COUNTERING CYBER CHAOS WITH HIPAA COMPLIANCE

Presented by
Paul R. Hales, J.D.
May 8, 2017
HIPAA Rules – Combat Cyber Crime

A Blueprint to Combat Cyber Crime
HIPAA Rules – Combat Cyber Crime

HIPAA Rules – Easy to Follow
Step-by-Step
When You Know the Steps
HIPAA Rules – Combat Cyber Crime

Paul R. Hales
Attorney at Law
HIPAA Privacy and Security

The HIPAA E-Tool®

Legal Education –

Not Legal Advice

Paul.Hales@AttorneyHales.com  Direct Tel: 314-534-3534
Are there still Cyber Crime Deniers?
(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain

(U) Cyber actors will likely increase cyber intrusions against health care systems—to include medical devices—due to mandatory transition from paper to electronic health records (EHR), lax cybersecurity standards, and a higher financial payout for medical records in the black market.
HIPAA Rules – Combat Cyber Crime

Anthem Hacking Points to Security Vulnerability of Health Care Industry
FEB. 5, 2015
By REED ABELSON and MATTHEW GOLDSTEIN

2015
HIPAA Rules – Combat Cyber Crime

2016

How to Protect Your Networks from
RANSOMWARE
In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cybersecurity professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations within their sector or community, but not via publicly accessible channels.

**Vulnerabilities and Post Exploitation IOCs for an Advanced Persistent Threat**

**Summary**
Advanced Persistent Threat (APT) cyber actors continue to target sensitive information stored on US commercial and government networks through cyber espionage. The CVEs and post-exploitation tools in this document were utilized in compromises in the last year. In addition to utilizing the exploits identified in this document, the adversary also uses spear-phishing e-mails as a vector to compromise networks. The FBI is making these CVEs, MD5s, and YARA rules available for network defense.
### HIPAA Rules – Combat Cyber Crime

#### Technical Details

The CVEs below were used by APT actors\(^1\) to compromise networks in the last year. The compromises were to build infrastructure and for exploitation. The FBI recommends patching internet-connected servers for vulnerabilities in the following products:

<table>
<thead>
<tr>
<th>Software:</th>
<th>CVE(s):</th>
<th>Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe ColdFusion</td>
<td>CVE-2013-0625; CVE-2013-0632</td>
<td>Affects versions 10 and earlier. The vulnerability allows for the circumvention of authentication controls, allowing the attacker to take control of the server.</td>
</tr>
<tr>
<td>Adobe ColdFusion</td>
<td>CVE-2013-0629</td>
<td>Affects version 10 and earlier. The vulnerability permits an unauthorized user to access restricted directories.</td>
</tr>
<tr>
<td>Apache Tomcat/JBoss</td>
<td>CVE-2010-0738</td>
<td>JBoss EAP JMX authentication bypass with crafted HTTP request.</td>
</tr>
</tbody>
</table>

\(^1\): APT stands for Advanced Persistent Threat.
HIPAA Rules – Combat Cyber Crime

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server. To receive your private key follow one of the links:

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: g46mbrrzpfszonuk.onion/9A9DAA8C483E9B5C
4. Follow the instructions on the site.

!!! Your personal identification ID: ______________________ !!!
HIPAA Rules – Combat Cyber Crime

Your Workforce
Your Strongest Defense
against Cyber Crime
– and your Weakest Link

Insider Threats
Cyber Criminal – Workforce Member?
Insider misuse is a major issue for the Healthcare industry; in fact it is the only industry where employees are the predominant threat actors in breaches.

Verizon Data Breach Report
April 28, 2017
HIPAA Rules – Combat Cyber Crime

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server. To receive your private key follow one of the links:

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: g46mbrrzpszonuk.onion/9A9DAA8C483E9B5C
4. Follow the instructions on the site.

!!! Your personal identification ID: ___________________________ !!!
Think Before You Click!

HIPAA Rules – Combat Cyber Crime

Workforce Training  Personal Stake
HIPAA Rules – Combat Cyber Crime
Agenda

Strategies to Combat Cyber Crime

1. Who are the Cyber Criminals & How Do We Defend against Them?
2. HIPAA – A Blueprint to Combat Cyber Crime
3. Prevent Cyber Crime
4. Respond to Cyber Crime
5. Recover from Cyber Crime

HIPAA Rules – Combat Cyber Crime
1. Who are the Cyber Criminals?

**4 Categories**

1. **Amateurs** – Unskilled Hackers
   - “Script Kiddies” – RaaS

2. **Professional Social Engineers**
   - With Sophisticated Malware

3. **Professional Hackers** including Nation States

4. **Insiders**
1. How Do We Defend Against Them?

Amateurs and Professional Social Engineers

Contingency Plan Policy and Procedures

Workforce Training

Information System Safeguards

• Protective Software

• Update and Patch All Software
1. How Do We Defend Against Them?

Professional Hackers

Contingency Plan Policy and Procedures

Trained Expert Workforce or IT Services

Information System Safeguards

- Managed Protective Software
- Information System Monitoring, Updating, Data Backup
1. How Do We Defend Against Them?

Insiders

Contingency Plan Policy and Procedures

Workforce Training – Alert to Unusual, Improper or Inappropriate Behavior

Trained Expert Workforce or IT Services

Information System Safeguards

• Employee Monitoring Procedures
2. HIPAA Blueprint - Combat Cyber Crime

Your Money or Your PHI: New Guidance on Ransomware

July 11, 2016

By: Jocelyn Samuels, Director, Office for Civil Rights

Summary:

To help health care entities better understand and respond to the threat of ransomware, the HHS Office for Civil Rights has released new HIPAA guidance.

FACT SHEET: Ransomware and HIPAA

www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Ransomware is a type of malware (malicious software) distinct from other malware, its defining characteristic is that it attempts to deny access to a user’s data. Malicious software means software, for example, a virus, designed to damage or disrupt a system.

HIPAA § 164.304
A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).

This document describes ransomware attack prevention and recovery from a healthcare sector perspective,

• including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and
FACT SHEET: Ransomware and HIPAA

Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?
Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware.

Can HIPAA compliance help covered entities and business associates recover from infections of malware, including ransomware?
Yes. The HIPAA Security Rule requires covered entities and business associates to implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack.
What should covered entities or business associates do if their computer systems are infected with ransomware?

The presence of ransomware (or any malware) on a covered entity’s or business associate’s computer systems is a security incident under the HIPAA Security Rule.

HIPAA covered entities and business associates are required to develop and implement security incident procedures and response and reporting processes that they believe are reasonable and appropriate to respond to malware and other security incidents, including ransomware attacks.
2. HIPAA Blueprint - Combat Cyber Crime

<table>
<thead>
<tr>
<th>Security Rule</th>
<th>SR-1</th>
<th>Security Management Process</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SR-2</td>
<td>Risk Management</td>
</tr>
<tr>
<td></td>
<td>SR-3</td>
<td>Security Rule Sanction Policy</td>
</tr>
<tr>
<td></td>
<td>SR-4</td>
<td>Information System Activity Review</td>
</tr>
<tr>
<td></td>
<td>SR-5</td>
<td>Workforce Security</td>
</tr>
<tr>
<td></td>
<td>SR-6</td>
<td>Authorization and/or Supervision</td>
</tr>
<tr>
<td></td>
<td>SR-7</td>
<td>Workforce Clearance Procedure</td>
</tr>
<tr>
<td></td>
<td>SR-8</td>
<td>Termination Procedures</td>
</tr>
<tr>
<td></td>
<td>SR-9</td>
<td>Information Access Management</td>
</tr>
<tr>
<td></td>
<td>SR-10</td>
<td>Isolating Health Care Clearinghouse Function</td>
</tr>
<tr>
<td></td>
<td>SR-11</td>
<td>Access Authorization</td>
</tr>
<tr>
<td></td>
<td>SR-12</td>
<td>Access Establishment and Modification</td>
</tr>
<tr>
<td></td>
<td>SR-13</td>
<td>Workforce Security Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>SR-13.A</td>
<td>Workforce Security Awareness and Training Supplemental Materials and Worksheet</td>
</tr>
<tr>
<td></td>
<td>SR-13.T-1</td>
<td>Recognize and Avoid Phishing Attacks - Workforce Training</td>
</tr>
<tr>
<td></td>
<td>SR-14</td>
<td>Security Reminders</td>
</tr>
<tr>
<td></td>
<td>SR-15</td>
<td>Prevention from Malicious Software</td>
</tr>
</tbody>
</table>

AAPC HIPAA Compliant Organization

Change Location

Update Organization Information

Logout
2. HIPAA Blueprint - Combat Cyber Crime

Security Rule

Section 5 - Introduction to the HIPAA Security Rule

Part A - Administrative Safeguards

Part B - Physical Safeguards

SR-27 Facility Access Controls
SR-28 Workstation Use
SR-29 Workstation Security
SR-29.A Bring Your Own Device (BYOD) Policy
SR-30 Device and Media Controls

Part C - Technical Safeguards

Part D - Organizational Requirements
2. HIPAA Blueprint - Combat Cyber Crime
2. HIPAA Blueprint - Combat Cyber Crime

FACT SHEET: Ransomware and HIPAA
Guidance – Blueprint to Combat Cyber Crime

1. Policies and Procedures
2. Workforce Training
3. Information System Safeguards
3. Prevent Cyber Crime

1. Policies and Procedures
   • Security Management Process
     *Risk Analysis – Risk Management*
   • Information Access Management
   • Protection from Malicious Software
   • Password Management
   • Workstation Security (BYOD)
   • Workforce Training
3. Prevent Cyber Crime

Risk Analysis – Risk Management = A 3 Act Play

Act 1 – Setup

Risk Analysis

1. Assemble Information
   • PHI Locations
   • Workforce - Business Associates
   • Threats and Vulnerabilities

2. Identify Risks
3. Prevent Cyber Crime

Act 2 – Confrontation

Risk Management Action

Act 3 – Resolution

Risk Management Plan

Active – Documented – In Place
3. Prevent Cyber Crime

Risk Analysis - Risk Management
Introduction - HIPAA Risk Analysis - Risk Management
RA-1 HIPAA Risk Analysis - Risk Management Policy and Procedures
RA-1 Risk Management Step-by-Step Instructions

Risk Analysis Part 1: Assess Risks - EPHI and Non-EPHI Locations, Workforce, Business Associates
RA-1.A Locations and Potential Risks to EPHI and Non-EPHI
RA-1.B Workforce Roster - PHI Access - Training
RA-1.C Business Associate Roster - Due Diligence and BAA


Risk Analysis Part 3 Identify Threats and Vulnerabilities
RA-3.A Threats to EPHI/Non-EPHI - Related Vulnerabilities

Risk Analysis Part 4 Assess Risk Level of Each Threat/Vulnerability Pair
RA-4.A Risk Assessment - Each Threat/Vulnerability Pair

Risk Management - Assign Responsibility
RA-5.A Risk Management Action - Locations of EPHI and Non-EPHI
Risks Identified in RA-1.A, Locations and Potential Risks to EPHI and Non-EPHI
RA-5.C Risk Management Action - Risks Caused by Threat/Vulnerability Pairs
Threat/Vulnerability Pair Risks Identified in RA-3.A and RA-4.A

Risk Management Documentation
RA-6.A Risk Management - Locations of EPHI and Non-EPHI
RA-6.B Risk Management - Workforce Training
RA-6.C Risk Management - Business Associate Due Diligence, BAA
RA-6.D Risk Management - Security Rule Checklist Completion
RA-6.F Supplemental Risk Analysis - Risk Management Documentation
3. Prevent Cyber Crime

RA-4.A Evaluate and Assign Risk Level to Each Threat-Vulnerability Pair

**About Form RA-4.A**
On Form RA-4.A you will assign a Risk Level ranging from Very Low (1) to Very High (5) caused by each Threat-Vulnerability Pair identified on Form RA-3.A. Each pair is listed on a separate row followed by 5 labeled buttons. Click the button in each row that best describes the Risk Level caused by the Threat-Vulnerability Pair.

Choose a Risk Level by using your best judgement to answer two questions:
1. What is the Likelihood this Threat will actually occur and exploit this Vulnerability?
2. If the Threat occurs, how severe will the resulting impact be to the Privacy and Security of your organization’s EPHI and Non-EPHI and on the normal day-to-day operations of your Organization? In other words - “How bad could it be?”

You do not have to assign a Risk Level to each Threat-Vulnerability Pair in one session. To end a session, click the Save Button at the bottom of the form. If you leave this form during a session without clicking “Save” the Risk Levels you have assigned during the session will not be saved. You will have to re-enter them. All Risk Levels entered and saved on this form in any earlier session will still be saved.

Risk Levels set for each Threat-Vulnerability Pair will be placed automatically on the list for Risk Management action (Form RA-5.C) and on the list to document management of the Risk (RA-6.E).

<table>
<thead>
<tr>
<th>Threat</th>
<th>Vulnerability</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss - Unencrypted Laptop</td>
<td>Unsecured PHI - No BYOD Policy</td>
<td>5</td>
</tr>
<tr>
<td>Ransomware</td>
<td>Workforce Not Trained to Avoid Phishing</td>
<td>5</td>
</tr>
</tbody>
</table>
2. Workforce Training

Combat Phishers

Amateurs

Professional Social Engineers

1. Phishing Emails – Anthem 78.8 M
2. Spear Phishing Emails
3. Malvertising
3. Prevent Cyber Crime

Phishing

Dear Customer,

Your Netflix account is temporarily suspended. We need your help resolving an issue with your account.

What's going on?
We are having trouble validating your credit card on file, hence cannot authenticate your Netflix account.

What to do next
Sign in below to enter your payment information again or use a different payment method. When done we will try to verify your account again to fully restore it.

<http://www.ccearabajal.com/web/components/tflix/index.php> If you have any question, we are happy to help.

Simply call us anytime at 1-888-579-7172.

Netflix
3. Prevent Cyber Crime

**Spear Phishing**

**From:** HR2017@

**Sent:** Monday, January 2, 2017 7:29 AM

**To:**

**Subject:** Benefit Plan Update

**Importance:** High!

**Dear [Name],**

We are excited to announce an important change in our benefit plan that will provide increased coverage effective immediately. Details can be found [here](#).

To protect your privacy you will be required to log in with your username and password.
Malvertising

3. Prevent Cyber Crime
3. Prevent Cyber Crime

Malvertising
# 3. Prevent Cyber Crime

## HIPAA Compliance Program of AAPC HIPAA Compliant Organization

<table>
<thead>
<tr>
<th>Document Number:</th>
<th>SR-13.T-1</th>
<th>Page 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Name:</td>
<td>Workforce Training – Recognize and Avoid Phishing Attacks</td>
<td></td>
</tr>
</tbody>
</table>

### Guidance Note
- This Page for Instructor’s Use Only – Lesson and Lesson Plan On Next Page

## Purposes of Training

1. Protect Security of Electronic Information System and Confidentiality, Integrity and Availability of EPHI by training Workforce to recognize and avoid Phishing Attacks on Electronic Devices that send /receive Email and have access to the Internet like Workstations, Laptops, Smartphones
2. Protect Information System from Malicious Software - Ransomware
3. Prevent Breaches of Unsecured PHI and Medical Identity Theft

## Workforce Members to be Trained

All Workforce Members who use Email, Electronic messaging systems or have access to the Internet to perform their duties at AAPC HIPAA Compliant Organization - on Electronic Devices owned by the Organization and, if permitted, Electronic Devices owned by the Workforce Member

## Category

Workforce Security Awareness and Training

## Specific Topic

Recognize, Avoid and Report Phishing Attacks

### Why is this Workforce Training Important?

1. Phishing is dangerous. Criminals trick Workforce Members into allowing Malicious Software to infect Electronic Information Systems or into revealing their passwords and usernames that they then use to get Access to the Electronic Information System of AAPC HIPAA Compliant Organization and The Workforce Member’s own personal accounts to steal information.

### Guidance Note
- People pay attention when they have a stake in the training.
3. Prevent Cyber Crime

Think Before You Click!

Workforce Training

Personal Stake
3. Prevent Cyber Crime

3. Information System Safeguards
   Risk Analysis – Risk Management
   • Include Ransomware Threat & Vulnerabilities
   • Identify Risk Levels – Ransomware T/V Pairs
   • Manage Risks
     ➢ Update Software – Operating & Applications
     ➢ Install and Update Protective Software
   • “Evaluation” - Periodic Technical & Non-Technical
3. Prevent Cyber Crime

3. Information System Safeguards

Protective Software
3. Prevent Cyber Crime

3. Information System Safeguards

Protective Software
3. Prevent Cyber Crime

3. Information System Safeguards

Managed Protective Software
3. Prevent Cyber Crime

3. Information System Safeguards

Professional Hackers

Managed Protective Software

Expert IT Services

• Monitor System, Protective Software, All Software Updates & Patches, Data Backup

Insiders

Expert IT Services

• Employee Monitoring Software
4. Respond to Cyber Crime

1. Policies and Procedures
   - Contingency Plan
   - IT Response Team Ready and Trained
   - Management Team Ready and Trained
   - Legal Counsel Ready and Prepared
   - PR Team Identified - Ready if Needed
   - Cyber Insurance
4. Respond to Cyber Crime
4. Respond to Cyber Crime
4. Respond to Cyber Crime

1. Policy and Procedures
   • Contingency Plan - All Elements including:
     ➢ Pay Ransom?
     ➢ When to contact Law Enforcement?
   • Breach Risk Assessment Tool
   • Security Incident Response and Reporting
   • Breach Notification Policy and Procedures
   • Sanctions
4. Respond to Cyber Crime

2. Workforce Training
   – Becomes Workforce Implementation

Workforce Members implement Contingency Plan
4. Respond to Cyber Crime

3. Information System Safeguards
   Expert IT Services
   • Contain and Mitigate Ransomware Attack
   • Forensic Analysis and Documentation
   • Maintain Operations with Data Backup
   • Implement Disaster Recovery Plan
   • Sanitize Affected Information System Components
5. Recover from Cyber Crime

1. Policy and Procedures
   • Implement Contingency Plan – Disaster Recovery Procedures
   • Sanctions
   • Risk Analysis - Risk Management Revise Policies and Procedures – Contingency Plan – Incorporate Lessons Learned
   • Revise Workforce Training - Incorporate Lessons Learned
5. Recover from Cyber Crime

2. Workforce Training
   • Explain What Happened and Why
   • Emphasize - Importance of Constant Vigilance
   • Provide Training - All Revised Policies and Procedures
   • Practice and Test New Procedures
   • Practice and Test Contingency Plan
5. Recover from Cyber Crime

3. Information System Safeguards
   • Risk Analysis – Risk Management – Evaluation
   • Keep IT Software Safeguards Up to Date
   • Data Backup
   • IT Response Team Ready and Trained
We Have Reviewed
Strategies to Combat Cyber Crime

1. Who are the Cyber Criminals & How Do We Defend against Them?
2. HIPAA – A Blueprint to Combat Cyber Crime
3. Prevent Cyber Crime
4. Respond to Cyber Crime
5. Recover from Cyber Crime
HIPAA Rules – Combat Cyber Crime

A Blueprint to Combat Cyber Crime
HIPAA Rules – Combat Cyber Crime

HIPAA Rules – Easy to Follow
Step-by-Step
When You Know the Steps
Your Workforce
Your Strongest Defense against Cyber Crime – and your Weakest Link
Insider Threats
Cyber Criminal – Workforce Member?

HIPAA Rules – Combat Cyber Crime
Think Before You Click!

Workforce Training  Personal Stake
Questions - Discussion

The HIPAA E-Tool®

info@hipaaetool.com  www.hipaaetool.com  800-570-5879