



OCR-Quality Security Risk Analysis™

By-the-Book

Steve Cagle, CEO, Clearwater

2019 HIPAA Summit
Washington DC
March 5, 2018

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.

Our Expertise & Experience

-  **Completely focused on healthcare cyber risk management and HIPAA compliance**
-  **Makers of IRM|Analysis™, the leading enterprise cyber risk management software for healthcare**
-  **Consulting engagements in 400+ healthcare organizations**
-  **Successful outcomes in dozens of OCR-enforcement cases**
-  **100% OCR-acceptance rate of risk analysis executed with our solutions**

Learning Objectives



Clarify what is and what is NOT a HIPAA Risk Analysis



Review OCR requirements for Risk Analysis



Learn how to implement nine steps of OCR's guidance on Risk Analysis using specific examples

89%

of ePHI related OCR Enforcement Actions cited Risk Analysis Failure



\$103.9M

PAID TO DATE

\$28.7M

PAID IN 2018

\$19.3M

PAID IN 2017

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:** does not have asset-threat-vulnerability scenarios
5. **NOT FOLLOWING OCR/NIST GUIDANCE:** 9 essential elements in OCR guidance
6. **NOT ENOUGH DOCUMENTATION:** little evidence of an adequate program

THERE HAVE BEEN

64

OFFICE FOR CIVIL RIGHTS
ENFORCEMENT ACTIONS
WITH MONEY PENALTIES

2016 Phase 2 Audit Results

- 1 = Meets
- 2 = Substantially Meets
- 3 = Minimally Meets
- 4 = Negligible Efforts
- 5 = No Serious Effort to Comply



CE Audits (166)

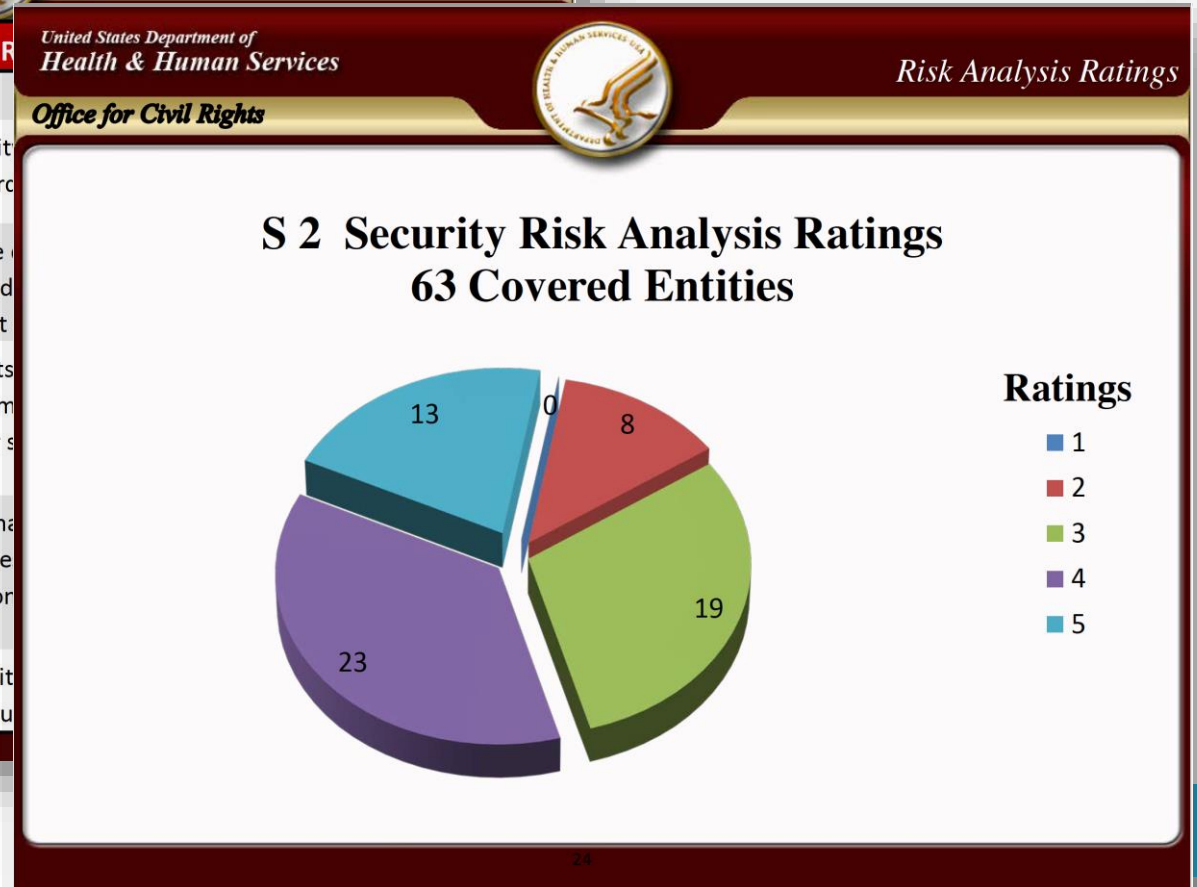
- Privacy and Breach
- Security (63)

BA Audits (41)

- Breach and Security

- 57%, 4s and 5s
- 86%, 3s, 4s and 5s

Compliance Effort Ratings	
Rating	Description
1	The audit results indicate the entity meets the objectives of the selected standard.
2	The audit results indicate that the entity maintains appropriate policies and evidence of implementation meet the requirements.
3	Audit results indicate entity efforts to comply with the requirements. Analysis indicates that entity has met requirements, but implementation is inadequate, or some requirements are not met.
4	Audit results indicate the entity may not meet all audited requirements - e.g. policies not copied directly from an association document and generic.
5	The entity did not provide OCR with the Rules and enable individuals to exercise their rights.



Security Evaluation v. Risk Analysis

45 C.F.R. §164.308(a)(8)

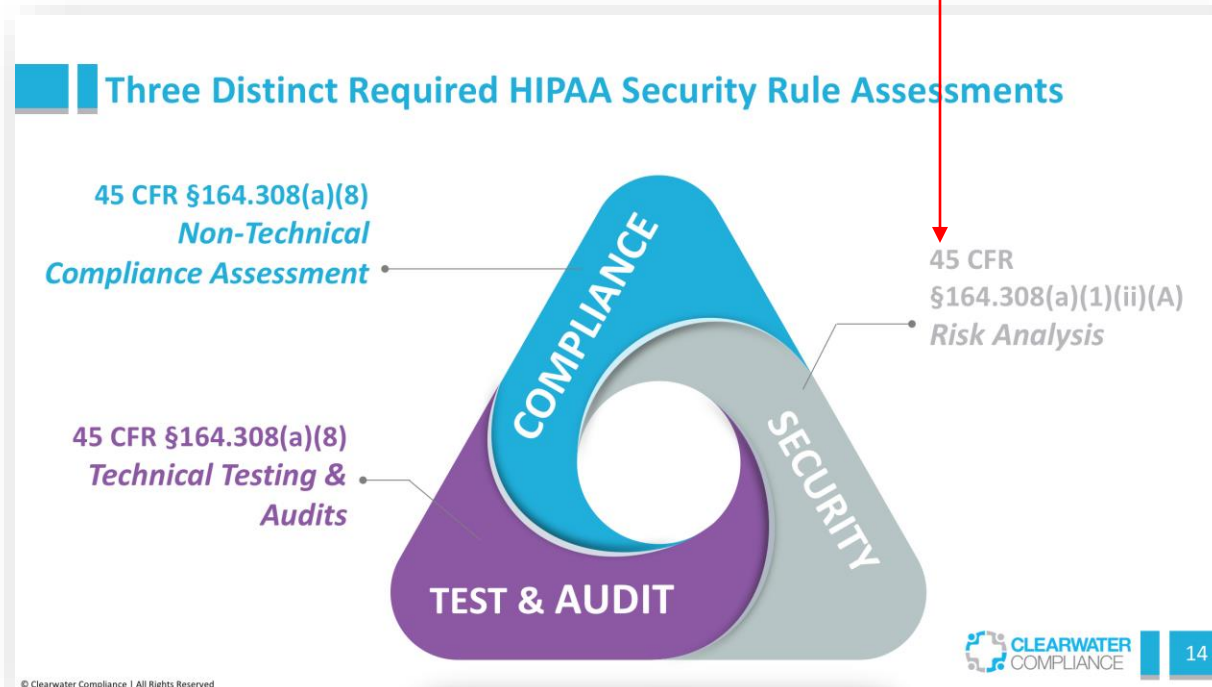
Standard: **Evaluation**. Perform a periodic **technical** and **non-technical** evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, **which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.**

45 C.F.R. §164.308(a)(1)(i) Standard: Security Management Process

(1)(i) Standard: *Security management process*. Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) Implementation specifications:

(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.



Today's Focus

Lots of Good Assessments, Only One Bona Fide Risk Analysis!

- External Security Assessment
- Architecture Assessment
- Internal Security Assessment
- Security Rule Compliance Assessment
- Wireless LAN Security Validation
- Information Security Program Assessment
- Meaningful Use EHR Technical Controls Assessment
- Social Engineering Assessment
- OWASP Web Application Assessments
- NIST CS Current Profile Assessment
- 15 Joint Tactical HIPAA and Cyber Risk Management Assessment
- Strategic Enterprise IRM Program Maturity Assessment
- ETC...

Today's
Focus

**Bona Fide, Comprehensive Risk Analysis Required at 45 CFR
§164.308(a)(1)(ii)(A) MEANS OCR Guidance and NIST SP800-30!**

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is the provisions in the HIPAA Security Rule guidances will assist organizations¹ in and appropriate administrative, physical, protected health information (e-PHI).² input from stakeholders and the public.

We begin the series with the risk analysis. Conducting a risk analysis is the first step that comply with and carry out the Security Rule. Therefore, a risk analysis detail before OCR can issue meaningful and technologies that will best protect

The guidance is not intended to provide the risk analysis requirement. Rather, it organizations working to meet these requirements most appropriate way to achieve compliance the organization and its environment.

We note that some of the content contents of the National Institute of Standards and publishes freely available material in the only federal agencies are required to fit represent the industry standard for good securing e-PHI. Therefore, non-federal when developing and performing compliance

All e-PHI created, received, maintained, Security Rule. The Security Rule requires their environments and to implement

¹ Section 13401(c) of the Health Information Technology
² As used in this guidance the term "organization" guidance will be updated following implementation of The HIPAA Security Rule: Health Insurance
³ The 800 Series of Special Publications (SP) is specifically, SP 800-30 - Risk Management Guidance
(<http://www.hhs.gov/ocr/privacy/hipaa/admin>)

Posted July 14, 2010

NIST Special Publication 800-30
Revision 1

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Guide for Conducting
Risk Assessments

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2012



U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology
and Director

OCR-Quality Risk Analysis – Risk Management Review

The Ten Risk Analysis Key Essential Criteria Are Derived From:

1. the HIPAA Risk Analysis implementation specification language at [45 CFR §164.308\(a\)\(1\)\(ii\)\(A\)](#) of the HIPAA Security Rule;
2. the methodology outlined in the HHS/OCR [“Guidance on Risk Analysis Requirements under the HIPAA Security Rule”](#);
3. the underlying NIST Special Publications for performing a risk assessment and, specifically [NIST SP 800-30 “Guide for Conducting Risk Assessments”](#);
4. the documentation found in OCR investigation letters and [“OCR Resolution Agreements / Corrective Action Plans”](#).
5. the [“OCR Audit Protocol – Updated April 2016”](#) specific to Risk Analysis and Risk Management .
6. our work with numerous organizations subjected to OCR enforcement actions that included reviews of organizations' risk analyses.



Rx: Your Review Plan → OCR Risk Analysis Guidance

Regardless of the risk analysis methodology employed...

1. Scope of the Analysis
2. Data Collection
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. Periodic Review and Updates to the Risk Assessment
10. Meet Emerging OCR Standard of Care (added by Clearwater)

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.¹ (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations² in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.³ An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.⁴ Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to

¹ Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.

² As used in this guidance the term "organizations" refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.

³ The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.

⁴ The 800 Series of Special Publications (SP) are available on the Office for Civil Rights' website – specifically, SP 800-30 - Risk Management Guide for Information Technology Systems. (<http://www.hhs.gov/oc/privacy/hipaa/administrative/securityrule/securityruleguidance.html>).

Review Point 1-A: Scope of the Analysis

Asset Inventory List

Assets > Asset

19 assets used out of unlimited ass

To add an Asset click the New button. To edit select a row and click the Edit Button



+ New

Edit

Delete

Search:

Id	Asset name	Asset description	# records	Owner	Inherited from	Created	Modified
7355	Automated Medication Cabinet	An automated dispensing cabinet (ADC) is a computerized drug storage device or cabinet designed for hospitals.	150,000	Jon Stone		2014-08-14 10:38	2017-01-10 08:53
95	Billing Information Systems	Used for Medical Billing	16,000	Jon Stone		2011-12-27 22:08	2016-09-08 09:06
21796	CCTV - System One	Closed Circuit Television System	10,000	Brad Park		2015-06-11 09:33	2015-11-09 09:14
57	Claim Payment System	Used to adjudicate claims. Hosted in our own data center.	100,000	Claims Director		2011-12-27 22:08	2016-09-08 09:07
2626	Core HIS	Hospital information system, an enterprise resource planning system that caters to hospital needs	10,000	Jon Stone		2013-08-07 10:30	2016-09-08 09:07
2729	CT Scan	Computed axial tomography (CAT scan) or computer assisted tomography is a medical	12,000	Sam Mark		2013-08-30 12:04	2017-01-10 08:53
53267	Document						

Show that you've included ALL Information Systems and their components with ePHI!

09:59

Does It Include all ePHI Systems & Devices?

Enterprise Risk Analysis Extends Well Beyond Your EHR System



Pharmacy



EHR



Appointment



Email



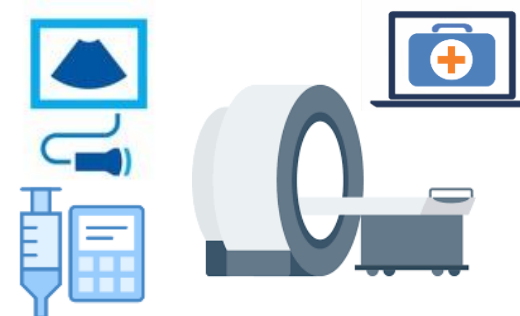
Patient Portal



Billing

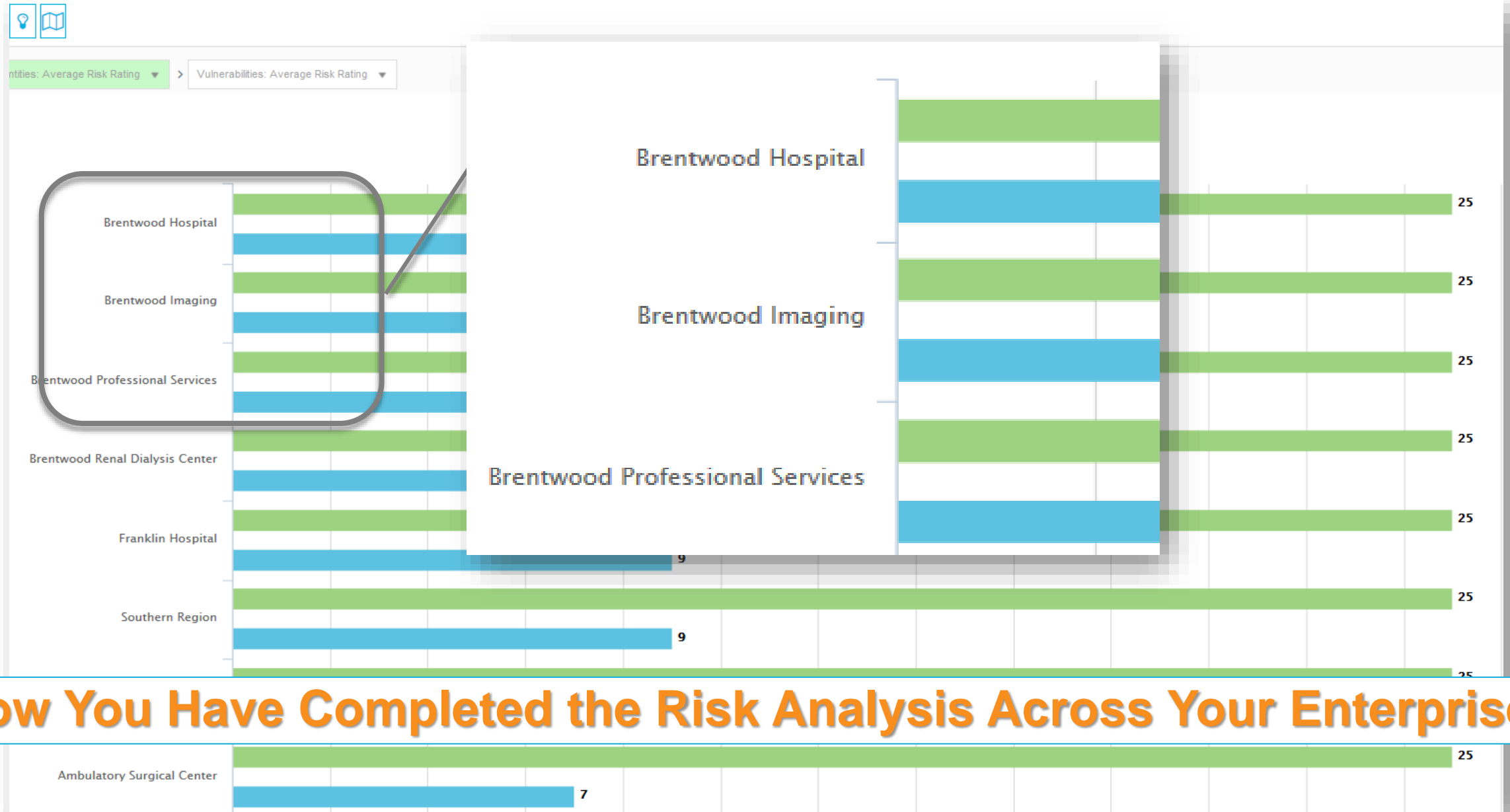


Laboratory



Medical Devices

Review Point 1-B: Scope of the Analysis



Show You Have Completed the Risk Analysis Across Your Enterprise

How “Enterprise” is Your Risk Analysis?



Clinics



Hospitals



LTC Facility



ASC



CHC



Hospice



Insurance



Home Health



EMS



Rehab Clinic



Imaging Center



Rural Clinic



Dialysis Clinic



Behavioral



Labs

Review Point 2-A: Data Collection

Asset Inventory List

Assets > Asset

To add an Asset click the New button. To edit select a row and click the Edit Button

18 assets used out of unlimited as

+ New

Edit

Delete

Search:

Id	Asset name	Asset description	# records	Owner	Inherited from	Created	Modified
7355	Automated Medication Cabinet	An automated dispensing cabinet (ADC) is a computerized drug storage device or cabinet designed for hospitals.	150,000	Jon Stone		2014-08-14 10:38	2017-01-10 08:53
95	Billing Information Systems	Used for Medical Billing	16,000	Jon Stone		2011-12-27 22:08	2016-09-08 09:06
21796	CCTV - System One	Closed Circuit Television System	10,000	Brad Park		2015-06-11 09:33	2015-11-09 09:14
57	Claim Payment System	Used to adjudicate claims. Hosted in our own data center.	100,000	Claims Director		2011-12-27 22:08	2016-09-08 09:07
2626	Core HIS	Hospital information system, an enterprise resource planning system that caters to hospital needs	10,000	Jon Stone		2013-08-07 10:30	2016-09-08 09:07
2729	CT Scan	Computed axial tomography (CAT scan) or computer assisted tomography is a medical imaging procedure that uses computer	12,000	Sam Mark		2013-08-30 12:04	2017-01-10 08:53
53267	Document Management		0			2016-09-08 09:59	2016-09-08 09:59

Show that you know where all the ePHI lives!

Review Point 2-B: Data Collection

Asset

Asset name *

Asset description

Asset Status ?

Type of Sensitive Data ?

Asset Details

Source of the sensitive information

Where or to whom the data is shared or sent

Physical Location of Asset

Number of end users and administrators *

Importance of asset ?

Approximate # of sensitive records stored on this asset

Select all items that create, receive, store, transmit or view sensitive information

Devices * ?

- ☒ Backup Media ?
- ☐ Desktop ?
- ☒ Desktop or Laptop ?
- ☐ Digital Camera ?
- ☐ Disk Array ?
- ☐ Electronic Medical Device ?
- ☐ Laptop ?
- ☐ Pager ?
- ☒ Scanners, Printers or Copiers ?
- ☒ Server ?
- ☐ Smartphone ?
- ☐ Storage Area Network ?
- ☐ Tablet ?
- ☒ USB key or flash drive ?

Third Parties ?

- ☒ Contractors / Consultants ?
- ☐ Platform-as-a-Service ?
- ☐ Software-as-a-Service ?


Asset Business Owner



First name

Last name

Collect all relevant data about the components that make up the information system

Review Point 3: Identify and Document Threats & Vulnerabilities

 Rating Review Risk Deter

Media/Label	Asset Name(s)	Threat Source	Threat Event	Vulnerability	Risk Likelihood	Risk Impact	Risk Rating
Desktop / Clinical / Patient Care Areas	Electronic Health Record System, Immunoassayer - Siemens	Careless IT Personnel	Insecure User Management	Vulnerabilities in Password Creation and Distribution ?	Almost Certain	Major	20
Electronic Medical Device / Radiology	CT Scan, Immunoassayer - Siemens MRI, PACS	Careless IT Personnel	Insecure Configuration of Systems	Vulnerabilities in System Configurations ?	Almost Certain	Insignificant	5
Laptop / Windows XP	Billing Information Systems, Electronic Health Record System, Workstation Applications	Careless IT Personnel	Insecure User Management	Excessive User Permissions ?	Almost Certain	Severe	25
Laptop / Windows XP	Billing Information Systems, Electronic Health Record System, Workstation Applications	Careless Software Developer	Insecure Development of Software	Vulnerabilities in Custom Applications ?	Almost Certain	Major	20
Laptop / Windows XP	Billing Information Systems, Electronic Health Record System, Workstation Applications	Careless User	Installation of Malicious Software	Overly-trusting Employees ?	Almost Certain	Insignificant	5
Storage Area Network / No Label	Document Management, Electronic Health Record System, LIS	System Cracker	Theft of Sensitive Data	Vulnerabilities in Custom Applications ?	Almost Certain	Insignificant	5
Desktop / Finance Department	Billing Information Systems, Claim	Careless User	Information Leakage	Destruction/Disposal Vulnerabilities	Likely	Moderate	12

Identify all reasonably anticipated threats & vulnerabilities for each of the components that are associated with your information systems.

Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Careless Software Developer	Insecure Development of Software	Insecure Software Development Processes ?	Likely	Major	16
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Fire	Fire Damage to Equipment	Insufficient Fire Protection ?	Likely	Severe	20
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Careless User	Installation of Malicious Software	Overly-trusting Employees ?	Likely	Major	16

Review Point 4-A: Assess *Relevant* Security Controls In Place

Media/Asset Group and Threat/Vulnerability

For this media selection you will respond to the questions below for this threat and vulnerability.

	Media/Label	Information Assets	Threat Source	Threat Event	Vulnerability
95.1%	Laptop Clinical Laptop	Claim Payment System, Electronic Health Record System	Burglar, Thief or Anyone Who Finds a Lost Device	Access to Sensitive Data Once in Possession of the Device	Vulnerabilities in User Authentication

One of 52 separate Threat/Vulnerability combinations associated with Laptops

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

Is the organization actively maintaining and enforcing the controls listed below that would prevent this threat from exploiting this vulnerability?

Control	NIST SP 800-53 Requirement	Response	Clear	Global		
Two-factor Authentication	IA-2 NIST	Yes In Progress No N/A			0	0
User Authenticated Locally	IA-2, IA-2 CE1, IA-2 CE2, IA-2 CE3, IA-2 CE4, IA-2 CE8, IA-2 CE9 NIST	Yes In Progress No N/A			0	0

Controls relevant to this Media/Asset/Threat/Vulnerability Combination

What controls are in place – at the Specific Asset-Threat-Vulnerability Level

Review Point 5: Determine Likelihood

Risk Likelihood

The likelihood of occurrence of a threat event initiated or caused by a threat source, combines an estimate of the likelihood of initiation or occurrence of the threat event, with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of initiation is typically based on: (i) adversary intent; (ii) adversary capability; and (iii) adversary target. For advanced persistent threat (APT). For other than adversarial threats, the likelihood of occurrence can be estimated using historical evidence, or the likelihood that a threat event will be initiated or will occur within a specified time frame (e.g., the next six months, the next year, or the next five years reached). If a threat event is almost certain to be initiated or will occur within a specified time frame, the assessment of risk may take into consideration the likelihood of threat occurrence can also be based on the likelihood of mission/business processes, enterprise and information systems and environments of operation (taking into consideration the likelihood of deployed safeguards and countermeasures (i.e., the likelihood of unauthorized or undesirable behavior, detect and limit mission/business capabilities).

From NIST SP800-30, Chapter 2, Page 9

How likely is it for the threat to exploit the vulnerability?

Risk Likelihood

Rank	Description	Percent Likelihood	Example
0	Not Applicable	0% likely in the next 12 months'	Will never happen
1	Rare	5% likely in the next 12 months'	May happen once every 20 years
2	Unlikely	25% likely in the next 12 months'	May happen once every 10 years
3	Moderate	50% likely in the next 12 months'	May happen once every 5 years
4	Likely	75% likely in the next 12 months'	May happen once every year
5	Almost Certain	100% likely in the next 12 months'	May happen multiple times per year

Review Point 6: Determine Impact

Risk Impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the unauthorized disclosure, modification, disruption, destruction, or loss of information and/or denial of service. Such adverse impact, and hence harm, can be experienced by a wide range of organizational and non-organizational stakeholders including, for example, mission and business owners, information owners/stewards, mission and business owners, information system owners, or individuals/groups in the public or private organization—in essence, anyone with a vested interest in the organization or individuals, including other organizations in partnership with the organization (and/or critical infrastructure-related considerations).

From NIST SP800-30, Chapter 2, Page 9

Risk Impact

Rank	Description	Example	# of Records	Productivity Lost	Financial Impact
0	Not applicable threat	No impact	0	0	0
1	Insignificant	No interruption, no exposed data	0	0	0
2	Minor	Multi-minute interruption, no exposed data	0	2	20,000
3	Moderate	Multi-hour interruption, minor exposure of data	499	4	175,000
4	Major	One day interruption, exposure of data	5,000	8	2,000,000
5	Severe	Multi-day interruption, major exposure of sensitive data	50,000	24	20,000,000

What harm or loss would occur?

Review Point 7: Determine the Level of Risk

Considering asset/media, threat, vulnerability & controls...

Media/Asset Group and Threat/Vulnerability

For this media selection you will respond to the questions below for the threat and vulnerability.

	Media/Label	Information Assets	Threat Source	Threat Event	Vulnerability
95.1%	Laptop / Clinical Laptop	Claim Payment System, Electronic Health Record System	Burglar, Thief or Anyone Who Finds a Lost Device	Access to Sensitive Data Once in Possession of the Device	Vulnerabilities in User Authentication ?

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

Is the organization actively maintaining and enforcing the controls listed below that would prevent this threat from exploiting this vulnerability?

+ Control		NIST SP 800-53 Requirement	Response	Clear	Global		
+ Two-factor Authentication ?	IA-2	NIST	Yes In Progress No N/A		<input type="checkbox"/>	0	0
+ User Authenticated Locally ?	IA-2, IA-2 CE1, IA-2 CE2, IA-2 CE3, IA-2 CE4, IA-2 CE8, IA-2 CE9	NIST	Yes In Progress No N/A		<input type="checkbox"/>	0	0

Add a Custom Control or Recommendation ?

Multiply Impact X Likelihood to get a risk score

Risk Rating for this Threat/Vulnerability for the Media/Asset(s) Listed Above

	Description	Level of Risk	Risk Rating ?	Risk Notes ?
Risk Likelihood ?	What is the probability (likelihood) of an adverse impact to the organization considering the ability of this threat to exploit this vulnerability given predisposing conditions, the controls listed above and other significant controls in place for this media/asset? ?	Likely ▼		0
Risk Impact ?	What is the magnitude of harm (impact) that can be expected to the confidentiality, integrity or availability of sensitive information if this threat were to exploit this vulnerability given the predisposing conditions, controls given above and other significant controls in place for this media/asset? ?	Severe ▼	20	

20



Review Point 7: Determine the Level of Risk at Granular Level

Asset	Threat Source / Action	Vulnerability	Likelihood	Impact	Risk Rating
Laptop	Burglar steals laptop	No encryption	High (5)	High (5)	25
Laptop	Burglar steals laptop	Weak passwords	High (5)	High (5)	25
Laptop	Burglar steals laptop	No tracking	High (5)	High (5)	25
Laptop	Careless User Drops	No data backup	Medium (3)	High (5)	15
Laptop	Shoulder Surfer views	No privacy screen	Low (1)	Medium (3)	3
Laptop	Lightning Strike	No surge protection	Low (1)	High (5)	5
Etc.					



Review Point 7: Establish Risk Threshold (e.g., 10)

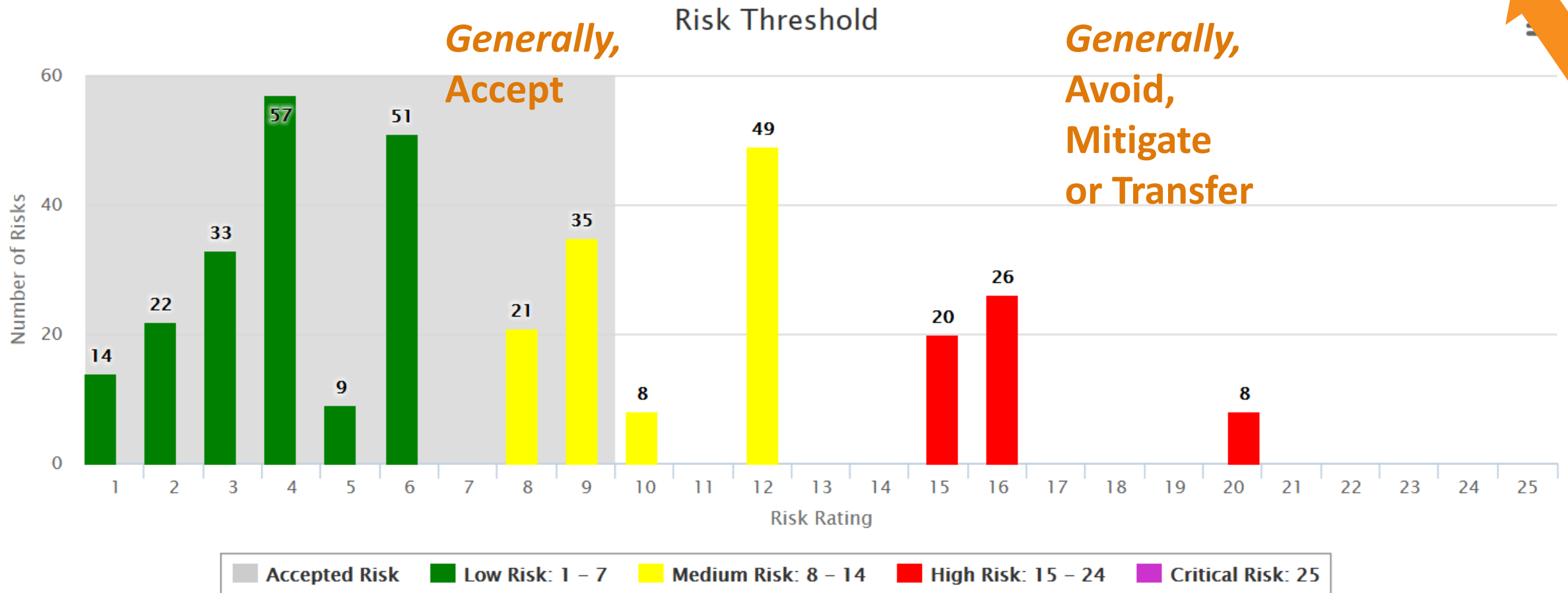


Risk Threshold

Framing/Governance > Risk Threshold



Risk Threshold
10 ▼



Review Point 8-A: Finalize Documentation

 Rating Review

Now you Have a Risk Register



Media/Label	Asset Name(s)	Threat Source	Threat Event	Vulnerability	Risk Likelihood	Risk Impact	Risk Rating
Desktop / Clinical / Patient Care Areas	Electronic Health Record System, Immunoassayer - Siemens	Careless IT Personnel	Insecure User Management	Vulnerabilities in Password Creation and Distribution ?	Almost Certain	Severe	25
Laptop / Windows XP	Billing Information Systems, Financial System, Workstation Applications	Burglar/Thief	Theft of Equipment	Physical Security Vulnerabilities ?	Likely	Severe	20
Laptop / Clinical Laptop	Claim Payment System, Electronic Health Record System	Burglar/Thief	Theft of Equipment	Physical Security Vulnerabilities ?	Likely	Severe	20
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Inclement Weather	Unavailability of Key Personnel	Lack of Key Person Redundancy / Cross-training ?	Likely	Major	16
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Power Outage/Interruption	Loss of Electrical Power	Insufficient Power Capacity ?	Likely	Major	16
USB key or flash drive / Company Provided	Billing Information Systems	Burglar/Thief	Theft of Equipment	Physical Security Vulnerabilities ?	Moderate	Severe	15
Desktop / Clinical / Patient Care Areas	Electronic Health Record System, Immunoassayer - Siemens	Burglar/Thief	Theft of Equipment	Physical Security Vulnerabilities ?	Moderate	Major	12
Laptop / Windows XP	Billing Information Systems, Financial System, Workstation Applications	Careless IT Personnel	Insecure User Management	Vulnerabilities in Password Creation and Distribution ?	Unlikely	Severe	10
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Careless IT Personnel	Insecure User Management	Excessive User Permissions ?	Moderate	Moderate	9
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Careless IT Personnel	Insecure User Management	Vulnerabilities in Password Creation and Distribution ?	Moderate	Moderate	9
Desktop / Administration	Workstation Applications	Burglar/Thief	Theft of Equipment	Physical Security Vulnerabilities ?	Moderate	Moderate	9
Laptop / Clinical Laptop	Claim Payment System, Electronic Health Record System	Careless IT Personnel	Insecure User Management	Vulnerabilities in Password Creation and Distribution ?	Unlikely	Major	8
Desktop / Finance Department	Billing Information Systems, Claim Payment System, Email	Burglar/Thief	Theft of Equipment	Physical Security Vulnerabilities ?	Unlikely	Moderate	6
Desktop / Clinical / Patient Care Areas	Electronic Health Record System, Immunoassayer - Siemens	Careless IT Personnel	Insecure User Management	Excessive User Permissions ?	Unlikely	Moderate	6

**Generally,
Avoid,
Mitigate or
Transfer**

**Generally,
Accept**

Review Point 8-B: Finalize Documentation

Know how risks are distributed!

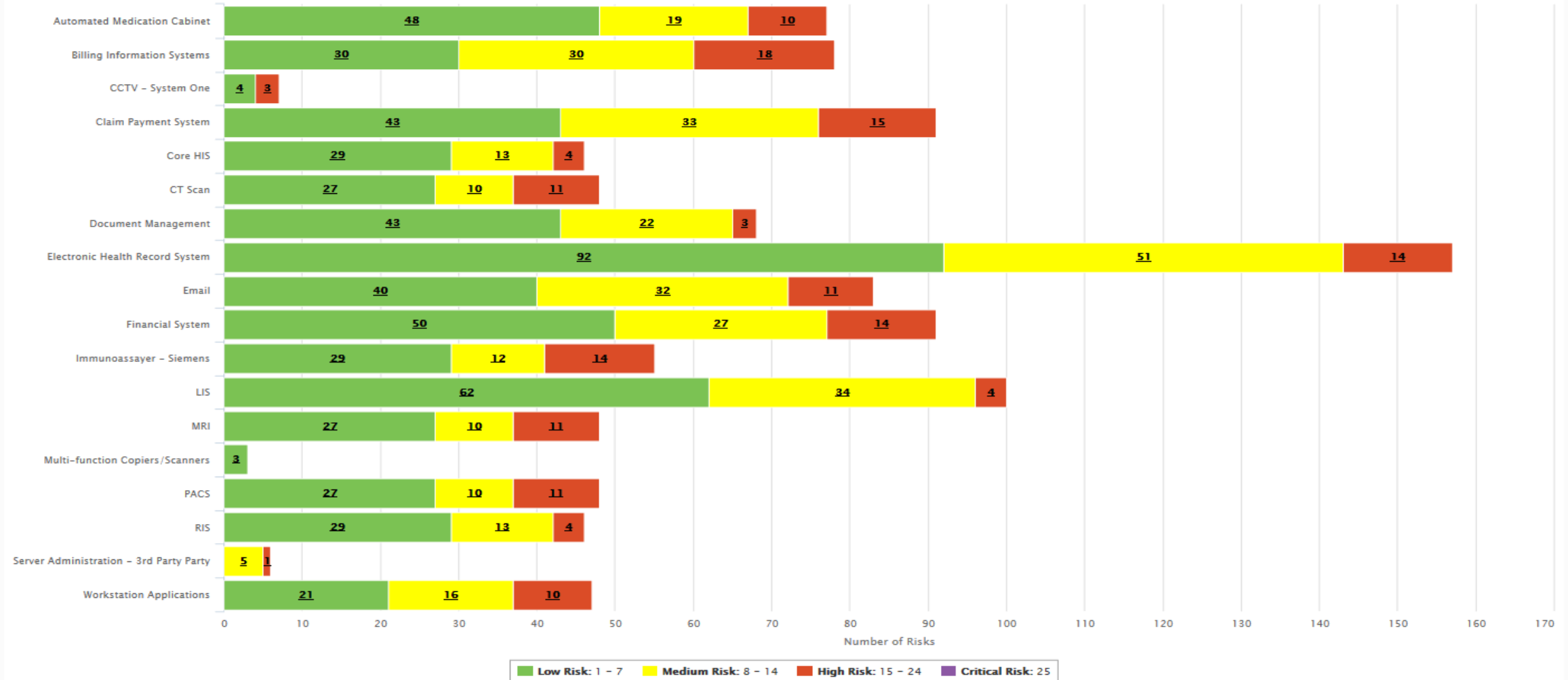
Rating Distribution By Asset

View your distribution of risks by information asset. Click for details.




history
current

Rating Distribution By Asset





Review Point 9: Periodic Review and Updates




Version History

Reports > Version History

Below is a list of versions (data snapshots) of your account.



+ New

Edit

Delete

Search:

Version Id ▾	Version Number ⇅	Date, Time ⇅	Note ⇅	Author ⇅
2675	1	04/30/2015 08:54 PM	Automated Analysis Snapshot - April 30, 2015	
4578	2	03/20/2016 05:34 PM	Scheduled Analysis Snapshot - March 20, 2016	
8035	3	01/02/2017 02:36 AM	Scheduled Analysis Snapshot - January 2, 2017	
9473	4	01/31/2017 11:59 PM	Scheduled Analysis Snapshot - February 1, 2017	
12951	5	07/01/2017 09:27 AM	Automated Analysis Snapshot - July 1, 2017	
15847	6	07/31/2017 09:19 PM	Automated Analysis Snapshot - July 31, 2017	
22972	7	01/01/2018 09:59 AM	Automated Analysis Snapshot - January 1, 2018	

25 ⇅

records per page

Showing 1 to 7 of 7 entries

First

Previous

1

Next

Last

Journey, Not Destination!

Show your Ongoing Effort!

The Risk Analysis Dilemma

Assets and Media
Backup Media
Desktop
Disk Array
Electronic Medical Device
Laptop
Pager
Server
Smartphone
Storage Area Network
Tablet
Third-party service provider
Etcetera...

Threat Agent
Burglar/ Thief
Electrical Incident
Entropy
Fire
Flood
Inclement weather
Malware
Network Connectivity Outage
Power Outage/Interruption
Etcetera...

Threat Actions
Burglary/Theft
Corruption or destruction of important data
Data Leakage
Data Loss
Denial of Service
Destruction of important data
Electrical damage to equipment
Fire damage to equipment
Information leakage
Etcetera...

Vulnerabilities
Anti-malware Vulnerabilities
Destruction/Disposal Vulnerabilities
Dormant Accounts
Endpoint Leakage Vulnerabilities
Excessive User Permissions
Insecure Network Configuration
Insecure Software Development Processes
Insufficient Application Capacity
Insufficient data backup
Insufficient data validation
Insufficient equipment redundancy
Insufficient equipment shielding
Insufficient fire protection
Insufficient HVAC capability
Insufficient power capacity
Insufficient power shielding
Etcetera...

NIST SP 800-53 Controls
PS-6 a The organization ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.
PS-6 b The organization reviews/updates the access agreements [Assignment: organization-defined frequency].
AC-19 a The organization establishes usage restrictions and implementation guidance for organization-controlled mobile devices.
AC-19 b The organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems.
AC-19 d The organization enforces requirements for the connection of mobile devices to organizational information systems.
AC-19 e The organization disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
Hundreds and hundreds

Millions of Combinations



Meet OCR's Emerging, Stringent Standard of Care

Media/Asset Group and Threat/Vulnerability

For this media selection you will respond to the questions below for this threat and vulnerability.

	Media/Label	Information Assets	Threat Source	Threat Event	Vulnerability
100%	Desktop or Laptop / B1	CareConnection, CareNet+, MyAdvocate, Tealeaf	Burglar, Thief or Anyone Who Finds a Lost Device	Access to Sensitive Data Once in Possession of the Device	Inadequate Device or Data Encryption ?

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

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

Is the organization actively maintaining and enforcing the controls listed below that would prevent this threat from exploiting this vulnerability?

+	Control	NIST SP 800-53 Requirement	Control Tags	Response	Clear	Global		
+	Encryption of Disks (Full Disk, File Based, etc.) ?	SC-13, SC-28, SC-28 (1) NIST	0	Yes In Progress No N/A			4	7

4. Assess Current Security Measures

5. Determine the Likelihood of Threat Occurrence

or the Media/Asset(s) Listed Above

	Description	Risk Rating ?	Risk Notes ?
Risk Likelihood ?	What is the probability (likelihood) of an adverse impact to the organization considering the ability of this threat to exploit this vulnerability given predisposing conditions, the controls listed above and other significant controls in place for this media/asset? ?	Unlikely ▼	0
Risk Impact ?	What is the magnitude of harm (impact) that can be expected to the confidentiality, integrity or availability of sensitive information if this threat were to exploit this vulnerability given the predisposing conditions, controls given above and other significant controls in place for this media/asset? ?	Major ▼	8

6. Determine the Impact of Threat Occurrence

7. Determine the Level of Risk

- The System Enables-
8. Finalize Documentation
9. Periodic Review and Updates

In Summary

**Bona Fide, Comprehensive Risk Analysis Required at 45 CFR §164.308(a)(1)(ii)(A)
MEANS OCR Guidance and NIST SP800-30!**

- **OCR has clearly defined what it expects in a risk analysis – not meeting these requirements has resulted in severe penalties and reputational damage.**
- **A risk analysis is not a technical evaluation, nor is it a check list – it's an information system based evaluation of the vulnerabilities and risk.**
- **A by-the-book risk analysis must follow the nine critical components described in this session and must be properly documented.**
- **Purpose built software can streamline the work, drive a by-the-book process, and ensure adequate documentation is on place.**
- **With a system in place you can effectively manage your riskiest exposures.**

Key Resources

- [Sample - HIPAA Security Risk Analysis FOR Report](#)
- [Guidance on Risk Analysis Requirements under the HIPAA Security Rule](#)
- [NIST SP800-30 Revision 1 Guide for Conducting Risk Assessments](#)
- [NIST SP800-39-final Managing Information Security Risk](#)
- [NIST SP800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach](#)
- [The Clearwater Definition of an Information Asset](#)



Additional Resources

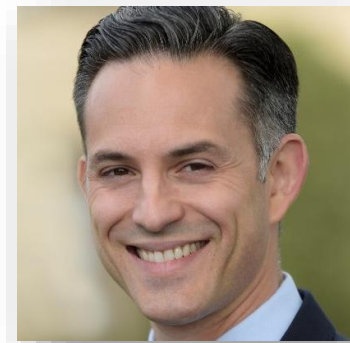
- [NIST SP800 53 r4 Security and Privacy Controls for Federal Information Systems and Organizations](#)
- [NIST SP800-115 Technical Guide to Information Security Testing and Assessment](#)
- [NIST SP800-34 Contingency Planning Guide for Federal Information Systems](#)
- [MU Stage 2 Hospital Core 7 Protect Electronic Health Info 2012-11-05](#)
- [NIST Risk Management Framework 2009](#)

Questions?





Thank You!



Steve Cagle, CEO

steve.cagle@clearwatercompliance.com

732.887.3949

@SteveCagle1 

www.linkedin.com/in/steve-cagle 

www.clearwatercompliance.com