Copyright Notice

Copyright Notice. All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

For reprint permission and information, please direct your inquiry to bob.chaput@clearwatercompliance.com

Legal Disclaimer

Legal Disclaimer. This information does not constitute legal advice and is for educational purposes only. This information is based on current federal law and subject to change based on changes in federal law or subsequent interpretative guidance. Since this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource regarding the matters covered, and may not be tailored to your specific circumstance. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND ADVICE PROVIDED HEREIN IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE. The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.
Instructional Module 4:
How to Prepare for and Manage an OCR Enforcement Action

Module 4. Overview

1. “How to Prepare for and Manage an OCR Enforcement Action”
2. Instructional Module Duration = 45 minutes
3. Learning Objectives Addressed In This Module
   - Defend the position that the only real way to prepare for an OCR Investigation is to become and remain compliant with the HIPAA Privacy, Security and HITECH Breach Notification Rules
   - Describe the OCR investigation process and how to participate efficiently and effectively
   - Valuable lessons learned now that we have experienced an OCR Investigation
4. Topics
   - Case Fact Set
   - OCR Investigation Process
   - Corrective Action Plan
   - Settlement Amounts versus Civil Monetary Penalties
How to Prepare for and Manage an OCR Enforcement Action

Gregory J. Ehardt, JD, LL.M.
Ehardt Law Office
Attorney
HIPAA Compliance Officer
Assistant Professor Healthcare Law

Are You Ready?

Data Request
04/03/2013

Please provide a summary of the actions, with any supporting documentation, taken by [redacted] in response to the breach incident reported to OCR on October 22, 2012, including:

Privacy Rule:
1. A copy of [redacted] investigation and timeline of the incident.
2. A copy of [redacted] policies and procedures regarding:
   - Use and disclosure of protected health information
   - Safeguards
3. Documentation of all corrective actions taken by [redacted], including measures implemented to prevent this type of incident from reoccurring, implementation of existing job aids related to the member mailing, and the discontinuance of the annual mailing of member ID cards.

Security Rule:
1. A copy of the most recent risk analysis performed for or by [redacted].
2. A copy of the most recent risk assessment performed for or by [redacted].
3. A copy of the incident report prepared by [redacted] regarding the breach report, including any corrective actions taken by [redacted].
4. A copy of policies and procedures regarding review of system access and audit logs.
5. A copy of policies and procedures regarding review of incident reports.
6. Policy and procedures regarding implementation of periodic technical and non-technical evaluations, include a copy of the latest evaluation relating to the filtering of case numbers.
7. Policies and procedures to protect electronic protected health information from improper alienation or destruction.
8. Documentation of security measures taken to reduce risks and vulnerabilities to a reasonable and reasonable level to ensure confidentiality, integrity, and availability of PHI in accordance with OCR regulations.
ARE YOU PREPARED TODAY TO ANSWER
THE FOLLOWING QUESTIONS, IF CALLED UPON TO DO SO . . .

OCR requests the continued cooperation of ISU in facilitating our review of this incident by providing the following information pertaining to ISU:

1. Description of its organizational structure, including relationship(s) with PFM.
2. Copy of its BAAs with PFM in place on the date the incident occurred.
3. Detailed description of network system(s) containing ePHI.
4. Detailed explanation of incident, including explanation for not knowing ISU had inadequate firewall protection for approximately 10 months.
5. Copy of evidence and documentation indicating that ISU had no impermissible access to ePHI while ISU had inadequate firewall protection.
7. Copy of risk assessment determining this incident was not a "breach" as defined by the Breach Notification Rule.
8. Evidence and/or documentation indicating ISU had implemented appropriate administrative, technical and physical safeguards to protect the privacy of PHI to the date the incident occurred. See 45 C.F.R. 164.530(c).
9. Copy of Risk Analysis performed prior to the date the incident occurred. See 45 C.F.R. 164.308(a)(1)(ii)(A).
11. Copy of procedures implemented, prior to the date the incident occurred, to regularly review records of Information System Activity. See 45 C.F.R. 164.308(a)(1)(ii)(D).
12. Copy of technical policies and procedures implemented prior to the date the incident occurred for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. See 45 C.F.R. 164.312(a).
13. Evidence that ISU implemented hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI prior to the date the incident occurred. See 45 C.F.R. 164.312(b).

ALL WITHIN 20 DAYS!

Learning Objectives . . .

• Why prepare for an OCR Audit / Investigation

• Describe the OCR investigation process and how to participate efficiently and effectively

• Valuable lessons learned now that we have experienced an OCR investigation
"Hopefully in coming months you'll see actual activity that will start up on the audit process," Susan McAndrew, OCR deputy director for health information privacy, said Feb. 24 at the 2014 HIMSS Conference.

Complaints

% Investigated

% of CAPs/Investigation

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html

OCR’s New Motivation?

- Although OCR made available to covered entities guidance that promoted compliance with the Security Rule, it had not assessed the risks, established priorities, or implemented controls for its HITECH requirement to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements. As a result, OCR had limited assurance that covered entities complied with the Security Rule and missed opportunities to encourage those entities to strengthen their security over ePHI.

- Because OCR did not perform the compliance audits mandated by HITECH, it had limited information about the status of Security Rule compliance at covered entities. Therefore, it had limited assurance that ePHI was secure and might have missed opportunities to motivate covered entities to strengthen ePHI security.

Final Omnibus Rule: New Civil Monetary Penalty System

<table>
<thead>
<tr>
<th>VIOLATION TYPE</th>
<th>MIN. PENALTY</th>
<th>MAX. PENALTY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 violation; annual max of $25,000 repeat violations</td>
<td>$50,000 violation; annual max of $1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$100 violation; annual max of $25,000 repeat violations</td>
<td>$50,000 violation; annual max of $1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>$10,000 violation; annual max of $250,000 repeat violations</td>
<td>$50,000 violation; annual max of $1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Not Corrected</td>
<td>$50,000 violation; annual max of $1,500,000</td>
<td>$100 violation; annual max of $1,500,000</td>
</tr>
</tbody>
</table>

The new penalty structure is as follows:

<table>
<thead>
<tr>
<th>VIOLATION TYPE</th>
<th>EACH VIOLATION</th>
<th>REPEAT VIOLATIONS/YR</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>$1,000 – $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>
</tbody>
</table>
| Willful Neglect - Not Corrected | $50,000 | $1,500,000
Learning Objectives 

• Why prepare for an OCR Audit / Investigation

• Describe the OCR investigation process and how to participate efficiently and effectively

• Valuable lessons learned now that we have experienced an OCR investigation

Case Study Pre-read

1. Read the following
   A. OCR Notice Letter
   B. April 5, 2013 Idaho State University Resolution Agreement & Corrective Action Plan
   C. Idaho State University Settles HIPAA Security Case for $400,000

2. Answer Questions on Following Page
Homework Questions

For each case (Settlement Agreements / Corrective Action Plans)

1. What triggered the OCR Investigation?
2. What was the root cause of the issue?
3. Was there a “Breach”?
4. What common requirements appeared in the Corrective Action Plans?
5. What were the unique CAP requirements to ISU and HONI?
6. What, if anything, was surprising about the case?

WHAT HAPPENED AT ISU?

• August 2010 – System Administrator disabled firewall on server at a clinic on the campus of Idaho State University for routine maintenance
• May 2011 – ISU IT discovered that the firewall had not been reactivated
  - No centralized event logging or vulnerability scanning system was in place
• Individually identifiable health information of approximately 17,500 individuals was vulnerable
• Following two months, ISU IT performed due diligence to determine if patient data had been compromised
  - Hired third party to perform additional forensic audit
• August 2011 – Both external auditor and ISU ITS determined that “no patient records were accessed and the data was not compromised”
• August 2011 – ISU self reports to OCR
ISU Self Reports (August 2011)

OCR sends “Demand Letters” (November 2011)

Idaho State University’s experience with the OCR . . .

Settlement and CAP executed (April 2013)

OCR performs onsite interviews (September 2012)

ISU Settles . . .

Should Idaho State University have reported this “INCIDENT” to the OCR?

Both the “internal investigation” by ISU ITS and the “external investigation” revealed that although the firewall was disabled and patient information was “vulnerable,” ePHI was not accessed by non-clinic personnel.

OCR News Release

“Idaho State University (ISU) has agreed to pay $400,000 to the U.S. Department of Health & Human Services (HHS) to settle alleged violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The settlement involves the breach of unsecured electronic protected health information (ePHI) of approximately 17,500 patients at ISU’s Pocatello Family Medicine Clinic.”
### How Would You Analyze ISU’s Fact Pattern?

#### Pre-Omnibus Rule
- **164.402** Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E of this part which compromises the security or privacy of the PHI.
- **1(i)** For purposes of this definition, compromises the security or privacy of the PHI means **poses a significant risk** of financial, reputational, or other harm to the individual.

#### Post-Omnibus Rule
- Presumption is “BREACH” unless demonstrate low probability PHI has been compromised based on following ...
  - What was the nature and extent of PHI;
  - Who is the unauthorized person who used the PHI or to whom the disclosure was made;
  - Whether the PHI was actually acquired or viewed;
  - The extent to which the risk to the PHI has been mitigated.

---

### NEW MATH UNDER MODIFIED PENALTY SYSTEM

**If ISU Reported Today:** Firewall disabled for 10 months leaving 17,500 patients’ healthcare data exposed. OCR determined that PHI was disclosed / confidentiality and availability were compromised.

**OCR May Say:** OCR investigation found violations:
- **Impermissible disclosure of PHI** (45 CFR §164.502(a))
- **Failed to implement safeguards** (45 CFR §164.530(c))
- **Did not appoint a security official** (45 CFR §164.308(a)(2))
- **Did not complete GAP Analysis (Risk Assessment)** (45 CFR §164.308(a)(8))
- **Did not ever complete a risk analysis** (45 CFR §164.308(a)(1)(i)(A))
- **Did not undertake risk management by implementing reasonable and appropriate controls** (45 CFR §164.308(a)(1)(ii)(A))
- **Did not conduct security awareness and training** (45 CFR §164.308(a)(5))
- **Failed to implement security incident response and reporting policies and procedures** (45 CFR §164.308(a)(6))
- **Did not have Information System Activity Review procedures** (45 CFR §164.312(b))

The violations were not addressed within 30 days of discovery...

And, organization was found to be in “willful neglect”...

© Clearwater Compliance LLC | All Rights Reserved

© Clearwater Compliance LLC | All Rights Reserved | 10
Civil Monetary Penalty calculation might be:

- Nine violations listed on previous slide
- 17,500 records x $50,000 per violation = $87,500,000 per violation, capped at $1,500,000 for identical violations during a calendar year ➔ $1,500,000 per violation
- 9 violations x $1,500,000 = $13,500,000

But wait, there’s more!!
- Impermissible Disclosure – 1 time $1.5M
- Every other violation:
  - 2006, 2007, 2008 ➔ 3 x 8 x $25K = $0.6M
  - 2009, 2010, 2011, 2012 ➔ 4 x 8 x $1.5 = $48.0M
  - Total = $50.1M

BE WARNED . . .

- The investigation will consume resources, money and personnel
- Early appropriate administrative backing must be a priority
- If done correctly, this can be a positive opportunity to put money into effective solutions
BE WARNED . . .

• The investigation will consume resources, money and personnel.
• Early administrative backing must be a priority.
• If done correctly, this can be a positive opportunity to put money into effective solutions.

THE "WINDOW" OF OPPORTUNITY WILL CLOSE!

Surround Yourself With Greatness

Hire QUALITY, EXPERIENCED COMMUNICATORS

Ask yourself . . .

• Have my team members been through an OCR investigation before?
• Will their experience be of benefit?

TEAM MEMBERS

• Internal Legal Team
• Outside Legal Counsel (Does their temperament match yours?)
• CIO (depending upon the nature of the incident)
• IT Security Firm (depending upon the nature of the incident)
• HIPAA Officer
Prepare Your Witnesses . . .
After All This is Similar to a Trial

Do not assume OCR is your “friend” even if agents are “friendly”

• Shocked how freely some felt to do a “mea culpa”
• Answers to questions should be direct and not EXPANSIVE
• Volunteering information not requested may open unwanted issues

Interviews (Live and Phone)

• Schedule “prep” time
• Schedule interviews for midweek rather than on Monday
• Legal Counsel and HIPAA Officer should attend
• Take Notes on all questions posed by OCR and share with subsequent interviewees

TWO-WAY COMMUNICATION IS THE GOLDEN RULE

• Remember, OCR is the LAW
• Show desire to learn and improve
• Show proper respect

This is where you seriously “reduce” your fines, penalties, settlement!
Learning Objectives . . .

• Why prepare for an OCR Audit / Investigation

• Describe the OCR investigation process and how to participate efficiently and effectively

• Valuable lessons learned now that we have experienced an OCR investigation

Commit to Compliance

Change the Paradigm!

• Attitude adjustments are often necessary
• Embrace the realities of compliance
• In my experience, they give partial credit for effort
• Give your attorney something to work with

“Be Proactive” . . . HOWEVER, if you choose not to be proactive, at least “React Quickly”
OCR requests the continued cooperation of ISU in facilitating our review of this incident by providing the following information pertaining to ISU:

1. Description of its organizational structure, including relationship(s) with PFM.
2. Copy of Business Associates and corresponding BAAs and due diligence, if any.
3. Detailed description of network system(s) containing ePHI (i.e., Application Criticality Analysis).
4. Detailed explanation of incident, including explanation for not knowing ISU had inadequate firewall protection for approximately 10 months.
5. Copy of evidence and documentation gathered by ISU indicating there was no impermissible access to ePHI while ISU had inadequate firewall protection.
6. Copy of policies and procedures that mirror privacy, security and breach notification rules.
7. Copy of risk assessment determining this incident was not a “breach” as defined by the Breach Notification Rule.

8. Evidence and/or documentation indicating ISU had implemented appropriate administrative, technical and physical safeguards to protect the privacy of PHI to the date the incident occurred. See 45 C.F.R. 164.530(c).
9. Copy of Risk Analysis performed prior to the date the incident occurred. See 45 C.F.R. 164.308(a)(1)(ii)(A).
11. Copy of procedures implemented, prior to the date the incident occurred, to regularly review records of Information System Activity. See 45 C.F.R. 164.308(a)(1)(ii)(D).
12. Copy of technical policies and procedures implemented for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights. See 45 C.F.R. 164.312(a).
13. Evidence that ISU implemented hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI prior to the date the incident occurred. See 45 C.F.R. 164.312(b).
11 Simple Practices Learned From Extensive Experience with the OCR

Practice 1: Know the Location of Your PHI
Practice 2: Use Strong Passwords and Change Them Regularly
Practice 3: Install and Maintain Anti-Virus Software
Practice 4: Use a Firewall
Practice 5: Control Access to PHI
Practice 6: Control Physical Access
Practice 7: Limit Network Access
Practice 8: Plan for the Unexpected
Practice 9: Maintain Good Computer Habits
Practice 10: Protect Mobile Devices
Practice 11: Establish a Culture of Compliance

Practice 1: Know the Location of Your PHI

- Document, Document, Document
  - OCR Interview Question . . . “Explain the tracking mechanism of PHI within your facility.”
- The location of PHI / ePHI is the foundation for all subsequent (mandatory) reports . . .
  - Risk Analysis, Security Assessment, Information System Activity Review, Policies and Procedures (BYOD), Back Up / Storage, Disaster Recovery Plan, etc . . .
- Prevent “overreaction” and “underreaction”
- Utilize Role-Based Access forms
Practice 2: Use Strong Passwords and Change Them Regularly

- Unique username and password
  - 8 characters in length (upper and lower case letters, one number and one symbol)
- Passwords are not shared with others
- Passwords are not written down or displayed
- Passwords are hard to guess but easy to remember
- Passwords are changed routinely

Practice 3: Install and Maintain Anti-Virus Software

- Installed and working properly
- Educate staff on how to recognize signs of malware or viruses and how to avoid them
- Allow for automatic updates

Practice 4: Use a Firewall

- Installed and configured properly
Practice 5: Control Access to PHI

- Use role-based access permissions/forms in your EHR so the role of each person determines their access to PHI
- User account should be tied to current and proper users
- Delete all users that are no longer employed or who no longer have permissions
- All computers using healthcare related systems are not available for other non-healthcare related functions
- Where possible, restrict files to authorized users only

Practice 6: Control Physical Access

- All devices containing PHI are inventoried and accounted for
- Physical access to secure areas is limited and monitored
- Devices located in high-traffic areas are properly secured
Practice 7: Limit Network Access

- Access to the network is restricted to authorized users and authorized devices
- Disable rogue access points that result from wireless routers
- Guest devices are prohibited from accessing
- Encrypt wireless networks
- Public instant messaging is disabled and private should be carefully scrutinized
- Prohibit staff from installing software without prior approval

Practice 8: Plan for the Unexpected

- Have a backup recovery plan
- Create an Application Criticality Analysis
- Backup in a timely manner and test the backups to make sure they work
- Backup media are physically secured (including offsite storage, if applicable)
- Before disposal, render backup media unreadable
- Consider multiple backups in the event of failure
Practice 9: Maintain Good Computer Habits

- Computers are free of unnecessary software
- Remote file sharing and printing (remote printing) are disabled
- Vendor remote maintenance connections are well documented and secured
- Systems and applications are updated regularly in accordance with the manufacturer's guidelines

Practice 10: Protect Mobile Devices

- Mobile devices are configured to prevent the unauthorized use
- PHI on mobile devices is encrypted
- Connections between authorized mobile devices and EHR's are encrypted
Practice 11: Establish a Culture of Compliance

- Regularly Train Workforce
- Provide regular HIPAA compliance reminders through email, meetings, website alerts, etc.
- Encourage “over” reporting until they learn
- Encourage workforce to provide needed input on ways to bring about culture of compliance
- Reward workforce for good ideas and good behavior

In Summary...

Requires Cross Functional Collaboration and Executive Support
Supplemental Materials

4-1. OCR “Lessons Learned from OCR Privacy and Security Audits_03-07-2013” presentation by Linda Sanches and Verne Rinker (PDF)
4-2. OCR 2012 “Documentation Request List OCR-audit-notification” (PDF)
4-3. OCR 2012 “Redacted OCR Audit-notification2” (PDF)
4-4. OCR 2012 “Sample NFR from OCR Audit” (PDF)
4-5. OCR 2013 “Redacted OCR Investigation Letter”
4-6. OIG on OCR and HIPAA Security Rule Enforcement (PDF)
4-7. OCR Audit Protocol web site

© Clearwater Compliance LLC | All Rights Reserved

Questions?

© Clearwater Compliance LLC | All Rights Reserved
Gregory J. Ehardt, JD, LL.M.

208-360-3997
greg@ehardtlaw.com

THANK YOU!