Legal Disclaimer

Although the information provided by Clearwater Compliance may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where 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 and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

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.

*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.
Top Reason For Risk Analysis Failures
A conversation with Former Acting Deputy Director of HHS Office for Civil Rights, Iliana Peters

Iliana Peters, JD, CISSP
Shareholder, Polsinelli PC
Former Acting Deputy Director HHS Office for Civil Rights

March 14, 2018
We’re excited about what we do because...

...we’re helping organizations *improve patient safety* and the *quality of care* by safeguarding the very personal and private healthcare information of millions of fellow Americans...

...And, keeping those same organizations off the Wall of Shame!
# Thank YOU!

<table>
<thead>
<tr>
<th>2018</th>
<th>#11: 2015 - 2017</th>
<th>2017</th>
<th>EXCLUSIVE ENDORSEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEST IN KLAS CYBERSECURITY ADVISORY SERVICES</td>
<td>CYBERSECURITY 500 WORLD’S HOTTEST SECURITY COMPANIES</td>
<td>Inc. 5000</td>
<td>SOFTWARE USED BY NSA/CAEs</td>
</tr>
<tr>
<td>INDUSTRY COLLABORATOR</td>
<td>INDUSTRY RESOURCE PROVIDER</td>
<td>SOLE SOURCE PROVIDER</td>
<td></td>
</tr>
<tr>
<td>NCCoE National Institute of Standards and Technology</td>
<td>U.S. Department of Commerce</td>
<td>Department of the Air Force</td>
<td>U.S. Department of Homeland Security</td>
</tr>
</tbody>
</table>

Giving Back
Polsinelli serves clients nationally across the full spectrum of their legal needs:

- **100+** services and **70+** industry areas
- **800+** Attorneys
- **20 Cities** – Metropolitan offices in:
  - Atlanta
  - Boston
  - Chicago
  - Dallas
  - Denver
  - Houston
  - Kansas City
  - Los Angeles
  - Nashville
  - New York
  - Phoenix
  - St. Louis
  - San Francisco
  - Silicon Valley
  - Washington, D.C.
  - Wilmington
With the help of our clients, we have reached noteworthy milestones:

- Ranked #24 for Client Service Excellence
  - 2018 BTI Client Service A-Team Report

- Ranked #10 for best client relationships
  - 2017 BTI Industry Power Rankings

- Named among the top 20 best-known firms in the nation
  - 2017 BTI Brand Elite
This Peer Monitor competitive rate analysis illustrates the value that Polsinelli delivers versus other AmLaw 100 firms and AmLaw 200 firms.
Some Webinar Logistics

1. Slide materials – Link In Chat Box. Should have also received in reminder email earlier today.

2. Please ask Questions in “Question Area”

3. In case of technical issues, check “Chat Area”

4. All attendees are in “Listen Only Mode”

5. Please complete Exit Survey when you leave session

6. Recorded version and final slides within 48 hours
Pause and Quick Poll

1. What type of organization do you represent?
2. Is this the first Clearwater Compliance webinar you have attended?
Mega Session Objective 1:

Help you understand the #1 Reason for Risk Analysis Failure and help you perform **three (3)** very specific AND different HIPAA Security Rule *assessment* requirements...
Most Common Risk Analysis Mistakes

1. **WRONG REPORT:** submission of a Non-Technical Evaluation or Technical Evaluation or something else

2. **NOT ASSET-BASED:** too many organizations treating as a checklist matter rather than a loss/harm matter

3. **NOT COMPREHENSIVE ENOUGH:** must include every asset in every LOB in every facility in every location

4. **NOT DETAILED ENOUGH:** not considering every asset-threat-vulnerability scenario

5. **NOT FOLLOWING OCR/NIST GUIDANCE:** 9 essential elements in OCR guidance / 4 steps and detailed sub-steps in NIST SP800-30

6. **NOT ENOUGH DOCUMENTATION/ENGAGEMENT:** little evidence of vibrant ongoing program and management engagement
Discussion Flow

1. Understand HIPAA Security Rule Assessment Essentials
2. Learn how to Complete These Assessments
3. Provide Resources to Assist You
Types of Assessments

1. **Compliance Assessments** *(Security Evaluation - Non-Technical, at 45 CFR §164.308(a)(8))*
   - Where do we stand?
   - How well are we achieving ongoing compliance?

   - How effective are the safeguards we have implemented?
   - Are the safeguards working?

3. **Risk Assessment** *(Risk Analysis, at 45 CFR §164.308(a)(1)(ii)(A))*
   - What is the exposure to information assets (e.g., ePHI)?
   - What do we need to do to mitigate risks?

4. **Risk of Harm Breach Risk Assessment** *(Breach-related, in HITECH parlance)*
   - Have we caused legal, reputational, etc harm?
   - Is there low probability of compromise of PHI?

Each Assessment Has Its Role and Proper Time
45 C.F.R. §164.308(a)(8) Standard: Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.

Pause and Quick Poll

3. To what extent do you agree that the HIPAA Security Rule requires three separate, distinct assessments?

- Strongly Agree
- Agree
- Not Sure
- Disagree
- Strongly Disagree
Data Request  
04/03/2013

Transaction # [redacted]

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] HIPAA 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/modification 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 nontechnical 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 alteration or destruction.
8. Documentation of security measures taken to reduce risks and vulnerabilities to a reasonable and appropriate level to ensure confidentiality integrity, and availability of ePHI in [redacted] possession.

Breach Notification Rule:
1. Documentation that the affected individuals were notified of the breach
2. A sample copy of the notification to individuals
3. Please state the number of individuals affected in each state/jurisdiction listed in the Breach Report, dated October 22, 2012.
4. Documentation that substituted notice was provided to individuals as necessary
5. Documentation that the media was notified of the breach
6. A copy of the notification to the media.
Discussion Flow

1. Understand HIPAA Security Rule Assessment Essentials

2. Learn how to Complete These Assessments

3. Provide Resources to Assist You

"Ok, so it’s carved in stone, but still open to interpretation, right?"
Three Distinct Required HIPAA Security Rule Assessments

45 CFR §164.308(a)(8) Non-Technical Compliance Assessment

45 CFR §164.308(a)(8) Technical Testing & Audits

45 CFR §164.308(a)(1)(ii)(A) Risk Analysis
People Are Not Trained and / or Not Following PnPs

Policies & Procedures (PNPs) DO NOT EXIST or ARE INCOMPLETE or ARE OUT OF DATE

Reasonable & Appropriate Actions Are Not Taken and / or Safeguards Are Not Implemented

Compliance Risk exists when....

This Methodology is Based on the OCR Investigation Process and Audit Protocol

1. Is it documented? Policies, Procedures and Documentation

2. Are you doing it? Using, Applying, Practicing, Enforcing

3. Is it Reasonable and Appropriate? Comply with the implementation specification

Think: Performance Audit ≠ Risk Analysis
Demonstrate Complete Coverage

Must rigorously cover every

- **Area**
  - **Standard**
  - Implementation Spec or Requirement
Examine Three Critical Self-Audit Questions

Policies/Procedures? Enforcing them? Reasonable and Appropriate?
Pause and Quick Poll

Three Distinct Required HIPAA Security Rule Assessments

- **45 CFR §164.308(a)(8) Non-Technical Compliance Assessment**
  - 

- **45 CFR §164.308(a)(1)(ii)(A) Risk Analysis**
  - 

- **45 CFR §164.308(a)(8) Technical Testing & Audits**
  - 

HIPAA Security Technical Evaluation

- **External** Vulnerability Assessment & Pen Testing
- **Internal** Vulnerability Assessment & Pen Testing
- Web Application Assessment
- Wireless Security Assessment
- Security Awareness Assessment
- Sensitive Data Discovery Scans

Think: Test of Efficacy and Effectiveness of Controls ≠ Risk Analysis
Technical Testing on New Public-Facing Website

01 Passive Reconnaissance (External Network)
Domain Squatting, Blacklist Checks, File Enumeration, Email Enumeration.

02 Footprinting (Port Scans, Banner Grabs)
Validate IP Ranges, Identify Live Hosts, Operating Systems, Services Offered.

03 Vulnerability Analysis

04 Penetration Testing
Creation of Attack Plan (using data from the tasks above); Execution of Attack Plan.
References


References

https://www.owasp.org/images/1/19/OTGv4.pdf

http://www.pentest-standard.org/index.php/Main_Page
Pause and Quick Poll

5. Has Your Organization Completed the Technical Evaluation (=Testing) of Your Environment (45 CFR § 164.308(a)(8))?
Auditing for Security Evaluation

2016 Audit Protocol - Evaluation

45 CFR §164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate’s security policies and procedures meet the requirements of this subpart.

- Does the entity have policies and procedures in place to perform periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI?

- Does the entity perform periodic technical and nontechnical evaluation in response to environmental or operational changes or newly recognized risk affecting the security of ePHI?
Three Distinct Required HIPAA Security Rule Assessments

45 CFR §164.308(a)(8) Non-Technical Compliance Assessment

45 CFR §164.308(a)(8) Technical Testing & Audits

45 CFR §164.308(a)(1)(ii)(A) Risk Analysis
Risk Analysis

1. What are ALL of the exposures for ALL of our information assets (e.g. ePHI)?

2. What are all the ways in which the confidentiality, integrity or availability of ePHI might be compromised?

Identify, Rate and Prioritize All Risks
Owners

Controls & Safeguards

Vulnerabilities

Threat Sources

Threats

Risks

Assets

- Adversarial
- Accidental
- Structural
- Environmental

Owners wish to minimize value to reduce that may possess that exist in protecting may be aware of that increase to that exploit leading to give rise to may be reduced by that may possess wish to or may abuse, harm and / or damage
Risk Analysis IS:

...the process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, ..., resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.¹

¹NIST SP800-30
HHS / OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule

1. Include all Sensitive Information in Scope of the Analysis
2. Collect and Document Data About All Information Assets
3. Identify and Document Potential Threats and Vulnerabilities
4. Assess Current Security Measures
5. Determine the Likelihood of Threat Occurrence
6. Determine the Potential Impact of Threat Occurrence
7. Determine the Level of Risk
8. Finalize Documentation
9. Periodically Review and Update the Risk Assessment

---

Consider Asset-Threat-Vulnerability Triples

Determine Level of Risk for Each

<table>
<thead>
<tr>
<th>Asset</th>
<th>Threat Source / Action</th>
<th>Vulnerability</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop</td>
<td>Burglar steals laptop</td>
<td>No encryption</td>
<td>High (5)</td>
<td>High (5)</td>
<td>25</td>
</tr>
<tr>
<td>Laptop</td>
<td>Burglar steals laptop</td>
<td>Weak passwords</td>
<td>High (5)</td>
<td>High (5)</td>
<td>25</td>
</tr>
<tr>
<td>Laptop</td>
<td>Burglar steals laptop</td>
<td>No tracking</td>
<td>High (5)</td>
<td>High (5)</td>
<td>25</td>
</tr>
<tr>
<td>Laptop</td>
<td>Shoulder Surfer views</td>
<td>No privacy screen</td>
<td>Low (1)</td>
<td>Medium (3)</td>
<td>3</td>
</tr>
<tr>
<td>Laptop</td>
<td>Careless User Drops</td>
<td>No data backup</td>
<td>Medium (3)</td>
<td>High (5)</td>
<td>15</td>
</tr>
<tr>
<td>Laptop</td>
<td>Lightning Strike</td>
<td>No surge protection</td>
<td>Low (1)</td>
<td>High (5)</td>
<td>5</td>
</tr>
<tr>
<td>etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Meet OCR’s Emerging, Stringent Standard of Care

1. **Scope of the Analysis** - all ePHI must be included in risk analysis
2. **Data Collection** – it must be documented
3. **Identify and Document Potential Threats and Vulnerabilities**

<table>
<thead>
<tr>
<th>Media/Asset Group and Threat/Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>For this media selection you will respond to the questions below for this threat and vulnerability.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Media Label</th>
<th>Information Assets</th>
<th>Threat Source</th>
<th>Threat Event</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop or Laptop / 81</td>
<td>CareConnection, CareNet+, MyAdvocate, Teleleaf</td>
<td>Burglar, Thief or Anyone Who Finds a Lost Device</td>
<td>Access to Sensitive Data Once in Possession of the Device</td>
<td>Inadequate Device or Data Encryption</td>
</tr>
</tbody>
</table>

**Applicable Controls for the Threat/Vulnerability for the Media/Asset(s) Listed Above**

<table>
<thead>
<tr>
<th>Control</th>
<th>NIST SP 800-63 Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption of Data (Full Disk, File Based, etc.)</td>
<td>80, 56, 58, 59, 68 (1)</td>
</tr>
</tbody>
</table>

**Identify and Document Potential Threats and Vulnerabilities**

4. **Assess Current Security Measures**

5. **Determine the Likelihood of Threat Occurrence**

6. **Determine the Impact of Threat Occurrence**

7. **Determine the Level of Risk**

8. **Finalize Documentation**

9. **Periodic Review and Updates**

The System Enables -
What A Risk Analysis Report Looks Like…

Show you’ve identified all risks!

Generally, Avoid, Mitigate or Transfer

Generally, Accept
“9. Please submit a copy of XYZ Hospital’s most recent risk analysis, as well as a copy of all risk analyses performed for or by copy XYZ Hospital within the past 6 years pursuant to 45 C.F.R. § 164.308(a)(1)(ii)(A). If no risk analysis has been performed, please state so.
Auditing for Risk Analysis

2016 Audit Protocol – Risk Analysis - I
45 C.F.R. §164.308(a)(1)(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the entity.

- Does the entity have policies and procedures in place for conducting a thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits?
- Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI it creates, receives, maintains, or transmits?
- Determine how the entity has implemented the risk analysis requirements.

See slides at end and 2016 OCR Audit Protocol and OCR Risk Analysis Guidance.

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing national guidance on the implementation of the HIPAA Security Rule. This series of guidelines will assist organizations in identifying and implementing the most effective policies and procedures for the protection of electronic protected health information (ePHI). The guidelines are based on the best practices currently available and will be updated as needed.

The purpose of this series of guidelines is to:

1. Provide guidance to organizations on the implementation of the Security Rule.
2. Help organizations understand their responsibilities under the Security Rule.
3. Assist organizations in developing policies and procedures for the protection of ePHI.

The guidelines in this series of guidelines are intended to provide a general framework for organizations. Organizations should customize the guidelines to meet their specific needs and requirements.

https://www.hhs.gov/ocr/privacy/hipaa/understanding/security-rule/index.html

Finalized July 14, 2010
6. Has Your Organization Completed a *comprehensive and accurate* HIPAA Security Risk Analysis \((45 \text{ CFR } §164.308(a)(1)(ii)(A))\)?
Three Distinct Required HIPAA Security Rule Assessments

45 CFR §164.308(a)(8) Non-Technical Compliance Assessment

45 CFR §164.308(a)(8) Technical Testing & Audits

45 CFR §164.308(a)(1)(ii)(A) Risk Analysis
Key Points to Remember

1. There are two kinds of risk to assess:
   1. Compliance Risk
   2. Security Risk
2. Three Separate & Distinct Assessments
3. Stay Business Risk Management and Patient/Member/Customer-Focused
4. Not ‘once and done’!
5. Large or Small: Get Help (Tools, Experts, etc)

...Simply Makes Good Business Sense...
Pause and Quick Poll

7. This webinar helped me understand that the HIPAA Security Rule Risk Analysis is one of three separate, distinct assessments.
Discussion Flow

1. Understand HIPAA Security Rule Assessment Essentials
2. Learn how to Complete These Assessments
3. Provide Resources to Assist You
Supplemental Reading

2. NIST SP800-115 Technical Guide to Information Security Testing and Assessment
4. NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments
5. Sample - HIPAA Security Risk Analysis FOR Report
7. Guidance on Risk Analysis Requirements under the HIPAA Security Rule
8. PTES Technical Guidelines
9. OWASP Testing Guide
10. OCR 2016 Audit Protocol
Educational Resources
Free Education!

41 Risk Analysis Cases to Review as of 02/07/2018

Compliments of – US Taxpayers

At Clearwater Compliance, we have a passion for education. This is why we offer so many complimentary HIPAA compliance and cyber risk management resources to anyone interested, regardless if you are a HIPAA Quality Risk Analysis Working Lab™.

REMOVE THE GUESSWORK out of OCR’s Risk Analysis Criteria & HELP ENSURE Your Cyber Risks are MINIMIZED

COMPLIMENTARY | INTERACTIVE | HANDS-ON SESSIONS

March 21, 28 & April 4 & 11
11:00am-12:00pm CT

Register Now:
At Clearwater Compliance, we have a passion for education. This is why we offer so many complimentary HIPAA compliance and cyber risk management resources to anyone interested regardless if you are a HIPAA Quality Risk Response Working Lab™. Designed to provide education on the NIST Requirements for tackling the Risk Response process. 

COMPLIMENTARY | INTERACTIVE | HANDS-ON SESSIONS

April 18 & 25, 2018 | 11:00am-12:00pm CT


**Pre-Requisite**
Registrants / Attendees must meet one of the two pre-requisites listed below before registering for this event:
• Attended all four sessions of a recent OCR Quality Risk Analysis Working Lab™
• Be a current Clearwater Compliance IRM|Analysis™ SaaS Account User
HOT TOPIC WEBINAR
Cyber Risk, Patient Safety and Captives

April 9, 2018 | 2:30—3:30pm ET

Speakers:
Mark Reynolds, CEO, Risk Management Foundation Harvard University
Chet Porembski, Deputy General Counsel, Ohio Health Corporation

Moderator:
Bob Chaput, CEO of Clearwater Compliance

Register by April 6 @
Questions?

Iliana Peters, JD, CISSP
Polsinelli PC
IPeters@Polsinelli.com
Phone: 202-626-8327
https://www.polsinelli.com/

Bob Chaput, CISSP, HCISPP, CRISC, CIPP/US
Clearwater Compliance LLC
bob.chaput@ClearwaterCompliance.com
Phone: 800-704-3394 or 615-656-4299
http://www.ClearwaterCompliance.com

Please Complete the Webinar Evaluation- We Value Your Feedback!
Thank You.

www.ClearwaterCompliance.com
LINKEDIN | http://www.linkedin.com/in/bobchaput/
TWITTER | @clearwaterhipaa
YOUTUBE | Search: ClearwaterCompliance
800-704-3394
References / Articles for Your Own HITRUST Due Diligence

- HITRUST or High Risk? The Health Information Trust Alliance’s Common Security
- An Open Letter to the HITRUST Alliance
- HITRUST Breaches Lay the Welcome Mat for Hackers and Paydirt
- Should Business Associates Be HiTrust Certified?
- HITRUST, CSF and Mandatory Certification
- 20+ Due Diligence Questions about the HITRUST Certification
- Research HITRUST Board companies on:
  - HHS Wall of Shame
  - ProPublica’s HIPAAHelper Privacy Violations, Breaches and Complaints page

We have never seen the OCR ever ask for Security Opinions (e.g., SSAE SOC2) or “HITRUST Certifications”

As of mid-May 2016, HITRUST Alliance Board Members’ ten (10) organizations have 26 listings on the HHS Wall of Shame, with responsibility for 122MM of 156MM records (79%) and 852 mentions on ProPublica’s HIPAAHelper web site for complaints / breaches. Three organizations are in the HIPAAHelper “Top 10.”
2016 Audit Protocol - Evaluation

45 CFR §164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

- Does the entity have **policies and procedures in place to perform periodic technical and nontechnical evaluation**, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes or newly recognized risk affecting the security of ePHI?

- Does the entity **perform periodic technical and nontechnical evaluation in response to environmental or operational changes or newly recognized risk** affecting the security of ePHI?
2016 Audit Protocol - Evaluation

45 CFR §164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate’s security policies and procedures meet the requirements of this subpart.

• Determine if such policies and procedures identifies how the evaluation of findings, remediation options and recommendations, and remediation decisions are documented; specifies that evaluations will be repeated on a periodic basis and/or when environmental and operations changes are made and/or newly recognized risk affects the security of ePHI; and identifies the frequency of when to evaluate and update the current policy and procedures.
2016 Audit Protocol - Evaluation

45 CFR §164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate’s security policies and procedures meet the requirements of this subpart.

Elements to review may include but are not limited to:

• Workforce members’ roles and responsibilities in the technical and nontechnical evaluation
• Management involvement in the process and approval of technical and nontechnical evaluation
• Coordination of technical and nontechnical evaluation among departments
• Specification of how technical and nontechnical evaluation will be conducted
• How technical and nontechnical evaluation findings will be addressed
2016 Audit Protocol - Evaluation

45 CFR §164.308(a)(8): Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, which establishes the extent to which a covered entity's or business associate’s security policies and procedures meet the requirements of this subpart.

- Evaluate and determine if such evaluation appropriately evaluates ePHI security measures; addresses evaluation findings associated with noncompliant security measures; identifies and measures risks associated with noncompliant security measures; and that evaluation findings are reviewed and certified by appropriate management.

- Obtain and review documentation of plans related to risk management or mitigation efforts in response to evaluations conducted due to a major technology change which affected the security of ePHI. Evaluate and determine if the identified risks associated with noncompliant security measures are addressed in a plan related to risk management or mitigation efforts.
• Does the entity have policies and procedures in place to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the electronic protected health information (ePHI) it creates, receives, maintains, or transmits?

• Has the entity conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all the ePHI it creates, receives, maintains, or transmits?

• Determine how the entity has implemented the requirements.

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
2016 Audit Protocol – Risk Analysis - II

45 C.F.R. §164.308(a)(1)(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

• Obtain and review risk analysis policies and procedures. Evaluate and determine if written policies and procedures were developed to address the purpose and scope of the risk analysis, workforce member roles and responsibilities, management involvement in risk analysis and how frequently the risk analysis will be reviewed and updated.

• Obtain and review the written risk analysis or other record(s) that documents that an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI was been conducted.

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
Evaluate and determine whether the risk analysis or other documentation contains:

- A defined scope that identifies **all of its systems** that create, transmit, maintain, or transmit ePHI
- **Details of identified threats and vulnerabilities**
- Assessment of **current security measures**
- **Impact and likelihood analysis**
- **Risk rating**

Obtain and review documentation regarding the written risk analysis or other documentation that immediately preceded the current risk analysis or other record, if any.
• Evaluate and determine if the risk analysis has been **reviewed and updated on a periodic basis**, in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.

• If there is no prior risk analysis or other record, obtain and review the two (2) most recent written updates to the risk analysis or other record, if any.

• If the original written risk analysis or other records have not been updated since they were originally conducted and/or drafted, obtain and review an explanation as to the reason why.

2016 Audit Protocol – Risk Analysis - IV
45 C.F.R. §164.308(a)(1)(ii)(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

• Does the entity have policies and procedures in place regarding a risk management process sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?

• Has the entity implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level?
2016 Audit Protocol – Risk Management - II

§164.308(a)(1)(ii)(B): (Required) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with General Requirements

• Obtain and review policies and procedure related to risk management. **Evaluate and determine if the documents identify how risk will be managed**, what is considered an acceptable level of risk based on management approval, the frequency of reviewing ongoing risks, and identify workforce members’ roles in the risk management process.

• Obtain and review documentation demonstrating the security measures implemented and/or in the process of being implemented as a result of the risk analysis or assessment. Evaluate and determine whether the implemented security measures appropriately respond to the threats and vulnerabilities **identified in the risk analysis** according to the risk rating and that such security measures are **sufficient to mitigate or remediate identified risks** to an acceptable level.