HIPAA Compliance Analysis

for

Foundation Services

By

Howard Harvey

Lewis University Class of 2011

Table of Content

Abstract:

Today, the security of information has become an important topic across a wide variety of industries. More over, it is a topic that is frequently misunderstood and under appreciated. Recently the government enacted legislation that forces organizations to question how they conduct operations, and protect the identity of their customers.

This paper addresses the security of protected information from the perspectives of providing health care services. It will expose why some health care service providers see value in proactively deploying measures to protect information. It will also attempt to explain why other organizations continue to struggle with information security, despite "do or die" legislative forces that threaten their ability to deliver services needed services to communities.

It will cover the Health Insurance Portability and Accountability Act of 1996 and explain why it contains provisions for securing patient information. It will answer why some organizations are motivated to become compliant, while some continue to struggle. It will conclude with a case study involving performing an audit of a not-for-profit health care service provider and end with recommending administrative controls for compliance.

Chapter 1: Introduction

1.1 The Sensitive Data Problem

Among the many challenges faced by businesses today are the additional risks associated with handling sensitive information. For some businesses, constant access to current information is the only way to remain competitive and deliver value to customers. [14] Some benefits of having up-to-date information are obvious; they may involve the use of customer information like phone numbers and shopping patterns to provide customized shopping experiences. Detailed information on customers can be a powerful tool for management to predict buying trends or manage inventories efficiently. Making information available where and when it is needed is of such vital importance to businesses that many inappropriately over-allocate resources to ensure its availability. [16]

Equally common are organizations that fail to recognize the value of their information assets. This undervaluation of information can lead to underestimation of the resources required for its security. According to James Broder in Risk Analysis and the Security Survey, [1] "Sixty-four to seventy percent of businesses that have major fires never recover. They go out of business for good, primarily because of the loss of vital business records, particularly their accounts receivable files." [14] Likewise, customer databases often contain lists of credit card numbers, social security numbers, or other sensitive information that if exposed could be maliciously used against their owner. [3]

Information is an important intangible asset. However, like tangible assets, the value of information to the organization should be determined so adequate resources can be allocated for its protection.

Similar to businesses whose primary purpose involves generating profits and building wealth for its owners, not-for-profit organizations measure success on the basis of the number of people they are able to reach. However, unlike for-profit enterprises, many not-for-profit organizations often lack funding to meet their strategic goals. [16] In the current economic climate, many not-for-profit organizations struggle to generate revenues to support the services they provide. This often means that core functions that deliver benefits directly to communities are regarded as high priority while controls that protect information systems take a lower priority. For some organizations, the burden is compounded by federal and state mandates specifically aimed at protecting the public. One such law is the Health Information and Accountability Act (HIPAA). It and others have the primary function of preventing disclosure of electronically protected health information (EPHI). Regardless of the organizations' size, volume of business or core function, if they are covered then HIPAA requires them to implement protective controls.

1.2 Foundation Services:

For over forty years, Foundation Services (a name used to conceal the true identity of the organization) has operated as a not-for-profit entity in the Midwest. The agency was established as an advocate and provider of residential, behavioral health, employment, and other services for people with disabilities. They are a recognized leader in providing community-based support services that enhances independence of its clients. Foundation Services' success is built on a tradition of providing high-quality customized services for its clients and partners. Foundation Services is licensed by local, state, and federal agencies and is accredited by CARF, the Commission on Accreditation of Rehabilitation Facilities.

Foundation Services accepts Medicaid and private insurance; additionally, the organization operates as a member agent of a large umbrella charity organization. Gifts of cash are accepted through a website and at their business office. The organization is also recognized as a federal statute 501(c)(3) charitable organization. [2]

Foundation Services has 475 staff members that serve a community of 750 clients daily. They operate 6 offices in relative proximity to the bulk of their clients. Foundation Services' staff must have timely access to accurate and detailed confidential patient information to perform their daily duties. High availability is important to proper patient care, because clients have unique needs and demand customized services. The integrity of information is also important to Foundation Services' operation because minor errors are potentially harmful.

Foundation Services' staff members possess various degrees of computer literacy. All new employees must undergo training to access patient records. Except for a few exceptions, all staff member are given unique usernames and passwords. This helps the IT department to manage access to data and audit computer usage efficiently. Staff can access patient records from a network of 240 computers, which are conveniently located in four of their six facilities. Staff can also access patient records from binders located in each facility. These four-inch thinks binders contain answers to "frequently asked questions" about individual emergency response procedures, medical conditions, and contact information for guardians. Foundation Services experience high employee turn over, which contributes to company-wide information leakage.

Throughout Foundation Services' history, the organization has operated with a strategy of making information available without regard for its regulatory obligations to protect confidential data. Their information infrastructure has historically grown from a reaction to the increasing needs of the organization for highly available information.

According to the Vice President and Chief Administration Officer, Foundation Services is concerned with the current legal climate in which the healthcare industry operates. They are also concerned that regulations, like HIPPA, expose the organization in ways they did not foresee. There is little background about the organization's security posture; consequently spending remains concentrated on providing controls to support information availability.

1.3 HIPAA and Foundation Services

Management is interested in becoming compliant with HIPAA. They also want to mitigate risks surrounding information management while using resources more efficiently. Specifically, they are interested in policies that govern the use and security of patient information. They believe the right administrative controls will help to eliminate mistakes, provide guidance for staff members and make it easier to hold them accountable. Past attempts to write appropriate policies have failed because they were haphazard, incomplete or unenforceable.

Furthermore, Foundation Services is concerned with inappropriate disclosure and leakage of confidential patient information. Management is aware that its 475 staff members lack awareness about the value and sensitivity of the information they handle daily. The organization took steps to limit information leakage by installing technical controls on each workstation to remove the functionality of USB drives, floppy drives and CD writers. According to the Information Technology Manager, "we've banned all removable storage media from our facilities but continue to struggle with loosing sensitive information."

In an effort to increase availability for off-site staff, Foundation Services allows them to remotely access patient records via secure socket layer (SSL) encrypted tunnels. Management

has growing concerns that this approach to making information available for remote users is not effectively addressing issues of security.

Management believes operating in a secure environment is becoming increasingly important to the future of the organization. They are motivated to become compliant, but they also recognize that there are potential business opportunities from lower risks. They also accept that the organization has a moral responsibility to secure their customers' confidential information. They have already researched HIPPA regulations that may affect them. However, they lack the internal expertise to determine their exposure or how to determine the effectiveness of controls.

1.4 Overview

The purpose of this project is to develop appropriate administrative controls to satisfy HIPAA compliance requirements at Foundation Services. After thoroughly reviewing their information systems and processes, relative to EPHI; appropriate policies will be generated. Relative to cost, policies are the most efficient form of control because they are the least expensive and the most flexible. Also, policies will addresses Foundation Services' areas of concern by providing guidance from a top-down approach. Since policies can be cost effectively updated to address new areas or concern, they are also appropriate to assist Foundation Services to achieving both long-term and short-term goals. Appropriate policies will also allow management to efficiently allocate funds by minimizing the cost of deploying physical and technical controls.

Security policies will be effective forms of controls because they are statements from senior management that dictate the role security will play in the organization. New policies will

relate Foundation Services organization structure to specific issue, or to specific systems. Foundation Services will benefit from an organizational security policy, because it establishes how or organization will setup future programs. It will also assign goals and responsibilities; show the strategic and tactical values of security; and outlines how security polices will be enforced. They will also take into account laws, regulations, liabilities, and how they are to be satisfied. An organizational security policy will also define Foundation Services risk appetite, which is an absolute necessarily before deploying controls.

System specific policies will represents management's directives for information systems. They will include policies for hardware, networks and applications. They will also provide an approved list of applications that can be installed on individual workstations. These policies will reflect acceptable uses of systems and databases. They will also describe how various systems are to be secured and describe how firewalls, intrusion detection systems and other counter measures are employed.

Policies for addressing specific issues will also be generated. They will address security specific matters that management believes require greater details. These policies will include explanations of specific issues to ensure employees have a thorough understanding of how to address unique situations. These policies will also be documented so employees will understand situations and also provide detailed explanations of how to comply.

HIPAA was drafted to ensure only minimal amount of specific information is disclosed and only when absolutely necessary. The law does not specify which controls are required to prevent inappropriate disclosure of EPHI, so a strategy of implementing policies is acceptable. Policies will allow Foundation Services to become compliant. They will also help the organization to create a framework, or procedures for completing certain tasks.

Developing policies will involve interviewing key stakeholder and employees who access electronic protected health information. A checklist from "*A Practical Guide to Security Assessments*" will be used to document feedback from interviews. This process is not an exact science; however, it will expose many of the organization's vulnerabilities to HIPAA related incidents.

The project's success will depend greatly on Foundation's management. They must understand the need for a thorough analysis of their systems and visibly champion it from initiation to completion. They must also make it clear to employees this project will be the basis for making important decisions and that their full cooperation is required to ensure its success.

The following chapter will explain the origins of HIPAA. It will discuss how the law relates to information system and why organizations like Foundation Services are motivated to become compliant. Chapter 3 will recommend HIPAA policies to start the compliance process. Chapter 4 will provide additional recommendations, which should be implemented prior doing a risk analysis. Finally Chapter 5 will state conclusions and how HIPAA will affect Foundation Services and similar entities.

Chapter 2

2.1 HIPAA's Purpose and Requirements:

HIPAA is the acronym for the Health Insurance Portability and Accountability Act. Congress passed the law in 1996. Senator Edward Kennedy and Senator Nancy Kassebaum originally sponsored the bill. [19] Consequently, HIPAA is also known as "The Kennedy-Kassebaum Bill". There are two main sections to HIPAA. Title 1 governs the availability and ranges of health insurance plans for individuals with pre-existing illnesses. It also focuses on eliminating discriminatory practices that unfairly increases premiums or deny certain types of coverage. Title I accomplished this by amending the Employee Retirement Income Security Act, the Public Health Service Act, and the Internal Revenue Code.

Title I also provides a mechanism to transfer and continue health insurance coverage for workers and their families when they change or lose their jobs. It also aims to reduce health care fraud and abuse while mandating industry-wide standards for health care information and electronic billing. In short, HIPAA includes provisions to create a safe environment for sharing health information while holding individuals and organizations responsible for inappropriate disclosure. [18]

Title II of HIPAA relates to privacy and disclosure of electronic protected information. It contains rules that establish and enforce regulations for the use and disclosure of Protected Health Information (PHI). [21] PHI includes any health information concerning an individual's health status. Furthermore, it includes information in any form, regardless if it is being processed, transmitted or how it is maintained. HIPAA privacy rules broadly cover information in any state that could potentially link patients to their health statuses. [22]

Title II of HIPAA, also known as the Administrative Simplifications, provides terms and conditions for electronic health care transactions, privacy and security. It does this by categorizing covered entities, into three domains. They are referred to as health plans, health care clearinghouses and health care service providers. [20]

Health-Plans include individual and group plans that provide or pay the cost of medical care. For example, health-plans include health, dental, vision, and prescription-drug insurers and health-maintenance organizations ("HMOs"). They also include employer-sponsored group health plans, government and church-sponsored health plans. Programs that are funded by the government, and whose principle activity is directly related to providing health care are considered health plans. They do not include group employer-administered plans with less than 50 participants. If an insurance entity has a separate line of business, one that includes a health plan, then HIPAA regulations apply to the entity with the health-plan line of business. [4]

Health Care Providers are those entities that, regardless of size, transmit health information in connection with certain transactions. Transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which the Department of Health & Human Services has established standards under HIPAA. HIPAA privacy rules cover health care providers whether they electronically transmit transactions directly or use a billing service. These entities include hospitals, physicians, dentists or others who invoice or are paid for health care. [4]

Health care clearinghouses are those that process nonstandard information into standard information. They include billing services, reselling companies, community health management information systems, and value-added networks and switches. [4] They often receive information from covered entities or send information to covered entities. In most cases, health care

clearinghouses receive individually identifiable health information when they are providing processing services to health plans or health care provider.

Title II of HIPAA relates specifically to the issue of information security. Title II makes it clear how covered entities should comply. It defines numerous offenses relating to healthcare and sets civil and criminal penalties for non-compliance. It also creates programs to combat fraud and abuse within the healthcare system.

Effective October 16, 2003, Administration Simplification (AS) sets standards for providers and health insurance companies to communicate information. AS aims to improve the efficiency and effectiveness of the nation's health care system. By creating rules and a standard format for information exchange, AS is expected to improve services and lower costs. Regardless of location, AS rules apply equally to all entities covered under HIPAA's policies, in addition to the policies of the Department of Health and Human Services (HHS) [21]

Upon request, covered entities must disclose PHI to the individual within 30 days of a formal request. [24] They are also required to provide information to other agencies for investigating cases of fraud or child abuse. With approval, a covered entity may disclose PHI; however, only to aid treatment, payment, or health care operation. In such situations, organizations must ensure that only the minimum amount of information is disclosed. Inappropriate disclosure of information or failure to comply with HIPAA can result in strict fines. For example, negligent disclosure of information can result in a $100.00 find for the first offence, with a maximum of $25,000 per year per person. If personally individually identifiable health information was knowingly disclosed, then fines can increase to $50,000. Fines can increase to more than $250,000 or ten years in prison for offenses that were found to have been committed with intent to sell, transfer, or cause malicious harm. [25]

Controls required by HIPAA are not specifically outlined in the law, but the rules are clear about the level of security that covered entities must achieve. They can use any combination of physical, technical or administrative measures to become compliant.

Physical access controls are generally designed to physically limit unauthorized access to facilities; while ensuring authorized access is allowed. These often include locked doors, security guards or any other reasonable counter-measures. Covered entities must implement policies and procedures to specify proper use of workstations and electronic media. For example, policies should clearly specify how workstations or other electronic devices should be secured. Policies should also clearly document what is acceptable and what is not acceptable behavior. Other policies and procedures should reference how electronic media should be reused, transferred or destroyed.

HIPAA requires covered entities to implement security safeguards that reduce risks and vulnerabilities to a reasonable level. [4] They must also engage in periodic assessments of how well security controls meet the requirements of the security Rules. This means administrative controls must also identify and analyze potential risks associated with maintaining and managing PHI. HIPAA achieves this by mandating the existence of a "Privacy Officer" or "Security Officer" role. Developing and implementing policies and procedures fall under the responsibly of the security officer. The role is important to implementing HIPAA because risks to inappropriate disclosure of information is constantly changing and cannot be eliminated. HIPAA recognizes that risks can only be reduced, so in many cases a responsible privacy officer can minimize risk further by managing controls and access to PHI.

HIPAA requires covered entities to provide appropriate authorization and supervision of workforce members who work with PHI. Organizations must train all workforce members about

its security policies and procedures. Administrative controls must also include appropriate sanctions against workforce members who violate its policies and procedures. [24]

2.2 Business Case HIPAA Compliance:

According to Mark Moody, President of O'pin Systems, an important component of HIPAA gap analysis involves examining the volumes and content of printed reports. Moody argues that, for covered entities, distribution of standard production reports may be the most overlooked and costly area for conducting operations. [26]

A survey on HIPAA compliance by American Health Information Management Association (AHIMA) showed that in 2006 the majority of covered entities were not compliant with the security rule [27]. It concluded that only one-quarter of respondents reported their organizations were between ninety-five and one-hundred percent compliant. Approximately half of responders rated their organizations at eighty-five to ninety-five percent compliant. The AHIMA forecasts only modest gains over recent years, but in some states they concede that the percentage of compliant organizations will decline. [27] Compliance becomes a complex challenge to manage because, regardless of how such high volumes of reports are generated, many covered entities experience increased cost and higher risk with a control framework. [26] The AHIMA's report is a clear case where HIPAA drives profitability by forcing covered entities to efficiently manage PHI. [26]

Some organizations are at higher risks because they generate more reports than others. The AHIMA reports that some medium sized organizations print more than fifteen hundred reports each month. Such high volumes of printed reports make it difficult to track documents

with HIPAA-related content. It also makes it impossible to enforce minimal disclosure and least privilege, required by HIPAA to protected information.

Document tracking is nearly impossible because hardcopy reports are frequently generated from a variety of sources. According to Moody, they can end up anywhere because they are frequently distributed to hundreds of users across dispersed locations throughout the organization.

Sometimes covered entities are forced to generate hard copies because legacy systems do not always communicate. This is an important area of concern for HIPAA as part of the strategy aims to control cost by reducing duplication and errors. Uncontrolled report generation can hinder communications because the information they contain can be potentially out of date. This also creates a chaotic situation for the business because accounting for waste can be difficult. Many businesses find it impossible to determine the exact number of printed documents because they cannot determine how many are reproduced from copies they cannot track.

There are costs associated with physically securing data as it moves throughout the organization. Most often, these costs cannot be quantified because accounting is unaware of them. Furthermore, they are usually associated with processes and systems prior to 1996, when HIPAA first became law.

Moody claims that it is common for some organizations to print more than two million pages per month [26]. At a rate of five cent per page, printing costs can rise to more than six hundred thousand dollars per year. For many covered entities, cutting costs are part of daily operations. This often means minimizing paper usage through automation, outsourcing or policy changes.

For some organizations, the "paperless office" represents a major step in delivering a higher quality of care to patients. In fact, some health care service providers view electronic document processing as the beginning of an industry-wide transformation.

With HIPAA reforms came legislation that provided a new emphasis on Healthcare Information Technology. The laws were created to redefine the way information is stored, evaluated and transmitted throughout the medical community. Some covered entities use HIPAA as the business case for increased automation and are dropping the use of electronic medical records (EMRs) to pursue electronic health records (EHR). EHR is a new initiative that takes the quantitative data from a standard digital health record and makes it accessible to a broader range of public and private entities, while keeping costs to a minimum. [28]

Professional document scanning companies using document scanning software and applying EHR technology makes it possible for covered entities to access digital charts and other medical records with ease. These systems also satisfy HIPAA security rules, while minimizing risks associated with PHI. Most professional document scanning companies will also work with covered entities to ensure patient data is highly secured and available. [28] The economic benefits pursuing HIPAA compliance are obvious when softer costs and benefits, such as the value of having information on time and the impact on productivity, are included.

2.3 Disadvantages of Compliance:

According to George Annas, an ethicist at Boston University, HIPAA regulations force covered entities to adhere to minimum federal standards. He also argues that the security rules lack ceilings on protection of privacy, which makes it difficult to know when entities are compliant. [29] Many claim the regulations are redundant because current laws already address

issues of privacy. They view HIPAA as compounding the complexity and the differences in interpretations of already complicated laws. [30]

Deciphering HIPAA regulations has created an industry of consultants and technical advisors, many of whom have profited from the fears of physicians, medical institutions, suppliers and healthcare insurers. [33] Failure to comply with HIPAA carries a risk of both civil and criminal penalties. The law can impose fines of up to $25,000 per year for each violation. Criminal penalties can be imposed if protected health information was knowingly obtained in violation of the law. For the most serious infractions, such as knowingly selling patients' health information, the Department of Health and Human Services can impose a $250,000 fine and up to 10 years in prison. [25]

Implementing HIPAA is a costly proposition for many covered entities. According Annas, HIPAA related expenditures for hospitals are expected to exceed twice the expenditures for Y2K. It is also expected to create additional financial stress on already strained hospital budgets. [29]

In April 2003, medical researcher Dr. Peter Kilbridge reported on the financial cost of HIPAA compliance to hospitals. He cited a study by the American Hospital Association that estimated the average cost of training to increase by sixteen dollars per employee. He also stated that the cost of printing HIPAA related advisory for each patient is a substantial burden on small hospitals. [33]

HIPAA requires covered entities to keep records of which patients received HIPAA notices. They must also change their behaviors, and their patients' behaviors. This often involves accepting the cost of rebuilding waiting rooms and registration areas to ensure compliance. Dr. Kilbridge cited data from the Healthcare Information and Management Systems

Society and Phoenix Health Systems that showed the cost for smaller hospitals ranges from $100,000 to $500,000. [30] The cost rose to more than $1 million for hospitals with more than 400 beds.

In July 2003, Medscape news reported on an incident that brought HIPAA's aim of increased accuracy into question. The care team for a patient who had undergone cardiac transplantation was notified that the organ donor had blood cultures that had revealed a bacteremia. To facilitate treatment, the hospital's infectious disease consultant contacted the hospital that had cared for the organ donor to gather additional information on the nature of the bacterial organism. Thought the donor had died, the consultant was declined access, because hospital believed HIPAA rules prohibited them from providing this life saving information. [29]

HIPAA transactions were designed to ease information exchange. However, many physicians continue to struggle with getting test results from labs. Medscape, claimed that consultants are unwilling to send documents because they do not know if the transmission will violate the law. Medscape sited a physician from New York, who said "It has been virtually impracticable to obtain faxed information for patients arriving at my institution's ER from other community hospitals. I am amazed that it was not possible to open the public's eye to the unimaginable high cost in terms of delayed care and expenditure." [33]

2.4 Compliance Audit:

A thorough audit is key to generating appropriate HIPAA related controls for Foundation Services. A risk analysis of information systems and business functions forms the basis for performing a thorough audit. It is crucial to do a risk analysis prior to an audit for two reasons. Firstly, high priority risks will draw the auditor's attention so they can be appropriately

addressed. Risks can be mitigated to acceptable levels, relative management stated risk appetite; so analyzing and prioritizing them is an important determinant for doing audits. Secondly, risks cannot be eliminated; so prioritizing them helps to quantify how controls are designed and deployed. Risks analyses are frequently used at the management level for making operational and strategic cost/benefit analysis; that greatly impact spending decisions.

Foundation Services had not completed a risk analysis. Management believes the benefits of a risk analysis will fail to satisfy the short-term needs of the organization and subsequently rejected a proposal to do one. Management conceded that strategically a risk analysis would yield benefits; however, they claimed it would not address their immediate needs for HIPAA related policies.

The audit process continued without the benefit of a risk analysis. It involved interviewing the IT manager and the Vice President of Operations. A HIPAA audit checklist from "*Information Security Risk Analysis*" was used to document responses. The full audit checklist is quite lengthy, and it appears in the Appendix for ease of reference. This checklist was a key component of the audit because is mapped to the actual law in the Federal Register. The next chapter presents a full risk analysis of Foundation using this checklist as a template.

Chapter 3.

3.1 New HIPAA Policies:

The policies resulted from thoroughly analyzing information derived from Foundation Services. They also follow suggested content from the National Institute of Standards and Technology (NIST) 800-66 Special publication on HIPAA Security Rules. NIST 800-66 was an important consideration because of its main function is to provide concepts and tools to assist local, state and federal agencies comply with HIPAA Security Rule. It also provides enough depth and breadth to help private organizations of various sizes select appropriate controls for their unique circumstances.

NIST 800-66 support the compliance efforts of covered entities by ensuring each organization is selecting the best methods and controls, which are appropriately their unique circumstance. It is equally suited for providing information on best practices for the development of compliance strategies. These are important attributes because the publication is used by diverse covered entities across the industry to effectively comply with the HIPAA Security Rule.

The following policies will provide Foundation Services with a basis for becoming compliant with HIPAA. They are documented in outline form so each section can be referenced and independently quoted. Each policy designed for easy reading and clearly outlines exactly what must be achieved.

Policies:

Responsibility to maintain Confidentiality and privacy

Foundation Services, in accordance with federal and state laws, including the **Health Insurance Portability and Accountability Act (HIPAA)** has developed a policy concerning all rights to confidentiality and the privacy that is inherent to this right. Confidentiality is a right and cannot be denied or abridged without the informed consent of the person served or his/her guardian.

Common Definitions:

I. **Records** are defined as any record kept by Foundation Services in the course of providing mental health or developmental disabilities services to individuals or family.

II. **Protected Health Information (PHI)** refers to individually identifiable health information that is transmitted by electronic media, or transmitted or maintained in any other form or medium.

Responsibility to Staff

A. All staff employed by Foundation Services, as a condition of employment, will maintain the confidentiality and privacy of the person served. This includes not only regular employees of Foundation Services, but also consultants and volunteers providing services. Failure to maintain confidentiality and privacy will result in disciplinary action.

B.

Responsibility of Foundation Services

A. Upon being hired by any program within Foundation Services, each employee will be required to read the current Foundation Services Confidentiality and Privacy Policy and to sign an agreement to adhere to it. This procedure will also be followed for all volunteers and consultants.

B. Foundation Services will provide additional, on-going training on confidentiality and privacy issues to all Foundation Services employees to ensure the continued implementation of confidentiality policies.

C. Foundation Services will designate one employee to assume responsibility for ensuring the confidentiality of Protected Health Information (PHI). This person will be designated as the HIPAA Privacy Contact or Privacy officer. All staff and individuals served will receive a Notice of Privacy Practices. Persons served will be asked to sign a Healthcare Agreement and Authorization to verify receipts of the notice.

Release Of Information

A. No information may be released about patients weather by telephone, in person, or in writing unless there is a written release signed by the patient or guardian. The consent form will specify all of the following:

1. The person or agency to whom disclosure is to be made
2. The purpose for which disclosure is to be made
3. The nature and form (i.e., verbal, written, audiotape, videotape) of the information to be disclosed

4. The right to inspect and copy the information to be disclosed
5. The consequences of a refusal to consent, if any
6. The calendar date on which the consent expires, not to exceed 1 year; if no calendar date is stated, information may be released only on the day the consent form is signed
7. The right to revoke the consent at any time

Foundation Services will release only the minimum necessary information for the purpose stated in the release.

Exceptions to Confidentiality

A. In cases where there is danger to the patient or others and the patient and/or guardian are unable to give consent for release of information, confidentiality may be suspended. This would include but not be necessarily limited to:

- Emergency treatment at a hospital
- Notifying police or appropriate agencies for a missing person
- Notifying state department representatives (Department of Public Health, Office of Inspector General) or other appropriate agencies in suspected abuse cases
- Other circumstances where the safety of the individual or others is at risk

B. When Foundation Services is being reviewed for purposes of funding, accreditation, reimbursement or audit by a state or federal agency or accrediting body, patient records may be used by the surveyor and personally identifiable information may be disclosed without consent, provided that it is necessary to accomplish the purpose of the review.

C. For the purposes of statistical compilation, research, evaluation or other similar purpose, information will not be disclosed unless the patient consents to the disclosure of the information.

Confidentiality Regarding Faxes

A. Any information regarding persons served that is faxed to another location will be accompanied with a cover sheet containing a Confidentiality Statement and reference to HIP AA.

Confidentiality Regarding Tours And Visitors

A. Periodically, tours of Foundation Services programs are given to prospective service recipients and community members for the purpose of program observation, education, and public relations. Because of the mandated rights to confidentiality and privacy the person conducting the tour will inform all visitors regarding privacy and confidentiality at the beginning of each tour.

B. Only first names of persons served may be given to tour members and persons served will be discussed only in very general terms. AU tour members will be

informed of Foundation Services' expectation that they will not divulge personal or identifying information obtained inadvertently during the tour or observation.

Confidentiality Regarding Use Of Photographs

A. Occasionally, photographs are taken of individuals or families participating in the programs at Foundation Services. Upon admission to the program, the person served or his/her guardian, if appointed, will be asked to sign a photo release stating whether or not the person will agree to be photographed. Each time a photograph is to be used for publication or any public display the client or guardian if one has been appointed, will be asked to give permission for use of the photograph. This permission will be in writing and will clearly state the specific purpose for the use of the photograph.

B. Persons served and their guardians have the right to refuse permission for photos to be taken or to revoke consent for a particular request at any time by submitting the revocation in writing.

Inspection Of Records

A. Persons served or their guardians have the right to inspect any information contained within their files and to have it photocopied. Foundation Services may charge a fee for copying files. Foundation Services staff will honor such requests for information within 3 business days.

B. If the person or his/her guardian does not understand the contents of the file, staff from Foundation Services will assist in interpreting any areas of concern. Access to the records cannot be denied if the person or guardian refuses such assistance.

C. If the person or guardian asks for modification of the record because they believe the information is inaccurate or misleading, they are entitled to submit a written statement about any disputed or new information. This statement must be entered into the record. This addendum must be disclosed whenever the questioned portion of the record is disclosed.

D. If a person believes that their record contains inaccurate or incomplete Protected Health Information, then a request for amendment can be made. A request to update the record by contacting the designated Privacy Contact and requesting a "Request to Amend Health Information form".

E. Whenever access or modification is requested, a note should be made in the record of the request and any actions taken.

Access To Records

A. Besides the patient and/or his guardian, access to confidential records will be limited to Foundation Services staff, consultants and interns hired to provide services to that individual. These persons will have access only to those portions of information necessary to provide effective responsive services to individuals.

Human Rights Committee

B. Because the Human Rights Committee includes persons who are not affiliated with Foundation Services and because the function of this committee is solely to ensure that the rights of each person served are not violated, access to records is permissible only when a rights issue is being reviewed. All behavior programs submitted to the Human Rights Committee will have all identifying information deleted to protect confidentiality and privacy. Additionally, all members of the Committee are reminded of their obligation to maintain confidentiality should any personal or identifying information be inadvertently revealed.

Volunteers

A. No personal information will be given to volunteers regarding persons served without the specific consent of the individual/guardian. Information regarding medical conditions or behavioral problems may be given to volunteers on a case specific basis at the discretion of the director of the privacy officer or designated appropriate program staff when that information disclosure may be necessary to ensure the safety of the person served and/or volunteer.

Confidentiality of Records

A. Entries in an individual's record referring to actions with another individual will be worded in such a way as to protect the confidentiality of the persons served. At no time will the name of a person served be put on any report, document or note, which

will be placed in the file of another person. This includes progress notes, incident reports and data sheets.

B. Signs or notices regarding individuals served will avoid the use of last names and will be placed in a location, which is not easily observable to visitors.

Conversations

A. Staff will be cautious in discussing persons served with anyone not entitled to information regarding the person. This includes, but is not limited to, conversations with parents, other persons served or persons in the community not connected to Foundation Services. Whenever it is necessary to discuss a persons served with others, staff will ensure that the identity of the person is protected. Foundation Services staff will also be discrete when discussing persons served with other Foundation Services staff when such conversations occur in a public place.

Safekeeping Of Records

B. Foundation Services accepts responsibility for the safekeeping of each individual's record and for securing it against loss, destruction or access by unauthorized persons.

C. In order to safeguard these records, all files will be kept in areas inaccessible to persons other than those authorized to use the files. Information such as behavior

management programs, reports of unusual incidents and data sheets will be kept in a locked cabinet or in an area not easily accessible to unauthorized persons.

D. All documents containing information about persons served will be kept in a location, which is not easily observable to visitors or other employees not entitled to the information.

Retention of records:

A. **Active records** will consist of information current to one year, excluding social histories, assessments and evaluations that are valid in excess of one year.

B. **Inactive records** will consist of documents purged from the active record. Each document will be maintained in the inactive record for a period of seven years, excluding that information that is permanently retained.

C. **Closed files** are created after the individual is no longer receiving services and will be permanently retained. This file will consist of a face sheet, the admission record, intake social history and the discharge summary. After discharge, the closed file will be placed in area designated for all closed files.

D. **Children's records** will be retained until the child reaches the age of 22 or 7 years from when the file is closed, whichever is later.

Removal of Records

A. At no time will the record/files of persons served be removed from Foundation Services premises except with the permission of the Security, appropriate manager, court order or subpoena.

B. Case management staff that work primarily from a home office will be allowed to keep records, files securely locked with the permission of the appropriate Privacy officer or Vice President of Operations.

Secure Storage of Electronic Protected Health Information

A. Any server, database, application, disk storage system, or similar device that contains EPHI should reside on a secure network with the following criteria:

1. The entire network is isolated from all other networks by at least one firewall that prohibits all inbound connecting traffic (other than through a VPN) to computers housing EPHI.
2. All devices comprising the physical network (routers, switches, VPN gateways, firewalls, etc) are configured, managed, and monitored by one organization solely responsible for the entire secure network.
3. Domain Name Service (DNS) entries for devices housing EPHI on the secure network will not be broadcast outside of the secure network.
4. Internally, the secure network will utilize network devices that prohibit

connected devices (such as network sniffers) from eavesdropping on network traffic. Diagnostic sniffing by authorized network management is allowed.

5. All data traffic entering and exiting the secure network via the VPN gateways and firewalls must be logged. Logs will be maintained for 12 months.
6. All network computer equipment (routers, switches, etc.) should be physically secured and access should be controlled

A. Only networks meeting the technical standards outlined in above will be considered secure. Exceptions may be considered on a case-by-case basis. All exceptions must be reviewed and approved by the Privacy Officer or his or her designee.

B. *(Note: There will be no permanent connection between secure networks). Occasional connectivity between secure networks is permitted as long as the connection is handled in a secure manner, such as a virtual private network (VPN) tunnel.)* Files containing EPHI should be stored on file servers residing on a secure network. Files may be stored on personal workstation local hard drives only under the following circumstances:

1. The personal workstation resides within a secure network
2. The personal workstation is not connected to any network or other computers.

C. Workstations accessing EPHI may reside outside the secure network. However, they may access EPHI data only through a secure method, such as a VPN.

D. An alternative mechanism for reasonably ensuring the privacy and confidentiality of EPHI hosted on servers is to establish network router based access control lists that only allow specific networks or devices to communicate with EPHI servers.

E. If it is impractical (financially or otherwise) to secure EPHI using one of the above methods then an explanation must be submitted to the privacy officer detailing the measures to be taken to adequately ensure the privacy and confidentiality of its EPHI. One such measure may be to encrypt EPHI on an unprotected server and implement 2-key access control. The Privacy Officer will be responsible for approving these measures.

Identification of Electronic Protected Health Information

D. Each database, application, set of files, or other electronic repository of PHI must be identified with the following information:

- General description of the data
- Where the data is stored
- Who owns or controls the data (custodian)

This information about PHI will be made available to the Privacy Officer upon request.

Access to Electronic Protected Health Information

A. Each custodian of a PHI repository is responsible for the security of that PHI. Custodians will determine, track, and monitor who has access to the PHI.

Custodians are responsible for determining that the level and type of access for each member of Foundation Services Workforce is appropriate and are based on Foundation Services' current HIPAA policies. Custodians of high-risk PHI repositories, such as those that are enterprise-wide in nature, contain data on a large number of Individuals, or are accessed by a large number of the Foundation Services Workforce, should keep a regular log of who accesses the PHI and when. Access should be disabled or deleted when a user is no longer authorized to access the system.

Credentials for Accessing Electronic Protected Health Information

A. PHI access should require at least two "keys" to be accessed. At least one of these "keys" must be user-specific password, such as a logon password used to gain secure network access. The other "key" may be an additional password (e.g. workstation/screen saver password, file level password, or application password); it may be a physical key, such as a locked office; or it may be the fact that the workstation is part of a secure network. PHI custodians should assign each authorized user a unique password that is to be protected by that person and not shared with others. Group usernames and passwords are permissible only for access to small, special-purpose PHI repositories associated with particular projects. In such circumstances it is important to establish difficult to guess usernames and passwords. A procedure for changing the usernames and passwords when group membership changes must be submitted to and approved by the Privacy Officer. Passwords should follow these guidelines:

- They must be at least six characters in length and contain both alpha and

numeric characters.

- All user-level passwords should be changed at least every six months.
- All system-level passwords (i.e., root, enable, system administrator, application administration accounts, etc.) must be changed at least quarterly.
- Passwords should not be reused within 3 iterations.

Foundation Services Workforce Accountability

A. Each member of the Foundation Services Workforce should access only those electronic systems or other electronic PHI repositories that they are authorized to access. Each person is responsible for keeping his or her password secure. Passwords should NOT be shared with anyone else. Users should NOT log onto any system or EPHI repository for someone else. Passwords should NOT be posted where they can be easily viewed. Users SHOULD change passwords regularly. Users SHOULD use passwords that are difficult to guess.

B. Each person should take reasonable steps to keep PHI secure from unauthorized individuals. For example:

- Workstations should not be left unattended and/or unprotected in public areas.
- Users should log out of any system or workstation when they have finished using it.
- Each person should report all security breaches or violations through one of the following channels (in order of preference):

    A. Individual's supervisor

    B. Supervisor's supervisor

C. Privacy Office

Electronic Sharing/Transmission of Data Containing Electronic Protected Health Information

A. PHI should only be shared with authorized parties, in accordance with all applicable laws, rules, regulations, and Foundation Services' policies.

B. When transmitting EPHI electronically outside of the secure network, one of the following methods should be used:

- Virtual Private Network (VPN) tunnel
- File encryption/decryption (e.g. PGP encryption)
- Secure Socket Layer (SSL) encryption

Communications of Electronic Protected Health Information by E-Mail

A. E-mail messages containing EPHI, which cannot be sent in encrypted form, should only be sent in limited circumstances, and with specific safeguards such as encryption. For provider to patient communication, PGP encryption or similar method is preferred. This allows for an email to be sent to the patient securely.

B. Email should also contain the following notification:

"The materials in this email are private and may contain Protected Healthcare Information. If you are not the intended recipient, be advised that any unauthorized use, disclosure, copying or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this

email in error, please immediately notify the sender via telephone or return mail."

Physical Security Measures to Ensure Protection of Privacy

A. Each Business Unit must define where and how PHI is stored or used in formats other than electronic. They should also require two key accesses. That is, access to PHI should require at least two "keys" to be accessed. Examples include a locked desk, file cabinet or overhead bin in a locked office and locked office, storage room or records room in a locked suite.

B. The "2-key concept" should be in place after working hours and at any time during the workday in which the storage area or clinical work area is unattended. Special attention will be given to persons who hold keys to the areas containing PHI and the distribution of keys should be recorded and adjusted as staff join or leave the Business Unit. A general criterion for deciding who should have keys is the minimum amount of access to PHI required to accomplish an assigned task.

C. Each Business Unit will develop a policy and process for records containing PHI to leave the secure area in which they are typically stored. Examples include medical record transportation from storage area to clinical Treatment area and any allowance for removal from the premises.

D. Process will include a method for logging records out and the ability to know the whereabouts of the records and responsible party at all times. Process will also ensure that the records are not left unattended at any time. Custodians of PHI stored in formats other than electronic are defined as those persons with authority to make decisions on who will have access to PHI and the extent to which PHI will be released to the requesting party. Any person qualifying as a custodian of PHI will abide by Foundation Services policies related to the use or disclosure of PHI.

E. Custodians must become be familiar with the term "designated record set" and configure the method for storing PHI that is in a non-electronic scheme in such a manner that isolates items that are not considered part of the Designated Record Set.

F. Each Business Unit will establish a policy related to visitors to areas in which PHI is stored during business hours.

G. Each member of Foundation Services Workforce should access only those physical PHI repositories that they are authorized to access. Logs and checklists containing PHI required as part of daily operations should be evaluated for best location in the work area to provide maximum security of the privacy of any one Individual. Breaches or violations of physical security should be reported the Privacy Officer.

Chapter 4.

Additional Recommendations:

A. Management should generate a corporate organizational policy that governs how Foundation Services will function. An organizational policy will serve as a base for all other policies, including an enterprise security policy.

B. A risk analysis should be completed before assessing current controls or implementing new ones. A risk analysis is important for a number of reasons. Firstly, it exposes many of the vulnerabilities and threats associated with current controls, or lack of controls. Furthermore, a risk analysis will allow management to prioritize the organizations risks for input to a cost benefit analysis.

C. Foundation Services collects donations from credit cards through a website and at their offices. Processing credit card transactions exposes the organization to additional risk associated with handling credit card information. Furthermore,

processing credit cards subject to organization to Payment Card Industry rules and the Data Security Standard rules.

Chapter 5.
Conclusion:

HIPAA security rules were drafted with the aim of improving delivery of health care across the US landscape, while protecting private consumer information. It is also becoming increasingly important to the health care system as the aging US population continue to drive up the cost of delivering care.

The government recognized the criticality of private information and included the security rules in HIPAA as a measure to protect the public. It was important to go beyond Administrative Simplification because many organizations handling consumer health information were primarily concerned with their core business strategies. Prior to HIPAA, health care organizations pursued strategies ranging from building shareholder equity to delivering not-for-profit humanitarian services. The changes brought by HIPAA resulted in transformation the business landscape and forced organizations to safeguard private information.

HIPAA security rules apply equally to all covered entities. Regardless of status as a for-profit or not-for-profit, covered entity must update their practices. New practices include

updating policies, adding technical controls or doing expensive renovations. HIPAA does not dictate the type of measures for protecting privacy. However, it does make the levels of security required very clear.

Covered entities with core strategies of pursuing profits are more likely to invest in costly controls to become HIPAA compliant. This is primarily due to the long-term competitive advantages they gain from compliance over the short-term benefits of non-compliance. Many for-profit organizations will invest in HIPAA controls because the business case is in line with their strategic vision. This includes the long-term gains in efficiency, profitability and improved corporate image.

Many not-for-profit covered entities will continue to struggle with investments in HIPAA. Though the benefits of compliance are common to both for-profit and not-for-profit covered entities, many not-for-profit organizations view the "long-term benefits" as less tangible, and consequently less valuable. Not-for-profit organizations have limited budgets. Most view the expensive controls, demanded by HIPAA, as hindrance to their short-term efforts of serving the immediate needs of the communities in which they operate. Additionally, business leaders view a strategy of diverting limited funds to projects, without immediate payback, as ignorance of their fiduciary duties. This view threatens many not-for-profit organizations and undermines their long-term survival.

A HIPAA audit is the mechanism by which covered entities measure compliance with the law. Audits result in an unbiased examination and evaluation of the covered entity's policies, procedures and controls. They are often powerful barometers of changes in the environment and the effectiveness of existing controls. Organizations change over time, so audits encourage stakeholders to adequately deliberate, based on facts. Most importantly, audits provide valuable

information so viewpoints or decisions can be explained if necessary. A risk analysis should be completed prior to an audit. Analyzing risks prior to doing is extremely important because it audits draws attention to problem areas; thus increasing the value of resulting information. Without the benefit of a risk analysis, controls cannot be effectively deployed because high-risk areas could be ignored.

Under HIPAA, covered entities must do regular audits. HIPAA does not clearly state the frequency of audits, but covered entities must do them at appropriate intervals to ensure the effectiveness of controls. For this reason, some entities find HIPAA requirements vague, but rely on established frameworks for audits. NIST 800-66 is the established standard for doing HIPAA audit. This is because the requirements come directly from the federal register. They are also used at the local, state and federal level to establish compliance. Lastly, NIST 800-66 is the standard because above and beyond the audit requirements, it recommends controls for becoming compliant.

Appendix

QUESTIONNAIRE STRUCTURE

The specific sections of the HIPAA security questionnaire are as follows:

1) Is the entity subject to the HIPAA security regulations?
2) What is the extent of the electronic protected health information?
3) HIPAA security requirements

– Administrative security regulations

– Physical security regulations

– Technical security regulations

This HIPAA security questionnaire follows the regulations from the *Federal Register*.

The questions in the HIPAA requirements section are structure as follows:

·Specification directly from the HIPAA security regulation (as stated in the *Federal Register*).

·For each requirement there are a set of questions to help determine whether a client is in compliance with the requirement. They are designed to help determine whether the company is in compliance with the specific HIPAA regulation.

This questionnaire is designed to be comprehensive as it covers the entire set of HIPAA security requirements. Although the requirements are fixed, the supporting questions used to determine compliance will vary according to the client's response.

IS THE ENTITY A "COVERED ENTITY?"

The applicability of HIPAA comes into question when a company provides some form of health care services. By providing health care services, the entity is most likely dealing with some patient records, which may be in electronic format and containing patient–identifiable information. In the *Federal Register*, the HIPAA regulations state that the HIPAA security standards are applicable to health plans, health care clearing houses and health care providers who transmit EPHI.

1. Is the entity a health plan?

Does the entity provide or pay the cost of medical care? If so then the entity falls into the following category:

1. Group health plan
2. Health insurance issuer
3. Health maintenance organization (HMO)
4. Part A or Part B of the Medicare program
5. The Medicaid program

6. An issuer of a Medicare supplemental policy
7. An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy
8. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers:
9. The health care program for active military personnel under title 10 of the United States Code
10. The veterans health care program under 38 U.S.C. chapter 17
11. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
12. The Indian Health Service program under the Indian Health Care Improvement Act
13. The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
14. An approved State child health plan
15. The Medicare + Choice program under Part C of title XVIII of the Act
16. A high-risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals
17. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2))

18. Health plan excludes (from 45 CFR 160.103 Definitions):
19. A group health plan
20. Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

21. A government-funded

– Whose principal purpose is other than providing, or paying the cost of, health care; or

– Whose principal activity is:

– The direct provision of health care to persons; or

– The making of grants to fund the direct provision of health care to persons

Guidance: The list above provides guidance to determine whether the entity is a health plan. This guidance is from the original HIPAA regulations.

Client Response: No we are none of those

2. Is the entity a health care clearinghouse?

Is the entity one of the following (from 45 CFR 160.103 Definitions):

· A billing service? **No**

· A repricing company? **No**

· A community health management information system or community health information system?

· A value-added network and switch? **No**

If the entity is one of the items listed above, does it perform one of the following functions (if so, the entity is a health care clearinghouse):

· Does it process or facilitate the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard *data elements* or a standard transaction? **No**

· Does it receive a standard transaction from another entity and process or facilitate the processing of health information into nonstandard format or nonstandard data content for the receiving entity?

Guidance: This guidance above is also directly from the regulation. To answer the questions to determine applicability as a health care clearinghouse, knowledge of the standard transactions is required. Interaction with those involved with implementation of the standard transaction code sets may be required.

Client Response: The client is not a health care clearinghouse

3. Is the entity a health care provider transmitting health information in connection with certain transactions?:

Does the entity transmit information with other parties to carry out financial or administrative activities related to health care where the following types of information are transmitted (If so, entity is a health care provider):

· Health care claims or equivalent encounter information? Yes

· Health care payment and remittance advice? Yes

· Coordination of benefits? Yes.

· Health care claim status? Yes.

· Enrollment and disenrollment in a health plan? Yes.

· Eligibility for a health plan? Yes.

· Health plan premium payments? Yes.

· Referral certification and authorization? Yes.

· First report of injury? Yes.

· Health claims attachments? Yes.

· Other transactions that the Secretary may prescribe by regulation? Yes.

Client Response: We are a health care service provider.

4. Is the entity a "business associate"?

Guidance: Business associate relationships arise when a person or entity provides services on behalf of a covered entity but is not a member of its workforce. If the work performed involves the handling of protected health information covered under HIPAA. The activities can vary and can include billing, claims processing, data analysis and others.

Client Response: This question does not apply as we are a health care service provider.

5. Does the organization work with third-party administrators that handle personally identifiable patient records at their offices or at their satellite offices (or home offices)?

Guidance: Based on the HIPAA definition of "covered entities," these third-party administrators are an extension of the company and are thus subject to the HIPAA security regulations.

Client Response: We work with other organizations but they do not administer our information. Information is transmitted primarily through fax and emails.

6. Are there individuals who work from home or remote sites where they handle or transmit personally identifiable health information? What specific processes are these employees performing?

Guidance: This is important to understand because the workforce of a "covered entity" includes everyone on site as well as everyone off site — i.e., the security standards must be implemented for all workers. The relevant implication here is that if people are working from home, the "covered entity" is required to ensure that the appropriate security standards are implemented.

Client Response: Yes, we have field workers that use laptops. They input and update client information that is transmitted to our servers over an encrypted vpn tunnel.

If the entity passes one of the criteria listed above, the HIPAA security requirements are applicable and the entity information security program should be assessed against those requirements.

APPLICABLE DATA AND PROCESSES — WHAT IS THE EXTENT OF PROTECTED HEALTH INFORMATION?

The questions in this section are to help in determining the scope of the HIPAA security review. Some of the main drivers of HIPAA security are where electronic protected health information resides and how it is transmitted. The questions below are not part of the actual regulation but are here to help determine which systems will require a detailed review and which types of

technology expertise will be required when conducting the assessment. For the questions in this section, as with the others, it is critical to talk to the appropriate business and technology owners.

1. Critical processes: Describe the processes related to patient records. What applications and systems are used to process patient records? This includes all patient processes including (but not limited to):

· Patient appointments

· Patient diagnosis

· Transcription services

· Patient billing

· Patient collections

Guidance: This is a general question meant to begin identifying the processes and systems as they pertain to electronic protected health information.

All of the processes above and probably some others (depending on the organization) deal with electronic personally identifiable health information being processed and stored. This information will help you drill down into detail about the relevant processes and systems.

Client Response: This is a difficult question to answer, since we have information located everywhere. Some is located in our exchange server because we send it in emails sometimes. Some could be is personal folders. In any case, all of the information is located at 777 Joyce.

2. Where is the data?

Guidance: This is an extension of the previous question.

· *Personally identifiable health information:* The HIPAA security requirements are only applicable to *electronic personally identifiable* health information. This includes anything in the patient's records that links a person to health-related information. The HIPAA security regulations *do not* apply to health data that cannot be correlated to specific persons. An example where an organization might have health-related data that is not subject to HIPAA security is research organizations, which collect vast amounts of data for research and analysis purposes.

· *Information in electronic form:* The HIPAA security regulations are not applicable to any data in *physical form.* In addition to information stored on specific machines, "electronic form" also refers to protected health information on magnetic tape, disks, or other readable media.

Client Response: Data is located in the following locations:

Database server at 800 Black road

Database server at 2401 Jefferson Street.

Database server at 134 Van Buren Street

Cloud Backup

3. Transmission of data: How is personally identifiable data transmitted and to whom is it transmitted?

Guidance: Under the HIPAA security regulations, electronic protected health information includes personally identifiable data while in transit, which could be within an internal network or out through the Internet. Although the data that resides on specific

machines can be identified by examining what is on the different systems, identifying data in transit will require that you speak to individuals who are familiar with how data flows across the network and how the different applications talk to each other.

Client Response: We transmit data by email. Primarily case notes.

4. Portable devices: Are portable devices such as personal digital assistants (PDAs) used for any processes using personally identifiable health information?

Guidance: Under the general term, "workstation," the definition in the HIPAA security standards includes (per the *Federal Register*), "…portable devices…any other devices that performs similar functions, and electronic media stored in its immediate environment." This can include PDAs (personal digital assistants) or other similar devices. If PDAs are in use, you will also have to look at the use of wireless networks at hospitals and what type of associated security measures are in place.

Client Response: Yes, 8 individuals with access to emails vie iPhones. The president, 2 VP's, IT Manager and 2 Maintenance staff.

5. Telephone and "faxback" systems: Are telephone and faxback systems in use where the entity provides protected health information via fax based on a telephone request? If so, the information faxed back would be considered protected health information.

Guidance: In this scenario, only the party that is faxing the information based on a telephone request is obligated to secure the protected health information being faxed as this is in electronic format. The initial request made using the telephone is not subject to HIPAA security regulations because this information is not in electronic form.

Client Response: Yes, lab results are transmitted by fax. Nurses have private faxes. Documents are printed to password-protected mailboxes.

6. Are there individuals who can access electronic protected health information via a wireless connection?

Guidance: Wireless is growing very quickly and there is a good chance that the entity being audited is using wireless. Doctors, nurses, etc., can use wireless in a number of different areas. In addition, doctors may also be using wireless at home to access hospital networks, where they may be accessing electronic protected health information or have the ability to do so.

Client Response: No, just by iPhones as stated in the previous question.

HIPAA SECURITY REQUIREMENTS

This section contains questions regarding the actual HIPAA security requirements.
Much of the information is directly from the actual law in the *Federal Register*. The guidance section in some of the questions contains some of the commentary that was given by the public, as the law was being reviewed and crafted. As you go through the questions, you should note that many of the requirements imposed in the HIPAA security regulations are simply good security practices. Many of the requirements map back to information security best practices such as the International Standards Organization (ISO) 17799.

Before going through the HIPAA security requirements, it is worth discussing how the HIPAA regulations are set up. The specific requirements are referred to as "standards." For most of the

standards, specific instructions for implementation exist, which are either "required" or "addressable." Each of these concepts is discussed in further detail below.

· *Standard* — Standards are the actual HIPAA requirements. They are similar to security policies as they are high-level requirements with which entities must be in compliance. As discussed in earlier chapters, however, these requirements or "policies" should be broken down into procedures to help personnel be compliant with them. The "procedures" in this case are the specifications, which are either "required" or "addressable" (discussed below). In some cases, the standard is very clear and consequently, no specifications exist. In these cases, the standard is supposed to serve as the instructions also. Keep in mind that standards must be complied with.

· *Required* — Covered entities must be in compliance with the "required" specifications — i.e., they have no choice. Essentially, these can be viewed as the minimum requirements with which all covered entities must be in compliance. As will be seen later, although these are minimum requirements, there is flexibility in how these specifications can be accomplished relative to technology and processes. In the context of a security assessment, security consultants should use their expertise to develop recommendations that address these "required" specifications in a cost-effective manner.

· *Addressable* — With the "addressable" specifications, entities have flexibility. These specifications are essentially suggestions, which entities should implement if they deem it is reasonable for their environment based on a number of factors determining the overall risk. If the measure is deemed reasonable, the entity must implement the "addressable specification." If it is not deemed to be reasonable, the entity can do one of two things:

– Implement an alternative measure that is more appropriate for their environment and that accomplishes the same goal

– Implement no measure, accept the associated risk, and document the rationale for not implementing the "addressable specification" In terms of a security assessment, companies should be advised regarding these "addressable" specifications. Whether or not to implement these specifications comes down to a few considerations:

·*Cost-benefit analysis* — Does the addressable specification make sense based on the risk being mitigated, and are there alternatives that can accomplish the same goal with less cost?

· *Justification* — If no measure is being implemented, can the entity provide a reasonable justification for not implementing the "addressable" specification? Consider the impact to the entity if a security incident results from not having the particular security measure in place.

· *Measure might not be applicable* — The entity might deem that a given measure is just not applicable to its environment and thus not do anything.

In any case, with all HIPAA specifications, the entity must ensure that they document whatever they do. In the case of "addressable" specifications in particular, it is crucial to document the rationale for whatever action the entity finally decides on.

The questionnaire is structured so that the required and addressable specifications are listed separately for each standard. For each set of specifications, some questions and guidance are provided in this questionnaire that could help you discuss them.

Some of the guidance and additional questions are based on the comments and questions received from the general public during the period when the public was reviewing the requirements. Note that in some cases, there are no specifications and only a standard. In these cases, the standard is required.

ADMINISTRATIVE PROCEDURES

Below are the questions for the Administrative Safeguards section, which is Section 164.308 in the Federal Register. The Administrative Safeguards are mostly the Security Management–related topics related to HIPAA. These specifications are similar to the "Security Policy" and "Organizational Security" sections of ISO 17799.

As stated earlier, many of the HIPAA requirements are recognized information security best practices.

1. STANDARD — SECURITY MANAGEMENT PROCESS

This standard requires that the covered entity "implement policies and procedures to prevent, detect, contain, and correct security violations"1 This statement basically requires covered entities to have a formal information security program in place.

The program requires a foundation of policies and procedures that secures the entity.

a. REQUIRED Implementation Specifications

i. Risk Analysis

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

In determining compliance with this requirement, below are some questions that can be asked. These questions are related to risk analysis and some key aspects that you should look for.

1. Did the covered entity perform a risk analysis to determine the potential risks to the confidentiality, integrity, and availability of electronic protected health information?

Guidance: Look for a risk analysis that is documented and recently performed. The document should contain specific vulnerabilities and risks as well as a mitigation strategy. Because environments from the information technology (IT) and organizational perspectives can change, it is important to understand when the risk analysis was performed and whether any significant changes have occurred since it was done. The risk analysis might have little value if it is too old.

Client Response: No.

2. Was the risk analysis independently performed?

Guidance: The risk analysis can arguably be viewed as the most critical component of the HIPAA security requirement because it defines what security measures need to be enhanced or put in place. An independent risk analysis lends significant credibility to a risk analysis. Independence can mean a third party or an independent internal group such as internal audit.

The basic point of this question is to ensure that the analysis was objective.

Client Response: This doesn't apply because we did not do a risk analysis.

3. Is the risk analysis documented with risks and recommendations clearly stated?

Guidance: The risk analysis should be documented so that evidence exists that it was done and so the findings resulting from it are clearly defined.

The risk analysis "deliverable" should map risks and recommendations to help facilitate mitigation activities. Ideally, the risk analysis should basically serve as the roadmap for

specific information security initiatives to achieve compliance with HIPAA security requirements.

Client Response: This doesn't apply because we did not do a risk analysis.

4. Does the risk analysis clearly define the extent to which electronic protected health information exists?

Guidance: From a methodology perspective, the risk analysis should clearly state the extent to which electronic protected health information exists. The risk analysis should have examined all processes and systems where electronic protected health information travels and resides.

Client Response: We will have to do a risk analysis in the future.

5. Does the risk analysis define what the critical systems are (i.e., where the electronic protected health information resides)? In addition, did the risk analysis accomplish the following:

· Were the technical security measures in place to protect these systems considered in the risk analysis?

· Was the network architecture considered?

· Was the security architecture considered (e.g., firewalls, intrusion detection, host level controls)?

· Was any hands-on testing performed to validate the security measures in place?

· Were the logging and monitoring processes considered?

Guidance: Similar to defining what the electronic protected health information is, the systems on which it resides are equally important. Once these systems are identified, the security architecture protecting these critical systems should have been evaluated and hands-on testing should have been conducted based on the level of risk.

Client Response: No risk analysis.

6. Does the risk analysis consider potential impacts of breaches of security related to the confidentiality, integrity, and availability of electronic protected health information?

· Were the potential impacts quantified to the extent possible?

· Were anticipated uses or disclosures of information identified as part of the risk analysis?

Guidance: To properly determine risk, the analysis must determine the potential impacts related to security violations. In this area, it is critical to make sure that individuals from the business side are involved as they will either know or be able to validate the potential impact. The quantification of the impact, if it is possible to determine it, helps determine how to prioritize security recommendations resulting from the risk analysis.

Client Response: No risk analysis

7. Did the risk analysis include meeting with both business process and technology owners?

Guidance: It is critical to involve both the business process and technology owners in the risk analysis process. Too often, the technology owners take the responsibility for performing the risk analysis and as a result, it is very focused on technology. Because we are concerned about electronic protected health information, where it resides, how it

flows, etc., it is critical to involve business process owners. They will typically have more knowledge of the importance of the electronic information and what some of the risks are. In addition, business process owners may be able to tell you more about the process that you would not necessarily know by talking to someone from the technology side.

Client Response: No risk analysis.

ii. Risk Management

"Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with"3 [Section 164.306 — requiring companies to periodically evaluate security measures].

This is effectively the next step after the risk analysis. Covered entities have a significant amount of flexibility in implementing security measures based on how appropriate the level is defined below (based on Code of Federal Regulations section 164.306):

· Ensuring the confidentiality, integrity, and availability of electronic protected health information

·Protecting against any reasonably anticipated threats or hazards to the security or integrity of the electronic protected health information

·Protecting against any reasonably anticipated uses of disclosures of electronic protected health information not permitted

Below are some questions to help determine compliance with this requirement.

1. Based on the risk analysis, have the risks been mitigated with specific security measures? If not, is a plan in place to ensure that the risks are mitigated?

Guidance: To meet this requirement, appropriate security measures must be put in place to mitigate risks identified in the risk analysis. If measures have not been implemented, having a plan in place should help ensure that corrective action is taken. You should verify mitigation steps based on the level of risk involved. Here, you can use a combination of tools and manual

procedures to perform testing.

Client Response: No risk analysis

iii. Sanction Policy

"Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."

The sanction policy is essentially the enforcement component of an information security program. It requires sanctions against individuals for noncompliance relative to the HIPAA security requirements. Below are some questions to help determine compliance with this requirement.

1. Is there a process in place for detecting noncompliance with HIPAA security requirements?

Guidance: Is there a way for the entity to know if a lack of compliance is present? In looking at noncompliance, automated means such as system alerts when noncompliance occurs are the most efficient method of knowing about noncompliance. With certain specifications, the only way to

check for compliance is to do it manually. In any case, there should be a process for determining noncompliance with HIPAA security requirements.

Client Response: No

2. Are there policies and procedures in place so that individuals know what they must comply with?

Guidance: There should be some standards or polices that personnel have access to, which state the security requirements that employees must follow. As discussed in earlier chapters, security policies are the foundation of an information security program and are a crucial component of enforcement. Without clear policies that are easily accessible, it is difficult to hold personnel accountable, as compliance standards will not be clear to them.

Client Response: Yes, but they are unrelated to HIPAA. They are also not very thorough.

3. Do a noncompliance policy and procedure exist?

Guidance: There will be instances where employees will not be able to comply with a requirement for a variety of reasons. To facilitate noncompliance reporting of these cases, a noncompliance policy and procedure, which require employees to report areas of noncompliance to management, should be in place. Along with the policy, a form for noncompliance should be used, where information including what specific policy was not followed, reason for noncompliance, and other mitigating controls is documented. This documentation is required by HIPAA and is a good practice because it creates an audit trail.

Client Response: No because we do not have detailed policies.

4. Do sanctions for noncompliance exist and are they based on severity?

Guidance: Sanctions are a key component of handling noncompliance issues. Without sanctions, no repercussion exists for personnel who do not follow the policy. Ideally, the sanctions should be based on severity and other relevant circumstances.

Client Response: Yes, but are not related to HIPAA. They are also not very clear.

5. Is an internal audit process in place?

Guidance: Internal audit will be covered later in this checklist; however, it is an important point when discussing sanctions. Audits provide management with a view of where some of the control weaknesses and noncompliance issues are. The audit process is also an excellent way to enforce HIPAA security requirements. Ideally, the internal audit process should audit for many of the HIPAA security requirements to help ensure compliance with HIPAA security.

Client Response: Not an HIPAA audit policy, but we have surprise audits three times a year from CARF to keep our accreditation.

iv. Information Systems Activity Review

"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

This specification is a "monitoring" requirement as it pertains to ensuring that information systems and data remain secure. Below are some questions to help determine compliance with this requirement.

1. Do documented procedures detail what reports should be reviewed to effectively monitor the systems (e.g., system logs, audit logs)?

Guidance: Activity review should be a planned activity that is documented. The level of review should be based on the criticality of systems, the level of activity on the relevant systems, and any other relevant factors. Depending on the amount of information generated, it might make sense to recommend that the entity use third-party tools to automate the log review process and provide exception reports. There should also be a process that outlines the frequency and nature of review based on the risk.

Client Response: No.

2. Are specific people responsible for log review?

Guidance: In many organizations, if log review is not assigned to someone, it is not done or if it is, it is purely reactionary. Although being reactivein some cases may be appropriate, it may not be when it comes to critical systems. Assigning this responsibility to specific individuals and having clear expectations with respect to logging will help ensure that logs are being reviewed appropriately.

Client Response: Yes, they are reviewed by the IT manager.

3. Who has access to the various logs used to monitor system activity? Can the people who have access to the logs change the information in the logs without being detected?

Guidance: Access to the logs and the ability to change them should be closely monitored. Segregation of duties should be considered so that people cannot perform any

malicious activity and hide their tracks. This will especially be a problem in small companies, where the staff is typically very small. In these cases, recommendations for alternative methods providing some mitigating controls should be suggested.

Client Response: The IT Manager and 2 administrators have access to the logs. They can also edit them.

b. ADDRESSABLE Implementation Specifications

i. None

2. STANDARD — REQUIRED — ASSIGNED SECURITY RESPONSIBILITY

"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity."

This standard requires someone to be identified who owns the responsibility for the development and implementation of the policies and procedures required by HIPAA security standards. This person can have different titles including Chief Security Officer, HIPAA Security Officer, Compliance Officer, etc. Note that this standard does not have any specifications — i.e., the standard serves as both the policy and instructions for implementing. Below are some questions to help determine compliance with this requirement. Note — there are no implementation specifications for this standard.

1. Does someone in the organization have the responsibility for development and implementation of policies and procedures relative to the HIPAA security standards?

Guidance: In the final regulations, the intent was that one person have the ultimate responsibility for security. Even in cases where different divisions of a larger company may assign responsibility at the division level, there still must be one person who has overall ownership for security. This person might have the title "Security Officer" or some other managerial security–type title. The "Security Officer" should ensure that the development and implementation of policies and procedures involve both business and technology representatives. If this is not the case, it should be flagged and a recommendation should be provided. Ideally, the "Security Officer" should be able to facilitate a coordinated effort in developing and implementing security policies and procedures.

Client Response: Yes, the IT manager is responsible.

2. Does a security awareness program exists to help ensure that implementation of security policies and procedures is successful?

Guidance: Awareness is an important part of implementation to help ensure that personnel know and understand security policies and procedures.

Once they know about them, they are more likely to follow them, and from management's perspective, they can be held accountable. When evaluating the awareness program, keep in mind that not all personnel have to attend all of the training — i.e., personnel should attend the training they need.

Client Response: Yes, but only for new employees. We don't have on-going awareness training.

3. Are security policies and procedures readily accessible so that personnel can refer to them as needed?

Guidance: Personnel will have questions as they apply the policy in their daily jobs. You should ensure that security policies and procedures reside where personnel can easily access them if they need to. If personnel cannot access these documents, it is difficult to enforce them.

Client Response: No, just those provided to new employees.

4. Does the "Security Officer" (or whatever that person's title is) ensure that security policies and procedures are updated as the business and IT environment change?

Guidance: Maintenance of security measures is a HIPAA requirement. Also, it is critical to ensure that policies and procedures are updated as needed. In addition, there should be a process to communicate updates to personnel. If needed, additional security awareness training might also be necessary.

Client Response: We don't have a designated security officer. That is what we are working on right now.

5. Does the Security Officer (or the person who owns security) have the ability to escalate issues to upper management?

Guidance: The Security Officer is something that is new and often, it does not get the visibility that is required for the role to be effective. Security policies and procedures are difficult to implement because people sometimes do not see their value, and they might need to change the way they do things. Aside from the education and awareness that

users are provided, the Security Officer needs to have access to upper management to escalate issues and gain resolution.

Client Response: I am playing the role of the security officer and yes, I can bring issues directly to upper management.

3. STANDARD — WORKFORCE SECURITY

"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, …and to prevent those workforce members who do not have access, …from obtaining access to electronic protected health information."

This requirement basically states that only those personnel who require access to electronic protected health information should have it and those who do not require access should be prevented from having access. Access should be given on a "need to have" basis. Note that this standard does not have any required specifications.

When conducting the HIPAA security review for this standard, you should review the questions from other questionnaires such as User ID Administration and Terminations.

a. REQUIRED Implementation Specifications

i. None

b. ADDRESSABLE Implementation Specifications

i. Authorization and/or Supervision

“Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.”

This specification pertains to access control pertaining to electronic protected health information. Access and authorization are at multiple levels including network, application, and database. The process should address these different aspects of access.

Below are some questions to help determine compliance with this requirement.

1. Does a documented process exist for obtaining authorization to access electronic protected health information? If formal authorizations are not granted, does supervision exist for personnel working with electronic protected health information?

Guidance: Ideally, a documented process should exist for obtaining authorization, at a minimum. The extent and granularity of the procedure willvary depending on the size and nature of the organization. The standard has given considerable flexibility in making this decision.

Client Response: No documented process.

2. Is there a form that is filled out or some type of workflow application to facilitate and document the process for obtaining access?

Guidance: Depending on the organization, this may be done on paper or via some type of workflow application such as Lotus Notes. The form or workflow process should document what information the individual will be able to access and, in the case of a contractor, how long the access is required. Access should be given once the form goes

through the proper approvals. Approvers of the access should understand that the access is to be given on a "least privilege" basis.

Client Response: No documented process.

3. Can the authorization be controlled so that access is given to only those records that are required for a person to do his or her job?

Guidance: If access to the electronic protected health information can be controlled at a granular level, it should be done. Keep in mind that there are maintenance issues associated with that type of access, so when making any related recommendations, make sure you understand the security and operational needs of the client.

Client Response: There are 3 levels of authorization relative to job duties, but no written policies.

4. Is the data owner involved in the approval process?

Guidance: The data owner is ultimately responsible for his data. As a result, any process for authorization should involve the data owner. The data owner should at least be informed and ideally, should be one of the individuals who approves access.

Client Response: No, approval is usually given by IT.

5. Is sharing of IDs prohibited?

Guidance: If personnel share IDs, accountability is lacking and enforcement becomes difficult. Also, because different people have different levels of access, each should have

his or her own ID. If cases exist where it is operationally not feasible to have separate IDs, some form of supervision or logging and review should occur.

Client Response: Yes, it is addressed in our new sign-on banner.

6. When users require passwords reset, is this done in a secure manner?

Guidance: In an attack scenario, password resets are one of the social engineering tools often used to gain unauthorized access to critical systems and data. Support desks or people handling the support function should properly authenticate people asking for password resets. In a small environment, most people know each other and that knowledge of someone is used to authenticate a person. Although this might be a valid method, it can be a problem in environments where there is significant turnover. It is best to have a secure method for doing password resets regardless of the size of the environment.

Client Response: No, with our current processes, we need to know all passwords.

ii. Workforce Clearance Procedures

"Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate."

This specification is relevant once it is determined that someone needs access to electronic protected health information. It requires that access to electronic protected health information be given on a "need to have" basis. Below are some questions to help determine compliance with this requirement.

1. Are roles and responsibilities and job descriptions clearly defined so that access can be provided to personnel on a "need to have" basis?

Guidance: Assigning access is dependent on knowing what a person does in the company and what that person will need to access to do his or her job. Roles and responsibilities are not always clearly defined, and this may cause problems when providing access. When performing a security assessment, lack of clear roles and responsibilities should be flagged as a weakness as this has a ripple effect on many other security processes such as user ID administration, incident management, and terminations.

Client Response: Not very granular. This is done base on job description.

2. How granular is the access control to electronic protected health information? Is this functionality used in providing personnel access to only what is required?

Guidance: What the system can do in terms of access control is very important because automated system measures are the best way to enforce it.

With granular access control, a balance must be maintained between security and the ongoing maintenance of providing very granular access.

Client Response: There are 2 levels of access; read-only, modify. Can disallow access to specific fields such as social security numbers.

3. Does the data owner (the person responsible for the electronic protected health information records) approve access? If not, is that person made aware?

Guidance: The data owner is ultimately responsible for the handling and security of the electronic protected health information, so that individual should approve or at least be aware of who is accessing the data. This helps provide the necessary accountability as it pertains to the safeguarding of the data.

Client Response: Yes, but we need a policy.

4. If access cannot be controlled by the system, what mitigating controls are in place to ensure that personnel are accessing only what they need?

Guidance: In some cases, there may be systems where there is little or no access control. In these cases, some type of supervision or other mitigating controls should be present. The client may consider log review or reviewing edit reports of key electronic protected health information to help ensure the integrity of the data.

Client Response: Access is controlled.

iii. Termination Procedures

"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in the Workforce Clearance Procedures paragraph."

The main point of this specification is to ensure that if an employee is terminated or leaves a company, any access that individual had to electronic protected health information should be disabled or deleted. Like other HIPAA security requirements, strong termination procedures are

a generally accepted information security best practice. Below are some questions to help determine compliance with this requirement.

1. Do documented policies and procedures for terminations exist?

Guidance: Termination policies and procedures should be documented so that all personnel know their responsibilities in the termination process.

Client Response: No, we need a policy.

2. As part of the termination process, are specific termination activities performed — e.g., return of items assigned to the individual (such as security badges and keys), change of locks, change of shared account passwords, change any systems where an individual shared access or had privileged access, etc.?

Guidance: Ideally, there should be a central repository where information is stored about what items an employee has to ensure that all are returned upon termination.

Client Response: Yes, but we need a policy.

3. Is access periodically reviewed to ensure that personnel have access only to what they need (relative to electronic protected health information)?

Guidance: With access to critical systems, periodic review of access or "purging" is a key control that should be performed periodically as a mitigating control in case access has not been assigned properly or in case terminated employees' access was not properly removed.

Client Response: No.

4. STANDARD — INFORMATION ACCESS MANAGEMENT

"Implement policies and procedures for authorizing access to electronic protected health information."

This standard addresses the process for actually accessing electronic protected health information. This standard is different from the Workforce Security Standard in that this one is more concerned with access to where the electronic protected health information resides, but the other is focused on the people who have the access.

a. REQUIRED Implementation Specifications

i. Isolating Health Care Clearinghouse Functions

"If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization."

1. Does the entity qualify as a health care clearinghouse?

> **Guidance:** Before going further with this set of requirements, it should be confirmed whether the entity is a health care clearinghouse based on the criteria from the first section of this questionnaire.
>
> **Client Response: No. Based on the criteria, we are a health care service.**

2. If the entity is a health care clearinghouse, are there documented policies and procedures that address access to electronic protected health information?

Guidance: Look for documented policies and procedures that address access to electronic protected health information for the health care clearinghouse. The policies should address how authorized access to electronic protected health information is obtained. In addition, all of the other related policies and procedures such as employee terminations should also be included.

Client Response: This question does not apply.

3. Does anyone from the larger organization have access to the electronic protected health information on the health care clearinghouse systems?

Guidance: If someone from the larger organization does have access to the health care clearinghouse systems, is this access authorized and has it gone through the proper approvals? Also, does the covered entity have a way of knowing who uses that access and whether those individuals should have it? This is related to measures such as purging IDs on a regular basis and ensuring that a solid user ID administration policy and procedure are in place.

Client Response: This question does not apply.

b. ADDRESSABLE Implementation Specifications

i. Access Authorization

"Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."

This specification addresses access to electronic protected health information wherever it resides.

1. Do documented policies and procedures for granting access to electronic protected health information exist? Are these policies and procedures readily accessible?

Guidance: For this specification, look for the documented policies and procedures. They might just be a part of the overall user ID administration policies and procedures. Situations where this might not be necessary include very small entities, where a limited number of people have access.

Client Response: No policies or procedures exist.

2. Are there specific workstations (or other devices) that are dedicated to certain functions and from which electronic protected health information can be accessed? If so, are there strict access controls to ensure that only those who require access have it?

Guidance: In health care facilities, there are often workstations used for certain medical functions where doctors, nurses, etc. can access electronic protected health information about patients. Access to these workstations should be restricted. Also, users should log out of the application after using it so other, unauthorized individuals cannot view sensitive information.

Client Response: No dedicated workstations. All workstations can download the user's roaming profile.

3. Where systems can facilitate access control to electronic protected health information at the transaction level, is this functionality used?

Guidance: If the electronic protected health information is accessed via some application, the access control features might allow access to be controlled at the transaction level. This is important because we sometimes tend to think of access at the network or file level. At the application level, features may exist that allow more granular control. Keep in mind, however, that there is maintenance associated with providing this type of access.

Client Response: No.

ii. Access Establishment and Modification

"Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."

This requirement addresses the modification of a user's access based on that individual's job requirements.

1. Is there a policy and procedure for the establishment and subsequent adjustment or modification of a user's access based on change in positions or other changes in status?

Guidance: This is very much related to the earlier specification on Access Authorization. The user ID administration policy and procedure should allow for people's jobs to be changed and their access be changed accordingly. Look for human resources (HR), department management, and IT to be involved in this process.

Client Response: There is no policy or procedure. I just change the access when we need to change it.

2. Is users' access reviewed on a regular basis?

Guidance: Although this is not a required item, it is a good idea in most cases. If the termination process is not effective, reviewing user access is a good mechanism for ensuring, on a regular basis, that only authorized users have access and that the level of access is appropriate. In very small entities, this probably will not be as important because "everyone knows everyone."

Client Response: No, we need a policy for this.

5. STANDARD — SECURITY AWARENESS AND TRAINING

"Implement a security awareness and training program for all members of its workforce (including management)."

As discussed in various parts of this book, awareness is a key component in the success of an information security program. This also holds true for HIPAA security requirements. During the initial comment phase of the HIPAA security regulation, some interesting comments, which are worth noting for clarification purposes, were submitted:

· Covered entities are not required to provide training to business associates or anyone else who is not a member of their workforces. Business associates must, however, be made aware of the entity's security policies and procedures.

·Covered entities have significant latitude in how much and what type of training they provide. Training should be based on the specific security risks the entity faces.

· The intention of this requirement is that awareness training is not a one time process but an evolving one as changes occur in personnel and in the business.

Some general questions that should be asked to assess the level of security awareness include the following. Although these requirements referenced in the questions below have not been specifically stated in the regulations, they help provide a good assessment of the level of awareness:

1. Are any security awareness programs in place?

Guidance: Before going further into the specifications, you should determine whether any security awareness programs are currently in place.

Awareness programs do not have to be formal in nature but can include such things as newsletters, security tips sent out over e-mail, etc.

Client Response: No security awareness programs are in place.

2. Are security policies and procedures readily accessible by employees?

Guidance: Having security policies and procedures easily accessible can help promote awareness. Some companies have a central repository on the company's intranet site where employees can easily find them. If a question arises about what should be done from a security perspective, the information is readily accessible.

Client Response: No, employees can ask HR for direction but nothing in place.

3. Does the entity have an orientation program for new employees and does it incorporate security policies and procedures?

Guidance: Orientation programs for new employees are a very effective way to communicate security policies and procedures. Relative to HIPAA, key provisions

affecting employees can be communicated so that new personnel understand their responsibilities relative to security. If there is an orientation that addresses security policies and procedures, employees should formally acknowledge that they were made aware of these policies.

Client Response: We do HIPAA training for new employees, but its not a full security training.

4. If personnel have questions about policies and procedures, are there people identified to whom they can go?

Guidance: Security policies and procedures can sometimes be difficult to understand, and it is helpful if employees have the opportunity to ask someone if they do not know what a policy means or whether their implementation of it is compliant. There is a greater likelihood of noncompliance if personnel do not understand and are unable to interpret security policies. This interaction is a very key component of a security program and will help promote compliance.

Client Response: They can go to HR or the IT manager, but we don't have a formal policy for that.

a. REQUIRED Implementation Specifications

i. None

b. ADDRESSABLE Implementation Specifications

i. Security Reminders

"Implement periodic security updates."

This requirement calls for periodic security reminders for employees.

1. What type of ongoing security awareness program is in place?

Guidance: With security, the more awareness, the better. Often, it takes more than one education session to raise security awareness to the appropriate level. With HIPAA security, awareness is even more important, considering the potential impacts of noncompliance, including fines and damage to the company's reputation. Some of the common ongoing type of "reminder" programs include newsletters, security tips via e-mail, and focused security education sessions.

Client Response: We don't have one.

2. What is the process for communicating any changes to security policies and procedures?

Guidance: There should be a formal process for communicating changes to security policies and procedures. Depending on the complexity of the policy, varying methods such as e-mail and formal education sessions can be used for communicating changes. Someone should be responsible and accountable for making and communicating changes to security policies and procedures. This function should be centralized to the extent possible to ensure that changes are communicated and that there is a common understanding of what changes were made. This communication should include the change and what the implications are for personnel from both the process and technology perspectives.

Client Response: We don't have one a formal policy; but if there is a problem then we will discuss it in our weekly meeting.

ii. Protection from Malicious Software

"Implement procedures for guarding against, detecting, and reporting malicious software."

This requirement, before the final draft of the regulations, was related only to computer viruses. The terminology was changed to "malicious software" to include malicious acts such as worms.

1. Have there been any recent incidents relating to viruses, worms, or other malicious software?

Guidance: Recent incidents relating to malicious software and how the entity reacted to it will provide significant information regarding how malicious software is handled. Many of the questions below can be answered as a result of this question.

Client Response: No.

2. Is anti-virus software in use in the IT environment?

Guidance: Anti-virus software should be running where appropriate based on the individual company's business requirements. To the extent possible, anti-virus software should be centrally managed and locked down on PCs, so that employees cannot prevent it from running.

Client Response: Yes, and all signatures are up to date.

3. Are virus signatures updated on a regular basis?

Guidance: Ideally, this should be done automatically with minimal human intervention. Depending on the risk, the company may consider multiple anti-virus vendors to decrease the associated risk.

Client Response: Yes.

4. Do users know what to do in the event that they encounter malicious software?

Guidance: This question speaks to incident handling, which is a related HIPAA requirement. There should be a documented process for incident handling complete with escalation guidelines, contact names, etc. (see Incident Handling questionnaire for further details)

Client Response: Yes, they know to call IT. But, we don't have a policy.

5. Do the security risks of the entity justify any type of network- or host-based intrusion management system? If not, what mitigating controls are in place to protect systems with electronic protected health information against malicious software or intrusions? How would the company know if someone was trying to gain unauthorized access to electronic protected health information?

Guidance: Depending on the complexity of the environment, how it is managed, and the associated risk, intrusion management might be a viable option for the entity. Within a security assessment, key factors must be considered when recommending intrusion management including monitoring capabilities, risks, and cost. Besides formal intrusion

management systems, there are specific logs already on a system, which, if reviewed, can also help mitigate some of the associated risk.

Client Response: Yes, we have a Sonicwall IDS.

6. On the systems where electronic protected health information resides, are the following measures taken to reduce the risk of malicious software?

· Application of appropriate security and other patches

· Systems hardened to the extent possible

Guidance: Earlier in this book, one of the points emphasized was the idea of layered security. System hardening and the application of security patches are two of these layers. During a security assessment, as critical systems are identified, the application of patches and system security should be tested using tools as well as manual procedures. Depending on the system, there are best practice guidelines, which can be used as a benchmark to evaluate how secure it is.

Client Response: Application and operating system patches are up to date, but we don't have procedures to protect the system.

iii. Log-In Monitoring

"Implement procedures for monitoring log-in attempts and reporting discrepancies."

This requirement gets into specific measures related to the log-in process. In systems such as Windows 2000, built-in logs readily provide this information. They key impact of this specification is that entities will potentially need to be proactive with regard to log-in monitoring.

1. Where the relevant systems support the following features, are they used?

· Are system controls used to record log-in attempts?

· Does the system lock users out after a certain number of failed log-in attempts?

· Are users' logins restricted by other means such as time of day?

Guidance: Where system features are available for enforcing company security policy, they should be used. If these features are not being used, there is a question as to how logins are being monitored. When recommending the use of system features for user administration security, consider the education and support impacts (from a help desk perspective).

These changes require awareness, and there will likely be an increase in help desk calls, which must be addressed.

Client Response: Yes, to all questions. This is done in Server2008 user manager.

2. Is there any real-time notification when failed log-in attempts occur on critical machines where electronic protected health information resides?

Guidance: Real-time notification is a proactive approach to dealing with intrusions, and this information may be available in the system logs. If no mechanism for notification exists, there might be a need for monitoring on a regular basis.

Client Response: No, we have to retroactively view the logs after incidents.

3. Are the appropriate logs that detail log-in attempts reviewed on a regular basis? Based on logs, are investigations made as needed?

Guidance: Many systems have logs that record information about log-in attempts, which should be reviewed on a regular basis. The review can either be done manually or by using third-party tools. If anything suspicious is found, an investigation should be initiated.

Client Response: The logs are review only when we need to do an investigating. We don't have a procedure for reviewing logs on a regular basis.

iv. Password Management

"Implement procedures for creating, changing, and safeguarding passwords."

This specification goes into the details of good password management. The HIPAA security regulations recognize the importance of passwords and that they are a first line of defense.

1. When a new account is created for the network or specific applications that access electronic protected health information, how is the initial password communicated?

Guidance: Falsely obtaining passwords is a common social engineering technique used by malicious individuals to gain unauthorized access. As a result, communication of initial passwords should be done in a secure manner. Steps should be taken to properly authenticate individuals receiving passwords. In some smaller environments where everyone is familiar with each other, this may not be taken as seriously. This becomes more of an issue as entities grow, where it becomes more difficult to know everyone.

Client Response: Passwords are told to the individual users. Users can change their passwords in ECASE management system but initially they are not secure.

2. Are users encouraged or forced to change their initial passwords?

Guidance: If possible, the system should be used to force users to change initial passwords. If not forced, may users will not change initial passwords. Depending on the support capabilities, it might be useful (and feasible) to walk users through this process so they understand it. If the system does not support it, the importance of changing the initial password should be taught to users in an education or awareness session.

Client Response: No, we need a new process before we have that type of policy.

3. Does the system enforce strong password standards?

Guidance: Passwords are the most basic level of protection, and a significant amount of risk related to unauthorized access can be eliminated with strong passwords. If available, the system should force users to have strong passwords. Keep in mind that clients might push back by saying that there will be too many support calls or that users will start placing their passwords on post-it notes stuck to their monitors. In this case, you should provide techniques for users to develop strong passwords such as using the first letters of words in a phrase or substituting certain characters for letters.

Client Response: No, we need a process and policy for this.

4. If the system does not enforce strong passwords, is the strength of passwords audited?

Guidance: If the system cannot enforce strong passwords, the strength of passwords should be audited as part of the standard IT audit process. There are third-party tools available for auditing password strength.

Client Response: No, this is not part of our process.

5. Are users encouraged or forced to change passwords on a regular basis?

Is there a policy on recycling old passwords?

Guidance: Passwords should be changed on a regular basis (at least every 45 to 90 days) and there should be a policy on not being able to recycle recent passwords. In addition, users should be discouraged from using passwords such as names of months and other obvious names (the system might be able to enforce this). This should be addressed within a security awareness program.

Client Response: No.

6. How are password resets handled?

· When passwords are reset, how are users authenticated?

· Are reset passwords communicated to users in a confidential manner?

· Are users encouraged or forced to change reset passwords?

Guidance: The password-reset process is something commonly used by social engineers to gain unauthorized access to systems. It is imperative that users are properly authenticated and that passwords are communicated in a secure manner. One issue often found is with smaller companies where IT support personnel "know everyone" and do not necessarily authenticate individuals. This practice is a problem because it sets the wrong expectations with users and becomes a problem if turnover occurs or if the entity grows. If the entity grows, it might be difficult to institute this practice. It is better to have a standard process that is always followed.

Client Response: We usually call the site and speak to a custodian who will reset the password. We still know the users windows password because we may have to log on as the user to fix his profile.

7. What measures are taken to ensure that users safeguard their passwords?

Guidance: One of the things seen in many companies is users having passwords on written on yellow sticky notes stuck to their monitors or underneath their keyboards. This should be addressed in a security awareness program and should be part of the IT audit process.

Client Response: We have a log in banner to remind them.

6. STANDARD — SECURITY INCIDENT PROCEDURES

"Implement policies and procedures to address security incidents."

The HIPAA regulations define a security incident as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

a. REQUIRED Implementation Specifications

i. Response and Reporting

"Identify and respond to suspected or known security incidents; mitigate, to the extent racticable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."

The requirements make up a standard incident handling policy that any entity should have in place as part of its security policies. This is another example of the similarity between HIPAA security regulations and information security best practices. The questions below are based on some of the comments and clarifications to the security incident requirement as documented in the *Federal Register*. In addition to the questions below, the Incident Handling checklist should be used when evaluating this HIPAA requirement.

1. Is an incident handling policy in place? (See Incident Handling checklist for further best practices related to incident handling.)

Guidance: For this requirement, there should be, at the minimum, an Incident Handling policy in place. Like the other security policies, it should be readily accessible by employees and be maintained. With incident management, some entities, particularly the smaller ones, will say that everyone knows what to do in the event of an incident. As with other security policies, this becomes a problem when the number of employees grows or if turnover occurs. In addition, the policy is a requirement for HIPAA purposes so it must be documented and used for handling security incidents.

Client Response: No, users call IT or HR depending on the incident.

2. As part of the incident handling process, are there any requirements for documenting the details of a security incident?

Guidance: Per the HIPAA regulations, there are no specific documentation requirements relative to security incidents. Documentation should be based on the individual entity's

business requirements. Specific recommendations for what to document are contained in the Incident Handling questionnaire in the appendices of this book.

Client Response: No.

3. Are there any business or legal requirements related to reporting incidents? If so, are they addressed in the Incident Handling policy?

Guidance: Based on the HIPAA security regulations comments and responses as documented in the *Federal Register,* no requirements exist for internal or external reporting. Companies are free to tailor their reporting based on their own business requirements. Keep in mind that an entity might have other reporting requirements that might drive the reporting aspect of its incident handling policy.

Client Response: There is an OIG policy with which we must abide, but it has nothing to do with Foundation or HIPAA.

b. ADDRESSABLE Implementation Specifications

i. None

7. STANDARD — CONTINGENCY PLAN

"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."

Note that this requirement is specific to having a plan only in those cases where electronic protected health information can be lost or compromised. Although comments during the comment period of the HIPAA security legislation process suggested this requirement be removed, it was kept in because in the event of an emergency, the usual security measures might either be ignored or not working. The contingency plan serves as a last resort to ensure the security of electronic protected health information in the event of an emergency. However, in all likelihood, contingency plans related to electronic protected health information (if they exist) are a component of a larger company-wide contingency plan.

a. REQUIRED Implementation Specifications

i. Data Backup Plan

"Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

Guidance: Refer to the Backup and Recovery checklist in this book to evaluate the data backup process. Note that for HIPAA security purposes, the backup requirements are only for the electronic protected health information. However, when performing a security assessment, other data supporting critical operations should be considered.

Client Response: We have off site backup but we could have any site back up within 4 hours. We do not have a hot site.

ii. Disaster Recovery Plan

"Establish (and implement as needed) procedures to restore any loss of data."

The questions below address some basic things you should see when looking at a disaster recovery plan.

1. Does the client have a disaster recovery plan in place?

Guidance: Based on this requirement, a formal documented plan should be in place.

Client Response: No written DRP.

2. Has the plan been developed using a recognized methodology?

Guidance: The value of developing a plan with a recognized methodology is that risks and business impacts are identified before the plan is developed. Identification of the risks is critical to the success of the disaster recovery plan. In the case of companies subject to HIPAA, you would formally identify electronic protected health information as critical data that must be adequately protected. In addition, using a recognized methodology, such as the one promoted by the Disaster Recovery Institute, provides a good degree of assurance that the plan is thorough.

Client Response: No DR plan in place.

3. What specific measures are taken for electronic protected health information to ensure its confidentiality and security?

Guidance: Because this questionnaire focuses on HIPAA, it is important to identify the specific measures that would be taken for electronic protected health information in the

event of a disaster. You should review this and determine whether it is adequate based on the risks facing the company.

Client Response: Reactive security measures. No policies or procedures.

4. Is someone responsible for updating the plan as the environment changes?

Guidance: Companies are constantly changing and some of the changes might impact the disaster recovery plan. For example, there might be a significant change to the IT environment resulting in critical data being housed on different machines; this can potentially affect the disaster recovery plan. The bottom line is that if the plan is not updated, it can quickly become obsolete. Someone must own this process to ensure that it is properly done.

Client Response: No plan.

5. Is the plan tested on a regular basis?

Guidance: Disaster recovery can be very complicated, and its certainly possible that personnel might not get it right the first time. To minimize the risk of not taking the right steps in the event of a disaster and to ensure that the disaster recovery plan works, the plan should be tested on a periodic basis. The testing can range from a simple tabletop exercise to a full-blown test.

Client Response: No plan.

iii. Emergency Mode Operation Plan

"Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode."

This requirement is essentially having an emergency plan in place. Each of the questions below addresses a specific element of an emergency plan. Below are some questions to help understand and review emergency plans.

1. What are the critical business processes that, in the event of a disaster, must continue to protect electronic protected health information? (This is how "emergency mode" is defined in the HIPAA security regulations.)

Guidance: The HIPAA security regulations require that certain processes be in place to protect electronic protected health information in the event of a disaster. Although these processes should likely be a part of a disaster recovery plan, this question should be asked to ensure that the processes relevant to HIPAA are identified as critical and that measures are in place to ensure that electronic protected health information is protected.

Client Response: Depends on the facility. Accounting, payroll in cloud. E-case manager is critical. Hosted at 777 Joyce. Database can be moved to another server in matter of minutes. Backup on tape and backed up in the cloud. Back-up Mozy Pro. @ mozy.com. redundant pipes for all buildings. CDW and dell Comcast as Internet provider.

2. Are there adequate provisions in the disaster recovery plan to ensure that these processes can continue with minimal disruption in the event of a disaster?

Guidance: Related to the question above, part of the HIPAA compliance effort should be to ensure that processes to protect electronic protected health information (identified in the question above) could be continued with minimal effort or interruption.

Client Response: No.

b. ADDRESSABLE Implementation Specifications

Both of the addressable specifications related to contingency plans are related to updating the contingency plan. Although these are addressable, i.e., they are not specifically required, no real alternatives exist. As a best practice, contingency plans and security practices in general should be evaluated on a regular basis, and adjustments should be made to reflect the current threats and vulnerabilities facing the business.

i. Testing and Revision Procedures

"Implement procedures for periodic testing and revision of contingency plans."

Guidance: As a best practice, contingency plans should be tested on a regular basis and updated as required. This was made an addressable specification to allow companies to do the level of testing and revision or alternative procedures that are best suited for their environment. The example cited in the *Federal Register* is related to smaller entities, which might not find it reasonable to test as frequently or extensively. For example, a full test might not be feasible, but a certain portion of a contingency plan might be tested or a tabletop exercise might be done.

When performing a security assessment, the level of testing and revision should be commensurate with the risk.

Client Response: We do not have contingency plans

ii. Applications and Data Criticality Analysis

"Assess the relative criticality of specific applications and data in support of other contingency plan components."

This requirement is essentially calling for conducting an assessment to determine criticality and risk related to specific applications and data.

Guidance: Although this is listed as a separate specification, the criticality of applications and data should be reviewed when performing the Risk Analysis — one of the first Administrative requirements in the HIPAA security regulations. As a best practice, however, the criticality of applications and data should be evaluated on a regular basis. Often, as new applications are rolled out, security and contingency plans are not always given consideration and are treated as afterthoughts. The person owning the plan should be active in the process of understanding the criticality of data and applications.

Client Response: This is something we will have to address in the future

8. STANDARD — EVALUATION (REQUIRED)

"Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational

changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart."

1. Does the client perform any type of ongoing security assessment?

Guidance: This requirement is essentially an ongoing assessment for which the initial risk analysis can be used as a baseline. The goal of this requirement is to ensure that entities do not just implement HIPAA security requirements and then forget about them. The reality is that operations change and as a result, the IT environment changes and the risks change.

Notwithstanding HIPAA, ongoing security assessments should be done for any entity to ensure that the information security program is properly aligned with the risks the company is facing. Some ways to comply with this requirement include ongoing IT audits or regular security assessments (using internal or external resources). Some aspects of this requirement, based on the comments received during the comment phase of the HIPAA security legislation process, include:

· Internal or external resources can do ongoing assessments. Entities have the option based on the cost and availability of resources.

· Although HIPAA does not have any "certified" products, entities should monitor the National Institute of Standards and Technology (NIST) for product recommendations.

Client Response: No.

9. STANDARD — BUSINESS ASSOCIATE CONTRACTS AND OTHER ARRANGEMENTS (REQUIRED)

"A covered entity, in accordance with §164.306 [qualifications for being a 'covered entity'], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) [business associate contract] that the business associate will appropriately safeguard the Information."

This regulation requires an entity to have assurance that if a "business associate" creates, receives, maintains, or transmits electronic protected health information on behalf of the covered entity, the business associate will appropriately safeguard the information. The business associate requirement does not apply to the following:

· Transmission of electronic protected health information between a covered entity and a health care provider concerning the treatment of an individual

· Transmission of electronic protected health information between a group health plan, HMO, or health insurance issuer to a plan sponsor

· Transmission of electronic protected health information from or to government agencies that are health plans and provide public benefits

1. Does the client have any business associate relationships and if so, how are they handled as it pertains to the security and privacy of electronic protected health information?

Guidance: "Business associate relationships occur in those cases in which the covered entity is disclosing information to someone or some organization that will use the

information on behalf of the covered entity."30 Examples of business associates are professional services such as accounting, law, consulting, and other services.

Client Response: Yes. We try to be aware of security when dealing with them, but we do not have policies or procedures.

a. REQUIRED Implementation Specifications

i. Written Contract or Other Arrangement

"A covered entity, in accordance with §164.306 (Security Standard General Rules), may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) (business associate contract regulations) that the business associate will appropriately safeguard the Information."

A covered entity using a business associate should have a written agreement that appropriately safeguards the electronic protected health information in the associate's possession.

1. Does the client have the appropriate contracts for any business associate working for the client?

Guidance: For any business associates, there should be a standard contract that is used. Some of the elements to look for in a contract are those that require business associates to do the following:

· Not use or further disclose the PHI (Protected Health Information) other than as permitted by the contract or as required by law

· Use appropriate safeguards to prevent unauthorized use or disclosure of the PHI

· Report to the covered entity any unauthorized use or disclosure of which it becomes aware

· Ensure that any agents, including subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to the business associate

On termination of the contract, return or destroy all PHI in its possession, or, where that is not possible, extend the protections of the contract for as long as the information is retained

Client Response: We have contracts, but they do not have relevant HIPAA language for protecting patient EPHI.

b. ADDRESSABLE Implementation Specifications

i. None

PHYSICAL SAFEGUARDS

The physical safeguards–related requirements are mostly "addressable" specifications. Note that these requirements are separate from the electronic security requirements, which cannot be performed in lieu of the Physical Safeguard controls listed below. There was some confusion over the meaning of "Physical Safeguards" when the HIPAA security requirements were first presented. Based on the *Federal Register*, Physical Safeguards are defined as: "Security

measures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion"

1. FACILITY ACCESS CONTROLS

*"*Entities should have policies and procedures in place to limit physical access to its electronic information systems and the facility or facilities where they are housed, while ensuring that properly authorized access is allowed"

a. REQUIRED Implementation Specifications

i. None

b. ADDRESSABLE Implementation Specifications

i. Contingency Operations

"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."

Policies and procedures should be in place to ensure that there is access to facilities to the extent required in restoring data as part of the disaster recovery plan and emergency mode operations. This specification is essentially a complement to the existing disaster recovery plan and emergency mode operations. Some level of access to facilities is required when executing a

disaster recovery plan or operating in emergency mode. Keep in mind that this is an addressable specification meaning that covered entities have significant flexibility in how these specifications will be implemented. The flexibility is good for small companies that have limited budget and staff.

1. Do specific policies and procedures to limit access to physical facilities exist?

Guidance: The basic policies and procedures are the foundation for limiting physical access and establishing good physical security controls. This enables personnel to be educated and provides management a basis for enforcement.

Client Response: We address physical security in an adhoc way. We do not have physical security policies or procedures.

2. Is physical access adequately addressed in the termination policy and procedure?

Guidance: Employee termination is a significant risk, and it is critical that physical access is removed as part of the process. If physical access is not removed, former personnel (especially disgruntled ones) can cause significant damage.

Client Response: No, we need help with this.

3. Is the list of people who have physical access periodically reviewed?

Guidance: As a mitigating control for the termination process, physical access lists should be periodically reviewed. Any unneeded access should be removed as part of the process. This will vary with the size of the company. In smaller companies, guards and

other employees probably know who should or should not be on the premises so the process is not as critical. In larger companies, this is absolutely critical.

Client Response: No, we need a policy for this.

4. Have facility access requirements been addressed in the disaster recovery plan and emergency mode operation?

Guidance: Although the facility access requirements are listed separate from the disaster recovery and emergency mode requirements, they are an integral part of both. If the facility access requirements are not addressed in the disaster recovery or emergency mode operations, where are they addressed? More importantly, are the facility access requirements in sync with the disaster recovery plan and emergency mode operations?

Client Response: No, since we do not have a DRP.

5. When the disaster recovery plan is tested, are the people in charge of facility access involved? Are they made aware of updates to the plan?

Guidance: Similar to the previous question, the disaster recovery plan should involve those individuals in charge of facility access. The plan test and update process is covered in more detail in the disaster recovery checklist.

Client Response: No.

6. Are there any awareness programs for the people in charge of facility access?

Guidance: Like all security policies and procedures, awareness programs should extend to those individuals in charge of facility access. At the minimum, they should understand and be aware of their roles in the event of a disaster.

Client Response: No.

ii. Facility Security Plan

"Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft."

Essentially, this part of the requirement is having physical security policies and procedures in place. Refer to the Physical Security checklist for further questions regarding physical security.

iii. Access Control and Validation Procedures

"Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision."

Procedures should be in place to control and validate individuals' access to facilities, and their access should be based on their role in the company. This specification also calls for controlling visitors (e.g., logging when they come and go, ensuring visitors walk with authorized personnel). Refer to the Physical Security checklist for questions relevant for this specification.

iv. Maintenance Records

"Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks)."

This specification is asking for records to be kept when making any repairs or modifications to security-related components. In addition to the question below, the Physical Security questionnaire in these appendices should be referenced for other relevant questions.

1. For any given facility, are the "security-related components" identified so that changes can be appropriately documented?

Guidance: To ensure that this HIPAA requirement is met, the specific security components should be identified. Ideally, all significant changes (regardless of whether related to security components or not) should be documented, and these records should be securely kept.

Client Response: No, we need a policy for that too.

WORKSTATION-RELATED REQUIREMENTS

The next two requirements deal with the use and security of workstations. Before going into the actual requirements, it is worth clarifying the definition of "workstation" as stated in the *Federal Register*:

Workstation — An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

This definition and terminology were a result of comments that the previous terminology "Secure workstation location" (used in the initial drafts of the HIPAA Security regulations) was vague. With the current definition of workstation, this could mean items such as personal digital assistants and other devices.

2. STANDARD — WORKSTATION USE (REQUIRED)

"Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information."

This specification is meant to ensure that personnel use their workstations in a secure manner.

1. Identify what workstations as well as other devices can be used to access electronic protected health information.

> **Guidance:** Because of the definition of workstation, other computing devices such as personal digital assistants and other wireless devices can be subject to this requirement. This question will help you in determining the scope as well as the associated risk.
>
> **Client Response: Cell phone, all servers and all workstations.**

2. Does a policy exist that addresses secure workstation use? Some of the things that should be addressed include:

· What functions should be performed by the workstation

· How those functions should be performed

· What the physical attributes are for the workstation environment

Guidance: This requirement also calls for having secure practices at the workstation to help ensure that electronic protected health information is protected. For example, the entity might require the use of screen saver passwords so other people cannot see sensitive information when the workstation is unattended. The specific function will vary based on the workstation. As part of this question, you should also ensure that personnel are aware of this policy.

Client Response: No.

3. STANDARD — WORKSTATION SECURITY (REQUIRED)

*"*Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."

One clarification of this specification is that the physical safeguards used are based on the entity's risk analysis process. Consequently, companies have flexibility in implementing this requirement.

1. Identify what workstations as well as other devices can be used to access electronic protected health information.

Guidance: Because of the definition of workstation, other computing devices like personal digital assistants and other wireless devices can be subject to this requirement. This question will help you in determining the scope as well as the associated risk.

Client Response: This would be every computer on our facility as well as 6 iPhones.

2. What physical security measures are taken to protect these devices or machines?

Guidance: Once these machines and devices have been identified, they should be secured based on risk. Protection will vary based on the device and can involve such things as locking down laptops with cables or other measures to protect devices such as PDAs.

Client Response: We have a card access system, but anyone can access these system if they gain access to the building. The removable storage devices have been deactivated.

3. Who has access to the physical workstations besides the individual user?

Are there facilities people who can potentially access the workstations?

If so, what security measures are taken to ensure that these individuals do not gain unauthorized access?

Guidance: One of the significant areas of weakness in many companies is that too many people have physical access to machines that access electronic protected health

information. Some examples include computers in public areas such as nurses' stations or in cubicles in a typical office.

Facilities personnel also have master key access to sensitive areas.

Depending on the risk, physical security measures such as locking cables and other devices should be used.

Client Response: Anyone can access the workstations if they can gain access to the building. Since facility people have keys then they have unrestricted access. We have no security measures.

4. Were there any workstation security–related findings in the initial risk assessment and if so, were they addressed?

Guidance: Workstation security should have been addressed in the initial risk assessment at the start of the HIPAA security compliance process. Any findings should be reviewed to determine whether or not those findings have been addressed.

Client Response: We did not do a risk analysis.

4. STANDARD — DEVICE AND MEDIA CONTROLS

"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."

This specification calls for policies and procedures to help ensure that any media containing electronic protected health information is adequately secured when it leaves or comes back to the facility.

a. REQUIRED Implementation Specifications

i. Disposal

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

This can apply to hard drives, backup tapes, etc. where electronic protected health information is stored. Measures such as overwriting disks must be performed to ensure that sensitive electronic protected health information cannot be compromised.

The disposal requirement is essentially based on best practices, and nothing is particular just to HIPAA. Questions related to data disposal are documented in the Media Handling questionnaire in the appendices and should be used to evaluate this requirement.

ii. Media Re-Use

"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

This requirement is similar to the disposal requirement in the sense that electronic protected health information must be properly destroyed. This will require multiple overwriting to ensure

that information cannot be recovered once the electronic media is available for reuse. Like the disposal requirement, there are no aspects that are particular to just HIPAA. As such, questions from the Media Handling questionnaire in the appendices should be used to evaluate compliance with this requirement.

b. ADDRESSABLE Implementation Specifications

i. Accountability

"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

This specification requires that some type of audit trail be kept of any movement of electronic media and hardware where electronic protected health information resides.

One clarification made in the comments section of the regulation is that this specification does not address audit trails within systems or software. The idea here is that because of the sensitive nature of information on the electronic media, it should be secure, and there should be accountability for it.

1. Are there clear roles and responsibilities for who can handle electronic media?

> **Guidance:** Because of the sensitivity of the electronic protected health information and the media where it resides, only certain individuals should be authorized to take it. A policy should identify what roles in the organization are authorized. In a security

assessment, one of the main aspects reviewed in virtually any area is roles and responsibilities. Similar to this HIPAA specification, it helps establish accountability.

Client Response: Access to tapes are restricted. They are locked in a safe. We need help with that.

2. When there is movement of electronic media, are there logs of who takes it and when they take and return it?

Guidance: This is a process question that maps back to the requirement.

There should be a log that records the movement of media. This log should be accessed by a limited number of individuals.

Client Response: No.

3. Is there proper segregation of duties relative to maintaining the log? (The people who are taking the electronic media should not be updating the logs.)

Guidance: With any log, segregation of duties is important because it speaks to the quality and integrity of the information contained in it. To achieve accountability, the logs are critical because they establish who had the electronic media and when they had it. If there is even a perception that the information in the log can be altered, the log loses value. The ideal scenario is to ensure that the individuals who take and handle the electronic media do not have access to the logs.

Client Response: No.

4. Is the log kept in a secure manner?

Guidance: Related to the question above, the logs should be kept securely. If electronic, they should have proper access controls (see User ID Administration checklist) and if paper based, they should be properly locked with only a limited number of people having access.

Client Response: They are locked in a safe.

ii. Data Backup and Storage

"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

The purpose of this specification is to minimize the risk related to electronic protected health information when moving systems and equipment. Like many of the other specifications, entities have considerable latitude in determining what is best for their environment. The comments received on this specification led to a number of clarifications:

·What is backed up (a retrievable and exact copy) is largely dependent on the risk analysis — i.e., where is the risk great enough to require a retrievable and exact copy?

·A guideline that can be used when determining what to back up is — what information would be required by the entity to continue "businessas usual"? This information should be available in the analysis done to determine what is required to run in "emergency mode."

For other questions related to this specification, refer to the Backup and Recovery questionnaire in the Appendices.

TECHNICAL SAFEGUARDS

1. STANDARD — ACCESS CONTROL

"Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management standard]."

These policies and procedures should be designed to allow access only to those persons or software that has been granted access rights as specified in the Administrative Safeguards section on Information Access Management. Although the Administrative Safeguards section required entities to have policies and procedures to grant access to systems where electronic protected health information is maintained, this Access Control requirement is essentially requiring that these policies and procedures be translated into technical policies at the technical level. With this requirement, entities should take advantage of the technical capabilities relative to access control to ensure that access is limited to only those who require it. Based on some of the comments received, access control was further clarified to include:

- Context-based access
- Role-based access
- User-based access

a. REQUIRED Implementation Specifications

i. Unique User Identification

"Assign a unique name and/or number for identifying and tracking user identity."

Unique user identification is generally accepted as an information security best practice and is one of the items covered in the user ID administration checklist. The ideas behind this requirement are making users accountable for what they do and enforcing the HIPAA security requirements. One item to note here is that there are several levels of access to be concerned about. Access is at several levels within organizations including network, application, and remote access. This requirement is specifically for access related to electronic information systems containing electronic protected health information.

1. Identify the systems that contain electronic protected health information and how they can be accessed.

Guidance: This information should already be available from the initial analysis but it is a good idea to confirm what systems contain electronic protected health information. In addition, all the different ways the systems can be accessed should be identified.

Client Response: We can access the exchange server from our iPones. We can also access the server from three other sites from outlook. We can also access the database server from the same sites. We have about 250 computer from where we can access the systems, but they all come back to 777 Joyce.

2. Do individuals accessing the identified systems have unique IDs for access?

Guidance: Systems containing electronic protected health information should be using unique IDs. There may be situations where applications access electronic protected health information and the applications do not have unique IDs for users. One potential issue is

people who do not access the systems very often (e.g., a backup person or someone who is temporarily helping) so when they do, they use someone else's ID.

Client Response: Yes, but some users have insecure user ID's because our process involves knowing them. We are working on a new process where we do not need to know windows passwords.

3. Do the systems have any default IDs or guest IDs and if so, 1) are they used? 2) have their default passwords been changed? 3) if not needed, are they (can they be) disabled?

Guidance: Default and guest IDs are a significant risk when it comes to unauthorized access to systems. These IDs are usually there out of the box, so if administrators do not change passwords or disable them, they can be used by someone with knowledge of the application or the system to gain unauthorized access. In fact, a malicious user can utilize the Internet to research what the different default IDs and passwords are and use that knowledge to gain unauthorized access. The default or guest ids should be taken care of during the initial deployment if possible.

Client Response: No default password, but we need a policy for this.

4. Do these systems have a way of tracking individuals' activities? For example, can specific transactions on these systems such as report generation be tracked to specific individuals? If specific information is accessed, can it be tracked to an individual?

Guidance: Tracking someone's activity relating to accessing electronic protected health information is necessary according to this requirement.

This tracking can include just accessing specific files or creating and modifying information via an application. At the application level, specific transactions should be tracked as that will provide a record of who made what changes. Besides the built-in mechanisms available in applications and systems, other mechanisms for fulfilling this requirement include tools such as integrity checkers.

Client Response: No, not individual file.

5. Who has access to the logs and if the logs were altered, could that be identified?

Guidance: The foundation of tracking activity is the logs. Access to the logs should be restricted to the extent possible. No one should have any access to modify any information on the logs. Depending on the risk, it might be appropriate to deploy tools to check the integrity of the logs.

Client Response: IT has access to the logs. We do not believe any EPHI remains on the laptops. We cannot tell is the logs were adjusted.

ii. Emergency Access Procedure

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."

This requirement relates to technical measures including backups and the ability to recover. The Backup and Recovery questionnaire in the Appendices and the emergency plan questions from the HIPAA questionnaire should be used to check compliance with this requirement.

b. ADDRESSABLE Implementation Specifications

i. Automatic Logoff

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

This was originally a "required" specification, which was changed to addressable because the automatic logoff feature is not always available. Based on the comments and responses documented, some type of equivalent measure based on a specific entity's risk analysis can also be used.

1. Where available, is the "automatic logoff" mechanism used?

> **Guidance:** This is a very specific control where you need to verify whether or not the system supports it. If it does support it but is not being used, it might be because the client is not aware of it. If recommending the use of this feature, warn the client that there will be some support issues in the beginning.
>
> **Client Response: No, only for remote connections. Workstation will lock no activity for 10 mins. Screen saver - 10 mins. User log on p/w required.**

ii. Encryption and Decryption

"Implement a mechanism to encrypt and decrypt electronic protected health information."

As a form of security, encryption provides confidentiality of information. This became an "addressable" requirement because it was questioned how valuable and feasible it was to encrypt data. The cost of encrypting information and the ongoing maintenance and support can be very expensive for small entities and even some larger entities. Making this specification "addressable" gave entities the option to encrypt data based on their specific risks.

1. Has the client's risk analysis addressed the issue of data encryption?

Guidance: The client's risk analysis should have considered the issue of encryption. Based on the risk analysis, the client should be able to articulate why encryption is or is not being used.

Client Response: No.

2. STANDARD — AUDIT CONTROLS (REQUIRED)

*"*Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

This standard essentially requires entities to evaluate the systems currently in use and determine if they can record and examine activities of individuals accessing electronic protected health information in the systems. Note that the standard specifically mentions hardware and software. Compliance with this standard may require new systems or custom coding of existing systems. Audit controls, by their nature, are flexible in nature and depend on the level of risk. The comments and subsequent responses as documented in the *Federal Register* clearly state that the audit controls should be based on the entity's own risk analysis. This specification should be

analyzed in conjunction with the related Privacy specifications, which require entities to account for disclosures of protected health information to individuals upon request.

1. As part of the risk analysis, has the client reviewed these hardware and software mechanisms for recording activity?

Guidance: This requirement is based on the risk analysis. When determining what is to be reviewed, the client should consider current staffing and how the additional work will be handled (assuming it is not being done already).

Client Response: We did not do as risk analysis.

2. For cases where activity is to be reviewed, does the client have documented procedures for what has to be reviewed, when logs are generated, etc.?

Guidance: The resulting reviews that are instituted to achieve compliance with this requirement are a process that should be documented. There should be minimum requirements for these reviews and there should be some expectation of what the review entails. A procedure is a good place to capture these requirements.

Client Response: No.

3. STANDARD — INTEGRITY

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

Integrity of information is one of the pillars of information security. The point of this standard is that electronic protected health information should not be altered in an unauthorized manner. The integrity standard ties into the earlier requirement that individuals' activities should be tracked to guard against unauthorized alteration of data. There are tools such as "integrity checkers" and intrusion detection systems that claim to do integrity checking. In addition, some systems might have native tools to check integrity. Software as well as existing system mechanisms should be investigated when evaluating compliance with this requirement.

a. REQUIRED Implementation Specifications

i. None

b. ADDRESSABLE Implementation Specifications

i. Mechanism to Authenticate Electronic Protected Health Information

"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."

As alluded to earlier, specific software and potentially existing tools on systems can corroborate that electronic protected health information has not been improperly altered. Examples of built-in data authentication mechanisms include error-correcting memory and magnetic disc storage. In addition, processes that utilize checksums or digital signatures can be considered.

1. Has the integrity of data been considered in the client's risk analysis?

Guidance: Review the risk analysis to determine whether it was considered.

Client Response: No risk analysis.

2. Are there any mechanisms such as "integrity checkers" in place?

Guidance: Some companies have deployed tools such as Tripwire to ensure the integrity of critical files. If the client does not have something like this in place, determine what tools, if any, are in use.

Client Response: No.

3. Based on the risk analysis, where (if anywhere) is it appropriate to deploy integrity-checking tools?

Guidance: Determine where electronic protected health information resides and where it makes sense to have which integrity checking tools. In different cases, you may be able to deploy cheaper solutions; it all depends on the risk analysis.

Client Response: Possible, we have not done a risk analysis.

4. STANDARD — PERSON OR ENTITY AUTHENTICATION

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

Guidance: This specification builds on the first specification in the Technical Safeguards section requiring users to have unique user IDs. In the initial draft, this specification listed actual technologies that can be used to come into compliance with this requirement. In the final adopted rule, any reference to technology was intentionally omitted to allow companies to use methods

that made sense based on their own risk levels. Some of the methods that can be considered when implementing this specification include (as documented in the initial draft):

· A “biometric” identification system

· A “password” system

· A “personal identification” system

· A “telephone callback” system

· Digital signatures

· Soft tokens

1. When providing support for technologies used in this specification, how are individuals authenticated?

Guidance: One of the most significant security risks is social engineering.

It is critical that users are properly authenticated when they are provided with any support related to gaining access to systems. This is often a problem in smaller companies where the attitude of support personnel is “I know everyone here.” Look for specific procedures for authenticating users.

Client Response: Based on familiarity or the subject matter. It is not reliable. We need a policy and procedure for doing this.

5. STANDARD — TRANSMISSION SECURITY

“Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.”

Guidance: The regulations thus far have been focused on the security of electronic protected health information that is in a system. This requirement focuses on the transmission of that information over an "electronics communication network." To clarify this further, the network is essentially an untrusted network, such as the Internet. To properly evaluate this requirement, a thorough process evaluation of how information is sent should be performed.

1. Identify all instances where information is sent over a public network (e.g., the Internet).

Guidance: Examples include: patient information sent electronically to other health care entities, agencies, insurers; billing information sent to insurers. Identifying these instances will define the scope of work required to come into compliance with this requirement. To obtain this information, it is imperative to involve process owners as well as technology owners. Once this list is complete, a risk analysis should be performed to determine what steps to take. As noted below, there are no "required" implementation specifications related to this standard. The specific measures to take are dependent on the level of risk.

Client Response: billing data, reporting data required by the state and funding. Entered thru their portals ,pull up client by social security number, enter data to receive payment for the services provided. fax - doctor's report, prescription information, case opening request - all necessary information to get the case opened with the agency.

2. Is instant messaging used for communicating electronic protected health information?

Guidance: Instant messaging has gone from being used for socializing to being used for business purposes. You should find out if it is being used and what is being transmitted using instant messaging software. There are solutions to secure instant message traffic.

Client Response: Not on computers, but possibly on iPhones. We need a policy for this as well.

a. REQUIRED Implementation Specifications

i. None

b. ADDRESSABLE Implementation Specifications

i. Integrity Controls

Security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until it is disposed of.

Guidance: Based on what is being transmitted, the risk analysis should consider the likelihood that electronic protected health information can be altered during transmission. Depending on the risk, different solutions can be implemented including software that can check integrity or other procedures that check to determine whether information has been altered.

Client Response:

ii. Encryption

1. Implement a mechanism to encrypt electronic protected health information as deemed appropriate.

Guidance: Encryption was one of the areas that received comments from the public in the earlier draft of the HIPAA security regulations. For many health care entities, particularly the smaller rural ones, the cost of encrypting communications over public networks can be daunting. As a result, encryption became an "addressable" specification. For example, information communicated over a dial-up line probably would not require encryption because the likelihood that the confidentiality can be compromised is slim.

The expectation is that companies should encrypt transmitted information if their risk analysis determines that encryption is warranted.

Client Response: Ecase management encrypts parts of the data. SSN is encrypted.

REFERENCE:

[1] Broder, J. F. (2006). *Risk Analysis and the Security Survey* (3rd ed.). Burlington, MA: Elsevier Inc.

[2] (2006, December 1). *About Foundation*. Retrieved February 20, 2011 from Foundation Services, Inc. Web site: http://www.cornerstoneservices.org/

[3] Stewart, D. (June 20, 2008). *Getting Down with Information Assets*. Retrieved February 20, 2011 from squidoo.com Web site: http://www.squidoo.com/Information-Assets

[4] U.S. Department of Health & Human Services (1996). HHS.gov. *Summary of the HIPAA Privacy Rule, , .* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[5] Bowen, P., Hash, J., Wilson, M. (2006). *Information Security Handbook: A Guide for Managers*. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[6] Payne, S. C. (2006). A Guide to Security Metrics. *SANS Security Essentials GSEC Practical Assignment*. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55

[7] Romig, T. (2001). HIPAA Compliance: Cost-Effective Solutions for the Technical Security Regulations. *SANS Institute InfoSec Reading Room, 1.2f, .* Retrieved from http://www.sans.org/reading_room/whitepapers/legal/hipaa-compliance-cost-effective-solutions-technical-security-regulations_51

[8] School, M., Stine,K., Hash, H., Bowen, P., Johnson, A., Smith, C. D., Steinberg, D. I. (2008). *An Introductory Resource guide for Implementing the Health Information Portability and Accountability Act (HIPPA) Security Rule*. Gaithersburg, MD: National Institute Retrieved from. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

[9] Alsbury, R. Dayle (2004). A Small Business Search for HIPAA Compliant E-mail Security. SANS Institute InfoSec Reading Room, 1.4b,. Retrieved from http://www.sans.org/reading_room/whitepapers/hipaa/small-business-search-hipaa-compliant-e-mail-security_1422

[9] Logan, K. (2006). University of Cincinnati. HIPPA Checklist, , . Retrieved from http://www.wvdhhr.org/han/security/HIPAASecurityChecklistLHDsv2.pdf

[10] Patterson, M., Peabody N. (2003). HIPPA Task Force Group. HIPPA Security Checklist, , . Retrieved from http://www.nixonpeabody.com/linked_media/publications/HIPAAChecklist_Patterson.pdf

[11] Freeburg, N., McCaughan. (2008). HIPPA for Dummies: A practitioner's Guide. counselingoutfitters.com, , . Retrieved from: http://counselingoutfitters.com/vistas/vistas08/Freeburg_Article_29.pdf

[12] Reynolds (2009). Health Data Stewardship: What, Why, Who, How. National Committee on Vital and Health Statistics. Retrieved from http://ncvhs.hhs.gov/090930lt.pdf

[13] Peterson, R. (2006). Medicaid management information system. Information system audit. Retrieved from http://www.nd.gov/auditor/reports/2300_02.pdf

[14]Hodge, C. (2010). Risk of collecting customer information. *Helium:General Management*. Retrieved from http://www.helium.com/items/1815411-risks-of-collecting-customer-information

[15]Kamat, M. (2009). Guideline for Information Asset Valuation. *ISO 27001 Security: ISO 27001 Implementer's Forum, 001,* 3. Retrieved from www.iso27001security.com/ISO27k_Guideline_for_Information_Asset_Valuation.pdf

[16] Schneider, F. B. (1998). *Trust in Cyberspace*. Washington, DC: National Academy Press. Retrieved from http://www.nap.edu/catalog.php?record_id=6161

[17] Welch, W. (2010). Thrift stores struggle to stay open, fund programs. *USA Today*. Retrieved from http://www.usatoday.com/news/sharing/2010-04-21-thrift-stores_N.htm

[18] (2007). Health Information Portability and Accountability Act. *CA.gov Department of Health Care Services*. Retrieved from http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00%20WhatisHIPAA.aspx

[19] Paul Starr, "The Signing of the Kennedy-Kassebaum Bill," August 22, 1996 (http://epn.org/library /signing.html).

[20]Austin, Bonnie J., and Emily A. Bosk. Administrative Simplification Project: Case Study – council of Affordable Quality Healthcare (CAQH). Washington, DC: AcademyHealth, 2008.

[21]PSbclf (2007). HIPAA Title II Blue Book. *Health Insurance Portabaility and Accountability Act of 1996,* 3. Retrieved from https://www.cms.gov/HIPAAGenInfo/Downloads/ASCALaw.pdf

[22](2005) Guidance on how to determine whether an organization or individual is a covered entity under the Administrative Simplification provisions of HIPAA. *Center for Medicare & Medicad Services, ,* 2. Retrieved from https://www.cms.gov/HIPAA GenInfo/Downloads/CoveredEntitycharts.pdf

[23](2005). Policy on Security of Electronic Protected Health Information (EPHI). *University of Pennsylvania Information Systems & Computing*. Retrieved from http://www.upenn.edu/computing/security/policy/EPHI_Policy.html

[24]DHHS/OS/OCR (2008). Your Health Information Privacy Rights. *Your Health Information Privacy Rights, ,* Pg. 1. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf

[25](2010).HIPAA Violations: HIPAA Fines and HIPAA Penalties for Non-Compliance. *www.training-hipaa.net.* Retrieved from http://www.training-hipaa.net/hipaa_resources/Violation_Penalties.htm

[26] Moody, M. (2002). HIPAA Patient Information Security and Privacy Mandates: Strengthen Business Case for Electronic Report Distribution Systems. *Compliancehome.com*. Retrieved from: http://www.compliancehome.com/whitepapers/HIPAA/abstract10378.html

[27] Adler, P. (). HIPAA Security Redux: A Re-evaluation Process and Recommended Areas to Review. *Allima Body of Knowledge*. Retrieved from http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_035867.hcsp?dDocName=bok1_035867

[28] (2010). HIPAA Laws and Electronic Medical Records. *Document Scanning & eDocument Storage*. Retrieved from http://www.scantronix.net/document-scanning-blog/hipaa-laws-and-electronic-medical-records-145.htm

[29]Annas GJ (2003). HIPAA regulations _ a new era of medical-record privacy?. *New England Journal of Medicine, 348,* 1486-1490.

[30] Kilbridge P. (2003). The cost of HIPAA compliance. *New England Journal of Medicine, 348,* 1423-1424.

[31] Kulynych J., &Korn D. (). The new HIPAA (Health Insurance Portability and Accountability Act of 1996) Medical Privacy Rule: Help or hindrance for clinical research? *Circulation, 108*, 912-914.

[32](2002). Standards for privacy of individually identifiable health information: Final rules. Federal Register. *Office of Civil Rights, Department of Health and Human Services., 67*(157), 53182-53272.

[33] Salem MD, D. (2003). HIPAA's Privacy Regulations: Costs of Compliance. *Medscape News, 4*(2), Retrieved from http://www.medscape.com/viewarticle/461703_4