Security Risk Analysis Report

<Organization Name>

<Organization Address>

Created date:

<Date>

Prepared by:

**Table of Contents**

[I) **Executive Summary** 4](#_Toc325100460)

[II) **Introduction** 6](#_Toc325100461)

[A) *Purpose* 6](#_Toc325100462)

[B) *Scope* 6](#_Toc325100463)

[C) *System Mission* 6](#_Toc325100464)

[III) **Risk Analysis Approach** 6](#_Toc325100465)

[A) *Methodology* 6](#_Toc325100466)

[B) *Participants on the Risk Analysis Team*: 7](#_Toc325100467)

[C) *Data Collection Phase.* 7](#_Toc325100468)

[D) *Risk Assessment Tools & Techniques.* 7](#_Toc325100469)

[IV) **System Characterization** (Step 1) 8](#_Toc325100470)

[A) *System Contacts & Authorizing Official* 9](#_Toc325100471)

[B) *System Related Information* 9](#_Toc325100472)

[V) **Threat and Vulnerability Identification** (Steps 2 & 3) 9](#_Toc325100473)

[A) *HIPAA Security and HITECH related security requirements Policies and Procedures**Risk Assessment* 9](#_Toc325100474)

[B) *General Threats & Vulnerabilities* 9](#_Toc325100475)

[VI) **Control Analysis** (Step 4) 9](#_Toc325100476)

[VII) **Risk Likelihood** (Step 5), **Impact Analysis** (Step 6), & **Determination** (Step 7) 10](#_Toc325100477)

[VIII) **Summary – Risk Management Recommendations** 10](#_Toc325100478)

[A) *Risk Mitigation Strategy* 10](#_Toc325100479)

[B) *Evaluate and Prioritize Risks* 10](#_Toc325100480)

[C) *Identify Controls to Mitigate or Eliminate Risks* (Step 8) 10](#_Toc325100481)

[IX) **Risk Mitigation** 11](#_Toc325100482)

[B) *Ongoing Monitoring* 11](#_Toc325100483)

[X) **Results Documentation** (Step 9) 11](#_Toc325100484)

[**Appendix A: Threat Identification Overview** 13](#_Toc325100485)

[**Appendix B: Risk Calculation Worksheet & Risk Scale and Necessary Actions** 14](#_Toc325100486)

[**Appendix C: Risk Likelihood, Risk Impact, and Risk Level Definitions** 15](#_Toc325100487)

[**Appendix D: NIST Risk Mitigation Methodology Activities** 16](#_Toc325100488)

[**Appendix E: Security-Related Policies and Procedures** 17](#_Toc325100489)

[**Appendix F: Supplemental Resources** 18](#_Toc325100490)

1. **Executive Summary**

<Organization> recognizes the best, most up-to-date health information is without value unless it is pertinent and accessible to the people it is meant to serve. The Risk Analysis Team has been tasked to conduct a security risk analysis (risk analysis) of <Organization>. This Risk Analysis Report summarizes the risk assessment completed. Completing the risk assessment offered us the opportunity to assess the vulnerabilities that are exploited by threats internal and external to <Organization>.

The scope of this risk analysis effort was limited to the security controls applicable to the <Organization> environment relative to its conformance with the Health Information Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). These minimum security requirements address general security controls in the areas of policies, procedures, computer hardware and software, patient data, operations, administration, management, information, facility, communication, personnel, and contingency. The purpose of this risk assessment was to identify conditions where Electronic Protected Health Information (ePHI) could be disclosed without proper authorization, improperly modified, or made unavailable when needed. This information is then used to make risk management decisions on whether current safeguards are sufficient, and if not, what additional actions are needed to reduce risk to an acceptable level.

This risk analysis was conducted based on many of the methodologies described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* (NIST SP 800-30). NIST SP 800-30 uses a nine step process to determine the extent of potential threats and the risk associated with systems. The methodology used to conduct this risk analysis is qualitative, and no attempt was made to determine any annual loss expectancies, asset cost projections, or cost-effectiveness of security safeguard recommendations.

As defined in NIST SP 800-66, a risk is the potential impact that a threat can have on the confidentiality, integrity, and availability of ePHI by exploiting a vulnerability. While it is not possible to be absolutely certain that all risks have been identified, the Risk Analysis Team identified as many as possible known to the organization at the time the assessment was done. This risk analysisidentified (#) of vulnerabilities: (#) were rated **High**, (#) were rated **Moderate**, and (#) were rated as **Low**. Vulnerabilities are weaknesses that may be exploited by a threat or group of threats. These vulnerabilities can be mitigated by taking measures to implement the recommended actions/controls (safeguards). Safeguards are security features and controls that, when added to or included in the information technology environment, mitigate the risk associated with the operation to manageable levels. A complete discussion of the vulnerabilities and recommended safeguards are found in the HIPAA Risk Assessment.

If the safeguards recommended in this risk analysis are not implemented, the result could be modification or destruction of data, disclosure of sensitive information, or denial of service to the users who require the information on a frequent basis.

1. **Introduction**
   1. *Purpose*

The purpose of this risk analysis, based on compliance with HIPAA and HITECH related security requirements, is to evaluate the adequacy of <Organization>’s security controls. This risk analysis provides a structured qualitative assessment of the operational environment. It addresses threats, vulnerabilities, risks, and safeguards. The assessment recommends cost-effective safeguards to mitigate threats and associated exploitable vulnerabilities.

* 1. *Scope*
     1. The scope of this risk analysis assesses the system’s use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threats internal and external to the organization and patients’ electronic protected health information (ePHI). If exploited, these vulnerabilities could result in:
        1. Unauthorized disclosure of data
        2. Unauthorized changes to the system, its data, or both
        3. Temporary or permanent loss or corruption of data
        4. Denial of service, access to data, or both to authorized end users
        5. Loss of financial cash flow
        6. Loss of physical assets or resources
        7. Noticeable negative affect on the organization’s mission, reputation, or interest
        8. Human death or serious injury
     2. This Risk Analysis Report evaluates the ***confidentiality*** (protection from unauthorized disclosure of system and data information), ***integrity*** (protection from improper modification of information), and ***availability*** (loss of access) of the system. Recommended security safeguards will allow management to make decisions about security-related initiatives to implement to reduce or eliminate identified risks.
  2. *System Mission*

<Insert Organization’s mission>

1. **Risk Analysis Approach**
   1. *Methodology*
      1. The risk analysis methodology and approach was conducted using guidelines in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. The assessment is broad in scope and evaluates security vulnerabilities affecting the confidentiality, integrity, and availability of ePHI. The assessment recommends appropriate security safeguards, permitting management to make knowledge-based decisions about security-related initiatives to implement to reduce or eliminate identified risks. The methodology addresses the following types of controls:
         1. Management Controls: Management of the information technology (“IT”) security system and the management and acceptance of risk.
         2. Operational Controls: Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls.
         3. Technical Controls: Hardware and software controls providing automated protection to the system or applications (technical controls operate within the technical system and applications).
      2. This Risk Analysis Approach section details the risk analysis process performed during this effort.
   2. *Participants on the Risk Analysis Team*:
      1. < Name(s), Title(s), Organization Name>
      2. < Name(s), Title(s), Organization Name>
      3. < Name(s), Title(s), Organization Name>

Potential team members:

* + 1. < Name(s)>, Information Security Officer, <Organization Name>
    2. < Name(s)>, Physical Plant Security Officer, <Organization Name>
    3. < Name(s)>, Systems Analyst, <Organization Name>
    4. < Name(s)>, Privacy Officer, <Organization Name>
    5. < Name(s)>, Risk Manager, <Organization Name>
    6. < Name(s)>, Compliance Officer, <Organization Name>
    7. < Name(s)>, Chief Information Officer, <Organization Name>
    8. < Name(s)>, Security/technology subject matter expert (such as an IT Consultant), <Organization Name>
    9. < Name(s)>, Any other individual knowledgeable about your privacy, security, and HITECH policies, procedures, training program, computer system set up, and technical security controls, <Organization Name>
  1. *Data Collection Phase.*

The data collection and assessment phase included identifying and interviewing key personnel within the organization and conducting document reviews:

* + 1. Interviews focused on the operating environment.
    2. Document reviews provided the Risk Analysis Team with the basis on which to evaluate compliance with security policies and procedures.
  1. *Risk Assessment Tools & Techniques.*

The following tools and techniques were utilized for the risk assessment:

* + 1. Threat and Vulnerability Identification.
       1. The Risk Analysis Team used NIST SP 800-30 as a basis for threat and vulnerability identification. Refer to Appendix A for the Threat Statement, definitions, and Threat Sources considered.
       2. Through the interview process, “most likely” system and location-specific threats and vulnerabilities were identified. A thorough understanding of the current security controls (technical & nontechnical) in place for an organization helps the organization identify opportunities to reduce the list of vulnerabilities, as well as the realistic probability of a threat attacking ePHI.
       3. Considerations included previous security incident reports, system break-in attempts, and system down times.
    2. Risk Calculation Worksheet: Converts the vulnerabilities into risks based on the following methodology (refer to Appendix B):
       1. Categorizing vulnerabilities
       2. Pairing with threats
       3. Assessing the probability of occurrence and possible impact
    3. Risk Level Identification: The Risk Analysis Team determined the degree of risk to the system. Risks were ranked based on risk tolerance and objectives which are important to the organization. Vulnerabilities may be identified as individual risks, or may be combined into a single risk based upon likelihood and impact. The determination of risk for a particular threat source was expressed as a function of the following:
       1. Likelihood Determination: The following factors were considered when calculating the likelihood that a vulnerability might be exploited by a threat (refer to Appendix C for likelihood determination definitions used):
          1. Threat source motivation and capability
          2. Type of vulnerability (flaw or weakness)
          3. Existence and effectiveness of current controls
       2. Impact Analysis: The impact of a security event is the loss or degradation of any, or a combination of any, of the following three security goals, based on successful exploitation of a vulnerability (refer to Appendix C for impact determination definitions):
          1. Loss of Confidentiality
          2. Loss of Integrity
          3. Loss of Availability
       3. Risk Level Determination: The risk determination levels calculated represent the likelihood, degree, and level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised (refer to Appendix B for risk level definitions).
    4. Risk Mitigation: After reviewing identified risks, a risk mitigation action plan was developed. Refer to Appendix D for recommended NIST Risk Mitigation Methodology Activities.
    5. Security Policies and Procedures (P&Ps): Refer to the attached list of the organization’s current security-related policies and procedures in Appendix E.
    6. Supplemental Resources: Any other documents, comments, and other materials that were utilized or relevant to the risk analysis are included in Appendix F.

1. **System Characterization** (Step 1)

In this step, the Risk Analysis Team defined the boundaries of the IT system, along with the resources and information that constitute the system, its connectivity, and any other elements necessary to describe the system. Dependencies were clarified. Sensitivity/criticality of the system and data was also determined.

* 1. *System Contacts & Authorizing Official*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Business Contact(s)** (Responsible for formally accepting each recommended control or rejecting it and providing an alternative) | **Security Official**  (HIPAA 164.308(a)(2)) | **Authorizing Official(s)** (Authorizedto make an informed decision about authorizing the system to operate) |
| **Name** | - | - | - |
| **Title** | - | - | - |
| **Address** | - | - | - |
| **Phone** | - | - | - |
| **E-mail** | - | - | - |
| **IT Systems** | -<List Systems> | -<List Systems> | -<List Systems> |

* 1. *System Related Information*

The Risk Analysis team completed an analysis of the environment by reviewing and updating a Network diagram as well as an Inventory Asset List. This includes is a list of all systems, applications, communication systems, and hardware that store, process, or transmit ePHI and their interdependencies, including the EHR, Practice Management System, lab systems, coding systems, etc. These documents are maintained by and may be requested from the <Security Official>.

1. **Threat and Vulnerability Identification** (Steps 2 & 3)
   1. *HIPAA Security and HITECH related security requirements Policies and Procedures**Risk Assessment*

Refer to the HIPAA Risk Assessment completed on <xx/xx/xxxx> which summarizes policies, procedures, safeguards, and controls in place currently used to protect the confidentiality, integrity, and availability of ePHI as required by HIPAA and HITECH. The HIPAA Risk Assessment is maintained by and may be requested from the <Security Official>.

* 1. *General Threats & Vulnerabilities*

The HIPAA Risk Assessment – Threats document completed on <xx/xx/xxxx> includes potential threats and vulnerabilities and the risks associated with each.

1. **Control Analysis** (Step 4)

Current technical and nontechnical safeguards and controls used are included in the Current State/Comments column of the HIPAA Risk Assessment. Included in the analysis are preventative controls that inhibit attempts to violate security policies, as well as detective controls to warn of violations and attempted violations of security policies.

1. **Risk Likelihood** (Step 5), **Impact Analysis** (Step 6), & **Determination** (Step 7)
   1. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls, as well as the level of adverse impact that would result from a threat successfully exploiting a vulnerability.
   2. The likelihood that a potential vulnerability may happen, the impact that would result from a successful threat exploiting a vulnerability, and the risk determination (level of risk) were determined by using the NIST SP 800-30 Risk Calculation Worksheet in Appendix B and the Risk Likelihood, Risk Impact, and Risk Level Definitions in Appendix C.
   3. Refer to the results in the Risk Mitigation Implementation Plan.
2. **Summary – Risk Management Recommendations**
   1. *Risk Mitigation Strategy*

Risk mitigation involves evaluating, prioritizing, and implementing appropriate safeguards to reduce identified risks during the risk analysis process. The goal is to ensure the confidentiality, integrity, and availability of ePHI.

* + 1. Because the elimination of all risk is impractical, senior management, the organization’s Risk Analysis Team, and business managers will assess control recommendations, determine the acceptable level of residual risk, perform cost-benefit analyses, and approve implementation of those controls that have the greatest risk reduction impact in the most cost-effective manner to meet Security regulation requirements.
    2. Refer to Appendix D for NIST Risk Mitigation Activities, and to NIST SP 800-30 for additional methods to mitigate known and potential risks.
  1. *Evaluate and Prioritize Risks* 
     1. Safeguarding recommendations are the results of the risk analysis process, and provide a basis by which the Authorizing Official can evaluate and prioritize the identified risks and their associated controls.
     2. The Business Contact will work with the Authorizing Official to develop a Risk Mitigation Implementation Plan, including recommended controls. At this point, the System Contacts can collaborate to either accept the control recommendations, provide alternative suggestions, or reject the control recommendations and accept the risk.
        1. Refer to the Risk Mitigation Implementation Plan in the HIPAA Risk Assessment document for risk mitigation strategies.
        2. The Risk Mitigation Implementation Plan includes risks identified as medium to high priority levels. Low risk priority levels are not included as they are assumed to currently be organizationally accepted risks, but should be evaluated once the medium to high priority risk levels are addressed.
  2. *Identify Controls to Mitigate or Eliminate Risks* (Step 8)
     1. Controls, safeguarding recommendations, and/or actions that could reduce or eliminate the likelihood and/or impact of the associated risks have been identified and documented in the Risk Mitigation Implementation Plan.
     2. The Risk Analysis Team considered all of the following factors when recommending controls and solutions to minimize or eliminate risks (note: these are not in order of importance):
        1. Sensitivity of the data and the system
        2. Previous security incidents
        3. Safety, reliability, and/or effectiveness of controls
        4. System compatibility and dependencies
        5. Incompatibilities with other controls
        6. Legislation and regulations
        7. Organizational policies and procedures
        8. Operational impact
        9. Budgetary constraints
        10. Other resource constraints

1. **Risk Mitigation**
   1. *Implement Controls*
      1. Implement the controls that have been approved and budgeted by senior management, in order of priority (e.g. greatest impact first)
      2. Wherever possible, objectively measure the effective reduction in risk as a result of the control, and document this result
      3. Identify and resolve unintended problems associated with the control implementation
   2. *Ongoing Monitoring*
      1. Ongoing monitoring will be done to determine if new risks have developed.
      2. Ongoing monitoring includes, but is not limited to, the following:
         1. Conduct periodic reviews/mini risk assessment of security controls to measure their ongoing effectiveness and document the results.
         2. Perform periodic system audits/mini risk assessment, such as before upgrading and purchasing new systems, with significant personnel changes, implementing new security policies, etc. When a new or upgraded system is introduced to the organization, a review must be done in order to determine if a new risk analysis must be conducted due to the introduction of new assets in the organization.
         3. After conducting ongoing risk evaluation mitigate new risks identified.
      3. Complete a Risk Analysis/Assessment on a scheduled basis (e.g. every year or as needed to meet the organization’s risk needs, regulatory requirements, other applicable Standards such as PCI, etc.).
2. **Results Documentation** (Step 9)
   1. Results of the risk analysis are documented in this report, in the HIPAA Risk Assessment document, and in the Risk Mitigation Implementation Plan.
   2. A summary of the Risk Analysis and the Risk Mitigation Implementation Plan will be provided to management to:
      1. help them understand the risks;
      2. help make decisions on policy, procedure, budget, and system operational and management changes; and
      3. allocate resources to reduce and correct potential and known risks.
   3. All risk mitigation strategies and processes will be fully documented, including:
      1. Those that have been approved, budgeted, and implemented
      2. Those that have been approved and budgeted, but not yet implemented
      3. Those that have been approved, but are not yet budgeted
      4. Those that were not approved (including the reason)
   4. The above documentation will all be maintained for at least six years by <Insert responsible individual>.

**Appendix A: Threat Identification Overview**

*This information was taken directly from the NIST SP 800-30*

**Threat Identification Overview**

NIST SP 800-30 describes the identification of the threat, the threat source and threat action for use in the risk assessment process. The following is a definition for each:

1. **Threat** – The potential for a particular threat-source to successfully exercise a particular vulnerability. *(A* ***vulnerability*** *is a flaw or weakness that can be accidentally triggered or intentionally exploited and result in a security breach or violation of policy)*.
2. **Threat Source** – Any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human or environmental which can impact the organization’s ability to protect ePHI.
3. **Threat Action** – The method by which an attack might be carried out (e.g., hacking, system intrusion).

**Threat Sources**

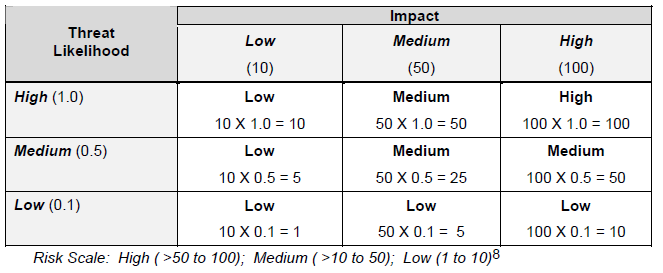
A threat-source is any circumstance or event with the potential to cause harm to an information technology system and its processing environment. Common threat-sources are natural, human, and environmental. Threat sources can threaten the facilities, systems, data, personnel, utilities, and physical operations and how they function, their ability to perform their responsibilities/duties, or exposes them to disruption and/or harm.

**Appendix B: Risk Calculation Worksheet & Risk Scale and Necessary Actions**

*This information was taken directly from the NIST SP 800-30*

**Risk Calculation Worksheet**

The following NIST SP 800-30 calculation worksheet provides instructions for determining the overall risk level for this report. History of past occurrences can help determine the threat likelihood level and impact level can take into account, financial impact, employee safety, and many other factors.

****

**Risk Scale and Necessary Actions**

The following Risk Scale and Necessary Actions table presents actions that NIST SP 800-30 recommends senior management (the mission owners) must take for each risk level. [<Organization> to determine if this will be used, or another methodology].

|  |  |
| --- | --- |
| **Risk Level** | **Risk Description and Necessary Actions** |
| **High** | If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. |
| **Medium** | If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. |
| **Low** | If an observation is described as low risk, the system’s Designated Approving Authority (DAA) must determine whether corrective actions are still required or decide to accept the risk. |

**Appendix C: Risk Likelihood, Risk Impact, and Risk Level Definitions**

*This information was taken directly from the NIST SP 800-30*

|  |  |
| --- | --- |
| **Level** | **Likelihood Definitions** |
| **High**  (1.0) | The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. |
| **Moderate**  (.5) | The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. |
| **Low**  (.1) | The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. |

Impact Analysis: The adverse impact of a security event in terms of loss or degradation of any, or a combination of any, of the following three security goals, resulting from successful exploitation of a vulnerability:

* Loss of Confidentiality – Impact of unauthorized disclosure of confidential information (ex. Privacy Act). Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.
* Loss of Integrity – Impact if system or data integrity is compromised by intentional or accidental changes to the data or system.
* Loss of Availability – Impact to system functionality and operational effectiveness should systems be unavailable to end users.

| **Magnitude of Impact** | **Impact Definitions** |
| --- | --- |
| **High**  (100) | Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury. |
| **Moderate**  (50) | Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impeded an organization’s mission, reputation, or interest; or (3) may result in human injury. |
| **Low**  (10) | Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an organization’s mission, reputation, or interest. |

Risk Level Determination: These levels represent the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised:

* The likelihood of a given threat source’s attempting to exercise a given vulnerability.
* The magnitude of the impact should a threat-source successfully exercise the vulnerability.
* The adequacy of planned or existing security controls for reducing or eliminating risk.

| **Magnitude of Impact** | **Risk Level Definitions** |
| --- | --- |
| **High**  (>50-100) | There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. |
| **Moderate**  (>10-50) | Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. |
| **Low**  (1-10) | The system’s Authorizing Official must determine whether corrective actions are still required or decide to accept the risk. |

**Appendix D: NIST Risk Mitigation Methodology Activities**

*This information was taken directly from the NIST SP 800-30*

|  |  |  |
| --- | --- | --- |
| **Input** | **Risk Mitigation Activities** | **Output** |
| Risk levels from the risk assessment report | **Step 1**. Prioritize Actions | Actions ranking from high to low |
| Risk assessment report | **Step 2**. Evaluate Recommended Control Options   * Feasibility * Effectiveness | List of possible controls |
|  | **Step 3**. Conduct Cost-Benefit Analysis   * Impact of implementing * Impact of not implementing * Associated costs | Cost-benefit analysis |
|  | **Step 4**: Select Controls | Selected controls |
|  | **Step 5**: Assign Responsibility | List of responsible persons |
|  | **Step 6**: Develop Safeguard Implementation Plan   * Risks and Associated Risk Levels * Prioritized Actions * Recommended Controls * Selected Planned Controls * Responsible Persons * Start Date * Target Completion Date * Maintenance Requirements | Safeguard implementation plan |
|  | **Step 7**: Implement Selected Controls | Residual risks |

**Appendix E: Security-Related Policies and Procedures**

**Appendix F: Supplemental Resources**

1. NIST SP 800-30 Risk Management Guide for Information Technology Systems, July 2002 <http://csrc.nist.gov/publications/PubsSPs.html>
2. NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule <http://csrc.nist.gov/publications/PubsSPs.html>
3. For instructions on how to submit notice of a breach of PHI to the Secretary of HHS, along with more information about HIPAA:

* <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

1. Sample policies and procedures are available and updated as the laws change on the HIPAA COW website: [www.hipaacow.org](http://www.hipaacow.org)
   * HIPAA COW documents include the State of Wisconsin regulations.
2. Publications providing additional guidance on how to meet each of the statute requirements: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>
3. HIPAA Security Guidance Document for Remote Use, from the Department of Health and Human Services (HHS) and the Office of Civil Rights (OCR) <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf>