Introduction
Since the introduction of the Health Information Portability and Accountability Act of 1996, the industry has seen several regulatory changes to the security and privacy of Personal Health Information (PHI). In January 2013, the U.S. Department of Health and Human Services ("HHS") released its long anticipated HIPAA Omnibus Final Rule1.

Among the significant requirements revised by the HIPAA Omnibus rule, the new regulations requires that a covered entity or business associate must “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity”2.

What is a HIPAA Risk Assessment?
The HIPAA Privacy rule outlines how a patient may protect and permit your Agency to use and disclose their medical information. On the other hand, the HIPAA Security rule is a framework that your Agency provides to both protect patients’ privacy and to make sure medical information is secure. 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.

A risk analysis is a process that requires your Agency 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 a covered entity.”3

A risk analysis means that your Agency must:
1) Identify your office tools and systems that hold ePHI, and
2) Identify the threats specific to your office to that ePHI, and
3) Identify the vulnerabilities in specific electronic system(s) that would permit these threats to impact your office ePHI, and
4) Identify what the loss or destruction of ePHI would mean to your office, and
5) Identify what controls your office can put in place to protect your office’s ePHI.

---
1 http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
2 See 45 CRF 164.308(1)(ii)(A)
3 See 45 CRF 164.308(1)(ii)(A)
Why Conduct a Risk Assessment?

Regulatory Requirement & Compliance:
The Security Rule does not require the use of a specific assessment tool or an exact protocol be followed; however a HIPAA Security Risk Analysis must be conducted in order to demonstrate compliance. In 2008, CMS conducted a series of HIPAA compliance review of 10 Covered Entities to verify their compliance with the HIPAA Security Rule and published its findings in the HIPAA Compliance Analysis and Summary of Results. These reviews were initiated as a result of complaints filed against each entity. While the CMS report may be presumed to be dated due to the many regulatory changes that have occurred since its publication, the findings are still current and applicable to many Hospice Organizations. Based on the complaints received, CMS’s focused its reviews on the following areas:

- Risk analysis and management
- Security training
- Physical security of facilities and mobile devices
- Off-site access and use of ePHI from remote locations
- Storage of ePHI on portable devices and media
- Disposal of equipment containing ePHI
- Business associate agreements and contracts
- Data encryption
- Virus protection
- Technical safeguards in place to protect ePHI
- Monitoring of access to ePHI.

In its summary document, CMS identified several consistent areas of deficiency which continue to be a challenge and struggle for covered entities in complying with the HIPAA Security Rule:

- Risk Assessment
- Currency of Policies and Procedures
- Security Training
- Workforce Clearance
- Workstation Security
- Encryption.

Penalties for Noncompliance:
The January 17, 2013 Final Omnibus Rule also adopted the HITECH Act's tiered system of increasing penalty amounts for violations based on increasing levels of culpability associated with each tier. Under the HIPAA Omnibus Rule, penalties for non-compliance are based upon the level of negligence, with potential maximum fines of $1.5 million per violation. The HHS Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Security Rules and enforces these rules in several ways:

- by investigating complaints filed with it,
- conducting compliance reviews to determine if covered entities are in compliance, and
- performing education and outreach to foster compliance with the Rules' requirements.

The OCR maintains an online “Wall of Shame” of all large data breaches – those that involve 500 or more individuals. It also periodically updates an online record of penalties levied against covered

4 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf
6 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html
7 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
8 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/
entities for noncompliance *along with best practices* on how covered entities can effectively comply with the requirements of the Privacy and Security Rules.

**Other Consequences for Non-compliance?**

- Ongoing Security Exposures
- OCR Potential lawsuits (Attorney General)
- Reputational harm from Negative Publicity
- More stringent State laws
- Resolution Agreements can force organizations to implement and maintain controls and to notify OCR for every security incident

**Part B Palliative Care Meaningful Use**

As part of the American Recovery and Reinvestment Act of 2009 (ARRA), Congress mandated payment adjustments to be applied to Medicare eligible professionals who are not meaningful users of Certified Electronic Health Record (EHR) Technology under the Medicare EHR Incentive Programs. These payment adjustments will be applied beginning on January 1, 2015, for Medicare eligible professionals.

CMS’s Certified Electronic Health Record (CEHR) Meaningful Use (MU) requirements impact each palliative care physician submitting claims to Medicare Part B if less than 90% of Medicare allowed charges are for other than inpatient hospital services. These physicians are classified as Eligible Professionals (EPs). While attesting to MU is not required of Part B physicians, if they meet the criteria of an EP, failure to implement a CEHR will result in payment penalties for all charges submitted to Medicare Part B. This payment adjustment will be applied to the Medicare physician fee schedule (PFS) amount for covered professional services furnished by the eligible professional during the year. Eligible professionals receive the payment adjustment amount that is tied to the year that they did not demonstrate meaningful use (e.g., A health care professional who is eligible for a payment adjustment in 2018 will receive a 4% PFS reduction regardless if this is their first or fourth year not demonstrating meaningful use). Depending on the total number of Medicare eligible professionals who are meaningful users under the EHR Incentive Programs after 2018, the maximum payment adjustment can reach as high as 5%.

Conducting a security risk analysis or reviewing (and updating as appropriate) an existing risk analysis is a core measure (Measure 9) of the MU program.

Specifically, the requirements of Measure 9 include:

1. Eligible professionals (EPs) must attest YES to conducting or reviewing a security risk analysis and implementing security updates as needed to meet this measure.
2. EPs must conduct or review a security risk analysis of CEHRT including addressing encryption/security of data, and implement updates as necessary at least once prior to the end of the EHR reporting period and attest to that conduct or review. The testing could occur prior to the beginning of the first EHR reporting period. However, a new review would have to occur for each subsequent reporting period.
3. The parameters of the security risk analysis are defined 45 CFR 164.308(a)(1) which was created by the HIPAA Security Rule. Meaningful use does not impose new or expanded requirements on the HIPAA Security Rule nor does it require specific use of every certification and standard that
is included in certification of EHR technology. More information on the HIPAA Security Rule can be found at [http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/).

4. In order to meet this objective and measure, an EP must possess the capabilities and standards of CEHRT at 45 CFR 170.314(d)(4), (d)(2), (d)(3), (d)(7), (d)(1), (d)(5), (d)(6), (d)(8), and optionally (d)(9).

All other elements of a risk analysis noted here must be included, however, for purposes of MU, when attesting ‘yes,’ the physician is specifically making a claim to the Federal government regarding the following component of the CEHR that has been implemented and documented (this is not an all-inclusive list):

1. Verify use of unique identifiers for every user with access to the EHR
2. Establish specific access permissions – what type of access a user is permitted to perform in the EHR.
3. Audit log technology has been implemented, has been secured against alteration, and audit logs are reviewed periodically.
4. EHR technology must be able to detect whether the audit log has been altered.
5. “Time outs” – Controls must be in place to prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.
6. Electronic health information that is stored must be encrypted in accordance with the standard
7. EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops.
8. The CEHR must be able to accommodate certain requirements of the HIPAA Privacy Rule such as attaching approved or denied amendments to the record that was requested to be amended or recording any accounting of disclosures

Conducting a Risk Assessment

A risk assessment is a component of an overall Risk Management Process. Once conducted, it becomes the foundation for an ongoing risk management plan. Besides being a regulatory requirement, a thorough and complete risk assessment provides the following key benefits:

1. Leaders can use the risk assessment results to prioritize compliance activities
2. Risk assessment activity will have answered most of the questions that OCR would ask if an agency is audited
3. Risk assessment activity provides protection against any risks and vulnerabilities in your IT Systems
4. A thorough risk analysis will strengthen your organization’s overall security posture.
Initial Readiness Assessment

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
</table>
| Initial Data Collection | - Overview of HIPAA Site  
- On-site Survey  
- Collect Data on workstations, computers, etc. |
| Secondary Data | - Gather data on any items missing, i.e. computers, tablets, etc.  
- Gather data on User IDs, logins, computer IDs, shared IDs, etc. |
| Gap Analysis | - Written report identifying areas of weakness  
- Prepare recommendations and a roadmap to correct the potential areas of weakness |
| Ongoing Assessment | - Continue to monitor and assess the corrective action plan to ensure it is being performed |

Phases of a Risk Assessment

**A Clearly Defined Scope**

The scope and purpose of the risk assessment is determined by whether it is an initial assessment to establish a baseline for the organization or whether it is a subsequent assessment to reassess changes whether resulting from the implementation of remediation initiatives or changes within the organization environment.

The HIPAA Security Rule requires implementation of appropriate:

1. Administrative Safeguards (see § 164.308)
2. Physical Safeguards (see § 164.310)
3. and Technical Safeguards (see § 164.312).

The scope of the risk assessment should include at minimum the assessment of these safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. For an initial risk assessment, the scope should include all systems and tools where ePHI is store, access, transmitted or dispose of within the environment. Future assessments can be limited in scope to assessing remediation implementation results or changes within the environment. Other items that should be considered is a Network Penetration Test to assess the security of the network and assess vulnerabilities.

**An Inventory Assessment**

An organization should approach the preparation for the risk assessment similar to preparing for an audit. It is important that proper documentation are readily available to the assessor. These include:

1. IT & Privacy Policies & procedures governing ePHI
2. List of applications, systems and databases that contains ePHI
3. List of vendors or Business Associates having access to ePHI
4. Personnel responsible for ePHI
In addition to reviewing policies, procedures and assessing systems controls, the assessor or auditor will also interview personnel responsible for the implementation of the administrative safeguards. An inventory list of these personnel should be prepared including the Privacy Officer, Director of IT, Facilities, VP of HR, etc.

The Compliance Assessment

In the compliance assessment phase, the assessor assesses the organizations compliance with the HIPAA Security Rule requirements for administrative, physical, and technical safeguards (See sample HIPAA Security Compliance Assessment Matrix.xlsx). Areas of non-compliance with the HIPAA requirements are identify and are documented as compliance gaps.

The Compliance Gaps Documentation

This is a written report of the assessment. Areas of non-compliance are clearly documented and categorized by administrative, physical, and technical safeguards and includes recommendations on corrective actions or steps to close each gap.

Sample:

<table>
<thead>
<tr>
<th>Technical Safeguards</th>
<th>Effective Date</th>
<th>Specification</th>
<th>Purpose</th>
<th>Owner</th>
<th>Test Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Controls</td>
<td>November 1, 2016</td>
<td>Unique User Identification</td>
<td>To provide a unique name and password for identifying and tracking user identity</td>
<td>Privacy Officer</td>
<td>The user is limited to one IP address and cannot be used by others.</td>
</tr>
<tr>
<td>Emergency Access Protocols</td>
<td>December 1, 2016</td>
<td>Access to Electronic Health Information</td>
<td>To allow access to protected health information during an emergency</td>
<td>Privacy Officer</td>
<td>The Privacy Officer ensures that access is granted only to authorized personnel.</td>
</tr>
<tr>
<td>Automatic Logoff</td>
<td>January 1, 2017</td>
<td>Encryption and Decryption</td>
<td>To ensure that all electronic protected health information is encrypted</td>
<td>Privacy Officer</td>
<td>The encryption is reviewed annually, and all laptops are encrypted.</td>
</tr>
</tbody>
</table>

The Remediation Implementation

Now that there is a written assessment report, the next step is to implement the corrective actions to close the gaps. If there are several areas of deficiency noted in the report, best practice is to begin with prioritizing the gaps by areas of greatest vulnerability to the security of ePHI. Entities should ensure that an overall plan is defined to implement corrective actions to bring closure to all gaps in a timely manner.

Use of Internal versus External Resource

There are several self-assessment tools available to organizations to conduct their own risk assessment. The following three tools will help your organization assess where there are deficiencies with HIPAA’s administrative, physical, and technical safeguards and can alert you of areas where ePHI may be at risk:
1) HHS/OCR Security Risk Assessment Tool\(^9\)
2) NIST HIPAA Security Rule Toolkit\(^{10}\)
3) HIMSS Risk Assessment Toolkit\(^{11}\).

In determining the use of internal resources versus consulting with a third party, consideration should be given to the following challenges that organizations typically face when seeking to conduct an assessment:

1) Availability of internal resources
2) Lack of auditing or assessment experience
3) Time required to conduct assessment
4) Creditability and validity of the outcome with internal and external stakeholders
5) Cost.

To minimize overall cost and in cases where there are known security gaps, entities can choose to use one of the above assessment tools to correct known issues and establish a minimum baseline and then contract with a third party consultant to perform a complete test and validation.

**Evergreen: Ongoing Plan**

Conducting a HIPAA Risk Assessment is the first step in identifying and implementing safeguards to comply with the Security Rule. However, best practice is that entities establish an ongoing compliance program to monitor, assess, and implement corrective actions to ensure ongoing compliance. An effective program should include:

- Ongoing Employee Awareness training on the importance of protecting ePHI
- Annual Mandatory Employee Awareness Training
- Periodic Risk Assessments to reassess your risk or as triggered due to changes within the environment (new software, new functionality, etc.)

**Other Considerations**

- **IPS/DLP Solutions** - Intrusion Prevention Solutions (IPS) detect and block common cyber-attacks at the network perimeter. Data Loss Prevention (DLP) solutions can prevent confidential data from being sent or transferred to unauthorized recipients such as via email or the use of a USB Drive. This solution should also be used to reinforce security awareness training and compliance with security policies.
- **Periodic Networking Penetration Testing** – technical security assessment to validate that system and network devices are adequately protected from cyber intrusion. For example, vulnerabilities are patched, systems are hardened, and access control is in place.
- **Disaster Recovery Plan** – systems and information must be recoverable in case of major IT outages. The plan and its recovery objectives need to support the business requirements.
- **Cyber Liability Insurance Coverage**

Increasingly not an option due to rising cost of record breaches. Throughout the world, companies are finding that data breaches are becoming common place and are extremely expensive to treat. With the exception of Germany, companies had to spend more on their investigations, notification and response when their sensitive and confidential information was lost or stolen. As revealed in the 2014 Cost of Data Breach Study: Global Analysis, sponsored by IBM, the average cost to a company was $3.5 million in US dollars and 15 percent more than...

---

\(^9\) http://www.healthit.gov/providers-professionals/security-risk-assessment
\(^{10}\) http://scap.nist.gov/hipaa/
\(^{11}\) http://www.himss.org/library/healthcare-privacy-security/risk-assessment
what it cost last year\textsuperscript{12}. \url{http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis}).

Entities should consider appropriate limits of coverage and should ensure coverage includes items such as:

\footnotesize
\begin{itemize}
\item \textsuperscript{12} \url{http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis}
Dictionary of Acronyms

- BAA - Business Associate Agreement
- HIPAA - Health Insurance Portability and Accountability Act of 1996
- ePHI - Electronic Personal Health Information
- IPS – Intrusion Protection System
- DLP – Data Loss Prevention
- OCR – Office of Civil Rights
- OIG – Office of Inspector General
- NIST – National Institute of Standards and Technology
- HIMSS – Healthcare Information and Management Systems Society
- MU – Meaningful Use
- CEHR - Certified Electronic Health Record

Acknowledgement

NHPCO would like to acknowledge and thank the provider members of the NHPCO HIPAA Security Best Practices Work Group who developed this resource:

- Jean Acevedo, Acevedo Consulting
- Croswell Chambers, Hospice of the Bluegrass
- Greg Kite, Consolo Services
- Gina Mazza, Fazzi Associates

Resources:

1. Office for Civil Rights (OCR), [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa)
