
HIPAA Reviews
Lessons Learned
HIMSS
NORTH CAROLINA Chapter
CompliancePoint

Identify

Quickly Identify any discrepancies putting you at risk

Mitigate

Effectively close gaps and correct discovered discrepancies

MANAGE

Proactively protect information on an ongoing basis

CompliancePoint®

Areas of Expertise

Health Information Privacy

HIPAA, HITRUST, HITECH, Meaningful Use, and MARS-E rules specific to protecting patient data.

PCI Security Standards

PCI security standards including PCI DSS, PA-DSS, P2PE and EI3PA requirements

Cyber Security

Requirements and best practices for protecting data from theft, damage, and disruption.

GDPR, ePrivacy, CCPA & More

General Data Protection Regulation compliance standards issued by the European Commission.

SSAE SOC 2&3

Requirements mandating certain controls that protect financial data and meet user needs.

Cloud Compliance

FedRAMP compliance standards and CSA's best practices for secure cloud computing.

FISMA & NIST

Standards specific to government agencies for implementing an information security program.

ISO 27001 & CobIT

Standards and frameworks specific to security management and governance.

CompliancePoint®

OCR Phase II Audit Results Common Themes

- Failure to Demonstrate appropriate risk management plans – 94% of covered entities reviewed!
- Failure to perform an information security risk analysis – 83%
- Incomplete or inaccurate notice to individuals of a breach -67%
- Incomplete or inaccurate Notice of Privacy Practices – 65%
- Failure to comply with requirements to provides patients access to their PHI – 89%

https://cynergistek.com/blog/ocr-desk-audits-preliminary-results/

2018 Enforcement Results
$28 MILLION

ENTITY	SETTLEMENT	ISSUES
Fresenius Medical Care North America	$3.5 Million	Failed to conduct an accurate and through risk analysis Failed to implement a mechanism to encrypt and decrypt ePHI
MD Anderson Cancer center	$4.3 Million	Failed to address risk analysis findings regarding the lack of device level encryption
Advanced Care Hospitalists	$500,000	Failed to conduct risk analysis Failed to obtain BAA with billing vendor
Cottage Health	$3 million	Failed to conduct risk assessment
Anthem, Inc.	$16 million	Failed conduct an enterprise-wide risk analysis

CompliancePoint Results

Risk Assessments	• Not performed • Risks not addressed
Policies and Procedures	• Incomplete • Not updated
Business Associate Agreements	• Not obtained • Not updated

Risk Management - Risk Analysis

HIPAA Definition requires the organization to “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 or business associate.” 45 CFR § 164.308(a)(1)(ii)(A).

Risk Management - Risk Analysis

- The questions you are trying to answer in the risk analysis are:
  - What could compromise the confidentiality, integrity and availability of the health information in our possession?
  - If that information is compromised, what is the impact to our business or to the individual?
  - What is the probability that it will happen?

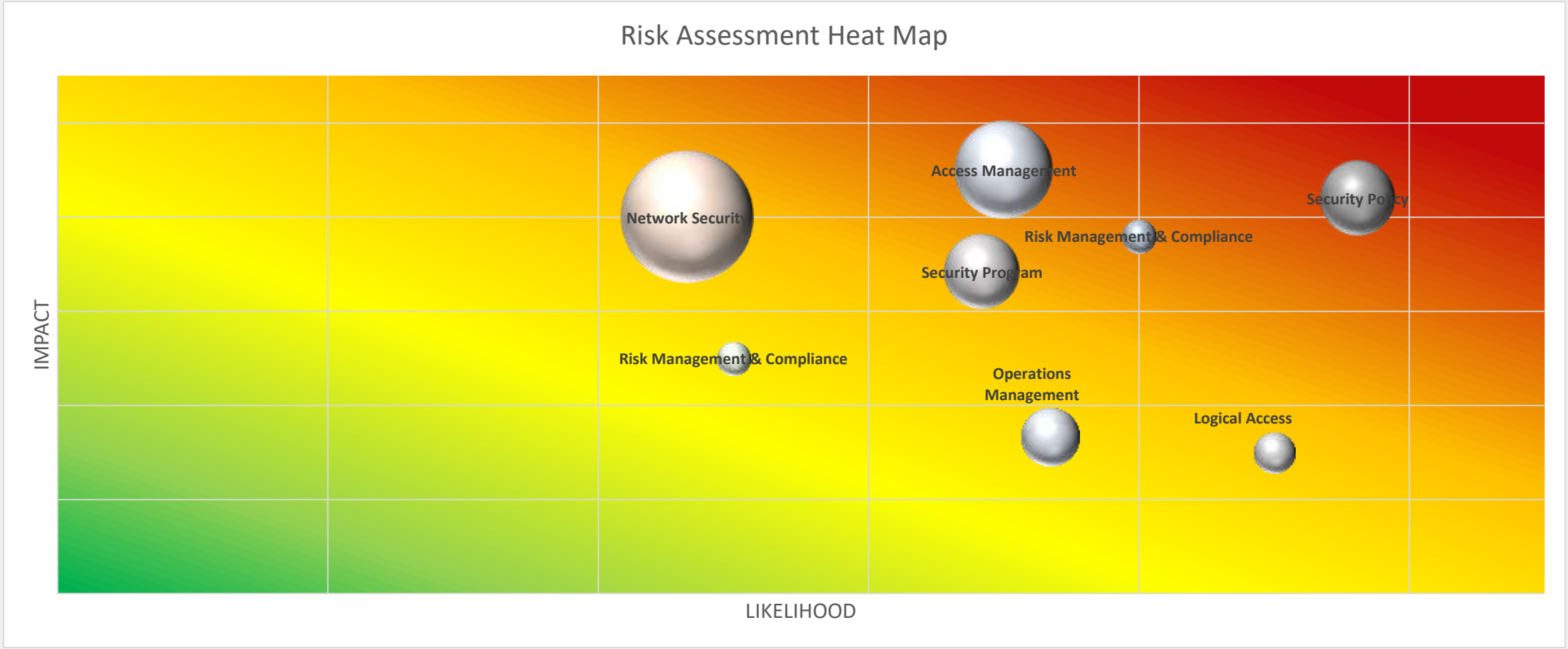
A Risk Analysis not only helps you comply with HIPAA but may help you identify opportunities for improvement in your organization.

Risk Analysis – Getting Started

- Identify the PHI that your organization creates, receives, stores and transmits
- Identify the threats to your PHI
- Assess your current controls
- Determine the 'likelihood and impact' of each risk
- Assign a risk level based on the average of the likelihood and impact
- Prioritize your workplan – high likelihood, high impact first
- Repeat at least annually

The HIPAA risk analysis, the rationale for the measures, procedures and policies subsequently implemented, and all policy documents must be kept for a minimum of six years.

Risk Analysis Reporting



Risk Analysis Improvement Opportunities

PHI Process Flows	• **Eliminate or reduce paper work flows** • **Ensure accuracy and completeness of Medical Record**
Employee Awareness	• **Texting, phishing, social media**
Incident Reduction	• **Gossip** • **Social breaches**
Proactive	

Breach Notification

How quickly do you need to respond?

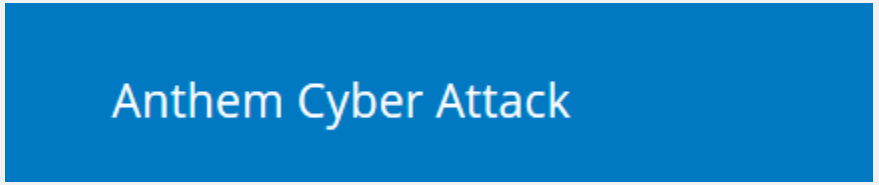
- Affected individuals must be notified within 60 days of discovery
- Business Associates must notify their covered entities

Assess the Breach

- The nature and extent of the protected health information involved
- The unauthorized person who accessed the PHI
- Was the PHI actually acquired or viewed
- Mitigation performed

Breach Notification

- Patient Notification Failures
  - More than 10 returned mail notifications?
    - Website posting



    - Toll Free Number
  - More than 500 affected?
    - Media Notification within 60 days of discovery
  - HHS Notification
    - More than 500 – within 60 days of discovery
    - Less than 500 – within 60 days of calendar year end for discovery year.
  - North Carolina Department of Justice Notification

Notice of Privacy Practices

Deliver at FIRST Contact

Prominently post on your website

- Audit Guidance: “An example of prominent posting of the notice would include a direct link from homepage with a clear description that the link is to the HIPAA Notice of Privacy Practices.”
- Review of 10 Physician Practices in the Raleigh Area
  - 6 did not have a link on their home page
  - 1 had a broken link

Provision Of Access

- Right to Access
  - Procedures
    - Cannot be dependent upon payment of claim
    - Cannot provide just a summary
  - Charges
    - Reasonable cost of labor for creating and delivering the record
    - Costs of supplies for creating the paper copy or for creating the electronic copy
    - Postage

What should I do?

1

Perform Assessment of current status

2

Develop Action Plan to address issues identified.

3

Develop OCR Response “tool kit”.

Audit Yourself

- Use the OCR Audit Protocol
- Be objective or use an objective auditor
- Conduct and critique in-person interviews
- Use network scanning tools to access technical vulnerabilities
- Don’t “assume”
- Keep auditing!

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html

Audit Example

Control	S40
Audit Type	Security
Safeguards	Physical Safeguards
Section	§164.310(d)(2)(ii)
Established Performance Criteria	§164.310(d)(2)(ii): Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
Audit Inquiry	Does the entity have policies and procedures established to remove ePHI before reusing electronic media and who is responsible for the overseeing those processes? Does the entity remove ePHI before reusing electronic media and who is responsible for the overseeing those processes? Obtain and review procedures related to media re-usage. Evaluate the content in relation to the specified performance criteria for removing ePHI from electronic media before they are issued for reuse. Elements to review may include but are not limited to:• Workforce members' roles and responsibilities in the media re-use process• How the removal of ePHI from electronic media is verified• How ePHI will be removed from electronic media before external and internal re-use. Obtain documentation demonstrating media re-use procedures being implemented and how ePHI has been removed from electronic media. Evaluate and determine if the process used for the reuse of electronic media is appropriate; that ePHI is properly removed from electronic media prior to reuse; that ePHI that is removed is unusable, inaccessible, and indecipherable; and that removal of ePHI from electronic media has been verified prior to reuse of electronic media.
Owner	IT Security Manger
Policy and Procedure	IT Policy 12.3
Review Results	IT Security Manager indicated that it's up to each individual department to delete ePHI from electronic media. No evidence of anyone doing this is obtained.
Review Recommendations	Policy says all media should be reviewed and ePHI deleted by IT. Implement policy. Develop tracking log to provide evidence.
Status	**Not Compliant**

High Risk Areas

Business Associate Agreements

- Do we have them?
- Are they current?
- Have we “audited” our associates compliance?
- Do we know what we have agreed to?

Risk Management

- Do we have a defined process for assessing privacy and security risks?
- Are we documenting actions taken to address identified risks?

High Risk Areas

Review of information system activity, such as audit logs, access reports, and security incident tracking reports

- IT is doing this?
- Can we prove we do it?

Terminating access to electronic protected health

- How long does it take?
- Are you verifying it’s done?

“Assumptions” can create issues

- Waiver of rights under the Breach Notification Rule or Privacy Rule.
  - Cannot be required for treatment or payment.
  - Is this in your policies and procedures?
  - “We would never do this, so we don’t need a policy”

- Denial of an amendment to PHI.
  - Must be in writing and include appeal procedures.
  - Notification by phone is not sufficient

Details, Details, Details

Policies and Procedures must cover ALL the requirements of the law

- Secret Service
- Corner’s office

Who, what, when, how?

Updated to reflect your changes?

“I’m from Internal Audit and I’m here to help”

Recommendations can both help improve operations and compliance

Use your audit to develop a “tool kit” to help you respond to questions/investigations

After the Breach – The Letter From the OCR

- Step 1 – Speed dial Legal
- Step 2 – Pull your mock audit results off the shelf
  - Policies and procedures
  - Documentation
  - Contacts
- Step 3 – Respond Timely
  - Last minute submittals may be viewed as a weakness
  - Provide evidence of your risk analysis and remediation

COOPERATE

OCR Response | **Have a Plan**

Develop and TEST a HIPAA audit response plan

1. Know where your documentation is and how to get it QUICKLY
2. Know how to get system – generated information such as audit logs, access monitoring etc.
3. Practice presenting documentation in an organized and responsive manner.

How we can help you

- Enable responsible interactions with your customers and the marketplace
- Privacy, Data Security, Risk Management and Compliance
- Governance, operations and technology
- Work with regulatory agencies
- 750 clients
- Since early 2000s

CompliancePoint®

Identify

Initiate
Organizational Goals, Priorities, Problem Definition & Applicability

Identify
Define PII, scope and potential impact to organization

Assess
Analyze and Evaluate risk

CompliancePoint®