincare employee left behind documents containing the protected health information (PHI) of 278 patients after moving residences.

- Read the HHS Press Release
- Read the Notice of Proposed Determination
- Read the ALJ’s Opinion
- Read the Notice of Final Determination
Small Provider Example

Private Practice Implements Safeguards for Waiting Rooms Issue

Safeguards: Impermissible Uses and Disclosures
  o Staff member discussions
  o Visible computer screens

OCR Action Plan:
  • Develop policies and procedures
  • Staff training on new P&P
  • OCR requirement new screen position
  • Privacy screens
Small Provider Fines

$750,000 HIPAA Settlement Underscores the Need for Organization Wide Risk Analysis - December 14, 2015

$800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014

$750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies - August 31, 2015
QUIZ
Effective HIPAA Compliance Program

- Breach
- HIPAA Security Risk Analysis/Assessment
- All HIPAA Documentation
- Year Long HIPAA Monitoring
- Yearly HIPAA Audit
Breach Guidance to Render Unsecured PHI unusable, unreadable, and indecipherable

Breach 4 Factors

If You Have A Breach
Guidance = Safe Harbor

Protected health information (PHI) is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

- Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption) and such confidential process or key that might enable decryption has not been breached.
- Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
- Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.
Breach 4 Factors

45 CFR 164.401(2):
1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.
If You Have A Breach

Don’t PANIC!

• Plan Ahead – breach plan
• Communicate Clearly and Calmly
• Talk and Train
• Big Fixes, Small Details
45 CFR.308(a)(1)(A) Risk Analysis: **Required**

**FREE TOOLS:**

All HIPAA Documentation

• Policies and Procedures
  – Contingency Plan
  – Training and Communicating Plan
  – Breach Plan
• Risk Analysis/Assessment Documentation
• Monitoring Plan
• Audit Plan
Cybersecurity insurance transfers some of the financial risk of a security breach to the insurer

- It is only a risk management strategy
- It is not a security breach solution
- Clear wording is essential
- It may not include coverage for privacy breaches
- It is different from liability insurance
- Diagnose your cybersecurity insurance policy
2016 Happenings ... already !!

- Healthcare Rules
- OCR Guidance
- ONC Guidance
- FDA Guidance
Healthcare Rules

- HIPAA Privacy Rules + NICS

- SAMHSA Confidentiality of Substance Abuse Disorder Patient Records
  http://www.hhs.gov/about/news/2016/02/05/hhs-proposes-changes-to-rules-governing-confidentiality-substance-use-disorder-records.html

- DOD Mental Health and Substance Use Disorder Treatment
  https://www.federalregister.gov/articles/2016/02/01/2016-01703/tricare-mental-health-and-substance-use-disorder-treatment
Individual Right of Access (to medical records)

- Blog  
  [http://www.hhs.gov/blog/2016/01/07/understanding-individuals-right-under-hipaa-access-their.html](http://www.hhs.gov/blog/2016/01/07/understanding-individuals-right-under-hipaa-access-their.html)

Real HIPAA Blog Series

- Blog post 1: The Real HIPAA Supports Interoperability
- Blog post 2: Permitted Uses and Disclosures
- Blog post 3: Care Coordination, Care Planning, and Case Management Examples
- Blog post 4: Quality Assessment/Quality Improvement and Population-Based Activities Examples
FDA Guidance

Cybersecurity Recommendations for Medical Device Manufactures

http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm
Litmos Healthcare

- Award winning Learning Management Platform
- Attentive and responsive Sales & Client Care
- Over 500 courses available
- Customizable
- Affordable

Free Trial

Sophisticate  Secure  Robust
Thank You

Please contact:

• Susan A. Miller, JD
• O = (978) 369-2092
• tmsam@aol.com