Ransomware & HIPAA
Prevent – Prepare – Respond – Recover

HIPAA Rules
A Blueprint to Combat Ransomware
Ransomware & HIPAA

Prevent – Prepare – Respond – Recover

HIPAA Rules are easy to follow
Step-by-Step
When you know the Steps
Ransomware & HIPAA

---

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:

- [http://example.com](http://example.com)
- [http://example.org](http://example.org)

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](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: `g46mbrrzpfsonuk.onion/9A9DAA8C483E9B5C`
4. Follow the instructions on the site.

---

Your personal identification ID: ____________

---

*-=~*|+_=~
=-.|.|=|~|=|=+*$
-|=~|$|=|=.*

!!! IMPORTANT INFORMATION !!!!
Ransomware & HIPAA

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
Ransomware & HIPAA

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: g46mbrrzpfszonuk.onion/9A9DAA8C483E9B5C
4. Follow the instructions on the site.

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

Workforce Training

Personal Stake
Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press ‘View’ to view the list of files that have been encrypted.

Press ‘Next’ for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 95 56 21 Next >>
Objectives – Takeaways

1. Ransomware Threats
2. HIPAA Rules that cover Ransomware
3. Prevent Ransomware Attacks
4. Prepare for Ransomware Attack
5. Respond to a Ransomware Attack
6. Recover from a Ransomware Attack

*HIPAA – Comply with Confidence*
1. Ransomware Threats

The Good Old Days

Just “Plain Ransomware”

• Unsophisticated – Easy to Use
• No Data Mining – Just Lock It Up and Get Paid
• Many Unskilled Hackers – “Script Kiddies”
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
1. Ransomware Threats

2017 – Much Worse
Ransomware – Leakware – Extortionware

• Ransomware Distraction – Steal PHI
• Resell or Use PHI and Medical Identity
• Leakware – Extortionware
• Ranscam – Ransom Paid – Data Remains Locked Up
• Ransomware as a Service (RaaS)
1. Ransomware Threats
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

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.

HIPAA Rules and Ransomware

Malicious software means software designed to damage or disrupt a system.

45 CFR § 164.304
2. HIPAA Rules and Ransomware

FACT SHEET: Ransomware and HIPAA

July 11, 2016

Guidance from HHS

The HIPAA Rules

*Blueprint to Combat Ransomware Attacks*
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.
2. HIPAA Rules and Ransomware

FACT SHEET: Ransomware and HIPAA

July 11, 2016

• A Ransomware Attack on a Covered Entity or a Business Associate that
• Encrypts Electronic Protected Health Information (EPHI)
• is Presumed to be

A HIPAA Breach

Unless
A Breach Risk Assessment demonstrates a Low Probability of Compromise to the EPHI
2. HIPAA Rules and Ransomware

The HIPAA E-Tool®

Breach R

Documents:
BN-1.B Breach Risk Assessment Tool

Glossary:
Breach Risk Assessment

Basic HIPAA Policies

AAPC HIPAA

« Introduction

READ M Service

AAPC HEALTHCON
2. HIPAA Rules and Ransomware
3. **Factor 3**
   Determine whether the PHI was actually acquired or viewed. For example, consider whether:
   
   C. **Ransomware Attack** - Expert forensic analysis is able to determine and document that EPHI on an Electronic Device or Information System Encrypted by a Ransomware Attack was not transmitted ("exfiltrated") from the Electronic Information System and could not have been actually acquired and viewed by an Unauthorized Person.

6. **Additional Factors related to Ransomware**

   **Guidance Note**

   HHS HIPAA Ransomware Fact Sheet published July 11, 2016 states that PHI may be Compromised when Ransomware causes high Risk to either the Availability or Integrity of PHI. In those cases, AAPC HIPAA Compliant Organization must provide Breach Notification to affected Individuals without unreasonable delay, particularly given that any delay may impact Healthcare service and patient safety. Describe any high Risks to the Availability or Integrity of PHI caused by a Ransomware attack in the Text Box below.
2. HIPAA Rules and Ransomware

FACT SHEET: Ransomware and HIPAA
Prevent – Prepare – Respond – Recover

1. The Privacy Rule – Primary HIPAA Rule
   45 CFR Part 160 and Subparts A and E of Part 164

2. The Security Rule – PHI in Electronic Form
   45 CFR Part 160 and Subparts A and C of Part 164

3. The Breach Notification Rule
   45 CFR §§ 164.400-414
2. HIPAA Rules and Ransomware

FACT SHEET: Ransomware and HIPAA
Prevent – Prepare – Respond – Recover

1. Policies and Procedures
2. Workforce Training
3. Information System Safeguards
3. Prevent Ransomware Attacks

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
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 Ransomware Attacks

Act 2 – Confrontation

*Risk Management Action*

Act 3 – Resolution

*Risk Management Plan*

Active – Documented – In Place
# 3. Prevent Ransomware Attacks

## Risk Analysis - Risk Management

<table>
<thead>
<tr>
<th>Act 1</th>
<th>Risk Analysis Part 1: Assess Risks - EPHI and Non-EPHI Locations, Workforce, Business Associates</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-1.A</td>
<td>Locations and Potential Risks to EPHI and Non-EPHI</td>
</tr>
<tr>
<td>RA-1.B</td>
<td>Workforce Roster - PHI Access - Training</td>
</tr>
<tr>
<td>RA-1.C</td>
<td>Business Associate Roster - Due Diligence and BAA</td>
</tr>
</tbody>
</table>

|-------|------------------------------------------------------------------------------------------------|

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Risk Analysis Part 3 Identify Threats and Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-3.A</td>
<td>Threats to EPHI/Non-EPHI - Related Vulnerabilities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act 4</th>
<th>Risk Analysis Part 4 Assess Risk Level of Each Threat/Vulnerability Pair</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-4.A</td>
<td>Risk Assessment - Each Threat/Vulnerability Pair</td>
</tr>
</tbody>
</table>

## Risk Management - Assign Responsibility

<table>
<thead>
<tr>
<th>Act 2</th>
<th>Risk Management Action - Locations of EPHI and Non-EPHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-5.A</td>
<td>Risks identified in RA-1.A, Locations and Potential Risks to EPHI and Non-EPHI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act 2</th>
<th>Risk Management Action - Risks Identified by Security Rule Checklist</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Act 2</th>
<th>Risk Management Action - Risks Caused by Threat/Vulnerability Pairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-5.C</td>
<td>Threat/Vulnerability Pair Risks identified in RA-3.A and RA-4.A</td>
</tr>
</tbody>
</table>

## Risk Management Documentaion

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Risk Management - Locations of EPHI and Non-EPHI</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-6.A</td>
<td>Risk Management - Locations of EPHI and Non-EPHI</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Risk Management - Workforce Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-6.B</td>
<td>Risk Management - Workforce Training</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Risk Management - Business Associate Due Diligence, BAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-6.C</td>
<td>Risk Management - Business Associate Due Diligence, BAA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Risk Management - Security Rule Checklist Completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-6.D</td>
<td>Risk Management - Security Rule Checklist Completion</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Risk Management - Threat/Vulnerability Pairs</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Act 3</th>
<th>Supplemental Risk Analysis - Risk Management Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-6.F</td>
<td>Supplemental Risk Analysis - Risk Management Documentation</td>
</tr>
</tbody>
</table>
3. Prevent Ransomware Attacks

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>
3. Prevent Ransomware Attacks

2. Workforce Training

Your Workforce is Your Strongest Defense – and your Weakest Link

Social Engineering

1. Phishing Emails – Anthem 78.8 M
2. Spear Phishing Emails
3. Malvertising
3. Prevent Ransomware Attacks

How Does Ransomware Infect Your Information System?

Phishing

From: Netflix <gwon@uwm.edu>
To: Me
Subject: (5) Netflix - Membership suspended
Date: Saturday, April 15, 2017 6:30:51 PM

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.cesarbajal.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 Ransomware Attacks

How Does Ransomware Infect Your Information System?

Spear Phishing

From: HR2017@ [redacted]
Sent: Monday, January 2, 2017 7:29 AM
To: [redacted]
Subject: Benefit Plan Update
Importance: High!

Dear [redacted],

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.
3. Prevent Ransomware Attacks

How Does Ransomware Infect Your Information System?

Malvertising
3. Prevent Ransomware Attacks

How Does Ransomware Infect Your Information System?

Malvertising
## 3. Prevent Ransomware Attacks

### Purpose 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 Ransomware Attacks

Think Before You Click!
3. Prevent Ransomware Attacks

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 Ransomware Attacks

3. Information System System Safeguards

Protective Software
3. Prevent Ransomware Attacks

3. Information System Safeguards

Protective Software
4. Prepare for a Ransomware Attack

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. Prepare for a Ransomware Attack
4. Prepare for a Ransomware Attack
4. Prepare for a Ransomware Attack

1. Policies and Procedures
   • Security Incident Policy and Procedures
   • Security Incident Response & Reporting Plan
   • Breach Notification Policy and Procedures
   • Potential Breach Investigation Procedures
   • Breach Risk Assessment Procedures that include New Ransomware Factors
4. Prepare for a Ransomware Attack

Documents:
- SR-18 **Security Incident** Policy and Procedures
- SR-19 **Security Incident** Response and Reporting
- SR-19.A **Security Incident** Report

Glossary:
- **Security Incident**
- **Security Incident** Procedures
4. Prepare for a Ransomware Attack

2. Workforce Training Practice

• Contingency Plan
• Include Key Business Associates
  ➢ IT Experts - Ransomware Removal
  ➢ Forensic IT Experts - PHI stolen (exfiltrated)?
  ➢ Legal Counsel
  ➢ PR Advisors
4. Prepare for a Ransomware Attack

2. Workforce Training Practice

• Security Incident Response & Reporting Plan
• Breach Risk Assessment
• Include Key Business Associates
  ➢ IT Experts - Full Disk Encryption Effective?
  ➢ Forensic IT Experts - PHI stolen (exfiltrated)?
  ➢ Legal Counsel
4. Prepare for a Ransomware Attack

3. Information System Safeguards
   - Risk Analysis – Risk Management – Evaluation
   - *Encrypt Everything*
   - Keep IT *All Software* Up to Date
   - Data Backup & Retrieval
   - Emergency Mode Operation Plan
   - Testing and Revision Procedures
5. Respond to A Ransomware Attack

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
5. Respond to A Ransomware Attack

2. Workforce Training
   - Recognize and Report Ransomware Attack
   - Contain - Isolate and Disconnect Infected Devices
   - Individual Contingency Plan Responsibilities
   - Practice Contingency Plan Procedures
   - Include Key Business Associates
5. Respond to A Ransomware Attack

3. Information System Safeguards
   • Contain and Mitigate Ransomware Attack
   • Implement Contingency Plan with IT Expert guidance to quickly regain access to data
     ➢ Use Uninfected Workstations
     ➢ Access Data from Backup
   • Create and Document Forensic Analysis of Attack
   • Remove Ransomware – Sanitize System
6. Recover from A Ransomware Attack

1. Policy and Procedures
   • Follow Contingency Plan
   • Risk Analysis - Risk Management - Evaluation
   • Revise Policies and Procedures – Contingency Plan – Incorporate Lessons Learned
   • Revise Workforce Training - Incorporate Lessons Learned
6. Recover from A Ransomware Attack

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
6. Recover from A Ransomware Attack

3. Information System Safeguards
   • Risk Analysis – Risk Management – Evaluation
   • Keep IT Software Safeguards Up to Date
   • Data Backup
   • IT Response Team Ready and Trained
Ransomware & HIPAA

In Conclusion

We have Reviewed

1. Ransomware Threats
2. HIPAA Rules that cover Ransomware
3. Prevent Ransomware Attacks
4. Prepare for Ransomware Attack
5. Respond to a Ransomware Attack
6. Recover from a Ransomware Attack
Ransomware & HIPAA

Prevent – Prepare – Respond – Recover

HIPAA Rules

A Blueprint to

Combat Ransomware
Ransomware & HIPAA

Prevent – Prepare – Respond – Recover

HIPAA Rules are easy to follow
Step-by-Step
When you know the Steps
3. Prevent Ransomware Attacks

Prevent – Prepare – Respond – Recover

Think Before You Click!