

DRAFT
HIPAA SECURITY SUMMIT
GUIDELINES

Last Revision: June 26, 2000

Table of Contents

1.	INTRODUCTION.....	1
1.1	Background On The Summit.....	1
1.2	HIPAA Security	1
2.	BUSINESS IMPACT ANALYSIS	2
2.1	Purpose of the business impact analysis.....	2
2.1.1	Organization awareness and initial roles and responsibilities	2
2.1.2	Executive and senior management buy-in.....	3
2.1.3	Develop an awareness program for all affected staff	3
2.1.4	Establish your security implementation team.....	3
2.2	Establish security training that is tailored to various staff, agents and contractors.....	4
2.2.1	Determining your BIA Scope	5
2.2.2	Baseline Assessment	5
2.3	GAP Analysis: Current Environment Vs Regulatory Requirements.....	5
2.4	Administrative Procedures	6
2.4.1	Certification.....	7
2.4.2	Chain of Trust Partner Agreements.....	7
2.4.3	Contingency Plan	8
2.4.4	Formal Mechanism for Processing Records.....	8
2.4.5	Information Access Control	9
2.4.6	Internal Audit	10
2.4.7	Personnel Security.....	11
2.4.8	Security Configuration Management	12
2.4.9	Security Incident Procedures.....	12
2.4.10	Security Management Process.....	13
2.4.11	Termination Procedures	15
2.4.12	Training	15
2.5	Physical Safeguards.....	16
2.6	Technical Services and Mechanisms.....	16
2.7	Electronic Signature	18
2.7.1	Risk Assessment.....	18
3.	SPECIFIC GUIDELINES FOR HIPAA SECURITY REQUIREMENTS.....	21
3.1	Administrative Procedures for Data Integrity, Confidentiality and Availability §.308 (A).....	21
3.1.1	Certification §.308(a)(1).....	21
3.1.2	Chain of trust partner agreement §.308(a)(2).....	22
3.1.3	Contingency plan §.380 (a)(3).....	23

3.1.4	Formal mechanism for processing records §.308(a)(4).....	23
3.1.5	Information access control §.308(a)(5)	24
3.1.6	Internal audit §.308(a)(6)	27
3.1.7	Personnel security §.308(a)(7).....	28
3.1.8	Security Configuration Management §.308(a)(8)	28
3.1.9	Security incident procedures §.308(a)(9)	29
3.1.10	Security management process §.308(a)(10)	29
3.1.11	Termination procedures §.308(a)(11).....	30
3.1.12	Training §.308(a)(12)	31
3.2	Physical Safeguards For Data Integrity, Confidentiality And Availability §.308 (B).....	31
3.2.1	Assigned security responsibility §.308(b)(1)	31
3.2.2	Media controls §.308(b)(2).....	32
3.2.3	Physical Access Controls §.308(b)(3)	32
3.2.4	Policy/guideline on work station use §.308(b)(4)	33
3.2.5	Secure workstation location §.308(b)(5)	33
3.2.6	Security awareness training §.308(b)(6).....	34
3.3	Technical Security Services §.308(c).....	35
3.3.1	Access Control §.308(c)(1)	35
3.3.2	Audit Controls §.308(c)(2)	36
3.3.3	Authorization Control §.308 (c)(3).....	36
3.3.4	Data Authentication §.308 (c)(4).....	38
3.3.5	Entity Authentication §.308 (c)(5)	38
3.4	Technical Security Mechanisms §.308(d)	41
3.4.1	Communications and Network Controls §.308(d)(1)	41
3.5	Electronic Signature §.310	42
3.5.1	Digital (Electronic) Signature §.310.....	42
4.	ON-GOING MONITORING AND REPORTING MODEL.....	44
5.	GENERAL GUIDELINES TO MONITORING AND REPORTING	48
	Appendix A:	51
	HIPAA Security Requirements Control Type Mapping.....	51
	Appendix B	53
	Reference Material List	53
	Appendix C	56
	Business Continuity Planning and Disaster Recovery	56

Revision History

Document	Date
Original 1.0	November 30, 1999
Version 1.1	January 12, 2000
Version 1.2	June 26, 2000

SPONSORS

The organizers and participants in the HIPAA Security Summit are very grateful to our corporate sponsors who provided the funding to underwrite the expense of convening the Summit, the distribution of the Summit Report(s), and future HIPAA Security Implementation Education Programs.

The Summit sponsors are:

COMPAQ
James Kooney
P.O. Box 692000
Houston, TX 77269-2000
(603) 893-2820

IBM Corporation
Shannah Koss
1301 K Street, NW
Washington, DC 20005
(202) 515-5044
shakoss@us.ibm.com

KSM Healthcare Resources
Ms. Terri Kinney
11711 N. Meridian Street
Suite 800
Indianapolis, IN 46240-0857
(317) 580-2000
tkinney@ksmcpa.com

Johns Hopkins Hospital
Bill Rider
1830 East Monument Street
Baltimore, MD 21205
(410) 955-1691
brider@jhmi.edu

Microsoft Corporation
Chuck Reeves
One Microsoft Way
Redmond, WA 98052
(425) 703-7621
creeves@microsoft.com

Shared Medical Systems
Jon Zimmerman
51 Valley Stream Parkway
Malvern, PA 19355
(610) 219-8289
jon.zimmerman@smed.com

TRW Healthcare Solutions
Ted Park
P.O. Box 1310
San Bernardino, CA 92402
(909) 382-6160
ted.park@trw.com

The ideas, recommendations, and information provided in the HIPAA Security Summit Guidelines do not necessarily represent the opinions or views of the HIPAA Security Summit sponsors.

1. INTRODUCTION

The HIPAA Security Summit was a working forum held on October 11-13, 1999 in Baltimore, MD, and was intended to produce industry developed methodologies and recommendations to assist providers, payers, clearinghouses and related affected health care organizations with their efforts to comply with the HIPAA security regulations.

The information contained in this document is intended to be used only as a guideline for each organization's development of security policies and procedures. Each organization will need to assess their own specific environment to determine what security features will need to be implemented in order to meet the security policies and procedures developed by the organization.

1.1 Background On The Summit

Based on their own efforts to increase awareness and prepare for HIPAA security, Johns Hopkins recognized the need for greater clarity in striving to implement a "HIPAA-Ready" security environment. The Health Care Financing Administration (HCFA) concurred with their assessment and encouraged Johns Hopkins to convene other industry leaders and facilitate a forum that spurred industry dialogue and that would ultimately provide much needed security guidance. Johns Hopkins teamed up with SMS to organize the HIPAA Security Summit - comprised of recognized leaders - to help the industry arrive at consensus in preparing for HIPAA security.

During the Summit, the participants reviewed existing industry materials, filled information gaps and clarified significant outstanding issues regarding HIPAA security implementation. This document is the output of the Security Summit.

1.2 HIPAA Security

The Security and Electronic Signature Standards have set the minimum level or "Floor" of security for individually identifiable health information maintained in or transmitted by health care organizations. These standards or controls, which make up this minimum level of security, are outlined in subsequent sections of this guide. Currently, many organizations are assessing their current security infrastructure to determine where it meets and where it does not meet the Federal security standards. When areas of an organization's security infrastructure do not meet the minimum-security standards, organizations are developing solutions to bring those aspects of their infrastructure up to the minimum level. Whether your organization's current security infrastructure meets the minimum security standards or not, every organization covered by the standards will need to have the ability to demonstrate that effective management, operational, and technical controls are in place and comply with the minimum level.

2. BUSINESS IMPACT ANALYSIS

2.1 Purpose of the business impact analysis

The purpose of a business impact analysis for HIPAA security is to determine the magnitude of the regulatory impact on an organization and to establish the scope of an organization's compliance effort. In the process of undertaking this initial analysis a number of the HIPAA security requirements can be satisfied if appropriately conducted and documented, these include: assigning security responsibilities; asset inventory, risk analysis, application and criticality analysis; and documentation requirements.

2.1.1 Organization awareness and initial roles and responsibilities

The HIPAA security requirements are very comprehensive and extend far beyond the Information technology environment. Consequently in larger organizations involvement in the compliance effort will require involvement of staff from many parts of the organization. Historically security has been housed in IT organizations without much visibility or authority. The security staff and their responsibilities will need to evolve to meet the HIPAA mandates.

Before an organization can start any of its initial security compliance including the business impact analysis, the organization must generate sufficient awareness throughout the organization to complete the analysis task and subsequent security activities. Security experts agree that a number of activities to ensure adequate support throughout the enterprise are needed.

Recommended activities include the following:

- Establish a framework for executive and senior management buy-in
- Develop an awareness program for all affected staff
- Establish your security implementation team
- Establish security training that is tailored to various staff, agents and contractors

Smaller or simple organizations will have fewer people involved and may undertake their HIPAA activities in a more tailored fashion. An example of a simpler organization an the likely drivers of a HIPAA effort is detailed below:

Definition of a **simple** environment:

1. Single site
2. Independent
3. Single lead practitioner (probably has RNs or assistant practitioners)
4. Users - 10 or less
5. Only dial up access to 3rd party networks
6. one system, multiple applications
7. 10 or less workstations
8. one platform, likely windows
9. has an existing confidentiality policy (not security)
10. Access control limited to ID and password, lock doors and cabinets
11. No assigned security lead

In simple example:

- office manager to lead effort
- partner w/IT person
- get vendors onboard
- professional organization input
- assume no or low technical experience

2.1.2 Executive and senior management buy-in

Organizations that have begun the impact analysis process and in anticipation of needed management and implementation support to carry out this phase and subsequent compliance activity know that a critical first step is gaining management buy in. Four activities to help gain the needed buy in are suggested: a brief high level organization impact analysis; a compliance overview; A detail briefing and a written HIPAA synopsis. These activities may or may not be appropriate to some or all of you management.

2.1.3 Develop an awareness program for all affected staff

An initial awareness program is also appropriate for all affected staff within the organization. There are many ways to drive the awareness program that should be tailored to what works in a given organization and what is appropriate to the size of the organization. Different audiences may best be reached through different media.

Questions to consider for your organization when evaluating these approaches include: what has worked in the past for awareness ad education campaigns; Is there a combination of approaches that works best; who should the message be coming from; and, what incentives could be established to encourage participation.

The awareness program should also be developed in anticipation of initial and on-going training that will be required under the HIPAA regulations. The initial awareness efforts should also be planned and conducted with some forethought on who will need to be a part of the security implementation team for the initial impact analysis phase and later phases.

2.1.4 Establish your security implementation team

Deciding who will be needed and able to manage and implement the security compliance effort may not be simple or easily accomplished. Many organizations are tasking their CIO, or someone within the CIO's organization. Due to the comprehensive nature of the regulations other individuals will need to be heavily involved and sponsorship of the effort beyond the CIO may have greater success. One emerging management model use the combination of the CIO and VP of corporate compliance as the joint sponsors of the HIPAA security initiative.

Regardless of who leads the effort a number of representatives from various parts of the organization will need to be involved in various capacities. The responsibilities that these individuals represent may be housed in one or two people in a small organization, but people with these responsibilities will need to be involved in the analysis and decision making for HIPAA security.

Involvement will be needed for all phases of implementation. There may be considerable overlap, only one team, or one or two people depending on the size of the organization. Steering committees are likely to be most important in large complex organizations where management is decentralized. The term business unit covers a wide range of possible organizational departments or responsibilities that may or

may not be present in a given organization. The term is meant to include all business processes that will be affected by the requirements and therefore may need to be involved in the analysis and decisions.

The following is a sample list of Business unit representatives:

- Human Resources
- Medical Records
- Risk Management
- Legal/compliance
- Research
- Ethics
- IT staff (network, system)
- Nursing informatics
- Financing/business office
- Accreditation group
- Provider liaison (for payers)
- Customer Service
- Government relations
- Facilities Manager
- Volunteer Services
- Critical (Key) Asset owners
- Major department managers,
e.g., claims, managed care, research, pharmacy, lab
- Physician advocates (for providers)
- Remote site and ancillary facility
- Patient Care Operations

2.2 Establish security training that is tailored to various staff, agents and contractors

Security training will be a requirement throughout an organization's compliance effort and is an ongoing requirement for a HIPAA security program. Ultimately organizations are responsible for not only training their own personnel, but their agents and contractors that have access to health information subject to HIPAA security. Initial training will need to include a review of the HIPAA requirements. Ultimately however, the training needs to be tailored to the specific security policies, processes and technology of your organization and to have the greatest impact should be tailored to the level of security responsibility for different segments of users . These could include the following: personnel that only have incidental exposure to systems and are not authorized users (cleaning crews, receptionists, volunteers); users with very limited access; users with substantial access; users that have explicit security roles e.g., determining access authorization; and, security and systems staff.

2.2.1 Determining your BIA Scope

Organizations need to determine the scope of their BIA activities. They can be narrowly focused on HIPAA compliance only or can look at overall business goals for all information assets, whether they are subject to HIPAA or not, and couch the analysis in a business strategy framework. Industry experts recommend looking at the cost-benefit of the BIA scope and to consider issues such as: cost savings; cost effectiveness or exposures including cost avoidance, data loss and the related business loss and overall breaches of security; and, potential benefits including leveraging standardization in your business environment, understanding an organization's vulnerabilities and making security a corporate initiative.

Organizations need to consider how to coordinate their transaction standards (EDI, code sets and identifiers) impact assessments with their security and privacy efforts. Although there is not tremendous overlap between security and the transaction standards initial analysis of business processes, strategic directions, building your HIPAA teams, and decisions on changes in you systems and business processes do overlap and will need to be coordinated.

In anticipation of the HIPAA privacy requirements it is recommended that organizations not distinguish or exclude their paper environment from the BIA particularly from a policy and process perspective.

Organizations should define the scope of their BIA effort before starting the data gathering for your analysis to determine the needed resources, roles and responsibilities. There are three main components to the BIA: a baseline assessment, a gap analysis and a risk analysis.

2.2.2 Baseline Assessment

The baseline assessment inventories a organization's current security environment with respect to policies, processes and technology. The scope of the BIA will drive how this should be done. If the BIA is narrowly tailored to HIPAA, the baseline assessment design can be driven by the regulatory framework. If however, an organization wants this to be integrated in their business processes and operations an organization might be better served to design the baseline to capture information in keeping with lines of business, departments or programs.

Capturing the baseline information along department, facility, or lines of business as well as for differing IT environments will support the appropriate level of detail that an organization will need for its gap analysis. Also defining which security components can be reviewed once because they are standardized throughout an organization will help avoid duplicate analysis, e.g., the WAN. It is however important to capture varying practices distinct from system capabilities, e.g., standard password assignment procedures, use and protocols does not mean that adherence is consistent

A HIPAA implementation feature can also be satisfied during the baseline assessment - the Security Configuration Management Inventory (the formal documented identification of hardware and software assets). Organizations will need to understand this inventory in order to know its potential vulnerabilities and determine what existing security capabilities reside in the assets as relevant. Using your Y2K asset inventory as a starting point will save time and resources. Organization then need to expand the inventory to incorporate HIPAA subject applications and information systems that may not have been included in the Y2K effort. Categorizing the inventory along the lines of the baseline assessment will also facilitate subsequent analysis.

2.3 GAP Analysis: Current Environment Vs Regulatory Requirements

Following the appointment of a person or persons to fill the role of assigned security responsibility (a HIPAA requirement) and creation of a cross-functional team to assist in development and oversight of HIPAA compliance initiatives, attention should be focused on the healthcare organization's current state of readiness relative to regulatory requirements. Qualitative measurement criteria should be developed as

a tool to evaluate the current environment for each of the security standards pursuant to identification of readiness gaps and potential vulnerabilities. The extent to which these gaps will be filled through remediation of processes or controls should be addressed by the **risk analysis**, required as a component of the security management process.

The measurement criteria suggested as part of the gap analysis could include rankings of current readiness weighed against HIPAA requirements, such as:

Scale:

- 0 No identified process or control**
- 1 Informal or partial process or control**
- 2 Process or controls implemented for many required HIPAA elements**
- 3 Process or controls fully implemented for all required HIPAA elements**
- 4 Process or controls exceed required HIPAA elements**

When preparing to perform the gap analysis, consideration should be given to the following:

- Each entity and line of business comprising the organization should be included in the readiness assessment, even if current security processes and controls vary widely or do not exist at all in some parts of the organization. Examples to include:
 - remote sites such as clinics, physician offices, home health agencies, SNFs
 - smaller lines of business or regional headquarters locations
 - home-based workers such as medical transcriptionists
 - A standard approach to evaluate differences throughout your environment should be established. Details as to where the gaps really are need to be captured. For instance saying an organization has only partial or informal controls is not sufficient detail to help determine how the gap would ultimately be filled. Instead stating that the mainframe environment has the necessary control, but the following remote sites are inadequate because... The design of an organization's baseline assessment by business process or department can help promote this standardized detail.
- Participants in the gap analysis should represent the entire organization and will need to include representatives from lines of business, legal/compliance, internal audit, information technology, training, human resources, facilities management, risk management. Typically, many of these participants will already be part of the cross-functional security team.

2.4 Administrative Procedures

This is the largest category of standards and relates primarily to policies, procedures and organizational practices dealing with the behavioral side of security. Significant input from non-technical resources across the healthcare organization will be required to adequately address potential gaps between current state and future readiness. The risk analysis can serve as the basis for determining the level of risk deemed acceptable to the organization and should drive the review of policy and procedures, as well as the selection process for enhanced security controls. Early determination should be made of the information assets requiring protection, as well as a formal assignment of responsibility and accountability for ownership and custody of such assets. In addition to information asset owners and custodians, other key resources who will play a role in performing the gap analysis for Administrative Procedures include: human resources professionals responsible for developing, implementing and enforcing personnel policy; legal and/or compliance staff; internal auditors with responsibility for reviewing system activity and developing certification guidelines; training professionals responsible for

development and implementation of personnel training programs; and information technology resources charged with contingency planning activities and other security functions requiring ongoing documentation.

A key to compliance is the requirement for complete and current documentation of all security measures in effect.

2.4.1 Certification

Pending HCFA's determination of requirements and logistics for conducting certifications by an external accrediting agency, healthcare organizations should prepare to self-certify that the appropriate security measures have been implemented.

Vulnerabilities in this area could include: lack of internal audit capability (no internal audit department) or constrained resources lacking availability to perform certification audits.

Specific issues for an organization to consider include:

- Do we have appropriate internal resources and skills to perform a self-certification (e.g. those skills from internal audit or compliance)? If no internal resources exist currently, can such skills be contracted externally from a professional organization, public accounting firm, or the like?
- What format will be used to document the results of a HIPAA security self-certification?
- What process is in place to handle remediation resulting from self-certification and the subsequent recertification?

2.4.2 Chain of Trust Partner Agreements

Ensuring that the same level of security will be maintained across the continuum of electronic transmission, chain of trust partner agreements should be instituted between healthcare organizations and those third parties with whom electronic health information is exchanged. Such contracts will provide the legal basis for maintaining consistent levels of data integrity and confidentiality. Issues to consider include:

- Have we solicited and engaged legal counsel to develop and review contract language for chain of trust partner agreements?
- How will we identify all parties to be included in the chain of trust contracts?
- How can we utilize and modify existing confidentiality agreements that are currently in place with third party electronic trading partners?
- How will we identify the data rights of the trading partners and incorporate such rights in the contract language?
- How will we determine our own security responsibility and the responsibility/accountability of our partners as part of the agreement?
- How will we identify the consequences of failure by either party to abide by the agreement?
- What monitoring techniques will be employed to ensure compliance by all parties subject to the agreements?
- How will we determine the audit points for which contracts will be reviewed for compliance?
- What procedure will be followed if a trading partner refuses to sign a chain of trust partner agreement with us?

2.4.3 Contingency Plan

A comprehensive contingency plan for responding to a system emergency will facilitate the assurance of continuity of key business systems and operations. Included is an **applications and data criticality analysis** used to assess sensitivity, vulnerability and security of key information assets, a **data backup plan** to ensure recovery of information lost or inaccessible, a **disaster recovery plan** to enable restoration of systems and data following a catastrophic event, an **emergency mode operation plan** to ensure operational continuity for some period of time, and **testing and revision procedures** to enable periodic updates and audits of all contingency plans.

Current state vulnerabilities in this area might include: no disaster plan in effect, or some disaster plan in effect covering only major enterprise systems; contingency plans left to the discretion of department managers to cover their departments, with no comprehensive plan in effect for the entire organization; or contingency plans in place that have not been updated recently and fail to cover all parts of the organization, including remote sites.

Contingency plans should be based on formal application and data criticality analysis assessments. Similar work products from Y2K could potentially serve as a starting point for this initiative. Plans should be regularly reviewed, tested and updated to account for changes in operations and address emergencies that affect physical sites and systems as well as data.

Issues to consider when developing contingency plans include:

- Is there a designated person(s) responsible for contingency planning in the organization? Are roles and responsibilities defined? Is there a formal sign-off and approval process?
- As part of an application and data criticality analysis, are systems, applications and modules listed and ranked for continuity prioritization? Is there a sequential order for restarting systems affected by an emergency? How is a minimal level of service defined and produced? How often is the criticality analysis reviewed and revised?
- On what basis is data backup performed (frequency, scope of backup)? Are data backups kept offsite? Do offsite locations have adequate security? Are data backups tested for retrieval and full restoration? Are all data backup procedures fully documented?
- Does the organization have a full or partial disaster recovery plan? Does the plan include an alternate (hot) site? What processes are in place to ensure periodic testing and revision of the disaster recovery plan? Is there a responsible, accountable disaster recovery team in place, or are resources assembled on an ad hoc basis in the event of a disaster?
- Does the emergency mode operation plan include notification procedures to affected personnel? Is there a documented, tested process for implementing downtime procedures, including the decision for invoking such procedures? Do procedures include checkpoint assessments of the status of the emergency and appropriate reporting to affected personnel?
- Are all contingency plans periodically reviewed, tested and revised? Is documentation maintained in all areas detailing 'lessons learned' from actual experiences with loss of business continuity?

2.4.4 Formal Mechanism for Processing Records

Processes should be implemented and documented to account for the flow of health information through an organization, from time of receipt or creation through manipulation and usage, storage, dissemination and transmission, and archival or disposal. Issues to be considered include:

- What process exists to govern the creation of health information, and how is that information validated for accuracy?

- If like data are created in multiple systems, what processes exist to determine the system of truth and how are discrepancies corrected when identified?
- What processes exist for determining who shall have the authority to change or manipulate data once created, and what audit trails exist to log such changes?
- What processes are in place to prevent unauthorized manipulation of data, and how are unauthorized changes logged and reported when they occur?
- What technical and administrative processes and mechanisms are in place to ensure storage of information? What parameters exist to govern how long data will be stored prior to its being archived or destroyed?
- What policies and procedures are in place to govern how health information will be disseminated within the organization that owns it and external to the organization? What policies dictate security accountability for data shared both internally and externally?
- What policies and processes are in place to protect data transmitted across internal and external networks? What governs secure transmission of health information across the internet or other open networks?
- What policies and procedures determine how health information will be disposed of securely, including destruction of media containing health information?

2.4.5 Information Access Control

This standard appears throughout the security regulations in a number of different contexts relating to personnel security requirements, physical safeguards, technical security services, and technical security mechanisms. As a component of the administrative procedures category, information access control is a required process in which a healthcare entity establishes and maintains formal, documented policies and procedures for granting different levels of access to healthcare information. Included are policies and procedures by which access is **authorized; established; and modified.**

Vulnerabilities in this area include ad hoc practices and/or incomplete policies and procedures for authorizing and establishing access to organizational systems; failure to include smaller, departmental systems in access control policies and practices; and broken processes to address modification and revocation of user access following job changes or termination.

Specific issues to be considered include:

- Do we currently have a documented access control policy?
- How is that policy communicated to all employees, physicians, researchers, volunteers, temporary staff, consultants and others who have access to health information?
- Does the existing policy cover the entire organization, including all sites, departments and corporate entities?
- Does the access control policy consider on-premise access as well as remote access?
- Does the policy consider only computer-based media, or other means of access including paper, fiche, voice, etc.?
- Does the existing policy speak to monitoring, enforcement and penalties to be utilized by the organization to ensure access controls are not violated?
- Does the policy state a need-to-know accountability for information access?

- What mechanism will be instituted to grant access to health information on all media, to include electronic and paper-based media?
- Are data owners defined for the various data elements or categories of patient information? Do data owners determine or participate in determining who should have authorized access to that data?
- Do procedures define the authorization requirements for various forms of patient information, and is special authorization required for more sensitive information (i.e. psychiatry, infectious diseases, genetic disorders)?
- Is access authorization for each employee, physician, researcher, volunteer, temporary employee, and third party contractor documented and maintained? Does this authorization have signoff of the appropriate data owner and level of management?
- Are ALL systems and applications containing health information subject to the same access control policies and procedures, or are some distributed systems outside the scope of current security practices? How is access control handled for these systems?
- What is the mechanism by which access is terminated for individuals who no longer need access to some or all patient information? How quickly is access termination completed and documented? How are access termination requests communicated to the appropriate authorities?
- What are the mechanisms to provide remote access to patient information? What are the procedures for authorization to allow remote access?
- What is the procedure to modify access and when is it required (i.e. changes in employment status, changes in job function, system implementations, technology changes, special and short term needs)?
- How does the organization authorize, implement and revoke emergency access needs?
- What is the procedure for password assignment? How are passwords maintained? How often do passwords need to be changed? Does the current policy explicitly forbid sharing of password and sign-ons? Are access passwords role-based and can you determine and document accountability?

2.4.6 Internal Audit

A periodic audit should be conducted of organizational systems which process health information to assess system activity and actual or potential security incidents. This initiative assumes that adequate records and logs are maintained of such activity and that reviews are conducted routinely and thoroughly.

Vulnerabilities in this area could include: lack of internal audit capability in the organization (no internal audit department), constrained audit resources, or lack of skills to review audit logs generated from organizational systems; lack of follow-up once irregular activities are recognized; and lack of participation by the internal audit staff in the design and planning of systems that will comply with the security policy; and inadequate or non-existent audit logs from one or more applications that process health information.

Specific issues to be considered include:

- Do we currently have internal audit resources who regularly review the records of system activity, or is this process performed by some other responsible party within the organization?
- If NO, what plans are in place to hire or engage the services of an internal auditor or external audit firm to review system activity and recommend appropriate action if discrepancies are found?
- Are processes in place to ensure that all applicable system activity is logged to sufficient levels of detail to ensure the ability to perform the audit function?
- Do processes need to be developed to ascertain that audit log functionality exists in all applicable systems dealing with health information and develop contingency plans if any affected vendors fail to incorporate such capability in their systems?

2.4.7 Personnel Security

Personnel security requirements are intended to ensure that all personnel (including agents and sub-contractors) who have access to health information have the required authorities and clearances as determined by the organization. Included are assurance of supervision of maintenance personnel by authorized, knowledgeable persons; maintenance of records of access authorizations; proper access authorization of operating, and in some cases, maintenance personnel; personnel clearance procedures; personnel security policies and procedures; and training of system users, including maintenance personnel.

Vulnerabilities in this area could include: minimal or no inclusion of security accountability in personnel policies, procedures and job descriptions; minimal or no clearance procedures included in personnel recruitment practices, including criminal history checks and investigation of past security violations; ad hoc or lack of procedures in place to ensure proper access authorization and supervision of operations and maintenance staff; limitation of personnel security policy scope to include only organizational employees, with no policies governing behavior of third parties with access to health information; and minimal or no security training provided to employees and third parties.

Specific issues to be considered include:

- Do policies exist for oversight of maintenance and operating personnel working in the vicinity of health information? Are they adhered to?
- Does formal documentation of policies and procedures exist to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances?
- Will criminal history checks be required as prerequisite to the hiring process and/or granting access to health information? Will such checks be repeated at predetermined intervals?
- What process exists to ensure that employees and contractors sign agreements which delineate individual security responsibilities and accountability for maintaining confidentiality? Is there a recertification process in place for this process occurring at specific intervals following the new hire process?
- Are system users, including maintenance and operating personnel, trained in security? Are third parties with access to organizational systems included in the security training process?
- Will criminal background checks be done on all applicants as part of the hiring process?
- What action will be taken to determine which applicants will not be hired due to the findings on the criminal background checks?
- Have current employees had criminal background checks done?

- What process is in place to do periodic criminal background checks on current employees?
- What action will be taken when there are findings on the criminal background check?
- Have applicants and current employees been checked against the OIG sanctions list?
- Is there a process in place to address those employees and applicants that show up on the OIG sanctions list?
- Is there a process to do an OIG Sanction list checks on a periodic basis?
- Has a work history been checked on applicants?
- Have references been checked on all applicants?

2.4.8 Security Configuration Management

Security configuration management includes integrated measures, practices and procedures necessary to work in conjunction with other organizational measures, practices and procedures in order to create a coherent security environment. Included are documentation; hardware and software installation and maintenance review and testing for security features; inventory of hardware and software assets; security testing; and virus checking.

Vulnerabilities in this area could include: incomplete, out-of-date, inaccurate or poorly-communicated documentation; faulty change control procedures are followed; development and test systems are not kept separate from production systems; security testing is rarely performed prior to introduction of new systems or applications; hardware and software assets are not inventoried and/or maintained across the entire organization; security testing, including intrusion testing, is not performed regularly on key systems; and virus checking controls are installed on some, but not all, systems and workstations and/or have been turned off to enhance performance.

Specific issues to be considered include:

- Do security measures for all information systems exist?
- Are security measures for disparate systems coordinated? If so, how?
- Are new applications tested for security prior to rollout?
- Is a physical inventory maintained and kept accurate and current of all hardware and software assets in the organization?
- Is security testing, including intrusion testing, performed regularly on systems and networks?
- Are virus checking procedures in place and utilized? Are tools in place to check for viruses as far out as individual workstations?
- What is the reporting and response process when viruses are detected?
- Is virus checking software kept current to ensure catching new viruses?

2.4.9 Security Incident Procedures

A formal process should be implemented to deal with identification, **reporting**, and ensuing **response** to real or potential violations of established security policy.

Vulnerabilities in this area could include: reporting and response procedures are conducted on an ad hoc basis, with no formally documented and communicated steps to be followed; no official responsibility for incident reporting and responses has been assigned; and potential evidence of violations is inadvertently altered or destroyed prior to review by management or law enforcement officials.

Specific issues to be considered include:

- Does our overall information security policy address the investigation and response to a security incident? If so, does the information policy define what is a security incident and differentiate between a serious and non-serious incident?
- Does the information security policy cover the handling of viruses?
- Does the information security policy cover who investigates the serious, non-serious and virus incidents (i.e. security analyst, Computer Incident Response Team)?
- Does the information security policy cover the timeliness for investigating and reporting the security incident, including recommendations, disciplinary action, etc.?
- Does the information security policy include the reporting of findings of the security incident and does the report describe the security incident, corrective action taken, recommendations, distribution of the report, and follow up?
- Does the information security policy include the coordination with local and federal law enforcement agencies?
- Does the organization have standards developed for anti-virus software, intrusion detection software, network software, etc.?

2.4.10 Security Management Process

The security management process includes comprehensive policies, controls and accountability to ensure that security breaches are minimized through the establishment, implementation and oversight of measures intended to ensure that risk is kept to an acceptable level, as identified by the organization. Implementation features required as part of this process include the following:

- **risk analysis** process in which the costs associated with implementation of security measures are balanced against the potential losses to the organization if such measures were not in place
- **risk management** process in which risk is assessed and used as the basis for mitigating such risk and maintaining it to an acceptable level
- **sanction policy** in which personnel (including third parties) are notified of the consequences and disciplinary actions that will accrue to those who misuse or misappropriate health information
- **security policy** in which organizational management states its intent through formal communication of information values, protection responsibilities and organizational commitment to confidentiality goals

Vulnerabilities in this area could include: minimal or no linkage of organizational policies, systems practices or business processes to risk analyses; lack of clearly defined information asset owners and custodians responsible for performing risk assessments for those assets; failure to update risk analyses to reflect changing environments or technology; loosely enforced and mis-communicated sanction policies; security policy which has not been updated to reflect current issues such as laptop computing, e-mail, remote access or internet risks; security policy fails to define specific security responsibilities within the organization; and no provision within the security management process has been made for agents and sub-contractors with access to the organization's health information.

Specific issues to be considered include:

- Is there accountability and a methodology for maintaining the organization's risk inventory/profile, data criticality/confidentiality classification scheme, and risk control analysis?

- Is there a process to select and implement appropriate risk mitigation measures?
- Does the risk management area have the ability to suggest/affect business process change if this is the best method for risk mitigation?
- Is there a process for ongoing assessment of effectiveness of control measures and for identifying and responding to problem trends?
- Does the risk management area have adequate resource and management support?
- Does the risk management area promote consistency and best practices?
- Are sanctions for external users incorporated in contractual agreements to the extent possible?
- Are sanctions for internal users incorporated in security/confidentiality policy statements?
- Are employees required to read and sign security and confidentiality agreements?
- Are there specific sanctions for specific types and levels of violations?
- Is there consistent enforcement?
- Is there senior management support backing up the security policy?
- Does the security policy include a rationale and clarification of its purpose and importance?
- Is the security policy comprehensive, covering all business and technical areas, systems, communications and storage media, and all affected personnel, both internal and external?
- Does the security policy outline responsibilities and accountability for security officers and administrators, managers and employees?
- Is the data criticality/confidentiality classification scheme documented in the policy?
- Does the security policy set forth what are acceptable and unacceptable media, methods of communication, and storage for sensitive and confidential data?
- Does the policy outline the following overall guidelines and expectations?
 - granting access and specific access privileges, have approved use of group profiles
 - guidelines for periodic reevaluation of access privileges
 - guideline methods for termination, timing, etc.
 - requirements for use of security audit software
 - procedures for violation monitoring and reporting
 - requirements for audit trail access logs which identify user activity
 - security requirements related to records management
- Does the policy cover exception and emergency access procedures?
- Does the policy set forth standard or accepted tools, products or methods for key security areas such as firewalls, encryption, program library control, and file protection software?
- Is there a process for personnel with central security responsibility to review and approve the detailed procedures as they are implemented in individual businesses which are subject to the central policy?
- Are security training and awareness programs required by the policy?
- Does the policy cover physical security as it applies to individual employees' equipment and records?

- Does the policy cover personal backup and recovery procedures?

2.4.11 Termination Procedures

Termination procedures should be formally established, documented and communicated for the purpose of ensuring that appropriate security measures are taken when an employee terminates employment or when user access must be revoked for other purposes, to include access revocation for third parties. Included in the termination procedures should be provisions for: **changing locks** or combinations to protected facilities or systems; **removal from access lists**; **removal of user accounts** granting access privileges to information, services and systems for which they currently have clearance; and **turning in of keys, tokens or cards that allow access** to buildings or equipment, preferably to occur prior to termination.

Vulnerabilities in this area could include: broken processes in which timely removal of user accounts does not occur relative to the date of physical separation; inconsistent enforcement of termination procedures across the various entities within the healthcare organization; responsibility and accountability are not clearly defined for ensuring that termination procedures are carried out completely; physical access items are collected prior to separation, but little or no attention is paid to revocation of system access ids and passwords; and user accounts for third parties with access to organizational systems (vendors, etc.) are not revoked when access is no longer warranted.

Specific issues to be considered include:

- Is there an employee termination policy and related procedures in place? Do they distinguish between employee and employer-initiated terminations?
- Are responsibilities clearly defined and understood? Is a communication protocol in place to address timing and channels?
- Are Human Resources systems and IT security controls linked to ensure timely revocation of user accounts?
- Is an exit interview conducted in which potential security concerns are identified, documented and acted upon?
- Is there assigned responsibility for signing off the termination process in each case?

2.4.12 Training

A security training program should be established for all employees and third parties with access to health information. Such training should include: **awareness education** covering the organizational security policy, password maintenance, incident reporting, and viruses; **periodic security reminders** conducted as updates to the basic security education; **user education concerning virus protection**, including identification, reporting and prevention measures; **user education in importance of monitoring log-in success/failure, and how to report discrepancies**, including employee responsibility for ensuring security of health information; and **user education in password management**, including organizational rules to be followed in creating, changing and ensuring confidentiality of passwords.

Vulnerabilities in this area could include: no security content in existing training programs for new hires; minimal security content included in new hire orientation process, but no ongoing reminders or updated security education; no security training for third party agents and sub-contractors with access to health information; no assigned responsibility for the security training program content or implementation; and security training program is not customized for the needs of each audience.

Specific issues to be considered include:

- Is there a formal organizational security training program? Is such a program kept updated to reflect changes in the security environment and security responsibilities of employees and contractors?
- If NO, what plans are in place to develop an enterprise-wide security training program? What timeframe has been established for the completion and rollout of this program across the enterprise?
- Is there an annual or more frequent recertification process in place to the security training program?
- How is the training program tailored to support the various classes of system users and the level of information sensitivity to which users have access? Are all system users included in the training program, including those employees and non-employees accessing organizational systems from remote sites?
- Does the security training program include requisite education regarding protection against and reporting of viruses, identifying and reporting potential security breaches, and managing individual passwords?

2.5 Physical Safeguards

NO RESPONSES WERE RECEIVED FROM THE WORK GROUP ASSIGNED TO THIS AREA. INPUT IS REQUIRED FROM THE INDUSTRY TO COMPLETE THIS SECTION OF THE HIPAA REGULATIONS.

2.6 Technical Services and Mechanisms

THE TECHNICAL SERVICES AND TECHNICAL MECHANISMS SECTIONS OF THE HIPAA REGULATIONS HAVE BEEN COMBINED BY THE INDUSTRY WORK GROUP. IT IS SUGGESTED THAT THE FINAL VERSION OF ANY DOCUMENT PRODUCED SHOULD ADDRESS TECHNICAL SERVICES AND MECHANISMS SEPARATELY IN CONSIDERATION OF THE REGULATORY FRAMEWORK.

Technical security services include security measures put in place by an organization to protect information and control individual access to information.

Technical security mechanisms include security measures put in place by an organization to guard against unauthorized access to data that is transmitted over a **communications** network.

Vulnerabilities in these areas could include: application constraints allowing use of common ids and passwords; application constraints precluding use of role-based or context-based access control; use of internet and other open networks to transmit patient information in unencrypted format; technical network weaknesses and susceptibility to intrusion; lack of network alarms to signal unusual occurrences; and lack of system and application functionality to allow both automatic logoff and generation of audit logs of system activity

Specific issues to be considered in the areas of technical services and mechanisms include:

- Is there a documented procedure for disabled logon ids and passwords?
- Is there a documented procedure for emergency access?
- Is there a process for screening unwarranted demands for access?
- Context-based access, role-based access, and user-based access:
 - Are there different levels of access based on data content?
 - Who defines access to healthcare and patient financial information?

- Do systems have the ability to match administrative controls?
- Does the system have the ability to log sign-on events? Who reviews them?
- Is it technically possible to aggregate?
- Are there reporting capabilities vs. alarm capabilities?
- Does the ability exist to consolidate all access for a single patient?
- Although encryption is not required, are best practices followed in encrypting passwords?
- Role-based access, user-based access:
 - Is the system capable of granting access based on roles?
 - What is this procedure?
 - Are technical mechanisms capable of matching release of data with consent?
 - Are technical mechanisms available to evaluate and validate readiness of trading partners?
- Does data authentication equal data integrity?
- Does the organization have the mechanisms to ensure the integrity of the data and know if/when the data have been altered/damaged?
- What technical mechanisms exist to know if systems/data bases have been altered by inappropriate means?
- Is authentication strong enough to enable identifying someone for disciplinary action?
- Are any of the following in use for authentication: password, Pin, SecureId token, digital certificate?
- Can passwords be forced to be changed periodically?
- Do systems have mechanisms for automatic logoff or timeout, or screen saver passwords? Are these mechanisms installed and monitored?
- Do systems allow for individual user ids and passwords?
- Do systems prohibit simultaneous access of the same user id/concurrent connections?
- Do systems allow for mapping to an individual?
- Can systems support one logon id with multiple passwords to coordinate group access requirements?
- Is the organization using an open network (need definition clarified)? If so, is data encryption in use?
- Do systems authenticate communications?
- Does the capability exist to ensure that the entities communicating with us are authenticated?
- Are there technical mechanisms to control the method of access by outside entities connecting to our proprietary network?
- Does the capability exist to produce and review an audit trail of access?
- Does the system have the ability to produce an alarm based on unauthorized access? Is it currently installed?
- Is there an alarm for unusual/inappropriate activities with volume thresholds?

2.7 Electronic Signature

The electronic signature standard is optional at this time. If an organization chooses to use an electronic signature as part of a particular transaction, **message integrity, non-repudiation, and user authentication** must be implemented. Other implementation features are optional.

Specific issues to be considered in this area would include whether or not an organization wishes to utilize this method of authentication and ensuring adherence to the three mandatory implementation features.

2.7.1 Risk Assessment

The gap analysis helps determine the area's where your organization has vulnerabilities. The risk assessment needs to evaluate the significance of the vulnerabilities in the context of your organization's operations. The types of questions a organization is trying to answer in a risk assessment are:

- What could compromise the confidentiality, Integrity and availability of my health information?
- What is the impact to my business? Or to the person?
- What is the probability that it will happen?

Conventional wisdom on risk assessment says that organizations need to look at the significance of an impact and the probability of the risk occurring, for purposes of security we're talking about the probability of a breach and the subsequent consequences. The X's in the table below indicate areas where most organizations are likely to focus for risk management, i.e., where the significance of the impact on confidentiality, integrity or availability is High and the probability is high or medium.

Risk / Impact significance	Low	High
High	X	X
Low		

Risk analysis is an implementation feature of the HIPAA Security Management Process requirement. This guide uses the term assessment because it does not include the cost benefit aspect included in the risk analysis definition of the rule. That step will need to wait until an organization is evaluating solution options.

Some organizations are contemplating an across the board determination that all risks are highly significant to avoid unnecessary expense on the risk analysis. Although this is potentially attractive from a initial workload perspective industry experts agreed that it does not support security solution decisions because it implies all information needs the highest level of control. An alternative approach would be to distinguish highly sensitive information from all other information such as: mental health, AIDS, reproductive, drug and alcohol and genetic screening.

If your organization intends to do a more systematic risk assessment the following guidance should be considered.

Risk assessment should be organized in a consistent fashion possibly in parallel with the baseline design along business process or department lines. Alternatively is could be organization along system or data process lines. Many characteristics influence the likelihood of breach. Organizations need to take the information from the gap analysis and then take into account other environmental factors including:

- Purpose of process/system/department
- Is it subject to HIPAA
- User questions
- Number of users
- Types of users, internal, external, on-site, remote, contract
- Type of access, level and scope of access
- Frequency of use
- Knowledge level of users
- Numbers of locations/sites
- Physical environment
- Number of systems
- Types of security controls
- Interdependencies and interfaces
- Data risk, type of information and confidentiality, integrity and availability risks
- Type of vulnerability accidental or intentional

This list would be used to characterize your business process consistent with the example below.

The following five steps should then be followed for whatever consistent unit of measurement your organization is using:

Step 1 Characterize your business process

Example:

For Business Process: Provider Billing,

Description - key entry bath claim process

Is process subject to HIPAA reg?

Purposes of process - getting paid

Users -data entry personnel

- registration office

- Who are they

- 10 users

- all internal

- remote/on-site

- knowledge

- 10 + management, trained on hiring locations/sites

- 1 local systems

-1 PMS, UNIX twisted pair network 3101 controls -

What's in place or available (policies, procedures, documentation, etc.)

How's it really being used (practices)

The IT organization can document the technical controls across the environment

Physical environment - public clinic, back office.

Interdependencies/interfaces - scheduling, coding, clearing house

Data risk - high, medium, low

Vulnerability - disclosure (accidental or intentional), stolen data, altered data

Step 2 Value the Asset

Once the business process is characterized the information asset can be valued. A few rules of thumb to consider: the more users and sites the higher the vulnerability and the greater the interdependencies the more significant the impact.

Step 3 Determine how current controls mitigate the risk

After the initial impact has been assessed if a breach occurred the next step is to determine how the existing controls mitigate the likelihood of the breach in the context of the environmental characteristics.

Step 4 Assess the vulnerability or the threat

Step 5 Assess the probability that the threat will happen.

The final step is assessing the vulnerability

Solution Strategy

3. SPECIFIC GUIDELINES FOR HIPAA SECURITY REQUIREMENTS

The following section provides specific guidelines and recommendations for each requirement listed in the Security NPRM. Each requirement provides a definition either taken from the NPRM or interpreted from the NPRM, and the control category for the particular requirement. Lastly, there are specific guidelines or recommendations outlined. In some cases examples may be listed for either small or large organizations. It would be left up to an organization to determine which category they would fit into. This may be based upon the level of risk an organization is willing to accept when implementing these requirements.

3.1 Administrative Procedures for Data Integrity, Confidentiality and Availability §.308 (A)

These are documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data.

3.1.1 Certification §.308(a)(1)

Definition:

Each organization is required to evaluate its computer systems or network design to certify that the appropriate security has been implemented.

Control Type:

Management

Specific Guidelines:

This document has been written before the final rules have been issued. It is expected that with the issuance of the final rules there will be some additional guidelines or recommendations about the certification process. One might expect that organizations such as JCAHO and NCQA will offer some type of certification process. At this writing there are not specific organizations who are “authorized” to perform certifications. However, to begin to prepare for the expected certification process following are some basic recommendations that can be followed.

Recommendations:

- be performed by individuals who are not responsible for the maintenance, supervision or execution of the specified IT controls;
- be an on-going process;
- do diligence required;
- documentation is a key part of the process;
- be performed by individuals with adequate training regarding generally accepted security guidelines and principles;
- be performed by internal or external parties;
- include an examination of evidential matter sufficient to obtain an understanding of the design and effectiveness of controls for each HIPAA security requirement and implementation;
- recommend monitoring the certification cycle of a minimum of once a year due to the changing nature of computer systems and accelerating rate of change of IT related security risks;

Examples of when an organization may want to review their certification would be when a new system is implemented, when there may be changes to their external networks, a change in value or use of information or an emergence of a new threat;

- be maintained for three years to provide for an adequate history of certification information and an audit trail of certification for reviewing bodies;
- be reviewed and authorized by executive management;
- should be documented in a memo from each entities executive management and compliance officer (similar to a management representation letter) that states 1) the compliance status by each HIPAA requirement and element, 2) management's action plans to address areas of control deficiency, and 3) any instances in which management is aware of security related control issues or deficiencies. This letter should clearly state management's responsibility for the effectiveness of the information security control structure.

Small Organizations, Small Provider Office – It is expected that the majority of the small organizations will choose self-certification. For example this could be done using a Regulatory Compliance Manual similar to the OSHA manual. At this writing the exact mechanism for self-certification is not definitive.

Large Organizations - It would be expected that there will be a mix here and that organizations will both self certify and choose to use an outside organization to certify.

3.1.2 Chain of trust partner agreement §.308(a)(2)

Definition:

If data are processed through a third party, the parties are required to enter into a chain of trust partner agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data.

Control Type:

Management

Specific Guidelines:

Chain of Trust Partner Agreements should:

- be signed contracts: any organization that exchanges confidential electronic data with external organizations must have a signed contract or agreement with the external organization that includes data handling and confidentiality. This agreement may be a free standing contract, a part of a larger contract, or an addendum to an existing contract;
- define the of Terms and Conditions: Each contract must contain language that defines confidential information, conditions for disclosure, data rights of each trading partner, and required security levels of responsibility and accountability for each partner;
- contain, at a minimum, the following elements:
 1. Signatures of agreeing parties;
 2. Contract start date, expiration date and/or Review/Renew dates;
 3. Definition of Terms and Conditions to include confidential information conditions for disclosure, data rights of each trading partner, and minimum levels of security to be maintained;
 4. Procedures for Reporting Breaches;
 5. Penalties for non-compliance with agreement (intentional versus unintentional); and

6. Retention and Destruction Schedules;

- be reviewed and/or renewed at the following intervals and evidence of such a review (i.e., regular certification audit) must be documented and attached to the contract or agreement:
 1. Upon contract renewal;
 2. Concurrent with full security review/certification review;
 3. Upon regulatory changes requiring revision; or
 4. Upon breach of agreement trigger;

Each party in the agreement must:

- keep an incident log of any breaches to the agreement. The party who breaches the agreement must notify the other of any breaches within an agreed upon period of time or provide the incident log for periodic inspection and upon demand.

3.1.3 Contingency plan §.380 (a)(3)

Definition:

Each organization is required to maintain a contingency plan for responding to system emergencies. The organization is required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place. To satisfy the requirement, the plan would include the following: add in the implementation features (change the numbering back).

Control Type:

Management / Operational

Specific Guidelines:

- Strategies and policies have been established to help ensure the business contingency of systems.
- Recovery testing should be periodically performed to help ensure the viability of the recovery plans.
- Procedures to store and recall media from offsite storage should help ensure the availability of the media.
- Processes should be in place to monitor computer and network operations to mitigate interruptions.
- Recovery tools and offsite facilities should be in place to support timely recovery in the event of a disaster.

For more information see Appendix C.

3.1.4 Formal mechanism for processing records §.308(a)(4)

Definition:

Organizations are required to maintain a formal mechanism for processing records, that is, documented policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.

Control Type:

Management

Specific Guidelines:

All organizations should have documented policies for processing health information. It is recommended that your policies should cover both electronic health information and also paper records.

3.1.5 Information access control §.308(a)(5)

Definition:

Each organization is required to establish and maintain formal, documented policies and procedures for granting different levels of access to health information. The following would be provided:

- Access authorization policies and procedures;
- Access establishment policies and procedures; and
- Access modification policies and procedures.

Access control is also discussed later in the document in the personnel security requirement and under the physical safeguards, technical security services, and technical security mechanisms categories.

Control Type:

Management

Specific Guidelines:

This section covers policies and procedures for granting different levels of access to health information. The following guidelines represent a set of best practices and guidelines for each Access Control requirement referenced in the NPRM. It is assumed that “need to know” requirements will be addressed in a Personnel Policy.

Scope and Purpose of Access Control Policies and Procedures:

The policies and procedures should be designed to prevent unauthorized uses, disclosures and issuance of system commands, as well as to prevent modification or destruction of resources. It is imperative that an organization builds accountability into the policy by identifying and authenticating individuals attempting to access health information. In other words, processes must exist to identify individuals who attempt to access health information and either authorize or deny access. Authorizing access to health information should be defined based on the minimum amount of information necessary to perform a function. The personnel security policy should define the “need to know” access.

Accountability is built into a policy when identification and authorization to access health information is monitored and logged, thereby linking the activities and access attempts to an individual user. Additional guidelines regarding ongoing monitoring and reporting requirements are discussed in a separate section of this implementation guide.

Once developed, a covered healthcare entity must communicate the policy throughout the organization and educate personnel. An organization must also enforce on a continuous basis and review the policies at least annually, via a security review board or a designated Security Officer.

Definitions:

There are three basic components to an access control policy: access, authentication and accountability, each of which is defined below. The definitions were taken from the RFC 2196 Site Security Handbook, published in September 1997:

“An **Access Policy** ... defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to a network, and adding new software to systems. It should also specify any required notification messages (e.g. ,

connect messages should provide warnings about authorized usage and line monitoring, and not just simply say “Welcome”).”

“An **Authentication Policy**... establishes trust through an effective password policy, and by setting guidelines for remote location authentication and the use of authentication devices (e.g. one-time passwords and the devices that generate them).”

“An **Accountability Policy**... defines the responsibilities of users, operations staff, and management. It should specify an audit capability, and provide incident handling guidelines (i.e. what to do and who to contact if a possible intrusion is detected.)”

Criteria

- Develop Access Control Policy, including an Authentication and Accountability Policy

Small Organizations/Small Provider Offices- This will depend on the capabilities of the operating system and applications used; eg, sign-in/out logs using passwords. Develop and use procedures for securing physical access, such as locking entry points, computers and storage areas.

Recommend use of privacy screens to prevent the casual observer from having unauthorized visual access to a computer monitor. Use of automatic logoff after a specific time of inactivity, or management with the use of power settings and screen savers. Establish procedures for adding or changing access controls with personnel changes: New hire, job change, visiting practitioner/intern, new type of user necessary as needs of organization change.

Large Organization - See references noted at the end of this section for additional detail on how to develop a comprehensive policy and procedure guide.

Access Authorization

- Define rules for granting access based on minimum amount of information needed to complete the task

Small Providers Offices- Doctor and office manager define the minimum amount of information a user needs to accomplish their assigned task. For example a Security Officer (likely the Office Manager), defines the minimum amount of data a user needs to accomplish their job based on the “need to know” personnel policy. A receptionist may not need access to the health records.

Large Organization - A larger organization should define the types of data/information stored or transmitted electronically, assess level of sensitivity and respective risk, and include a comprehensive list of data sources, applications and type of data. The Security Officer or System Administrator will set up access authorizations when a user is added to the system.

- Define types of users, roles and access labels to assign

Small provider office – This will be dependent upon their role in the practice. A small organization will likely rely on user-based or role-based exclusively at the application level and/or workstation level, depending on the application.

Large Organization - This will vary greatly depending on size and complexity of organization. Large organizations can define access levels, based on application groups, user groups, and roles. More sophisticated organizations may elect to use label-based access controls.

- Define level of detailed information a user can access (system, workstation, application, file, record, field, etc...)

Small Organization - For the small organization, this process should be fairly straightforward. For example: A Doctor, nurse and nurse practitioner should have access to the patient record.

Administrative and billing personnel should only have access to scheduling and billing information.

Large Organization - A larger institution will have to define the information access levels granted to users. This may require that the organization develop a decision tree or access matrix based on business rules defined above.

Establish Access

- Security policies and rules that determine an entity's initial right of access to a terminal, transaction, program process or some other user. Define access points when access control mechanisms are required

Small Organization/Small Provider Office- Establish security policy including schedule of access and use. For instance keep a record of days when personnel are scheduled to use the computer and days allowed. Know when access should be given from a procedural sense. Set up a sign-in/out log for visitors.

Large Organization - Define access controls in detail. Establish access type (Refer to ASTM E 1986-98 and the NIST Computer Security Policy Handbook for details on the types of access controls used.) Applications may allow for varying levels of access at the data-level, and allow for configuration at the user level. However, from an enterprise perspective, the consistency of this approach will vary greatly. The advent of CCOW will foster more consistent types and levels of access profile definitions at the data level.

- Define technical and procedural mechanisms to control access based on the definitions above. Determine how to monitor and enforce based on levels defined.

Small Organizations/Small Provider Offices – Establish procedures with documentation of access and use by each employee. This can be handled with logon passwords and audit trails. For instance a book can be kept locked up containing passwords and times allowed to utilize the computer.

Large Organization - A large organization should base their approach on the policy, but will control and monitor with technical mechanisms. Will require an additional layer of sophistication and diversity given the level of complexity. Access controls must be configurable at the location, workstation, user group, application and user level, with multiple types of control options. This will enable organizations to customize the access controls to their environment.

- Verify identity of individual attempting to access

Small Organization/Small Provider Office – the verification process should be as automated as possible using password controls. The use of passwords should be adequate to verify an individual's identity and that they be changed routinely.

Large Organization - Should be systematic based on rules defined above and access control lists. Ensure identification is authenticated before providing access to health information.

- Define the party or department responsible for defining the above-mentioned policies and establishing new access. Includes security awareness training for personnel.

Small Organization/Small Provider Office - Office Manager or System Administrator is responsible for administering the practices established. However, it should be a joint effort with the management staff. Train all personnel initially when hired and retrain personnel periodically. Ensure that changes to policies and procedures are tested.

Large Organization - Will likely be the responsibility of a Security Officer. While IT areas may have responsibility for driving this process, it is the ultimate responsibility of the CEO and CIO to ensure ownership of these tasks - initially and those maintained over time. Test changes to policies and procedures.

Modify/Terminate Access

- Define scenarios when access rights will change

Small Organization/Small Provider Offices – When changes in personnel occur, or changes that alter administrative or clinical roles, new user profiles should determine access codes. The scenarios in this environment will be fairly limited. Specific scenarios should be spelled out in the policies and procedures manual.

Large Organization - Changes in access will be contingent on the scenarios defined for the small organization. Due to the dynamic nature of the healthcare environment access rules should be reviewed annually.

- Who will modify or terminate a user's access profile? How will the System Administrator be notified of the change? How soon will the change/termination take effect?

Small Organization/Small Provider Offices - Office Manager or System Administrator should go through a simple checklist. For example verify employment and passwords on a specified schedule.

Large Organization - System or Network Administrator should follow a checklist to ensure all system/application rights are modified or revoked as requested.

- Recommended Access policies and procedures:
 - Evaluate and establish as employees are hired; and
 - Reevaluate as the employee's role changes.

In addition,

- Rules shall apply equally to permanent, temporary, or contract staff;
- Expiration dates should be associated with access rights when it is known that a user's work will only require privileges for a specified period. Extension beyond that period should be at the discretion of the system manager;
- Access rights should never be transferred between users, even on a temporary basis; and
- An internal security review board should periodically review these policies and procedures on an annual basis or immediately following an incident affecting the policy;

3.1.6 Internal audit §.308(a)(6)

Definition:

Each organization is required to maintain an on-going internal audit process, which is the in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by the organization.

Control Type:

Management

Specific Guidelines:

Create policies for the internal audit process. (See Technical Security Services - Audit Controls for the specific guidelines)

3.1.7 Personnel security §.308(a)(7)

Definition:

There would be a requirement that all personnel with access to health information must be authorized to do so after receiving appropriate clearances (authorizations). This is important to prevent unnecessary inadvertent access to secure information. The personnel security requirement would require entities to meet the following conditions:

- Assure supervision of personnel performing technical systems maintenance activities by authorized, knowledgeable person.
- Maintain access authorization records.
- Insure that operating, and in some cases, maintenance personnel have proper access.
- Employ personnel clearance procedures
- Employ personnel security policy/procedures.
- Ensure that system users, including technical maintenance personal are trained in system security.

Control Type:

Management / Operational

Specific Guidelines:

No additional recommendations.

3.1.8 Security Configuration Management §.308(a)(8)

Definition:

Each organization is required to implement measures, practices, and procedures for the security of information systems. These are required to be coordinated and integrated with other system configuration management practices in order to create and manage system integrity. This integration process is important to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses. This requirement would include the following:

- Documentation
- Hardware/software installation and maintenance review and testing for security features
- Inventory procedures.
- Security testing.
- Virus Checking.

Control Type:

Management

Specific Guidelines:

This applies to a stand-alone environment also.

3.1.9 Security incident procedures §.308(a)(9)

Definition:

Each organization is required to implement accurate and current security incident procedures. These are formal, documented instructions for reporting security breaches, so that security violations are reported and handled promptly. These instructions would include the following:

- Report procedures.
- Response procedures.

Control Type:

Management / Operational

Specific Guidelines:

No additional recommendations.

3.1.10 Security management process §.308(a)(10)

Definition:

Each organization is required to maintain a process for security management. This involves creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches. We would require the organization to have a formal security management process in place to address the full range of security issues. Security management includes the following mandatory implementation features:

- Risk analysis.
- Risk management.
- A sanction policy.
- A security policy.

Control Type:

Management / Operational

Specific Guidelines:

These need to be modified into guidelines.

1. Define controls and the specific items necessary to monitor the effectiveness of the controls. No controls or control measurements may be specified out of the context of an organization's operational context. The "threat checklist" identifies the following "drivers" or potential sources of risks to information security, including:
 - Users: users vary in their intent to do harm with the majority of breaches occurring inadvertently through ignorance and carelessness. A comprehensive, recurrent training program as mandated by HIPAA constitutes the primary control of inadvertent, careless errors. Monitoring this control uses requires extrinsic-simple measures that organizations of all scales may deploy. Trainees should sign an attendance sheet that must be collated and compared against staff lists to document individual compliance and the percent of collective compliance. When training occurs on-line, documentation of attendance and calculating compliance potentially occurs automatically.
 - Locations: HIPAA requires controls of a range of location-specific issues from workstation access to general physical controls. Obtaining general information about system locations may

occur as part of asset inventory; but, specific controls must be created responding to the varying threats of different type of location. Monitoring workstation access may require controls of all four types. Video-cameras may survey and record who uses a monitor in a particular place. In real time, a guard in some remote location may watch the screen and respond appropriately in sensitive locations. Alternatively, for less sensitive locations, guards may archive and consult the videotape only in event of a possible security incident. Alternatively, a workstation may exist in a public place with logon and password controls that give access only to basic demographic data. Data about use emerges as users log-on, but, again, may only be consulted during investigation of an incident.

- **Systems:** HIPAA focuses attention on the security implications of information systems configuration and management. Monitoring performance of the information technology team in assuring adequate system configuration control falls under the domain of organizational management practice. Measuring compliance requires assessing policies on system configuration control, observing execution of system changes, reviewing documentation of system changes, and questioning of individuals responsible for executing system changes. The complexity of measuring these processes varies with the complexity of the system. These kinds of extrinsic measurements of whatever complexity may be part of routine management but often appear in the context of an external audit. HIPAA requires at a minimum documentation of system configuration control.
- **Communication:** When the public thinks of risks to health information, they often associate them with new communication technologies such as the Internet. Being able to document that an organization's communication networks function securely potentially offers great value in preemptive marketing. With respect to the property space outlined above, firewalls, intrusion detection devices, and audit logs generally fall into the Intrinsic-complex cell. The devices document traffic and signal events; but, often in such great detail that even sophisticated organizations may not routinely analyze the data. The importance of analyzing the data, however, derives precisely from the fact that breaches of the communication network pose major risks for great intangible losses of reputation as well as direct repair and lost opportunity costs.
- **Controls:** HIPAA requires documenting the entire risk management process from initial assessment, to control deployment, to monitoring the impact of controls, and finally analysis and reassessment of the risk management plan. This cyclic process necessarily entails review of all controls. Controls that do not perform as expected require reevaluation.

3.1.11 Termination procedures §.308(a)(11)

Definition:

Each organization is required to implement termination procedures, which are formal, documented instructions (including appropriate security measures) for the ending of an employee's employment or an internal/external user's access. These procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized to access the data. Termination procedures would include the following mandatory implementation features:

- Changing the combination locks (if appropriate)
- Removal from access lists and profiles
- Remove access to user accounts
- Turn in keys, tokens, or cards that allow access.

Control Type:

Management

Specific Guidelines:

The above would be implemented as appropriate.

3.1.12 Training §.308(a)(12)

Definition:

Each organization is required to provide security training for all staff regarding the vulnerabilities of the health information in an entities possession and procedures which must be followed to ensure the protection of that information. This is important because employees need to understand their security responsibilities and make security a part of their day-to-day activities. The implementation features that would be required to be incorporated follow:

- Awareness training for all personnel, including management, (this is also included as a requirement under physical safeguards)
- Periodic user reminders
- User education concerning virus protection
- User education in importance of monitoring login success/failure, and how to report discrepancies
- User education in password management

Control Type:

Management

Specific Guidelines:

No additional recommendations.

3.2 Physical Safeguards For Data Integrity, Confidentiality And Availability §.308 (B)

These relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. It covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

3.2.1 Assigned security responsibility §.308(b)(1)

Definition:

Each organization is required to assign the security responsibility to a specific individual or organization, and the assignment must be documented. Responsibilities would include:

- Use of security measures to protect data; and
- The conduct of personnel in relation to the protection of data.

Control Type:

Management

Specific Guidelines:

This definition is scalable to both a small and large organization. In a small organization this may be an office manager. In a large organization there may be many people that grant access but there must be an ultimate owner of security for an organization.

3.2.2 Media controls §.308(b)(2)

Definition:

Each organization is required to establish media controls in the form of formal, documented policies and procedures that govern the receipt and removal of hardware/software (diskettes, tapes) into and out of a facility. Mandatory implementation features include:

- Controlled access to media;
- Accountability (tracking mechanism);
- Data backup;
- Data storage; and
- Disposal.

Control Type:

Management

Specific Guidelines:

For disposal of media, you must ensure that the information contained on the media has been removed. For controlled access to media this may be as simple as locking media in secure environment when not in use.

3.2.3 Physical Access Controls §.308(b)(3)

Definition:

Each organization is required to establish formal, documented policies and procedures for limiting physical access to an entity while ensuring that properly authorized access is allowed. Mandatory implementation features include:

- Disaster recovery;
- Emergency mode operation;
- Equipment control (into and out of site);
- Facility security plan;
- Procedures for verifying access authorizations prior to physical access;
- Maintenance records;
- Need to know procedures for personnel access;
- Sign in for visitors and escorts; and
- Testing and revision.

Control Type:

Management

Specific Guidelines:

There are many ways to provide equipment control. These may include assignment of liability, property pass, desktop lock, and property alarm device. Facility security may include access cards, cipher locks or just a lock on the door.

3.2.4 Policy/guideline on work station use §.308(b)(4)

Definition:

Each organization is required to establish a policy/guideline on workstation use. These documented instructions / procedures would delineate the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a terminal unattended). This would be important so that employees will understand the manner in which workstations must be used to maximize the security of health information.

Control Type:

Management

Specific Guidelines:

Documented functions to be performed at specific computer terminal based on sensitivity of information accessible from that site. Segregate workstation based on function for highly sensitive information when possible. This requirement should be handled in conjunction with the requirements on access control, physical security and secure workstation locations.

3.2.5 Secure workstation location §.308(b)(5)

Definition:

Each organization is required to put in place physical safeguards to eliminate or minimize the possibility of unauthorized access to information. This would be important especially in public buildings, provider locations, and in areas where there is heavy pedestrian traffic.

Control Type:

Management

Specific Guidelines:

Considerations should be made to placing the monitor in such a manner where the screen contents cannot be viewed by the general public. Screen savers may also be employed. This is also a training issue.

Limit access to resources, including:

- Building
- Office
- Workstation
- Systems
- Printers & faxes
- Printed reports
- Downloaded data
- Removable media
- Remote devices

Restricted areas:

- Operating rooms Labs
- Medical records storage areas

Small Organizations/Small Provider Offices - Protect access to named resources. Discourage unauthorized access via signage. Ensure secondary exits are locked at all times to prevent entry from outside. Ensure all workstations are protected from unauthorized use and view (for example: screen savers, passwords, and monitor positioning). Limit accessibility to printed material by access and proximity to unauthorized personnel. Ensure systems have the ability to define user or role based accessibility. As needed and dependent upon the security risk, downloaded data could be compressed and encrypted until user need arises. Copying of data should not be permitted unless the user's role requires it. All backups must be kept locked up in a designated area. Mechanisms are used to report incidents where security or privacy issues may have been violated, for instance a worksheet placed in appropriate section in a Security manual.

Large Organizations - Refer to the standards referenced for additional guidelines for physical safeguards.

Protect medical records rooms - keep locked or protected with PINs, RF badges or biometrics. Even though this information falls outside the scope of HIPAA, these rooms are often unprotected and represent a vulnerability that can be easily rectified.

3.2.6 Security awareness training §.308(b)(6)

Definition:

Each organization is required to establish security awareness training for all employees, agents, and contractors.

Control Type:

Management

Specific Guidelines:

Security awareness training should be conducted:

- At initial orientation for new personnel; and
- As on-going training, at a minimum, on an annual basis.

There are various ways to heighten awareness for personnel. Organizations can establish periodic reminders via e-mails, bulletin boards, posters, etc. For example, organizations should put a visual reminder at the point of reference to reinforce best practices (like posting a notice by all pre-locked doors to remind people to now allow others to enter behind them.)

An organization should maintain training records to keep an account of the subject matter covered and the employees in attendance. This information will be important should disciplinary action or other action need to be taken following a security breach.

Anytime an incident occurs with an individual, organizations should conduct one-on-one consultation to review the incident and the appropriate practices that should have been followed. This will likely fall under the Security Officer's responsibility, but also may become the responsibility of the individual's immediate supervisor.

In addition to the above, the CPRI –HOST Toolkit has a security awareness training checklist which can be referenced on-line at www.3com.com/healthcare/securitynet/hipaa/toc.html.

3.3 Technical Security Services §.308(c)

These are the processes that are put into place to protect information and to control individual access to information.

3.3.1 Access Control §.308(c)(1)

Definition:

Each organization is required to maintain a mechanism for access control that would restrict access to resources and allow access only by privileged entities. Mechanism should ensure that access to health information is limited to those employees with a business need to access it. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation. The following implementation feature would be used:

- Procedure for emergency access
- In addition, at least one of the following three implementation features would be used:
 - Context-based access
 - Role-based access
 - User-based access.

The use of encryption would be optional.

Control Type:

Management / Technical

Specific Guidelines:

Emergency access

Small Organizations/Small Provider Offices – Determine the organization's policy regarding who will have access to system passwords. The organization must have a back-up procedure to provide access to health information in the event of an emergency. One example a procedure a small provider can implement would be to store the password in a physically secured location (locked cabinet in the physician's office) and document the use of the password in the emergency situation. In the event the emergency password is needed, the use should be logged for future reference.

Large Organization - In addition to the recommendations noted for the small organization, there should be a "break-the-glass" procedure in the event there is a catastrophic circumstance that renders the system inaccessible or one component of the system unusable. The Sys Administrator should be able to get around restrictions and assist approved personnel with gaining access. If the entire system is down, there must be back-up procedures - either archives or secondary sources that can be used for emergency access.

Select and implement one of the following types of access controls based on the access control policy and procedure described above:

Small Organization - A small organization will utilize the capabilities inherent in the operating system and applications.

Large Organization - A large organization will utilize the capabilities inherent in the operating system and applications. However, the level of complexity will require systems and applications that can support the discretionary access controls defined under the policies and procedures.

Optional - Encryption

Small Organization - Smaller organizations do not need to encrypt the access control lists or files. It is recommended that authentication mechanisms (password, PIN, biometrics) always be encrypted. It will likely be the responsibility of the vendor to support this requirement in a small environment.

Large Organization - Larger organizations do not need to encrypt access control lists and files assuming they are protected by discretionary access controls. It is recommended that authentication mechanisms (password, PIN, biometrics) always be encrypted.

3.3.2 Audit Controls §.308(c)(2)

Definition:

Each organization is required to maintain audit control mechanisms to record and examine system activity. Mechanism should ensure that the organization could identify suspect data access activities, assess its security programs, and respond to potential weaknesses.

Control Type:

Operational / Technical

Specific Guidelines:

Create a process to monitor the access to the data:

- review of the audit logs for failed logon attempts or security incidents
- how often do these need to be reviewed,
- what is the escalation process,
- determine the level at which audit logs will be kept,
- what is the mechanism to review the logs,
- what is the impact on system performance,
- what is the retention period.

Small Organizations/Small Provider Offices - If you have a small organization where all users have access to all information, such as a single person as office manager, and receptionist and you have a stand-alone PC with no external connection (including Internet), then this control may not be necessary. More sophisticated small offices should use the resources available with the application.

Other Organizations - It would be expected to have some type of audit mechanism in place.

3.3.3 Authorization Control §.308 (c)(3)

Definition:

Each organization is required to maintain mechanisms for obtaining consent for the use and disclosure of health information. These controls would be necessary to ensure that only properly authorized individuals use health information. Either of the following implementation features may be used:

- Role-based access.
- User-based access (see access control above).

Control Type:

Operational / Technical

Specific Guidelines:

Group logons can no longer be used.

Authorization Control

The mechanisms for obtaining consent for the use and disclosure of health information. (Must include either role-based access or user-based access),

Small Organizations/Small Provider Offices - Authenticate the identity of an individual accessing or attempting to access health information according to the entity authentication mechanisms inherent in the application and operating system. For example, the use of passwords could be used to control the level of information at the role-based or user-based level. Passwords should be changed on a regular frequency and under no exception should passwords be shared or given out. These rules would be reviewed and signed-off using an implementation checklist.

Large Organization - Authenticate the identity of an individual accessing or attempting to access health information according to the entity authentication mechanisms inherent in the application and operating system.

3.3.4 Data Authentication §.308 (c)(4)

Definition:

Each organization is required to provide corroboration that data in its possession has not been altered or destroyed in an unauthorized manner. Examples of data corroboration include use of:

- Check sum;
- Double keying;
- Message authentication codes; or
- Digital signatures.

Control Type:

Technical

Specific Guidelines:

No additional input received for this section.

3.3.5 Entity Authentication §.308 (c)(5)

Definition:

Each organization is required to implement entity authentication, which is the corroboration that an entity is who it claims to be. The following implementation features should be used:

- Automatic log off;
- Unique user identification; and
- At least one of the following: Biometrics identification system, Password system, Personal identification number, Telephone callback, or Token system, which uses a physical device.

Control Type:

Technical

Specific Guidelines:

When developing guidelines for this requirement you will want to factor in the requirements for access controls and authorization controls also.

Entity Identification and Authentication

Each user must be uniquely identified in a system with a Unique User ID, paired with an authentication mechanism: password, PIN, token, biometrics or telephone callback. Authentication mechanisms fall into three basic categories, with varying levels of security and irrefutability:

- Something you know: Passwords & PINS
- Something you have: Tokens (Smart Cards, etc...)
- Something you are: Biometrics (Fingerprint is most widely utilized, iris scan, etc...)

There are a number of industry resources and standards that explain in great detail the importance for having strong, irrefutable authentication. Each organization must assess balance the risk they wish to assume when employing an authentication mechanism. The pros and cons of each are discussed in

detail in the reference resources. Resources that explain the benefits of authentication mechanisms include:

- The 2000 Guide to Health Data Security - Chapters 4, 9 and 10
- NIST Computer Security Policy Handbook - Chapter 16 - Identification and Authentication
- Site Security Handbook.(RFC 2196) - Chapter 4

Few operating systems provide an automatic logoff, but will provide an automatic screen lock. Consequently the auto logoff implementation feature will have to be implemented at the application level.

There are a few concerns about terminating a session after a period of inactivity. There is a risk of data loss or data corruption if the session is terminated. If a user is interrupted and is later called away, creating a period of inactivity, how are the changes preserved? It then becomes the responsibility of the application to determine whether the changes should be saved or lost.

In addition, there is a concern over whether the session should actually be terminated following a period of inactivity. There are a number of applications that invoke a screen saver and mask an active session, allowing the user to save/lose the changes. In addition, this prevents the user from having to log onto the application a second time. This becomes an even greater concern with the use of Internet browsers in healthcare.

Auto Logoff - Required

Small Organizations/Small Provider Offices – Many applications have auto logon but few have auto logoff. This may require the use of auto savers before termination after a period of inactivity. When leaving the workstation the application should be shut down unless auto logoff feature is available. Small organizations are going to have to request that their vendors add an automatic logoff feature since most do not support this capability. Most operating systems provide a screensaver (blocker) There are a number of applications that invoke a screen saver and mask an active session, allowing the user to save/lose the changes. In addition, this prevents the user from having to log onto the application a second time.

Large Organization - Large organizations may or may not have automatic logoff capability. Although the screen saver function that masks an active session is recommended although this option may not be the optimal solution for many organizations.

Unique User ID - Required

Small Organizations/ Medical/Dental Offices/Small Provider Offices - Individuals must be assigned and use a Unique User ID. For example passwords can be used to log/logoff. Users can no longer share ids. They must be role or user based and removed upon termination. These should also be routinely changed over a specified period of time. Re-authentication is required to regain access to health information following an automatic logoff or if a screen saver is evoked.

If passwords are used, the following rules should apply:

- Minimum of 6 characters
- Disallow common dictionary words
- Change periodically, at least once every six months.
- Passwords cannot be the same as the User ID

Large Organization - Users can no longer share User Ids. Individuals must be assigned and use a Unique User ID. Re-authentication is required regain access to health information following an automatic logoff, or if a screen saver is invoked.

Plus, required to use one of following authentication mechanisms:

- Password
- PIN
- Token
- Biometrics
- Telephone callback

PINS (normally 4 characters in length) should only be used in conjunction with a token or other authentication device and should not be used as the sole means of granting access to health information. Four character PINS can be compromised using a 600 MHz machine in a matter of a few minutes.

If used, PINS should never be the same value as the User ID.

Sharing of PINS is prohibited.

Evaluate other, more secure forms of authentication, as economically feasible.

Token - A physical item that is used o provide identity typically an electronic device that can be inserted in a door or computer system to gain access. (i.e. replaces the User ID).

If tokens are used, they should be protected with a password, PIN or biometrics. Establish a policy to report lost/stolen tokens. Tokens should not be shared between users since the token takes the place of a User ID.

Biometrics - Train personnel who enroll users. Train users how to properly use the sensors: Most systems log failed access attempts. Without the appropriate training, personnel who use the readers inappropriately will have a high percentage of failed attempts.

Large Organization - If passwords are used, run a “cracker” program to evaluate the strength of user passwords 1-2 times per year.

Use strong password guidelines as described in the following resources:

- Site Security Handbook (RFC 2196)
- NIST Computer Security Policy Handbook (Published September 1997)

PINS (normally 4 characters in length) should only be used in conjunction with a token or other authentication device and should not be used as the sole means of granting access to health information. Four character PINS can be compromised using a 600 MHz machine in a matter of a few minutes.

If used, PINS should never be the same value as the User ID. Sharing of PINS is prohibited

Token - A physical item that is used o provide identity typically an electronic device that can be inserted in a door or computer system to gain access. (i.e. replaces the User ID).

If tokens are used, they should be protected with a password, PIN or biometrics. Tokens are often used to generate a one-time password. While this method is highly accepted and recommended, it is not required when tokens are used. Establish a policy to report lost/stolen tokens. Tokens should not be shared between users since the token takes the place of a User ID.

Biometrics - Train personnel who enroll users. Train users how to properly use the sensors: Most systems log failed access attempts. Without the appropriate training, personnel who use the readers inappropriately will have a high percentage of failed attempts.

3.4 Technical Security Mechanisms §.308(d)

These relate to processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.

3.4.1 Communications and Network Controls §.308(d)(1)

Definition:

Each organization that uses communications or networks are required to protect communications containing health information that are transmitted electronically over open networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access systems through external communication points. When using open networks, some form of encryption should be employed. One of the following must be implemented:

- Integrity Controls;
- Message Authentication; and
- One of the following (Access Controls or Encryption).

If the organization employs a network, the following features must be implemented:

- Alarm;
- Audit Trails;
- Entity Authentication; and
- Event Reporting.

Control Type:

Technical

Specific Guidelines:

Data encryption is required for open networks (defined as internet or dial-in access). Data encryption is not required for private networks (private lines or VAN services).

Access Controls and Encryption

Small Organizations/Small Provider Offices - Any data containing health information that are transmitted electronically over open networks must be encrypted. Not all browsers contain encryption and application providers should insure this feature is present. Compression may be helpful to speed up the transmission, but must preclude encryption. This will aid in integrity controls since encrypted data cannot be compressed. Message authentication can be accomplished by creating a message digest.

Large Organization - Network devices (like routers) should be protected with discretionary access control mechanisms in the same manner that other computer systems are protected. Any LAN Analyzer or Network Sniffer should be protected by discretionary access controls and secured under lock and key. Users should also log the use of these devices. Network connections should be

disabled when not in use to prevent unauthorized users from accessing the network. Detailed guidelines are available in the resources noted at the end of this guide.

Integrity Controls and Message Authentication

In addition, if using an open network (i.e., Internet), the following four implementation features must be used.

- Alarm
- Audit
- Entity Authentication
- Event Reporting

Small Organizations/Small Provider Offices - If implementation of above features (Compression, Encryption and Authentication) are present, there is no further need for additional requirements such as audit, and event reporting, except by the Application Service Provider.

Large Organization - Large organizations should implement a network management system used to monitor the health and integrity of their network.

It is highly recommend that organizations seeking additional guidance on these measures refer to other resources, including:

- Site Security Handbook
- NIST Computer Security Policy Handbook
- HCFA Internet Policies

3.5 Electronic Signature §.310

3.5.1 Digital (Electronic) Signature §.310

Definition:

If an electronic signature is employed, the following features must be implemented:

- Message Integrity;
- Non-repudiation; and
- User Authentication.

Other features, which may be used, are:

- Ability to add attributes;
- Continuity of signature capability;
- Countersignatures;
- Independent Verifiability;
- Interoperability;
- Multiple Signatures; and
- Transportability.

Control Type:

Technical

Specific Guidelines:

no additional info. May want to wait until final rules are published.

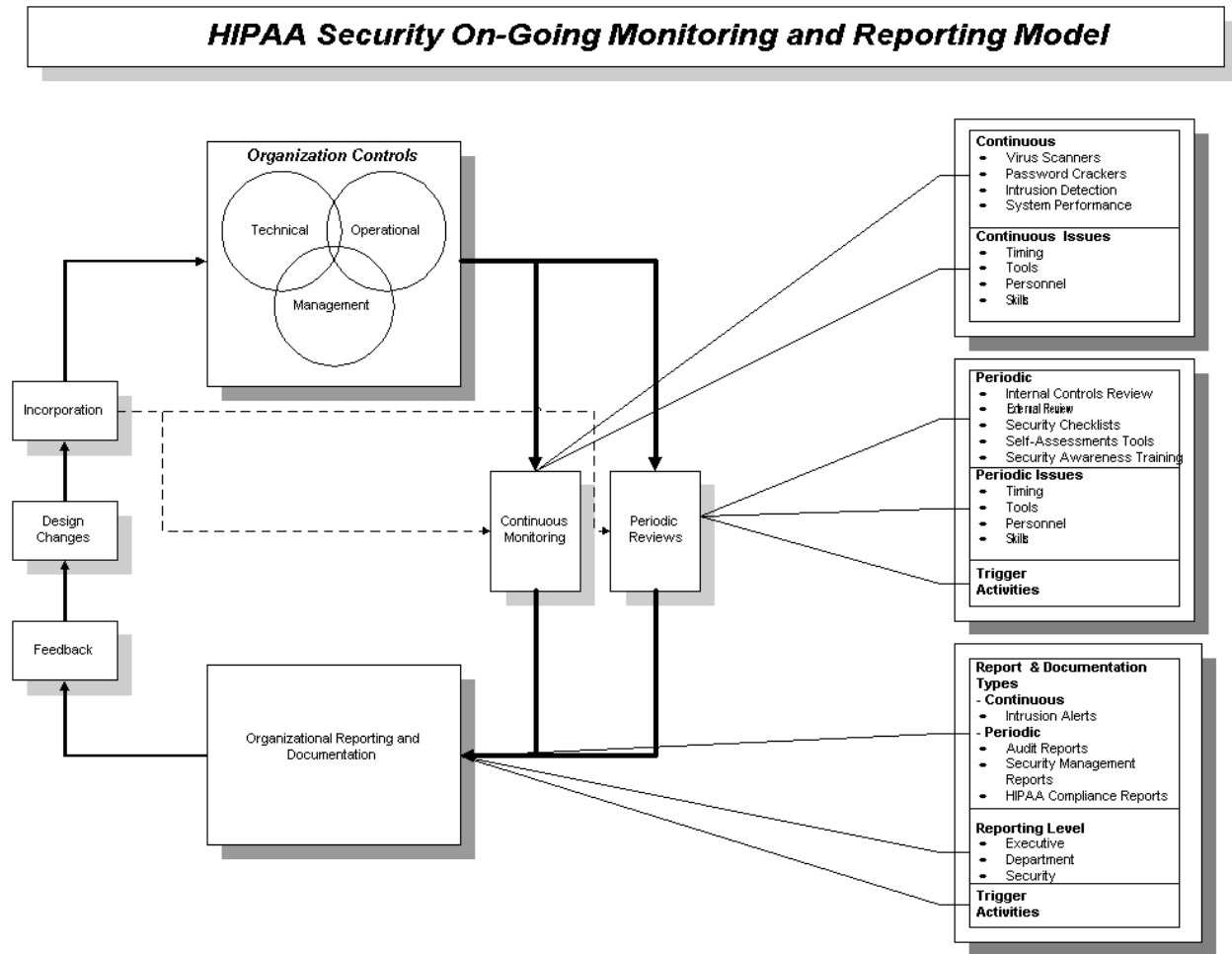
4. ON-GOING MONITORING AND REPORTING MODEL

In the short-term, the addition of new security controls appears to be the most difficult aspect of creating and/or improving your organization's security infrastructure, because the up front costs and resources required to design and implement these new controls can be quite high. From a long-term or total cost perspective, the up front costs and resources expended by your organization could be small in comparison to the costs and resources required to monitor and maintain these controls over time. Based on this long-term perspective, organizations need to consider these costs up front and early as they design new controls to meet the security standards or put mechanisms in place to demonstrate the effectiveness and compliance on current controls. Finally, because of the cost and resource requirements needed over time to maintain and monitor the effectiveness of an organization's controls, this area is usually the first area of the security infrastructure to breakdown.

In this section, we will, through the use of a model, outline a set of best practices for monitoring the effectiveness your organization's security infrastructure and demonstrating its compliance with the Security and Electronic Signature Standards.

The On-Going Monitoring and Reporting (OGM&R) Model, shown in Figure 1, was designed to provide a framework in which an organization can view the types of controls and the process needed to maintain the effectiveness of those controls. The model is composed of four sections: 1) organizational controls, 2) continuous monitoring and periodic review, 3) reporting and documentation, and 4) feedback, changes, and incorporation. All components are interrelated to form a dynamic loop or process, which must be constantly working in order to be effective.

Figure 1: On-Going Monitoring and Reporting Model



Section 1 - Organization Controls¹

The controls that organizations can use to protect their information resources can be divided into categories: Management; Operational, and Technical. Management controls generally focus on the overall management of the security program designed to protect the information resources within the organization. Examples of management controls include a computer security policy or awareness and training. Operational controls are safeguards put into place that are implemented and executed by people. Examples of operational controls include user administration, auditing and compliance. Technical controls are safeguards that information systems execute as part of an organization’s security infrastructure. Examples of technical controls include entity authentication and encryption.

The combination of management controls, operational controls, and technical controls encompass an organization’s security infrastructure, which do overlap, but are needed to provide a comprehensive security infrastructure. For instance, if the organization’s management and operational controls are weak (meaning that user are given access without getting the proper authorization as designated in the organization’s security policy), then the technical controls will not prevent unauthorized access since the individual user were setup with legitimate, but unauthorized accounts. Appendix A assigns each of the HIPAA security requirements to one or more of the control category types.

¹ Source: An Introduction to Computer Security: A NIST Handbook.

Section 2 - Continuous Monitoring and Periodic Review of Controls

Once the management, operational, and technical controls are put into place for an organization, the controls need to be either constantly monitored or reviewed periodically to ensure the controls are working effectively. The type of organization control (management, operational, or technical) will determine whether it is constantly monitored or reviewed on a periodic basis to determine its effectiveness. Technical controls such as virus scanners, intrusion detection, or firewalls must be monitored on a continuous basis, since they need to be working effectively 24 hours a day, 7 days a week or 24X7 basis. Management and operational controls need to be in place, but are not necessarily used on a 24X7 basis. For example, a user does not typically submit an access authorization form at 12:00 AM in order to get access to an organization's information resources. Although management and operational controls need to be checked on a periodic basis to ensure that users are actually submitting access authorization forms with the appropriate signatures before they are given access in accordance with the organization's security policy. The periodic reviews should take place at the times designated by the organization's overall security management policy and procedures.

In order for organizations to perform continuous monitoring and periodic reviews of the organizational controls in place, they will need to consider, at a minimum, the following items:

- **Timing** for when to conduct periodic reviews and identifying what activities would trigger the need to perform a review (either periodically or incident related);
- **Tools** needed for continuous monitoring and to generate the appropriate documentation for periodic reviews;
- **Personnel** necessary to maintain the organization's ability to continuously monitor and conduct periodic reviews; and
- **Skills** necessary to support both continuous monitoring and periodic reviews.

Section 3 - Reporting and Documentation

Organizations will need to decide how they will report on the controls in place in their organization to mitigate the risk faced by the organization and to meet the security requirements outlined in HIPAA. As part of the organization's reporting and documenting of the controls in place, they will need to consider, at a minimum, the following items:

- Types of reports, either automatically generated or generated a part of a review;
- The appropriate level of detail of the reports, which will be dictated by the level (i.e. department or executive) of management the report is being sent to for decision making purposes;
- The type of documentation needed to prove the control are effective and that they were reviewed;
- The timeframe for retention of the reports and documentation; and
- The activities would trigger a review of the reports and documentation (either periodically or incident related).

Section 4 - Feedback, Change and Incorporation

The last section of this model addresses the issue of degradation and reduced effectiveness of controls over time. Technology is in a state of constant change, and organizations are implementing new technology just as quickly as it evolves. As organizations implement new technology, they must also incorporate controls to ensure that it is adequately protected. Organizations may simply upgrade existing

controls or design and implement new controls in order to address additional risks that are associated with the new technology. The bottom line for the organization is the need to get feedback from the monitoring and review process, and incorporate appropriate changes into the existing security infrastructure. This includes changes to the controls themselves and changes to the monitoring and review processes.

5. GENERAL GUIDELINES TO MONITORING AND REPORTING

Controls are defined as “The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.”² It is further recognized that the effectiveness of the detailed Information Systems controls operated within an organization is limited by the effectiveness of the management and monitoring of the use of information systems in the organization as a whole.

The On-Going Monitoring and Reporting Model (shown in Figure 1) defined three categories of organization controls: Management, Operational and Technical. To be effective, the organization controls pertaining to security policies, procedures and practices should be:

- Documented in writing
- Endorsed by management
- Communicated to staff
- Actively implemented
- Monitored for compliance
- Updated as needed

As controls are designed to achieve the security objectives that have been established by HIPAA, they should be supported by eight fundamental core principles: accountability, awareness, multi-disciplinary, cost effectiveness, integration, reassessment, timeliness and societal factors. Each of these principles is discussed briefly below³.

1. **Accountability**—Responsibility and accountability must be explicit. Security of information requires an express and timely appointment of responsibility and accountability among data owners, process owners, technology providers and users. This accountability should be formalized and communicated. Issues to consider include:
 - Specification of ownership of data and information;
 - Identification of users and others who access the system in a unique way;
 - Recording of activities through the provision of management audit trails;
 - Assignment of responsibility for maintenance of data and information; and
 - Institution of investigative and remedial procedures when a breach or attempted breach of the security objective occurs.
2. **Awareness**—Awareness of risks and security initiatives must be disseminated. In order to foster confidence in information, anyone with a legitimate interest to learn or be informed, must be able to gain knowledge of the existence and general extent of the risks facing the organization and its systems and the organization’s security initiatives and requirements. This would include data owners, process owners, technology providers, users and other parties. Security measures are only effective if all involved are aware of their proper functioning and of the risks they address. Issues to consider include:

² Source: “Control Objectives for Information and Related Technology”, ISACA

³ Source: “International Information Technology Guide-Managing Security of Information”, IFA

- Level of detail disclosed must not compromise security;
 - Appropriate knowledge is available to all parties, not just users, who have a legitimate right to be informed;
 - Awareness is part of the induction program for new employees so as to build security awareness as part of the corporate culture; and
 - Recognition that maintaining awareness is an on-going process.
3. **Multidisciplinary**—Security must be addressed taking into consideration both technological and non-technological issues. Security is more than technology. It also covers administrative, organizational, operational, and legal issues. Accordingly, technical standards should be developed with and, be reinforced by, codes of practice; audit; legislative, legal and regulatory requirements; and awareness, education and training. Issues to consider include:
- Business value or sensitivity of the information asset;
 - Impact of the organizational and technological changes on the administration of security;
 - Technologies that are available to meet the security objectives;
 - Requirements of legislation and industry norms; and
 - Requirements to carefully manage advanced security techniques.
4. **Cost Effectiveness**—Security must be cost effective. Different levels and types of security may be required to address risks to information. Security and associated costs must be compatible with the value of the information. Issues to consider include:
- Value to and dependence of the organization on particular information assets;
 - Value of the data or information itself, based on a pre-defined level of confidentiality or sensitivity;
 - Threats to the information, including the severity and probability of such threats;
 - Safeguards that will minimize or eliminate the threats, including the costs of implementing the safeguards;
 - Costs and benefits of incremental increases to the level of security;
 - Safeguards that will provide an optimum balance between the harm arising from a security breach and the costs associated with the safeguards; and
 - Where available and appropriate, the benefit of adopting established minimum security safeguards as a cost-effective alternative to balancing cost and risks.
5. **Integration**—Security must be coordinated and integrated. Measures, practices, and procedures for the security of information should be coordinated and integrated with each other and with other measures, practices and procedures of the organization and third parties on whom the organization's business processes depend, so as to create a coherent system of security. This requires that all levels of the information cycle-gathering, recording, processing, storing, sharing, transmitting, retrieving, and deleting are covered. Issues to be considered include:
- Security policy and management included as an integral part of the overall management of the organization;
 - Concurrent development of security systems with information systems or, at least, harmonization of all security processes to provide a consistent security framework;

- Review of interrelated systems to ensure that the level of security is compatible; and
 - Risks relating to third parties on whom the organization's business processes depend.
6. **Reassessment**—Security must be reassessed periodically. The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time. Issues to consider include:
- Increase in dependence on the information systems requiring an upgrade to the business continuity plans and arrangements;
 - Changes to the information systems and their infrastructure;
 - New threats to the information systems requiring better safeguards;
 - Emerging security technologies providing more cost effective safeguards than were possible earlier; and
 - Different business focus, or organizational structure, or legislation necessitating a change in the existing level of security.
7. **Timeliness**—Security procedures must provide for monitoring and timely response. Organizations must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner in proportion with the risk. The increasingly interconnected real-time and trans-border nature of information and the potential for damage to occur rapidly, require that organizations act swiftly. Issues to consider include:
- Instantaneous and irrevocable character of business transactions;
 - Volume of information generated from the increasingly interconnected and complex information systems;
 - Automated tools to support real-time and after-the-fact monitoring; and
 - Expediency of escalating breaches to the appropriate decision making level.
8. **Societal Factors**—Ethics must be promoted by respecting the right and interest of others. Information and the security of information should be provided and used in such a manner that the rights and interests of others are respected and that the level of security must be consistent with the use and flow of information that is the hallmark of a democratic society. Issues to consider include:
- Ethical use and/or disclosure of data or information obtained from others;
 - Fair presentation of the data or information to users; and
 - Secure destruction of data or information that is sensitive but no longer required.

**Appendix A:
HIPAA Security Requirements Control Type
Mapping**

	Requirement	Control Category
1.	Administrative Procedures	
A	- Certification	Management
B	- Chain of Trust Partner Agreements	Management
C	- Contingency Plan	Management
D	- Formal Mechanism for Processing Records	Management
E	- Information Access Control	Management
F	- Internal Audit	Management
G	- Personnel Security	Management / Operational
H	- Security Configuration Management	Management / Operational
I	- Security Incident Procedures	Management / Operational
J	- Security Management Process	Management
K	- Termination Procedures	Management
L	- Training	Management
2.	Physical Safeguards	
A	- Assigned Security Responsibility	Management
B	- Media Controls	Management
C	- Physical Access Controls	Management
D	- Policy/Guidelines on Workstation Use	Management
E	- Secure Workstation Location	Management
F	- Security Awareness Training	Management
3.	Technical Security Services	
A	- Access Controls	Management/Technical
B	- Audit Controls	Operational/Technical
C	- Authorization Controls	Operational/Technical
D	- Data Authentication	Technical
E	- Entity Authentication	Technical
4.	Technical Security Mechanism	
A	- Communication/Networking Controls	Technical
B	- Network Controls	Technical
5.	Electronic Signature	
	- Digital Signature	Technical

Appendix B
Reference Material List



Reference Material Listing

A. General

- An Introduction to Computer Security: A National Institute of Standards and Technology (NIST) Handbook
- NIST Generally Accepted Principles and Practices for Securing Information Technology Systems.
- *For the Record—Protecting Electronic Health Information*
- *CoBIT*

B. Specific

Standards Referenced:

A number of industry resources were consulted in the creation of these guidelines. Rather than regurgitate or reinterpret the security concepts, policies and guidelines covered in these resources, this guide provides practical guidelines for a healthcare provider, institution or payer implementing HIPAA security requirements. The resources consulted are mentioned here as a point of reference for organizations going through the planning and implementation process.

Request for Comments (RFC): 2196 Published in September 1997: This guide makes security recommendations for Technical Security Services, specifically for use of the Internet. While the scope of this publication primarily covers the Internet, the principles, guidelines and recommendations can be easily adapted to non-Internet environments.

- National Institute of Science and Technology (NIST) Computer Security Policy Handbook: This handbook provides a comprehensive overview of security control components.
- Department of Defense Trusted Computer System Evaluation Criteria (December 1985)
- ASTM Standards:
- E1869-97 - Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records
- PS115-99 - Provisional Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
- E1986-98 - Standard Guide for Information Access Privileges to Health Information
- E1762-95 - Standard Guide for Electronic Authentication of Health Care Information
- E1985-98 - Standard Guide for User Authentication and Authorization

1. Administrative Procedures

- Federal Information Processing Standards (FIPS) 102: Accreditation and Certification

2. Physical Safeguards

- Federal Information Processing Standards (FIPS) 31

3. Technical Security Services

- **FIPS 186 & 186_1**
- **FIPS 196**

4. **Technical Security Mechanism**
5. **Electronic Signatures**

Appendix C
Business Continuity Planning and Disaster
Recovery

The following section provides some guidelines in developing a business continuity plan and a disaster recovery plan. The section maps to several requirements, which are noted.

Business Continuity Planning	Requirement	Implementation
Critical Business Function Analysis & Prioritization		
1. Mapping critical business functions to applications	Contingency Plan	<ul style="list-style-type: none"> • Applications and data criticality
2. Mapping applications to technologies (platforms, LANs/WANs, data storage, imaging, EDI, etc.)	Contingency Plan	<ul style="list-style-type: none"> • Applications and data criticality
3. Impact of business cycle on prioritization (end of month, quarter-end, year-end, etc.)	Contingency Plan	<ul style="list-style-type: none"> • Applications and data criticality
4. Strategy for regular update and review	Contingency Plan	<ul style="list-style-type: none"> • Testing and revision
5. Clear statement of risk assumption	Contingency Plan Security Management Process	<ul style="list-style-type: none"> • Applications and data criticality analysis
6. Definition of minimum acceptable level of service and detailed actions to get to that level	Contingency Plan	<ul style="list-style-type: none"> • Risk Analysis • Risk Management • Applications Analysis and data criticality
7. Management participation and signoff on prioritization recommendations	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan • Emergency Mode Operations Plan • Applications and data criticality

Business Continuity Planning	Requirement	Implementation
Manual Procedures		
1. Local (desktop) transaction capture & tracking	Media Controls	<ul style="list-style-type: none"> • Data Backup • Data Storage • Disposal
2. Customer interface procedures	Contingency Plan	<ul style="list-style-type: none"> • Emergency Mode Operations Plan
3. Work-in-process (WIP)	Media Controls	<ul style="list-style-type: none"> • Data Backup • Data Storage • Disposal
4. Transaction flow	Media Controls	<ul style="list-style-type: none"> • Data Backup • Data Storage • Disposal
5. Supply Chain procedures	Chain of Trust Partner Agreement	
6. Forms Controls	Security Management Process	<ul style="list-style-type: none"> • Risk Management • Disaster Recovery Plan
<ul style="list-style-type: none"> • Negotiable Documents Controls • Records Retentions • Forms Inventories 	Contingency Plan	

Business Continuity Planning	Requirement	Implementation
Work Around Procedures 1. Hardcopy 2. Reference Manuals 3. Contact Information 4. Procedures 5. Paper Transactions 6. Inventories a) Transactions b) Equipment c) Forms d) Personnel e) Services f) Communications	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan & • Emergency Mode Operations Plan
Business Unit Contingency Teams Organization 1. Emergency Management/Crisis Management guidelines/procedures/decisions 2. Public relations/Media Interaction guidelines 3. Emergency notification process and responsibilities 4. Hardcopy, local backup strategies 5. Key vendor information 6. Recovery Logistics 7. Human Elements 8. Teams Composition a) Skill set match b) Training c) Testing 9. Specific procedures for activating and de-activating contingency operations a) Authorization to activate/de-activate b) Quantified service level thresholds for activation/de-activation c) Triggers to activate/de-activate d) Methods for quantifying degradation of service e) Responsibilities/Authorities/Accountabilities during contingency operations	Contingency Plan Contingency Plan Contingency Plan Contingency Plan Contingency Plan Contingency Plan Contingency Plan Contingency Plan Contingency Plan	<ul style="list-style-type: none"> • Emergency Mode Operations Plan • Emergency Mode Operations Plan • Disaster Recovery Plan & • Emergency Mode Operations Plan • Disaster Recovery Plan • Disaster Recovery Plan • Disaster Recovery Plan • Disaster Recovery Plan • Disaster Recovery Plan • Disaster Recovery Plan & • Emergency Mode Operations Plan

Business Continuity Planning	Requirement	Implementation
10. Voice Communications a) As part of business functions b) As part of BCP	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan & • Emergency Mode Operations Plan
11. Business Continuity Plan Controls a) Plan Distribution b) Plan Maintenance c) Plan Testing d) Responsibilities e) Authorities	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan & • Emergency Mode Operations Plan
Crisis Management Teams & Procedures 1. Crisis Management Teams a) Technical b) Functional 2. Crisis Management Procedures a) Public Relations b) Notifications c) Escalations	Contingency Plan Contingency Plan	<ul style="list-style-type: none"> • Emergency Mode Operations Plan • Emergency Mode Operations Plan

Disaster Recovery Planning	Requirement	Implementation
Critical Applications Analysis & Prioritization 1. Strategy for prioritization	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis
2. Strategy for regular review & update	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis • Testing and Revision
3. Change in prioritization based on shift in business cycle	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis • Testing and Revision
4. Management review/signoff on prioritizations	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis • Testing and Revision
5. Application dependencies/interdependencies	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis
6. Mapping critical applications to business functions	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis
7. Application downtime procedures	Contingency Plan	<ul style="list-style-type: none"> • Applications and Data Criticality Analysis • Disaster Recovery Plan

Disaster Recovery Planning	Requirement	Implementation
Hardware Backup Strategies	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan
Software Backup Strategies	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan
Network Backup Strategies	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan
Testing Procedures	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan • Testing and Revision
Maintenance Procedures	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan • Testing and Revision
Business Impact Analysis & Risk Assessment Map Risks and Impacts Quantify & Qualify Risk Impacts Develop Recovery Strategies Mapped to Risks	Security Management Process Contingency Plan Security Management Process	<ul style="list-style-type: none"> • Risk Analysis • Risk Management • Disaster Recovery Plan • Risk Analysis • Risk Management
Asset Management Inventory	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan
Procedures for return to normal operations	Contingency Plan	<ul style="list-style-type: none"> • Disaster Recovery Plan

Appendix D

SAMPLE POLICIES AND PROCEDURES

Attached are sample policies and procedures that have been contributed by different organizations. These are provided as starter examples only and will need to be reviewed by your organization for applicability and compliance relevance to your situation. The contributors nor the authors accept any responsibility for the use of the attached documents.

In addition to the attached policies there are a few on-line sites that also have posted policies. These include:

- www.privacyexchange.org/buscodes/icp/health_med
- www.3com.com/healthcare/securitynet/hipaa/toc.html

The following attachment on Business Continuity Planning has been contributed by CPRI-HOST.

Business Continuity Planning and Disaster Recovery Planning

The proposed rules for data security and electronic signature, published by the Department of Health and Human Services call for a contingency plan in the section on administrative procedures to guard data integrity, confidentiality, and availability.

The requirement states: “We would require a contingency plan to be in effect for responding to system emergencies. The organization would be required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place. To satisfy the requirement, the plan would include the following:

- Applications and data criticality analysis,
- A data backup plan,
- A disaster recovery plan,
- An emergency mode operation plan, and
- Testing and revision procedures.”

Several web sites offer information on business continuity and disaster recovery planning. The Disaster Recovery Institute International was founded in 1988 to provide a base of common knowledge in contingency planning that serves as the industry's best practices standard “The Professional Practices for Business Continuity Planners”.

It covers:

1. Project Initiation and Management
2. Risk Evaluation and Control
3. Business Impact Analysis
4. Developing Business Continuity Strategies
5. Emergency Response and Operations
6. Developing and Implementing Business Continuity Plans
7. Awareness and Training Programs
8. Maintaining and Exercising Business Continuity Plans
9. Public Relations and Crisis Coordination
10. Coordination with Public Authorities

It is available as at <http://www.dr.org>. DRII also administers the industry's only global certification program for qualified business continuity/disaster recovery planners and provides training courses.

Other web sites with useful information include:

The Disaster Recovery Journal (<http://www.drj.com>) and The Contingency Planning & Management Magazine (<http://www.contingencyplanning.com>).

