

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules



Electronic Healthcare Network Accreditation Commission

www.ehnac.org

© 2010 Electronic Healthcare Network Accreditation Commission, All Rights Reserved



Healthcare Information and Management Systems Society

<http://www.himss.org/ASP/index.asp>

© 2010 Healthcare Information and Management Systems Society, All Rights Reserved



NACHA – The Electronic Payments Association

<http://www.nacha.org/>

© 2010 Healthcare Information and Management Systems Society, All Rights Reserved



Workgroup for Electronic Data Interchange

www.wedi.org

© 2010 Workgroup for Electronic Data Interchange, All Rights Reserved

Disclaimer

This document is Copyright © 2010 by the Electronic Healthcare Network Accreditation Commission (EHNAC), the Healthcare Information and Management Systems Society (HIMSS) Medical Banking Project, NACHA – The Electronic Payments Association (NACHA), and the Workgroup for Electronic Data Interchange (WEDI). It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holders. This document is provided “as is” without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by EHNAC, HIMSS, NACHA, or WEDI. The listing of an organization does not imply any sort of endorsement and EHNAC, HIMSS, NACHA, and WEDI take no responsibility for the products, tools, and Internet sites listed. The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by EHNAC, HIMSS, NACHA, WEDI, or any of the individuals or organizations that contributed to this paper.

This document is for Education and Awareness Use Only.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Contents

Disclaimer 2

Executive Summary 5

Introduction..... 7

 Business Purpose of the White Paper..... 7

 Covered Topics..... 8

 Out of Scope 8

 Background of the Publishing Organizations..... 9

Overview of Applicable Regulations..... 10

 HIPAA 11

 HITECH 13

 Implications for Financial Institutions..... 13

Guidelines..... 14

 1. Determining the Financial Institution’s Eligible Services and Status 14

 2. Recommended Corporate Infrastructure and Governance..... 17

 3. Conduct a Risk Analysis..... 19

 4. Conduct a Risk Audit 20

 5. Update Technology Systems..... 23

 6. Develop a Communication Plan..... 24

 7. Workforce Training 26

 8. Compliance Tool Sets from Independent Third-Parties..... 28

Conclusion 29

List of Contributors..... 30

Appendix I – Important Definitions from HIPAA 31

Appendix II – Hybrid Entity: Definition and Conducting the Analysis 39

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Appendix III – Financial Institutions 41

Appendix IV – NACHA and the Automated Clearing House Network 42

Appendix V - Technology Best Practices 44

Appendix VI - Glossary of Acronyms and Terms 59

Appendix VII - References 64

Appendix VIII 2004 NCVHS letter to HHS..... 65

Executive Summary

The recent passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) directly affects financial institutions and their services for the healthcare sector. HITECH modifies and amplifies the existing data privacy and security rules for protected healthcare information under the Health Insurance Portability and Accountability Act (HIPAA). There are new breach reporting requirements and tougher penalties. Financial institutions may find they must be able to meet the HIPAA data privacy and security measures if they deliver services to the healthcare sector.

Financial institutions first need to determine whether HIPAA and HITECH are applicable to them. This can be accomplished by determining whether the financial institution has access to protected health information (PHI) through the services they provide to organizations within the healthcare sector. If the financial institution has access to PHI, then they need to identify their potential status as a “covered entity” or a “business associate” under HIPAA and HITECH. If the financial institution meets either definition, it must develop and implement procedures and policies that help ensure compliance with using and disclosing protected health information only in the manner set forth in the HIPAA privacy and security provisions. This white paper, “Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules,” can help financial institutions evaluate eligibility and build a blue print for a compliance program. Although each financial institution will need to ultimately determine its own eligibility and required tasks, this white paper provides guidelines in the noted areas.

HIPAA Eligibility and Status

Is the financial institution a covered entity or a business associate under HIPAA and HITECH? There are definitions of each type of covered entity as well as a definition of a business associate. The white paper covers another type of covered entity, the “hybrid entity,” which may help financial institutions reduce the administrative costs associated with implementing HIPAA data privacy and security measures. There are also key questions that a financial institution should ask while reviewing services to determine its status.

Infrastructure

What kind of internal reporting structure is needed to achieve compliance? What are the key roles? When the HIPAA data privacy and security rules apply, the financial institution compliance programs need a corporate-level sponsor as well as a HIPAA Privacy Officer and a Security Officer. In addition, business unit managers, the legal department, and marketing/product development departments each play a role in a solid compliance program. This white paper lists some of the typical responsibilities for each role.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Risk Analysis

The HIPAA Security Rule requires covered entities and business associates to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI.

Risk Audit

What is the recommended practice for conducting a risk audit to identify issues and mitigating controls or control gaps? This paper describes the risk audit process in four stages: planning, testing, reporting, and follow-up. A sample Risk and Control Matrix is included for reference.

Technology Systems

Financial institutions must be able to recognize and identify protected healthcare data as sensitive data in order to apply the proper technology and related processes. Financial institutions cannot meet the HIPAA and HITECH reporting requirements if the technology does not support a way to identify data privacy and security breaches. In addition to the overview of technology considerations within this topic, the white paper includes an appendix of “Technology Best Practices” that details specific recommendations across seven areas: physical data security, data encryption, logging, authentication, authorization, intrusion detection, and related technology policies.

Communications Plan

A communication plan must address the needs of many audiences: workforce members, customers, the public, government, and the media. Financial institutions must be prepared to share compliance efforts to attract and maintain business. It is also critical to address communication crisis management in the event of a data privacy or security breach.

Workforce Training

General privacy and security training may not be adequate for the HIPAA data privacy and security rules. Initial training regarding the regulations, requirements, and handling of protected health information must occur before the workforce member has access. Demonstrating participation in training is not sufficient. The financial institution should be able to demonstrate the workforce members received and understood the training in policies and practices.

Compliance Tool Sets from Independent Third-Parties

Finally, this white paper presents various third-party programs that financial institutions may use to assess compliance programs for healthcare data privacy and security measures to demonstrate performance to the public and customers.

Introduction

The evolution of electronic business processes in healthcare is occurring rapidly after the passage of the American Reinvestment and Recovery Act (ARRA) with \$20 billion earmarked for health information technology investment. This new “Era of ARRA” has accelerated mission-critical operational links between the provision of healthcare services and payments for those services. Electronic linkages between administrative information technology systems and financial institution networks in other industries have created systemic value and spurred new market competition, fundamentally transforming industry alignments. Administrative simplification enabled by electronic integration across industries tends to create new value for end users just as the SABRE computer reservation system has done for various travel industries. This market dynamic applied within the healthcare setting, known as “medical banking™”, is inevitable as organizations seek solutions to paper-based inefficiencies across the healthcare stakeholders (MBProject, 2001).

With the convergence of banking and healthcare technologies, the public has growing concerns about who uses or has access to healthcare information. While financial organizations are highly regulated and maintain some of the highest standards for data protection across all industries, new laws under the HIPAA and HITECH acts include increased penalties for the disclosure of protected health information. These laws clearly impact some financial services in the healthcare sector, and financial institutions need to understand the application of these laws on their operations. In light of these factors, volunteers from financial institutions, trade associations, independent consulting firms, and professional organizations in healthcare technology and industry regulations collaborated to develop the “Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy And Security Rules.”

Business Purpose of the White Paper

This paper provides information that financial institutions can use to evaluate and guide their compliance needs under HIPAA and HITECH¹. It includes an overview of the HIPAA and HITECH acts with emphasis on the impact on financial institutions. It also provides guidelines for assessing the institution’s classification under HIPAA and which functions or programs may be covered. The paper then follows with recommended approaches for setting up compliance program governance, performing a risk audit, updating technology systems, developing communication plans, and providing required workforce training. Financial institutions will also find helpful information about two third-party programs for assessing compliance with healthcare data privacy and security rules and demonstrating this compliance to the public,

¹ There is a new [draft NPRM](#) from the Department of Health and Human Services intended to modify HIPAA, including many key definitions, for the stated purpose of implementing the HITECH amendments and strengthening protections of individually identifiable information. Published July 14, 2010, this draft NPRM is open to public comment through 9/13/2010. Since the rule is not final, the authors cannot comment on the impact in this white paper. The reader should be aware of the shifting landscape.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

business partners, customers, and the government. Finally, appendices offer more details, including a glossary and technology best practices.

Covered Topics

First, there is an overview of the HIPAA and HITECH acts with emphasis on the key areas that relate to the growing field of “medical banking™” – banking and/or financial services specialized for the healthcare industry. Financial institutions can also find guidelines for assessing their entity classification under HIPAA. The guidelines also include recommended approaches to setting up compliance program governance, performing a risk audit, updating technology systems, developing a communication plan, and updating workforce training. Financial institutions will also find helpful information about two different third-party accreditation programs that can assess measures for healthcare data privacy and security and demonstrate performance to the public, business partners, customers, and the government. Finally, there is a series of appendixes that offers more detail, including a glossary and technology best practices.

This white paper builds on an earlier paper entitled “Financial Services Current State in Healthcare,” published jointly by WEDI and EHNAC in November 2009. That paper provides a general landscape view of financial institutions entering the healthcare sector, including the challenges they face in meeting ever-increasing healthcare regulations. Financial institutions and other interested parties may obtain a copy of this paper from the [EHHAC web site](http://www.ehnac.org/assets/files/PDF/Financial_Services_Current_State_in_Healthcare-FINAL.pdf). (URL: http://www.ehnac.org/assets/files/PDF/Financial_Services_Current_State_in_Healthcare-FINAL.pdf)

Out of Scope

While this white paper or its founding principles have been approved by the respective boards of the Workgroup for Electronic Data Interchange, the Electronic Healthcare Network Accreditation Commission and the Healthcare Information Management Systems Society², it cannot cover every aspect of HIPAA and HITECH. This paper is not a legal opinion. The statements made herein by the group of volunteers do not necessarily represent the views of each respective organization or the publishers.

In addition, this paper does not provide guidance on state laws regarding healthcare data privacy and security. There are many state laws and regulations protecting health information that support a state’s right to care for the public health, safety and welfare of its citizens. Generally, HIPAA and HITECH set a floor, not a ceiling, for data privacy and security. State laws are often more stringent, providing greater protections in certain cases such as mental illness,

² On June 18, 2010, the HIMSS Board voted to affirm a letter drafted by the chair of the National Committee on Vital and Health Statistics in 2004 that: (1) recommended that all covered entities execute business associate contracts with their banks and financial institutions when there is access to protected health information; and, (2) acknowledged that some banks by virtue of the work they perform for clients are covered entities under the HIPAA statute. These principles, developed in the marketplace after numerous forums between 2001-2004 conducted by MBProject and drafted into the NCVHS letter, form the basis for the application of HIPAA policy within banking, financial clearinghouses, financial institutions and the financial services sectors.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

AIDS/HIV status, drug or alcohol addictions, and genetic testing. Some states also have stricter laws regarding the use and disclosure of protected health information as well as greater penalties for breaches.

Background of the Publishing Organizations

EHNAC

“Founded in 1993, the Electronic Healthcare Network Accreditation Commission (EHNAC) is a federally-recognized, standards development organization and tax-exempt, 501(c)(6) non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare. An independent, self-governing body, EHNAC represents a diverse cross-section of healthcare stakeholders. Electronic health networks, payers, hospitals, physicians, consumer groups, financial services firms, security organizations and vendors are all working together to establish sound criteria for self-regulation. Through this collaboration, EHNAC is realizing a shared vision and providing a valuable service through accreditation services that promote standards, administrative simplification and open competition in the marketplace. Each EHNAC-recognized organization improves business processes, encourages innovation, improves quality of service, ensures HIPAA compliance, and expands market opportunities.”
[“About EHNAC”. EHNAC. 6/23/2010 <www.ehnac.org>.]

HIMSS

HIMSS is a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. Founded 50 years ago, HIMSS and its related organizations have offices in Chicago, Washington, DC, Brussels, Singapore, Leipzig, and other locations across the United States. HIMSS represents more than 30,000 individual members, of which 68% work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 470 corporate members and more than 85 not-for-profit organizations that share the mission of transforming healthcare through the effective use of information technology and management systems. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, and research initiatives designed to promote the contributions of information and management systems to improving the quality, safety, access, and cost-effectiveness of patient care. For more about HIMSS, its members, and how to join; please visit the website at www.himss.org.

NACHA – The Electronic Payments Association

“Established in 1974, NACHA —The Electronic Payments Association was formed by the California ACH Association, the Georgia Association, the New England ACH Association, and the Upper Midwest ACH Association, to establish uniform operating rules for the exchange of Automated Clearing House (ACH) payments among ACH associations. The ACH Network had its start in the early 1970's when a group of California bankers formed the Special Committee on Paperless Entries (SCOPE) in direct response to the rapid escalation of check volume in the

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

United States. The Committee set out to explore the technical, operational, and legal framework necessary for an automated payments system, leading to the formation of the first ACH association in 1972. Similar groups soon formed around the country. By 1978, it was possible for two financial institutions located anywhere in the United States to exchange ACH payments under a common set of rules and procedures. By 1988, the number of ACH payments exceeded 1 billion annually. By 2001, the volume of ACH payments grew by more than 1 billion in a single year. More than 18.2 billion ACH payments were made in 2008, an increase of 1.2 billion over 2007. ACH payment volume continues to double every five years. The 2007 Federal Reserve Payments Study revealed ACH payments had the largest compound annual growth rate, 18.6 percent, of all U.S. non-cash payments. The ACH Network remains one of the largest, most efficient, and safest payment systems in the world.” [“History”. NACHA – The Electronic Payments Association. 7/30/2010 <http://www.nacha.org/c/aboutus_History.cfm>]

WEDI

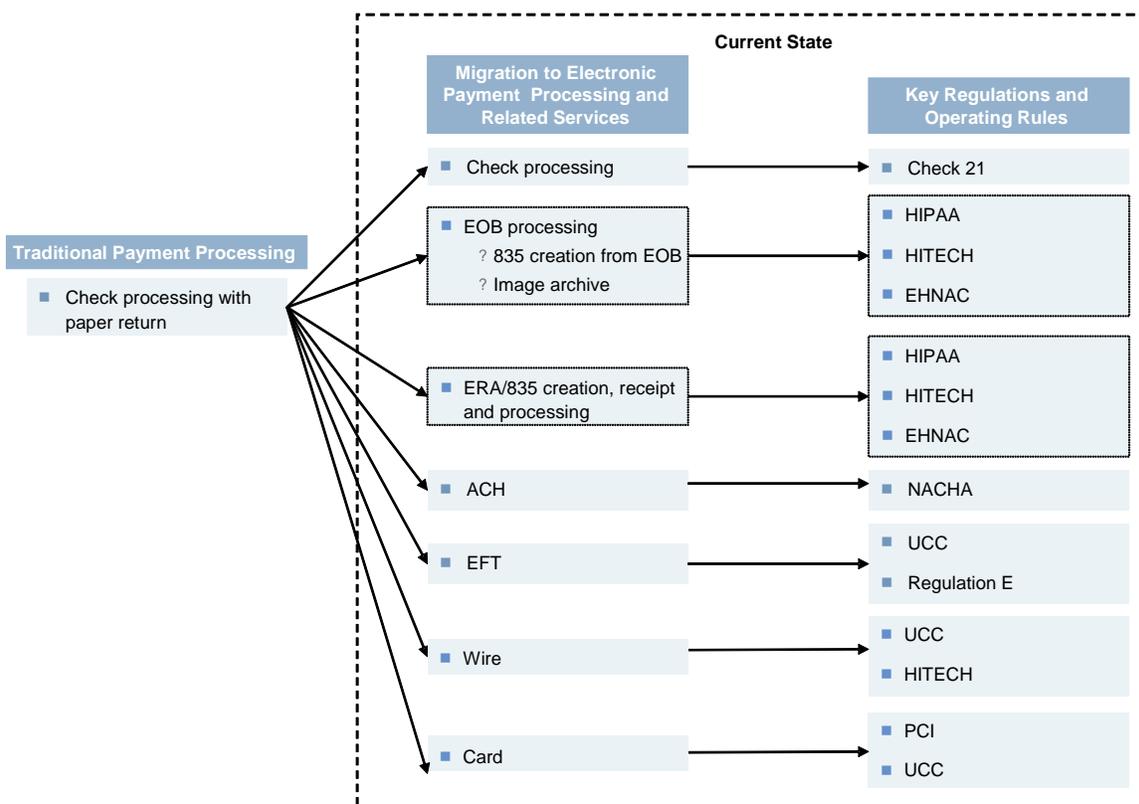
“The Workgroup for Electronic Data Interchange (WEDI) was established in 1991 in response to a challenge from then Secretary of Health and Human Services, Louis Sullivan, MD. The challenge was to bring together a consortium of leaders within the healthcare industry to identify practical strategies for reducing administrative costs in healthcare through the implementation of EDI. WEDI quickly became a major advocate in promoting the acceptance and implementation of the standardization of administrative and financial healthcare data. WEDI continued its EDI advocacy and helped secure passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996. WEDI's unique position and influence was acknowledged in its designation in the HIPAA legislation as an advisor to the Secretary and as a facilitator of industry consensus on the implementation and fulfillment of this mandate. Today, WEDI's membership includes providers, health plans, consumers, vendors, government organizations, and standards groups committed to the implementation of electronic commerce in healthcare and EDI standards for the healthcare industry.” [“WEDI History”. WEDI. 6/23/2010 <www.wedi.org>]

Overview of Applicable Regulations

Due to advances in technology and changes in the healthcare landscape, financial institutions are expanding the services they provide for the management of healthcare revenue. For example, services may extend beyond payment processing into converting the paper Explanation of Benefits (EOB) statements into electronic remittance advice files delivered to a lockbox with a check payment. The landscape of the evolution of financial services and resulting regulations and operating rules is illustrated in Figure 1.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Figure 1: Evolution of Financial Services and Resulting Rules & Regulations



This paper focuses on the HIPAA and HITECH Act regulations. The passage of HIPAA in 1996 and its modification by the HITECH Act in 2009 created responsibilities for the financial sector to safeguard “protected health information” (PHI) as defined in the final regulations issued by the Department of Health and Human Services. (Refer to [Appendix I](#) for the regulation definition of PHI.)

HIPAA

Enacted in 1996, the Health Insurance Portability and Accountability Act (HIPAA) includes the Administrative Simplification subtitle to promote efficiency in the healthcare industry through the use of standardized electronic transactions while protecting the privacy and security of health information. Under this law, the Department of Health and Human Services (HHS) issued regulations to adopt standards for Electronic Data Interchange (EDI) as well as standards for health information privacy (Privacy Rule) and security (Security Rule). The law directly applies to three defined covered entities:

- Healthcare Providers that conduct electronic transactions
- Health Plans
- Healthcare Clearinghouses that receive nonstandard health information and convert it to a standard transaction or vice versa

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Historically, many financial institutions considered HIPAA a regulation that only applied to human resource functions. However, a series of industry events led to a much more detailed review of the application of HIPAA on financial institutions. In 2001, the Medical Banking Project developed a roundtable at the 3rd National HIPAA Summit to launch a substantive dialogue on the issue. This event spurred further research by industry groups including a taskforce developed by the NACHA-Electronic Payments Association (National Automated Clearing House Association) and the American Bankers Association as well as legal articles and opinions published by LexisNexis. By 2004, the National Committee on Vital and Health Statistics (NCVHS), a statutory advisor to the Department of Health & Human Services (HHS), organized two panels of experts to evaluate the matter. NCVHS then drafted a letter recommending that covered entities that use financial institution services execute a business associate agreement until HHS provided further clarification. (The letter is in [Appendix VIII](#).)

The HIPAA Privacy Rule and Security Rule regulate the allowed uses and disclosures of PHI, which the law defines as individually identifiable health information in any form with minor exceptions. (See the HIPAA definitions in [Appendix I](#) for more detail about PHI and individually identifiable health information.) Since other entities may support the efforts of covered entities in the management of health information, HIPAA's regulations also define another class of entity called a "business associate." A business associate is a person or organization that performs an activity on behalf of a covered entity but is not part of the covered entity's workforce. The definition of business associate specifically addresses financial institutions as it includes entities that provide "...financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person."

By regulation, covered entities are only allowed to share PHI with business associates that are engaged under an agreement which requires the business associate to protect the information in ways equivalent to the requirements for covered entities. The only exemption is defined under §1179 [42 U.S.C. 132d-8] for financial institutions. Section 1179 excludes the following services performed by or on behalf of a financial institution: "authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting, a payment for, or related to, health plan premiums or healthcare, where such payment is made by any means, including a credit, debit, or other payment card, an account check, or electronic funds transfer." The interim final rule with comment (IFC) "Administrative Simplification: Adoption of Standards for Health Care Electronic Funds Transfers (EFTs) and Remittance Advice", issued January 10, 2012, clarified the section 1179 exemption for financial institutions and states "even absent section 1179 of the Act, the HIPAA Privacy and Security rules would not apply to the transmission of health care EFT standards adopted herein." The health care EFT standard adopted in the IFC is the NACHA CCD+Addenda and does not carry PHI.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

However, when financial services process transactions with protected health information between healthcare providers and payers, HIPAA fully applies. Financial institutions must conduct such services under business associate agreements with all the restrictions and potential risks that may result, including legal, financial, and reputational risks.

HITECH

The national Health Information Technology for Economic and Clinical Health Act (HITECH Act) passed on February 17, 2009, as part of the American Reinvestment and Recovery Act. About \$20 billion was allocated to promote the use of health information technology such as electronic health records to reduce healthcare costs. Effective on February 10, 2010, many HITECH provisions modified and amplified the HIPAA provisions that affect financial institutions. As a result, financial institutions need to be knowledgeable about HITECH to assess whether the provisions impact current or planned services to guide development of reasonable internal policies, practices and procedures to help ensure compliance.

In particular, HITECH modifies HIPAA in three key areas:

1. HITECH extends the Privacy Rule and Security Rule requirements directly to business associates.
2. HITECH adds strict breach reporting requirements.
3. HITECH toughens enforcement mechanisms and penalties.

Implications for Financial Institutions

The passage of the HITECH Act has added accountability for financial institutions that provide medical lockboxes and other types of services to healthcare providers and payers. It is critical to evaluate compliance responsibilities. Financial institutions need to identify their potential status as a covered entity or a business associate under HIPAA and HITECH. If the financial institution meets either definition, it must develop and implement procedures and policies that ensure compliance with using and disclosing protected health information only in the manner set forth in the HIPAA privacy and security provisions. Under the HITECH Act, a business associate is now held to many of the same requirements as a covered entity, especially in the areas of documenting and maintaining policies and procedures related to PHI and reporting information security breaches. Many financial institutions that act only as business associates will find that they have a short period of time to understand and implement the rules by which they must now conduct business.

In addition, financial institutions that are business associates or covered entities are now under the direct supervision of the Office for Civil Rights (OCR) of the Department of Health and Human Services which is the regulatory agency responsible for ensuring compliance with these privacy and security regulations. This supervision does not replace other regulatory supervisory relationships.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Any unauthorized acquisition, access, use, or disclosure of protected health information triggers the requirement that a business associate notify the covered entity immediately (see 45 CFR 164.410 Notification by a business associate). Reporting requirements are significant: “Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed.” The covered entity must then notify individuals affected “... without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.” For breaches affecting fewer than 500 people, annual reporting is required. Larger breaches must be reported to “prominent media outlets” and to HHS “contemporaneously” for posting on the HHS web site.

Guidelines

Financial institutions will find the listed tasks helpful to develop and implement the policies and procedures for achieving compliance and mitigating risk. Although each financial institution will need to ultimately determine its own required tasks, this white paper provides guidelines in each area.

1. Determine eligible current or planned services and the financial institution’s status as a covered entity or business associate under HIPAA and HITECH.
2. Set-up the infrastructure to successfully achieve compliance. This task includes the selection of a corporate-level program sponsor as well as a privacy officer and a security officer. These roles may be assumed by one or more individuals.
3. Conduct a risk analysis.
4. Conduct a risk audit and identify controls or control gaps.
5. Review and update technology systems as needed.
6. Develop a communications plan.
7. Update workforce training.
8. Consider data privacy and security accreditation or certification by an independent third-party such as EHNAC or HIMSS.

1. Determining the Financial Institution’s Eligible Services and Status

A financial institution must determine its status as a covered entity or business associate under HIPAA and HITECH through a review of offered or planned services that encounter health information. HIPAA does not necessarily apply to all activities involving encounters with health information. It is the responsibility of the financial institution to determine for itself whether it meets the criteria of a covered entity or a business associate subject to HIPAA.

As noted under the HIPAA topic within the “Overview of Regulations” section, a business associate is a person or organization that performs an activity on behalf of a covered entity but is not part of the covered entity's workforce. This activity includes financial services where the provision of the service involves the disclosure of protected health information. Table 1 includes

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

the “covered entities” as defined in Title 45, §106.103, of the HIPAA law. Covered entities are required to abide by and comply with HIPAA standards and regulations.

Table 1: HIPAA Covered Entities

Covered Entity	Definition	Examples
Health Plan	An individual or group plan that provides or pays the cost of medical care.	Health insurance issuer, an HMO, Medicare, Medicaid
Healthcare Clearinghouse³	A public or private entity that does either of the following functions: (1) 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. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.	A billing service, repricing company, community health information system, “value-added” network
Healthcare Provider	A provider of medical or health services and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business. The healthcare provider is only a covered entity under HIPAA if the provider transmits any health information in electronic form in connection with a transaction for which standard HIPAA requirements have been adopted.	Includes facilities such as hospitals and clinics as well as individuals such as doctors, nurses, and other medical specialists.

Which Financial Institution Services Are Covered by HIPAA?

Although each financial institution must ultimately determine its own status, Table 2 lists a few possible considerations and questions that financial institutions should review when determining if a service in the healthcare sector may qualify the organization as a covered entity

³ Initially, HIPAA defined Health Care Clearinghouses in such a way that they could translate to and from paper or other non-standard forms of information on behalf of the non-compliant provider or payer. Since the intent was to cover only transactions between payers and providers, section 1179 was added to assure financial institutions that transactions made on behalf of consumers were not covered.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

or a business associate under the HIPAA privacy and security rules. Each service should be evaluated separately.

Table 2: Guiding Questions for Determining HIPAA Status

Consider the listed items when evaluating HIPAA status...
1. Does this service involve passing protected health information to a covered entity?
2. Does this service involve modifying protected health information for a covered entity?
3. Does this service involve storing or archiving protected health information?
4. If the answer to question 1, 2, or 3 is “yes,” which workforce members can access the protected health information?

The Hybrid Entity Advantage: When Financial Institutions Provide Covered and Non-Covered Services

The HIPAA law and regulations recognize that there are organizations that provide services for the healthcare industry that are not the primary line of business. For example, a county government may operate a hospital. A financial institution may provide services that qualify the organization as a covered entity or as a business associate. However, these services, or covered functions, are not typically the financial institution’s primary functions. In recognition of this reality, the HIPAA rules include a provision that allows financial institutions and other organizations to self-identify as a “hybrid entity” to isolate the covered functions or services subject to HIPAA from the non-covered functions. [Appendix II](#) includes details about the HIPAA definition of a hybrid entity and guidelines for conducting a hybrid entity analysis.

Each financial institution must conduct its own analysis and make a legal determination of which component(s) perform covered functions and which components perform non-covered functions. The HIPAA privacy and security rules apply only to the covered components, reducing the overall cost of administration and operations. **If the financial institution elects not to conduct a hybrid entity analysis and document its status, then the entire organization is automatically a covered entity if it performs any covered functions.** The compliance requirements and associated risks would apply to all aspects of the financial institution and its employees.

For example, a financial institution has 10,000 employees, and only 500 of them work directly or indirectly with the lockbox operations which includes processing electronic transactions with protected health information. The remaining 9,500 employees are not involved in these operations. Without conducting a hybrid entity analysis and documenting the status, the entire financial institution and its workforce are subject to the HIPAA data privacy and security requirements. In contrast, if the financial institution documents its status as a hybrid entity after conducting a proper analysis, then the HIPAA rules may only apply to the 500 members of the workforce involved with the lockbox service. Costs are likely reduced because only the 500

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

employees within the designated healthcare components require the HIPAA controls and training.

In addition, some financial institution compliance officers believe that the hybrid entity analysis reduces the risk of violating HIPAA privacy and security because a smaller portion of the organization is subject to direct oversight by the “Office of Civil Rights,” and now some state government(s), under HITECH. It is important to note that a hybrid entity would also be well advised to implement proper physical and logical security controls to effectively create a real data privacy and security boundary, or “firewall,” between the hybrid entity component(s) and the non-covered components.

2. Recommended Corporate Infrastructure and Governance

After identifying its status and the applicable covered functions, a financial institution should adopt a written compliance program to meet its needs. As part of a comprehensive program, the financial institution needs to align the corporate governance framework and operational infrastructure to support the requirements of the HIPAA and the HITECH acts. It should define the roles of the key players and identify the affected individual business units. It should also define the frequency and strategy for conducting periodic analysis for risk management and the monitoring of protected data security and privacy.

Identify Key Players and Responsibilities

Here are a few key infrastructure questions the financial institution will need to address:

1. Who is the corporate sponsor with oversight responsibility of the compliance program to ensure the privacy and security of protected health information?
2. Who is the designated Privacy Officer or Security Officer?
3. Who is responsible for working with the officers to represent each business unit and work to maintain compliance?

Table 3 lists key players in a compliance program and their typical responsibilities. These key players work together to design and implement the appropriate data controls and procedures.

Table 3: Compliance Program Roles and Responsibilities

Role	Possible Responsibilities
Chief Compliance Officer / Corporate Sponsor	<ul style="list-style-type: none">• Oversee the compliance program; develop and maintain the written HIPAA Program.• Complete periodic risk assessments of individual business units and communicate results.• Provide subject matter expertise in application of HIPAA Privacy Rule and Security Rule.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Role	Possible Responsibilities
	<ul style="list-style-type: none"> • Monitor regulatory changes and work with the team to identify the impact and corresponding required program changes. • Serve as a member of the HIPAA Incident Response Team. • Create or review the appropriate training modules.
<p>HIPAA Privacy Officer / Security Officer</p>	<ul style="list-style-type: none"> • Serve as compliance program administrators. • Conduct periodic HIPAA reviews and evaluate individual business unit compliance. • Partner with the Corporate Compliance Officer and business unit liaisons to develop processes to identify and safeguard protected healthcare information and implement controls. • Provide subject matter expertise in the application of the HIPAA Privacy Rule and Security Rule. • Review new vendor relationships for HIPAA implications requiring Business Associate Agreements. • Serve as a member of the HIPAA Incident Response Team to investigate and respond to suspected privacy and security breaches as well as incidents of non-compliance. • Create or review the appropriate training modules. • Respond to third-party inquiries related to disclosure of protected health information.
<p>Business Unit Management / HIPAA Liaisons</p>	<ul style="list-style-type: none"> • Be aware of the compliance program requirements, HIPAA requirements, and the business unit level impact. • Ensure that the business unit adheres to the compliance program and HIPAA regulations. • Ensure efficient and effective management of HIPAA risks associated with business processes, products, and services. • Adhere to incident management protocol associated with suspected data privacy or security breaches. • Notify the Corporate Compliance and the HIPAA Privacy/Security Officer(s) of <i>changes</i> in existing processes, services, or vendor contracts that involve health information. • Consult with the Corporate Compliance Officer and the HIPAA Privacy/Security Officer(s) regarding <i>new</i> processes, services, or vendor contracts that involve health information so HIPAA impact can be determined prior to implementation. • Notify and consult with HIPAA Privacy Officer prior to the disclosure of protected health information. • Review and communicate changes to HIPAA policies and procedures to employees to ensure continued compliance.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Role	Possible Responsibilities
	<ul style="list-style-type: none">• Ensure that all workforce members within the business unit receive mandatory compliance training.
Legal Department	<ul style="list-style-type: none">• Develop and update response policies and procedures for notification, litigation, or investigations related to data privacy and security breaches.• Monitor HIPAA or HITECH rule changes and notify the Compliance, Security, and Privacy Officers accordingly with any changes.• Develop policies and procedures for staff response to problems and breaches.• Review and update Business Associate Agreements.• Review all third-party contracts for PHI access or storage for the necessary data privacy and security measures.• Develop and maintain the HIPAA policies and procedures for the contractual relationship with the customer.
Marketing / Product Development	<ul style="list-style-type: none">• Be prepared to respond to business proposal opportunities (RFP's) from healthcare payers and providers who seek assurance that the financial institution complies with HIPAA privacy and security regulations. Work with other areas as needed to address the potential questions about risk management, data privacy and security policies, physical and environmental security measures, information system security measures, breach incident management, and business continuity planning.• Review and ensure that new or enhanced products and services that require compliance with HIPAA and HITECH are designed and promoted appropriately.• Review standing products for compliance issues; take appropriate steps to correct any deficiencies.• Work with Legal to review vendor relationships with remarketed products.

3. Conduct a Risk Analysis

The HIPAA Security Rule requires covered entities and business associates to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI. One effective approach to meet this requirement is to conduct the analysis as part of a standard annual corporate regulatory risk assessment. The purpose of this analysis is to identify all protected health information and mitigate any existing risk to the

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

security of this data. Each subsequent annual analysis will verify the previously identified risks as well as detect any new risks due to business changes or changes in the law.

The Office for Civil Rights (OCR) published guidance about the requirement on May 7, 2010 (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf>). This was OCR's first publication of guidance in compliance with their requirement to issue annual guidance on the provisions in the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) These initial guidelines provide sample questions organizations could consider as elements of a risk analysis with a list of resources available for risk analysis and risk management.

4. Conduct a Risk Audit

Effective February 17, 2010, the Secretary of the Department of Health and Human Services (HHS) is required to periodically audit covered entities and business associates for compliance with the HITECH Act and the HIPAA privacy and security rules. Although the financial institution may not be selected for an HHS audit, it is prudent to be prepared by conducting an internal risk audit. The financial institution's internal auditors, the HIPAA Privacy Officer, or the HIPAA Security Officer may perform this task. Alternatively, the financial institution can contract with a third party such as an accounting firm or accreditation organization such as EHNAC. Regardless of who conducts the risk audit, it can be broken out into four main processes: (1) Planning the Audit, (2) Testing, (3) Reporting Issues, and (4) Follow-Up.

Planning the Audit

First, the financial institution must determine the areas that are subject to the audit. This may be accomplished by meeting with senior executives to determine the areas of risk. For example, departments that have access to protected health information would be considered high risk. After identifying the review areas, the auditor must gain an understanding of the key business processes (such as new customer set-up) and identify the likely risks.

To develop a comprehensive understanding of the business processes, the auditor should walk through each process with various levels of employees. In addition, the auditor can compare employee descriptions of the processes to written policies and procedures to determine if the actual practices reflect the written policies and procedures. The auditor is responsible for maintaining documentation of the covered processes within the audit. This documentation may include a narrative of the process, any affected general ledger or internal demand deposit accounts, and the software applications or hardware systems used to conduct the process.

The auditor should further evaluate the policies and procedures to ensure they adequately mitigate risk. Risks fall within these categories: Market Liquidity/Interest, Credit, Operational, Legal/Compliance, Strategic/Reputation, and Fraud. A risk may be classified as low, moderate, or high depending on the probability and the business impact of it occurring.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

After identifying the possible risks, the auditor should determine whether the organization has implemented controls to mitigate each risk. Controls may be automated, manual, or a combination of these methods. In addition, the controls may be classified as either preventive or detective:

- A preventive control gives the business unit or company a chance to correct a deficiency before it becomes a problem.
- A detective control alerts the business unit or company as soon as possible after a problem occurs so it can be resolved quickly.

If there are no controls to mitigate an identified high or moderate risk, then the auditor should escalate this finding to management for appropriate action. If there are controls in place to mitigate risk, then the auditor can develop a testing strategy. The auditor can use the “Risk and Control Matrix” in Table 4 to detail the risks and controls. Table 4 also includes a sample identified risk with the associated controls. Table 5 contains the legend for the matrix.

Table 4: Risk and Control Matrix

RISKS				CONTROLS			
Risk	Type	Probability	Impact	Control	Type	Method	Key Y/N
<i>Risk #1 (e.g., process xyz is not done accurately, not done timely, not properly approved, etc.)</i>	M/C/O/ LC/SR/FR	L/M/H	L/M/H	1. Mitigation Control for Risk #1 <i>(Note: If no control is in place, then identify the gap. The auditor could list the desired control here in italics.)</i>	P/D	A/M/C	
1. Potential data security breach during new customer setup test process: PHI sent via unsecured e-mail.	LC/SR/O/ FR	M	H	1. E-mail Monitoring Software 2. SECURE e-mail encryption	P P	A C	Y Y

Table 5: Legend for the Risk and Control Matrix

Risk Type	Risk Probability	Risk Impact	Control Type	Control Method	Key Control? Y/N
M – Market Liquidity/Interest	How likely is the risk to occur?	If it occurs, how serious is the business impact?	P – Preventive D – Detective	A – Automated M – Manual C – Combined	Is this a key control?
C – Credit Risk	L – Low	L – Low			
O – Operational Risk	M – Moderate	M – Moderate			
LC – Legal/Compliance	H – High	H – High			
SR – Strategic/Reputation					
Fr – Fraud					

Testing: Performing the Audit Fieldwork

Audit fieldwork consists of testing the key controls identified and documented during a risk audit as illustrated in Table 4. The auditor tests the controls to determine if they are operating

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

effectively to mitigate the risks. First, the auditor should determine the appropriate test sample that represents the population so the conclusions are valid. Once the sample is selected, management can give the auditor access to the necessary materials to conduct testing. The auditor designs the testing procedures by identifying a number of attributes to review. For example, if an auditor was testing to ensure adherence to data breach procedures, the auditor could utilize the following test attributes:

- Review the incident report for completeness.
- Review the incident report for accuracy (may be necessary to validate key data fields in systems of record).
- Review the incident report for evidence of the employee who completed the form and a supervisor/manager review (signatures).
- Determine if the HIPAA Privacy Officer took the appropriate action (i.e., reported the breach to internal management and to HHS, etc.).

Report on Audit Issues

The auditor should keep meticulous records of testing procedures and results, especially exceptions. The auditor should communicate issues to key stakeholders in writing. The auditor should also report exceptions to management to validate the accuracy of the findings and to provide an opportunity for remediation. It is in the auditor's best interest to validate the results with the responsible manager. The auditor will lose credibility if the reported issue is later determined to be inaccurate. To provide clear and concise reports, an auditor can reference the following framework:

- Detail the root cause of the issue. For example, "The quality control review is not effective for the abc process."
- Explain the exception or scenario that led to the determination of the root cause. "In testing, the auditor identified six data integrity errors out of a sample of 10 that the supervisor did not detect."
- Provide the risk of the issue. "A lack of data integrity can result in inappropriate access to protected health information." It is also helpful for executive and senior management to have the auditor's assessment as to whether the risk presents high, moderate, or low impact to the financial institution.

Follow-Up

The financial institution should have a mechanism to track and follow-up on identified issues to ensure that they have been corrected. The financial institution may have a database to provide a comprehensive list of all reported open and closed control issues. Management should provide a target closure date to the auditor. Once management has notified the auditor that the appropriate corrective action has been taken, the auditor can determine whether follow-up testing should be performed to validate that the corrective action resolved the identified control weakness. Usually, re-testing is performed if the issue was considered high risk or significant to

the control environment of the organization. In subsequent audits, the auditor should review the closed issues to make sure corrective actions are still working.

If remediation does not occur within a reasonable amount of time or within the timeframe prescribed by federal or state law, the auditor must follow the established escalation process which may include suspension of the non-compliant business activity (or activities) if the deficiency is of substantial severity in light of any potential risk. If non-compliant services cannot be suspended or terminated, the financial institution is required to report the matter to the Department of Health and Human Services under HITECH for further resolution.

5. Update Technology Systems

As an industry, financial institutions are familiar with technologies that help ensure sensitive data is properly handled. With HIPAA and HITECH, the challenge is to recognize and identify protected healthcare data as sensitive data so that the financial institution can apply the proper technology and related processes and document the application of that technology. In addition, financial institutions cannot meet the HIPAA and HITECH reporting requirements if the information technology does not identify data privacy and security breaches. IT audit procedures are often oriented toward detection and repair of database errors, not toward unauthorized uses or disclosures of protected health information. For example, if an internal auditor's laptop is stolen, can the financial institution prove that all protected health information was properly encrypted? If not, can the financial institution identify each individual whose information was on that laptop for notification purposes? These compliance requirements may require significant rethinking of procedures, technology upgrades, or software replacement.

Many financial institutions are considering new cash management, lending and other services that require the processing and archiving of healthcare data. In some cases, the financial institution will outsource a portion or all of the processing. The financial institution is still obligated under the business associate agreements to ensure that their vendors are properly handling the data. When considering vendors, the financial institution would do well to remember that the chain-of-trust is only as strong as its weakest link.

For example, a financial institution may offer a service that allows hospitals and physicians to extend the current basic lockbox service to the conversion of receivables into files that can be posted to the customer's healthcare systems. The financial institution may also archive this information so that back office workers at the hospital or doctors office can view the information online. The financial institution may further include matching the healthcare provider's submitted claims to the received remittances and also allow the healthcare providers to view this information through the online financial institution portal. When the financial institution provides these services to healthcare providers, it is processing or archiving protected health information and is required to safeguard it. Within this example, the related technology safeguards include:

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

- 1) Perform the work in a data center (or data centers) that contains proper physical security and redundancy provisions.
- 2) Proper encryption and tracking of files received from and transferred to healthcare provider customers.
- 3) Proper logging of work in process such that every process performed and every bit of information viewed by a workforce member or customer is logged. The logs must be kept and available on request for a minimum of seven (7) years.
- 4) Proper application authentication and password control so that workforce members and customers who view data through the system are authenticated and authorized to do so.
- 5) The application and the authorization process must be designed so workforce members and customers are exposed only to the minimal amount of protected health information necessary to facilitate the administrative task they need to perform.
- 6) Proper intrusion detection and multiple firewall security should be employed to protect against unauthorized outside intrusion into the system.
- 7) Finally, the financial institution needs to adopt policies that incorporate the technologies they employ to address the issues outlined above.

The “[Technology Best Practices](#)” appendix within this paper outlines specific recommendations related to the seven points in this section.

6. Develop a Communication Plan

Compliance is about more than meeting government regulations. Communicating compliance efforts permits the financial institution to gain the confidence of its stakeholders that its business practices fully address publically recognized standards. For the privacy and security of sensitive healthcare information, this is especially important because it has become the subject of significant public concern and advocacy. HIPAA and HITECH mandates, in particular, provide a recognized framework for an effective communications strategy and plan that will help financial institutions achieve a return in their investment in HIPAA and HITECH compliance. This section of the white paper identifies the various audiences, communication purposes, and communication methods that the financial institution should cover as part of their corporate communication plan.

Target Audience and Communication Purpose

Employees

HIPAA mandates that organizations educate affected employees on their responsibilities related to maintaining the security and privacy of protected health information. Therefore, a targeted workforce education program concerning HIPAA responsibilities needs to be a key component

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

of the organization's HIPAA compliance program. Other workforce members should also be aware of such compliance efforts so they can support the efforts of affected members as well as help convey the financial institution's compliance efforts to customers and business partners, as the opportunity arises.

Customers and the public

HIPAA and HITECH privacy and security requirements are a result of public concerns about health information. Financial institutions have a major opportunity to build on the historic public trust in their capability to securely manage financial transactions, extending it to handling healthcare information. For such audiences, a financial institution may want to consider taking advantage of advertising and communicating through simple messages such as those resulting from achieving EHNAC accreditation or incorporating the HIMSS Gold Seal compliance practices as described in section "7. Compliance Tool Sets from Independent Third-Parties" in this white paper. In addition, a financial institution may want to consider which compliance documentation is appropriate to make available upon inquiry. Covered entities have been increasingly likely to request detailed compliance information from their business associates.

Government

Proactive HIPAA and HITECH compliance programs provide the financial institution a seat at the table in determining which regulatory requirements are appropriate. There are currently many gray areas of interpretation in financial institution operations. Financial institutions need to be able to quickly point out their compliance efforts, especially in case of a data privacy or security breach.

Media

Developing and publicizing a rigorous compliance program provides an opportunity to build public trust in an institution. Furthermore, HIPAA and HITECH already receive substantial, if sometimes confused, media attention. Media communications on HIPAA compliance efforts can also help give greater visibility to programs and services related to healthcare. For example, a financial institution's HIPAA compliance program can demonstrate it can be trusted to handle sensitive information confidentially which is an important consideration when seeking services among various vendors.

Communication Means and Purposes

In addition to targeting stakeholders, the financial institution needs to consider several different types of communications needs.

Detailed Communications

Business associates and employees involved with protected health information need a detailed understanding of institutional policies, practices and procedures as they relate to work performed on behalf of the financial institution.

Targeted Communications

Short, targeted communications may be more appropriate for most stakeholders who are not involved in day-to-day operations and thus do not need detailed information. These communications need to convey financial institutional leadership in meeting the requirements and public expectations. Certification and compliance programs, such as EHNAC accreditation and the HIMSS “Gold Seal,” can help quickly identify that an institution has a compliance program in place.

Crisis Management

HIPAA mandates that entities involved with protected health information have a “disaster recovery” program to protect this information in the event of a disaster or business interruption. In addition, both HIPAA and HITECH require covered entities and business associates to establish policies and procedures for actions taken in the event of a security breach. A component of both of these programs is how the organization handles its communications.

7. Workforce Training

Some financial institutions may believe that the general privacy and security training is sufficient for HIPAA, but this is not the case. The HIPAA Privacy Rule is very specific in many areas with requirements that are unique to HIPAA that must be met by the covered entity and by their business associates.

Requirement

HIPAA requires a covered entity to implement a workforce data privacy and security awareness training program. This includes training workforce members on policies and procedures with respect to protected health information as needed to conduct work functions. While the regulations are less clear for business associates, the advent of HITECH confers many of the same risks of noncompliance on business associates. Therefore, developing a compliance training program for any staff members involved with PHI would be an appropriate risk management strategy whether the financial institution is a covered entity or a business associate.

HIPAA regulations require that initial training occur within a reasonable period of time after an individual joins the covered entity’s workforce. As a best practice, covered entities are encouraged to interpret the phrase “a reasonable period of time” to mean “before the workforce member has access to PHI.” Thereafter, covered entities must retrain their workforce at least annually, though more frequent training may be required if the workforce member’s function changes materially or if there are new or significantly modified policies, procedures or practices. As with the initial training, training on new requirements or processes must occur within a reasonable period time after the change becomes effective.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Content

HIPAA's standards and regulations do not equally impact the financial institution's workforce. The impact depends on the nature of the job responsibilities and direct involvement with protected health information and the financial institution's privacy and security controls. A financial institution may choose a targeted approach to HIPAA training as the most effective way to educate groups of workforce members on specific requirements.

Simply providing a copy of the HIPAA regulations to a workforce member is not a sufficient training method. This action does not demonstrate that the individual fully understands the requirements and expected practices. Financial institutions have the responsibility to decipher regulations and determine the applicable requirements to business unit functions. A short example outline of the potential training program is provided in this section. This is only one example. Each financial institution will need to determine its training program needs.

1. Background
 - a. Summary regulatory content
 - b. HIPAA history
 - c. HITECH history
 - d. Definition of terms
 - e. Why these regulations apply to this financial institution
2. HIPAA and HITECH content applicable to workplace functions
 - a. Privacy requirements
 - i. Confidentiality
 - ii. Minimum necessary
 - b. Security provisions
 - i. Administrative
 - ii. Physical
 - iii. Technical
 - iv. Disaster planning
 - c. Documentation and reporting requirements
 - d. Human resource issues
 - e. Penalties
3. Specific policies and procedures of organization, including breach procedures
4. Test on materials

Recordkeeping

HIPAA also requires covered entities to document training has been provided to workforce members. Organizations can accomplish this task by tracking training session participants and requiring workforce members to sign that they received and understood the related policies and procedures. Many organizations also issue employees a certificate for their own files indicating completion of the training program.

8. Compliance Tool Sets from Independent Third-Parties

There are third-party programs available to financial institutions that can support compliance efforts and help demonstrate these efforts to the public, business partners, customers and the government. These programs complement or supplement the financial institution's internal compliance program and assessments. Third-party programs of nationally recognized organizations include:

- The EHNAC Financial Services Accreditation Programs
- The HIMSS Gold Seal Program

EHNAC Financial Services Accreditation Programs⁴

The EHNAC Financial Services Accreditation Programs (FSAP) help ensure that financial institutions follow HIPAA privacy and security rules as well as meet a range of criteria applicable specifically to financial electronic health networks. These accreditations are nationally recognized programs for financial institutions and vendors who process protected health information, manage insurance payments, or provide healthcare reimbursement management services. There are two different EHNAC FSAP programs:

- The FSAP-Electronic Health Network (FSAP-EHN) accreditation program is for financial institutions that also provide Electronic Healthcare Network (clearinghouse) services for any of these transactions: claims, eligibility, remittance advice, referrals or authorizations, and claim status. Program participation and accreditation demonstrates high quality standards in handling protected health information and ensures the financial institution follows industry-established criteria for processing payments and other financial transactions. This program includes criteria specific to the financial services industry and criteria to ensure general IT controls are met to assist with preparation for other audits such as SAS 70 or Sarbanes-Oxley.
- The FSAP-Lockbox accreditation is for financial institutions that provide lockbox services that include processing healthcare transactions. It differs from the FSAP-EHN program in that certain performance metrics are modified or not included. There are specific document handling and delivery criteria unique to this program.

Healthcare Information and Management Systems Society (HIMSS) Medical Banking Project's Gold Seal Self-Assessment Program⁵

The HIMSS Gold Seal Program guides financial institutions through HIPAA's security requirements using a detailed web-based application. In addition to supporting effective compliance administration, the display of the HIMSS Gold Seal, informs customers that the financial institution is following a process aimed at meeting the highest standards of data

⁴ <http://www.ehnac.org/accreditation-programs/fsap-accreditation.html>

⁵ http://www.mbproject.org/arc_goldseal.php

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

privacy and security compliance mandated under banking and healthcare regulations, including HIPAA. Some benefits of the HIMSS Gold Seal process include:

- Ensure appropriate controls are in place so that individuals using medical banking services can be assured of the confidentiality, privacy and security of their data.
- Identify any gaps in an existing compliance process and policy and highlight areas for effective remediation.
- Demonstrate and document organizational due diligence.
- Provide an independent assessment of compliance with relevant rules and regulations, including the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and related operational privacy and security standards using a common set of best practices criteria.
- Provide a level of accreditation that is appropriate and cost effective for organizations that are classified as business associates, covered entities or both, under HIPAA.
- Assist in market acceptance and credibility of new and evolving medical banking solutions.
- Promote market confidence in medical banking programs through the public and government acceptance of the HIMSS “Gold Seal” standard.
- Provide evidence to government regulators that a program and management infrastructure is in place to achieve continued compliance.

Conclusion

As financial institutions continue to offer and develop value-added services for the healthcare industry, they must be aware of the applicable HIPAA privacy and security regulations to capture market opportunities and avoid legal penalties. This white paper, “Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules,” can help financial institutions steer the development of a robust compliance program to meet the industry demand. As customers of financial institutions, healthcare providers and payers need assurances that financial institutions can safeguard protected health information with appropriate technology systems, infrastructure, and procedures for risk management and incident management. Workforce training and communication plans are also key success factors. Third-party organizations such as EHNAC and HIMSS offer compliance tool sets specifically for financial institutions for the evaluation of data privacy and security measures.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

List of Contributors

The listed volunteers contributed to the creation and publication of this white paper, “Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules.”

Contributor	Title	Company
1. Lee Barrett	Executive Director	EHNAC
2. William R. "Bill" Braithwaite, MD, PhD	Independent Consultant	Expert in Health Information Policy and Strategy
3. John Casillas	Senior Vice President	HIMSS Business-Centered Systems
4. Alberto Casas	Director, North America Receivables	Citibank
5. Tom Dean	CEO	Revenue Management Solutions, LLC
6. B. P. Fulmer	Managing Partner	Exchange EDI, LLC
7. Nancy Grant	Senior Director, Research & Standards	NACHA – The Electronic Payments Association
8. Stuart M. Hanson,	Vice President	Healthcare Solutions, Fifth Third Bank
9. Debra Hopkinson, RN MS	Operations Director	EHNAC
10. Sharon R. Klein	Esquire	Pepper Hamilton LLP
11. Steven S. Lazarus, PhD, CPEHR, CPHIE CPHIT, FHIMSS	1. President 2. Co-Founder	1. Boundary Information Group 2. Health IT Certification, LLC
12. Rick Morrison	President	Medical Banking Rx
13. Ronald S. Moser, CISA	Consultant	EHNAC
14. James J. Moynihan, MBA, FHFMA, CTP, CHBME	Sr. Vice President	U.S. Bank Healthcare Payment Solutions Division
15. John Phelan, Ph.D.	Technology and Management Consultant	Milliman, Inc.
16. Marian Reed	1. Director of Product Security 2. Vice Chair, Marketing/Communication	1. McKesson Corporate 2. WEDI
17. Jessica Schopp	Vice President, Receivables Product Management	J.P. Morgan
18. James Schuping, CAE	EVP/CEO	WEDI

Appendix I – Important Definitions from HIPAA

1. [What is covered by HIPAA?](#)
2. [Who is covered directly by HIPAA?](#)
3. [Who is covered indirectly by HIPAA?](#)
4. [Use and Disclosure](#)
5. [What are the general requirements of the Security Rule?](#)
6. [What are the general requirements of the Privacy Rule?](#)

1. What is covered by HIPAA?

Protected Health Information (PHI)

PHI is individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

- (i) Transmitted by electronic media;
- (ii) Maintained in electronic media; or
- (iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

- (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
- (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
- (iii) Employment records held by a covered entity in its role as employer.

Individually Identifiable Health Information (IIHI)

IIHI is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and

- (i) That identifies the individual; or
- (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Health Information

Any information, whether oral or recorded in any form or medium, that:

- (1) Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

Healthcare

Care, services, or supplies related to the health of an individual. *Healthcare* includes, but is not limited to, the following:

- (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
- (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

2. Who is covered directly by HIPAA?

Covered Entity

- (1) A health plan.
- (2) A [healthcare clearinghouse](#).
- (3) A [healthcare provider](#) who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Health Plan

An individual or group plan that provides, or pays the cost of, [medical care](#), as defined in this section.

- (1) *Health plan* includes the following, singly or in combination:
 - (i) A [group health plan](#), as defined in this section.
 - (ii) A [health insurance issuer](#), as defined in this section.
 - (iii) An [HMO](#), as defined in this section.
 - (iv) Part A or Part B of the Medicare program under title XVIII of the Act.
 - (v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

- (vi) An issuer of a Medicare supplemental policy, as defined in this section.
- (vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
- (viii) 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.
- (ix) The healthcare program for active military personnel under title 10 of the United States Code.
- (x) The veterans' healthcare program under 38 U.S.C. chapter 17.
- (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4)).
- (xii) The Indian Health Service program under the Indian Healthcare Improvement Act, 25 U.S.C. 1601, et seq.
- (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
- (xiv) An approved State child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
- (xv) The Medicare + Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
- (xvi) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
- (xvii) Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of [medical care](#).

(2) *Health plan* excludes:

- (i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits (as listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1)):
 - (A) Coverage only for accident, or disability income insurance, or any combination thereof.
 - (B) Coverage issued as a supplement to liability insurance.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

- (C) Liability insurance, including general liability insurance and automobile liability insurance.
 - (D) Workers' compensation or similar insurance.
 - (E) Automobile medical payment insurance.
 - (F) Credit-only insurance.
 - (G) Coverage for on-site medical clinics.
 - (H) Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits; and
- (ii) A government-funded program (other than one listed in paragraph (1)(i)-(xvi) of this definition):
- (A) Whose principal purpose is other than providing, or paying the cost of, healthcare; or
 - (B) Whose principal activity is:
 - (1) The direct provision of healthcare to persons; or
 - (2) The making of grants to fund the direct provision of healthcare to persons.

Group Health Plan

An employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

- (1) Has 50 or more participants; or
- (2) Is administered by an entity other than the employer that established and maintains the plan.

Health Insurance Issuer

As defined in section 2791(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2), a Health Insurance Issuer means an insurance company, insurance service, or insurance organization (including a health maintenance organization) which is licensed to engage in the business of insurance in a State and which is subject to State law which regulates insurance (within the meaning of section 514(b)(2) of the Employee Retirement Income Security Act of 1974 [29 U.S.C. 1144(b)(2)]). Such term does not include a group health plan.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Health Maintenance Organization (HMO)

As defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3), an HMO is:

- (A) a Federally qualified health maintenance organization (as defined in section 300e(a) of this title),
- (B) an organization recognized under State law as a health maintenance organization, or
- (C) a similar organization regulated under State law for solvency in the same manner and to the same extent as such a health maintenance organization.

Medical Care

As defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2), Medical Care means amounts paid for:

- (A) the diagnosis, cure, mitigation, treatment, or prevention of disease, or amounts paid for the purpose of affecting any structure or function of the body,
- (B) amounts paid for transportation primarily for and essential to medical care referred to in subparagraph (A), and
- (C) amounts paid for insurance covering medical care referred to in subparagraphs (A) and (B).

Healthcare Clearinghouse

A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:

- (1) Processes or facilitates 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.
- (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Healthcare Provider

A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business.

3. Who is covered indirectly under HIPAA and directly under HITECH?

Business Associate

(1) Except as provided in paragraph (2) of this definition, *business associate* means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized healthcare arrangement (as defined in § 164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized healthcare arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized healthcare arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized healthcare arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized healthcare arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized healthcare arrangement.

(3) A covered entity may be a business associate of another covered entity.

4. Use and Disclosure

Use

Sharing, employment, application, utilization, examination, or analysis of individually identifiable health information within an entity that maintains such information.

Disclosure

The release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

5. What are the general requirements of the Security Rule?

§ 164.306 Security standards: General rules.

(a) General requirements. Covered entities must do the following:

- (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
- (4) Ensure compliance with this subpart by its workforce.

(b) Flexibility of approach.

- (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.
- (2) In deciding which security measures to use, a covered entity must take into account the following factors:
 - (i) The size, complexity, and capabilities of the covered entity.
 - (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
 - (iii) The costs of security measures.
 - (iv) The probability and criticality of potential risks to electronic protected health information.

6. What are the general requirements of the Privacy Rule?

§ 164.502 Uses and disclosures of protected health information: general rules.

(a) Standard.

A covered entity may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

(1) Permitted uses and disclosures.

A covered entity is permitted to use or disclose protected health information as follows:

- (i) To the individual;
- (ii) For treatment, payment, or healthcare operations, as permitted by and in compliance with § 164.506;
- (iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of § 164.502(b), § 164.514(d), and § 164.530(c) with respect to such otherwise permitted or required use or disclosure;
- (iv) Pursuant to and in compliance with an authorization that complies with § 164.508;
- (v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and
- (vi) As permitted by and in compliance with this section, § 164.512, or § 164.514(e), (f), or (g).

(2) Required disclosures.

A covered entity is required to disclose protected health information:

- (i) To an individual, when requested under, and as required by §§ 164.524 or 164.528; and
- (ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subpart.

Appendix II – Hybrid Entity: Definition and Conducting the Analysis

CFR 164.103 defines a hybrid entity as a single legal entity:

- (1) That is a covered entity;
- (2) Whose business activities include both covered and non-covered functions; and
- (3) That designates healthcare components in accordance with §164.105(a)(2)(iii)(C).

Section 164.105(a)(2)(iii)(C) describes the responsibilities of the covered entity:

The covered entity is responsible for designating the components that are part of one or more healthcare components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates a healthcare component or components, it must include any component that would meet the definitions of a covered entity if it were a separate legal entity.

Healthcare component(s) also may include a component only to the extent that it performs:

- (1) Covered functions; or
- (2) Activities that would make such a component a business associate of a component that performs covered functions if the two components were separate legal entities.

How to Conduct a Hybrid Entity Analysis

The best way to conduct a hybrid entity analysis is to map the flow of data and documents containing protected health information (PHI) throughout the organization.

Step 1

Identify where the organization initially receives PHI. Trace its flow through the business to the point where it leaves the organization and is made accessible or delivered to the healthcare customer (a covered entity). Document all functions which involve modification or storage of PHI for the covered entity.

Step 2

Identify all of the supporting services for the functions listed through Step 1. Examples may include general infrastructure such as IT support, facility operations, and human resources. These employees may have access to the PHI in a support role. For example, the IT help desk may look at data which includes PHI in the process of fixing a problem for staff. The facility operations team is responsible for the physical security of data. Human Resources may develop and maintain the HIPAA policies and procedures for employees covering data privacy and security expectations. It is important to also document the role each of the identified supporting functions has in access, manipulation, storage, or delivery of PHI both within and external to the organization.

Step 3

Ensure inclusion of all external service providers under outsourcing or subcontract arrangements that support the covered business functions. For example, a third-party vendor is contracted to provide a covered healthcare clearinghouse service, then this function must be included as a covered component under the hybrid entity.

Step 4: Documentation of the Hybrid Entity Analysis

Once the hybrid entity analysis is complete and the financial institution has identified its covered business component functions, then the findings and the rationale must be formally documented. As a recommended best practice, the governing body of the financial institution should approve the analysis as it is the Board of Directors who ultimately has the responsibility for compliance and service level performance to the customers. Another best practice recommendation is to establish a periodic review the hybrid entity analysis to make sure that it is current, as organizational restructuring and changes in business relationships could impact the hybrid entity analysis.

Appendix III – Financial Institutions

Banks hold either a national charter or a state charter, and are governed accordingly. Those with national charters are regulated by the Board of Governors of the Federal Reserve System (loosely called “the Fed”), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC). Thrift institutions – typically former savings banks and savings and loan associations – may be regulated by the Office of Thrift Supervision (OTS). Banks with state charters are governed by their individual states’ laws and regulations, which in many cases require the banks to be insured by the FDIC. Banks with state charters can also, but do not have to, join the Fed.

Credit unions, which are typically not-for-profit organizations, are governed by the National Credit Union Administration (NCUA), an independent federal agency that charters and supervises federal credit unions and that also administers the National Credit Union Share Insurance Fund (NCUSIF), which insures member accounts in all federal credit unions and the substantial majority of state-chartered credit unions. Credit unions that do not have federal charters are chartered by their state.

The major purpose of banks and credit unions is to accept deposits and lend the funds to borrowers.

Appendix IV – NACHA and the Automated Clearing House Network

The ACH Network is a widely used, trusted, and efficient batch processing, store-and-forward network for the direct, electronic movement of money and information between bank accounts, including Direct Deposit of payroll, government payments, and corporate trade payments. It carries more than \$30 trillion each year to and from the financial accounts of consumers, small businesses, corporations, and government.

Because electronic payments need to be accessible to all consumers, all businesses, all financial institutions, and all government entities, it is critical that both payments and related information are formatted and sent in a common manner. This is all enabled by adaptive operating rules that have incorporated various types of standards and regulations over time.

NACHA is the not-for-profit association responsible for the administration and enforcement of the operating rules for the ACH Network – the NACHA Operating Rules. These Rules support payment products and business practice standards in the areas of electronic bill payment, ecommerce, echecks, electronic data exchange, and international payments. NACHA represents and brings together over 10,700 member financial institutions of all sizes and types throughout the United States, both directly and through our 18 Regional Payments Associations, and more than 450 other companies and organizations through our industry councils and Affiliate Membership program. This structure allows NACHA to be inclusive of many different types of organizations. The U.S. Treasury has adopted NACHA Operating Rules for its electronic transactions.

These transactions are governed largely by:

- NACHA Operating Rules
- Regulation E
- Uniform Commercial Code (non-consumer transactions)

These are described briefly below.

NACHA Operating Rules

The *NACHA Operating Rules* provide the legal foundation for the ACH Network. The *Rules* cover definition, roles and responsibilities of the participants; types of transactions – both payment and informational - and the data and information that accompany the payments; authorization requirements; legal framework; warranties and liabilities; audit requirements; compliance and enforcement procedures; formats and file structures; data security requirements; schedules; and other topics that pertain to processing through the Network.

NACHA owns the *NACHA Operating Rules*.

Regulation E

Regulation E is the Federal Reserve regulation that governs consumer electronic transactions. While probably best known for its provisions that govern handling disputes between consumers and their banks, the regulation also covers requirements concerning information that must be conveyed to consumers for electronic transactions and as well as establishing requirements for consumer authorization of transactions.

Commonly called “Reg E,” this regulation is the result of the 1977 Electronic Fund Transfer Act. The regulation was first implemented in 1978 and has been updated several times, as has the official Staff Commentary, which interprets the law and regulation for specific situations. Regulation E’s most recent changes became effective in August 2010.

UNIFORM COMMERCIAL CODE (UCC)

UCC is the body of law governing commercial practices, including negotiable instruments and contracts, adopted in one form or another by all states. Electronic transactions not covered by Reg E are covered by provisions of the UCC, particularly Article 4A, which covers business-to-business credit transactions.

Appendix V - Technology Best Practices

Data Center Requirements and Recommendations

The listed attributes are recommended for a data center:

1. Hardened facility
2. 24-inch raised flooring (appropriate rack capacity and/or private cage space)
3. Appropriate Support Space for workers when needed
4. Network Operations Center (NOC)
5. Power Capacity of 150W Per Sq. Ft.
6. Biometric/Proximity Card-Key Access Control
7. Secure Man-trap
8. Digital Video Surveillance and Recording
9. Conference Rooms/Customer Staging Area/Loading Dock
10. Disaster Recovery Office Space
11. Environmental Monitoring and Control
12. Dual Interlock Dry-Pipe Fire Suppression
13. 99.999% Facility Up-Time

There are also five (5) key areas of redundancy: Power, HVAC systems, Security, Connectivity, and Networks.

1. Power

Dual Grid Power / Parallel Switching Gear / Wrap around ATS
UPS: 1.6 Megawatts N+1 APC
Diesel Generators - (2) Megawatt Cummins Each With 24 Hour
Day Tanks
10,000 Gallon Extended Life Fuel Tank
-48 Volt Power Plant for Telecommunications Providers

2. HVAC – these systems or comparable

Liebert CRAC Units - 560 Tons N+1
Liebert XD in-row cooling for high density areas (up to 30KW per rack)
Portable Units - 5 Tons x 4

3. Security

BioMetrics
Proximity Sensors/logging - All Entrances & Cabinets
Monitored Building Security
External cameras / Internal Cameras - 24x7 Digital Recording / DVR System

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

4. Connectivity

Multiple Gig-E connections from Tier 1 Backbone Providers
Self-Healing Fiber Ring Technology
Multiple Ingress/Egress
Virtually Unlimited Private Connectivity Options

5. Network

Multi-homed IP - Gig-E Connections
BGP4 Routing
VSS – Internal
High Availability Design - Multiple Routers and Switches - Private VLANs
Dual-path to all Equipment
Private VLAN Per Customer

SAS 70 Considerations

This section includes related management assertions to look for in the SAS 70 type II if you are hosted by someone else or assumptions you should have in your SAS 70 if you have an internal data center.

Physical Data Center Access and Environmental Controls

Each data center is a single purpose facility engineered to address security and network redundancy enabling the facility to offer high availability to its customers. The below description of the environmental and physical access procedures and controls are common to data centers.

Ideally, each data center maintains Customer Service personnel and Network Engineers onsite according to the following schedules:

(2.1) While facility personnel are not onsite, security at each data center is monitored by third party electronic surveillance and members of the Executive Team are notified in the event an alarm sounds.

(2.2) Exterior doors to the data centers are locked at all times and proximity keys and readers are utilized to restrict access.

(2.3) The Company maintains a lobby at each data center which is utilized to verify visitor access.

(2.4) The Company utilizes proximity access cards to limit access within each data center.

(2.5) Employees are provided with proximity cards which contain access tailored to their job requirements. Access privileges are approved by a member of the Executive Team either upon an employee's hiring or upon changing of their access privileges.

(2.6) A listing of personnel provided with these cards is periodically reviewed by a member of the Executive Team to ensure that the list includes only current employees and the access

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

privileges are correct based on current job assignments.

(2.7) The Company has procedures in place to grant temporary access to visitors of the data centers (primarily vendors and customers) after certain verification procedures have been performed. Visitors are required to check in at a computer visitor log station located in the lobby of each data center. Visitors are required to enter their information including name, purpose of visit, and submit their fingerprint prior to being granted access.

(2.8) Visitor information, fingerprint, and a photo, are recorded into the digital visitor log.

(2.9) If the individual is part of a customer's Access Control List (ACL), which contains a list of customer personnel granted access by the customer to their equipment and which was established during their data center implementation, they are granted access to the Network Operations Center (NOC) or an inner holding area before accessing their cage in the facility.

(2.10) Individuals not part of an ACL must be escorted or authorized via written communications from a Customer on the ACL.

(2.11) Changes to the ACL require formal documented approval from designated customer personnel.

(2.12) Customers are typically escorted to their cabinet which is then unlocked by data center personnel. Keys to customer cabinets are maintained in a lockbox in the NOC.

(2.13) Customers may be granted a temporary access card for access to and from the restrooms only. Vendors are escorted by Network Engineers or provided a temporary access badge for prolonged visits.

(2.14) Visitors are required to return their temporary access badges and log out at the computer visitor log station prior to leaving each data center. Upon checkout, facility personnel will then lock the customer's cabinet.

(2.15) Daily, Customer Service personnel at each data center verify that all visitor badges have been returned and if a badge was not returned, it is disabled and the visitor assigned to the badge is contacted.

(2.16) Each data center facility is monitored using a CCTV surveillance system with multiple color cameras which record full-motion video to DVRs and timestamp video clips each time a door in the facility is opened.

(2.17) System monitors both inside and outside of the facility and its images are digital and can be retained indefinitely. Each data center also maintains concrete and steel reinforced barriers which surround a fenced-in equipment yard outside of the facility.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

(2.18) The data centers each contain various environmental controls including multiple redundant Computer Room Air Conditioners (CRAC's) to maintain a constant temperature and humidity level in the data centers.

(2.19) Multiple High Sensitivity Smoke Detection (HSSD) sensors continuously sample the air throughout the facility at adjustable periods of time.

(2.20) Chemical fire extinguishers located prominently throughout the facility

(2.21) Dual Interlock, Dry Pipe, Pre-Action sprinkler system

(2.22) Temperature and humidity are continuously monitored via real-time monitoring software. If this software identifies any deviations with pre-established requirements, an alert is automatically e-mailed to several key personnel within the facility who work together to resolve any issues in a timely manner.

(2.23) Monitoring system log is also reviewed daily by Operations personnel to identify potential issues.

(2.24) Temperature, humidity, fire, and smoke detection and action systems are tested on a quarterly basis to help ensure that they are operating properly with the exception of the fire alarm, sprinkler system and fire extinguishers which are tested annually.

(2.25) Power systems at the data centers have been designed to run uninterrupted in the event of a power outage. Conditioned UPS (Uninterruptible Power Supply) units are utilized to supply power for short term power issues and these units are monitored real-time to help ensure that they are healthy and can be used in the event of an issue.

(2.26) In the event of an extended power outage, on-site diesel generators are in place at each data center to generate power for the facility until power is restored. These generators are tested weekly to help ensure that they will operate in the event of an emergency.

(2.27) The Company's network is constructed with routers and switches which leverage state-of-the-art silicon and software technologies (including redundant backplane and processor technology and a 100% network headroom policy) resulting in unparalleled service quality and continuous uptime. Redundant routing and switching equipment is used to eliminate single points of failure resulting in the ability to help ensure network uptime.

(2.28) State-of-the-art routers are also utilized for customer access to their equipment from outside of the data center.

(2.29) The Company has implemented the following monitoring procedures to ensure the integrity of its network:

- (2.30) the use of redundant SNMP monitoring servers which report errors, alerts, and status of chassis on a real-time basis.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

- (2.30a) in the event of a server failure, backups of configuration files are maintained and utilized.
- (2.30b) in the event of a network chassis failure, facility maintains an Out-Of-Band (OOB) emergency network which permits facility personnel to use backdoor access to each chassis for console configuration access. Pertinent OOB data is backed up and locally stored.
- (2.30c) the use of steady ICMP or ping packets for each chassis to monitor the responsiveness of facility equipment. If an ICMP packet is not returned by a chassis, an alert is generated which is addressed by a Network Engineer.
- (2.30d) The use of multiple telecommunication carriers whereby traffic is routed through multiple upstream networks to ensure customers are not affected by upstream bottlenecks or outages a single provider may experience.
- (2.30e) If the Company experiences a network interruption from an individual or multiple carriers, the interruption would be identified by internal systems and alerts which are automatically e-mailed to Customer Service personnel and Network Engineers.
- (2.30f) The Company's Network Engineers are responsible for pursuing, resolving and documenting network issues. If the issue occurs during non-business hours, the Company's Executive Team Member on call is responsible for resolving the outage. Customers are notified of outages by Customer Service personnel.

Redundancy and Business Continuity Policy Recommendations

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data. Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

Intrusion Detection or Prevention Options

Healthcare organizations are in the midst of a complete turnaround in regard to information security and privacy. Years ago a healthcare facility was viewed as an “open environment.” With hospital networks interconnected with Universities, clinics and other hospitals, the demand for security is implemented but not really enforced at times. With this “open environment” medical students could browse through medical records with ease. Hackers could get into the system and prevent authorized users from obtaining medical records. Today those security issues have changed. Healthcare facilities are becoming more secure and accountable for patient information and access to it.

The primary reason for healthcare facilities to insure security and privacy of patient information is because of the Health Insurance Portability Act (HIPAA) of 1996. Congress enacted this act with a focus on healthcare reform. HIPAA is aimed to improve the efficiency of healthcare data and processing through the standardization of administrative and financial data transactions, while protecting the privacy and integrity of patient information. The HIPAA regulation includes specific sections on privacy and security. The privacy standards require the protection of patient data from inappropriate and unauthorized disclosure or use. (3) The security standards require the safeguarding of patient data from unauthorized access. The securities fall into three categories: Administrative, Physical and Technical Safeguards.

Administrative safeguards administer actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information. Physical safeguards measures policies and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from unauthorized intrusion. Technical safeguards protect health information and control access to it.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Healthcare organizations are challenged to make information more available to physicians and patients. Patients want to access their medical data online. Physicians want immediate access to lab reports and diagnosis – at times remotely. More and more medical devices are also being connected to large healthcare networks, often with exposed commercial operating systems.

Today healthcare providers are using high tech security methods in compliance with the HIPAA Act. Providers are using biometrics, smart cards, RFIDs and other IPS hardware and software components. Most hospitals, government health agencies and other facilities are using intrusion prevention systems (IPS) to secure patient information. Intrusion prevention systems were invented independently by Jed Haile and Vern Paxson. IPSs are considered “the next level of security technology with its capability to provide security at all system levels, from the operating system kernel to network data packets.” (6) Along with an IDS, it provides policies and rules for network traffic and sends an alert when a hint of suspicious traffic has tried to enter. IPS makes an attempt to stop any potential attack.

The IPS is a better version of IDS and firewall protection at the application layer. IPS is similar to IDS because it has two types of intrusion prevention systems, host-based and network-based. Host-based intrusion prevention systems (HIPS) are used to protect both servers and workstations through software. HIPS catch suspicious activity on the system and then notify the system or block the attack from happening. It monitors application or data request, network connection attempts and read and write attempts. A network-based intrusion prevention system (NIPS) intercepts all network traffic and monitors it for suspicious activities and events. It usually scans for intrusion signatures, searches for protocol anomalies, detect commands not normally executed on the network and more.

If the system finds an offending packet of information, it can rewrite the packet so the hack attempt will fail. When this happens the organization can take this information and use it as future references when something like this happens again. They would know what to expect and how to handle the situation in a timely manner. The main disadvantage to intrusion prevention systems is the cost. The cost to install the software to each and every server and workstation within the organization may be very expensive. The HIPS on each system must also be updated frequently to that attack signatures are up-to-date. Some network request that may be legitimate may also be blocked which would cause the network performance to drop. To be effective an Intrusion Prevention system must also be a very good Intrusion Detection system to enable a low rate of false positives.

With all the security features out today and the HIPAA Act in place, many healthcare entities feel that they need to improve their security of information by installing an IPS. According to Bonnie Norman, system security engineer for Wellstar Health System, “The main reason they wanted to use some form of IPS is because of what they learned in the SANS Hacker Tools and Incident Handling Class. It showed us the tools the hackers are using and how they get around the standard defenses that we and other organizations were using.”

Without some form of security hackers can get into the system and obtain patient information. If a worm, virus, or denial-of-service attack occurs, doctors are unable to access electronic patient records or digital images which can compromise patient care. It could also hinder

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

administration from filing insurance claims. Universities that are connected with medical centers are more vulnerable to malicious activities. Thanks to technology available today, medical centers can protect their information from getting into the wrong hands of student users and other potential hackers.

When Hurricane Katrina hit the Gulf Coast, government health agencies would be handing a nearly unprecedented volume of new, temporary networks, systems and shelters. Those networks would serve as a major communications link between hurricane survivors and their families and friends, as well as between the numerous shelters and the main office. Ensuring the confidentiality and availability of the information traveling through these networks would prompt healthcare organizations to implement IPSs in their network. Without the use of high-tech security methods patient's information is left out for everyone to view and take advantage of. It's a problem now with victims trying to regain their identity and trying to get things back to normal. The last thing they want to worry about is someone obtaining their medical information and maybe altering it.

This could affect the patient in many ways. Someone could tamper with their medical records and put things that may not be true which could affect the patient in the long run. They could be prescribed a medication that they may be allergic to, but the record doesn't say anything about this. I think that it's a very important issue to all people, but especially to Katrina victims. The question would be, "Will health organizations in the Gulf Coast be fined if medical records were disclosed to the public?" Would this be a special circumstance and if something tragic like this happened again would the government continue to let things "slide" because of what happened? People's information is still being let out in the open regardless of the situation. If the American Red Cross can implement IPSes, there is no reason for other healthcare entities to not place IPSes in their network.

In conclusion, personal information is just that, personal. No one wants their medical records to be published or tampered with. It's up to the healthcare industry to make sure this doesn't happen. Individuals trust this industry to keep all confidential information inside their environment and would hope that one can obtain such information. It's up to the healthcare organizations to make sure no one tampers with their network.

Patient confidentiality is just as important as social security numbers and any other personal information and should never have a chance to be released. Healthcare organizations should go above and beyond the call to make sure they have the latest technology and security features such as Intrusion Detection or Intrusion Prevention Systems in their networks. Hackers are always finding new ways to get around certain networks.

References

- *1. Securing Critical Data and IT Infrastructure in Healthcare Environments Article www.tippingpoint.com
2. Briggs, Bill 2004, 'Two technologies Let Hospitals Pass on Words', *Health Data Management*, September
- *3. "NC DHHS HIPAA – What Is HIPAA?", North Carolina Department of Health and Human Services, <http://hipaa.dhhs.state.nc.us/hipaa2002/whatishipaa/whatishipaa.html>

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

- *4. McGee, Marianne Kolbasuk, "Intrusion Prevention Trumps Detection In Health Care", InformationWeek, September 2004
- 5. Martin, Zach, "Username and Passwords Still Reign in Health Care," IDNewswire, Vol. 4 No. 2 January 28, 2005
- 6. www.webopedia.com
- *7. Wellstar Health System, "What Works in HIPAA Compliance Using Intrusion Prevention" January, 2005

Secure Architecture of Applications, Especially Web-Based Applications

All customer data should be stored on secure servers in one or two data centers that are SAS-70 compliant and ideally have earned EHNAC accreditation. The systems architecture is ideally designed for at least a three-tier solution. Each segment is isolated by a firewall and utilizes a specific protocol when communicating with the other tiers. The methods of communication are TCP/IP, HTTPS, and TCP Sockets.

- Tier 1 - Web services layer
- Tier 2 - Business Logic layer
- Tier 3 - Database layer
- The application requires a user token that must be validated on each call made to the system. The user token consists of the user id, user connection id and an SDK key that were granted upon successful login. The login request is done from a dedicated secure website using a unique user name and password. The password is encrypted using a SHA1 or similar encryption.
- Internet/Tier 1 – Users are connected to the application via HTTPS connection. The data is encrypted with 128 bit SSL for HTTP communication and SHA512 or similar for passwords.
- Tier1/Tier 2 – The external web servers connect to the application servers via TCP sockets or similar direct connection using and specific IP routing through the firewall. The data is encrypted with SHA512 for SDK or similar encryption.
- Tier2/Tier3 – The application servers communicate with the database and image servers through TCP sockets or similar direct routing and specific IP routing through the firewall.
- Customer data is stored on a secure SQL server, encrypted content database, or secure storage device. Data can only be accessed through the client application using secure web services or directly from the server by an IT administrator through the administration software

Secure File Transfer of Files Containing PHI: Overview of File Transfer Protocol

The preferred method of transferring file between businesses or remote sites is to use sftp protocol. This allows encrypted file transfer without the need for VPN or other encryption methods. However where protocol is noted as sftp or secure ftp the same methods can be used for business-to-business VPN and standard ftp protocols. Likewise, the “pushing” of files can be replaced by “pulling” of files. Please note however, these changes increase the complexity of the file transfer structure.

Password Protection – Encryption

This is an example acceptable Encryption Policy.

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all ban employees and affiliates.

3.0 Policy

Proven, standard algorithms such as 3DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. The bank's key length requirements should be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the bank. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

6.0 Revision History

Be sure to document any modifications and effective dates in the policy's Revision History.

Authentication

Login

As mentioned previously, applications should be architected requiring a user token that must be validated on each call made to the system. The user token consists of the user id, user connection id and an SDK key that were granted upon successful login. The login request is done from a dedicated secure website using a unique user name and password. The password is encrypted using a SHA512 or similar encryption.

Minimum Password Requirements

- The ID is user assigned by domain.
- Minimum password length is 7 characters
- Password must contain at least one the following characters. (Alpha upper case, Alpha lower case, Numeric, and Symbol)
- The Password cannot contain spaces.
- Password Expiration
- The Password expiration is set by domain and will require the user with an expired password to change his password before the user will be allowed access to the application.
- A Password history is set by domain and has a minimum of 3. COMPANY will maintain a history passwords set by a user and disallow any new password that matches one previously used.
- Passwords are encrypted in a hash at all times

Password login violation logging

Successful and unsuccessful user logins are logged to the audit database. Upon 6 unsuccessful login attempts with a login id, the user account is locked and cannot be reset by the user. The user must contact Bank's Help Desk department or have their site administrator reset their password to unlock their account.

Audit and Control Systems

Financial institutions need systems that can determine who touched what data and when.

HIPAA Covered System and Application Logging Policy

1.0 Purpose

HIPAA covered components at COMPANY are required to be in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

This policy will ensure that systems processing and storing electronic Protected Health Information (PHI) are identified, monitored, and reviewed for compliance with existing

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

COMPANY policy, procedures, and federal HIPAA regulations related to system activity controls. It will also discourage, prevent, and detect security violations.

2.0 Scope

This policy covers all computer systems in the HIPAA covered components at COMPANY that create, access, transmit, or receive electronic PHI used for treatment, payment, or healthcare operations or any form of electronic PHI where the host system is configured to allow access by multiple people.

Examples include:

- a server with file shares containing electronic PHI,
- a system which contains primary source electronic PHI, and
- other systems designated as covered by the COMPANY HIPAA privacy officer.

Check with your HIPAA liaison or the HIPAA privacy officer if you are not sure your system is covered by this policy.

3.0 Policy

3.1 General

This policy identifies requirements for reviewing activities on computer systems containing electronic PHI at COMPANY.

To the maximum extent possible, logs from systems and applications containing PHI must capture information and events as described in the following table:

Risks or Control Objectives	Requirement
General controls	<ul style="list-style-type: none">• Record who did what to which object, when, and on which system.• Record what events each system is capable of logging.
General events to capture	<ul style="list-style-type: none">• Machine startup and shutdown; startup and shutdown of audit function.• Successful/unsuccessful login and logout of users; denial of service events.• Add, modify, and delete actions on all data/files/objects; plus read/view actions on data classified as restricted.• Use of all privileged accounts and utilities.• Changes to user accounts or privileges (creation, modification, deletion).

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Risks or Control Objectives	Requirement
	<ul style="list-style-type: none"> • Automatic logout of a user after exceeding a locally defined time of inactivity or excessive login attempts. • Switching to another user's access or privileges after logging in. • Software or hardware modification. • All access to security files, attributes, or parameters; any action to circumvent security controls including access to anti-virus software.
Operation events to capture	<ul style="list-style-type: none"> • Login attempts with failed identification or authentication, also known as failed login attempts. • Changes of the time or date of the system clock. • Emergency mode operation. • Detection of a virus. • Detectable hardware and software errors; log failure and restart events. • Changes to log files (creation, deletion, and configuration).
Communication events to capture	<ul style="list-style-type: none"> • Network link failures. • Device connection failure due to device identification or authentication failure (also known as a failed connection attempt). • Network and device connections dropped. • Data integrity verification failure for information transmitted over a network. • Message authentication failure for information transmitted over a network. • Overrides of network abnormality ala Company and alerts. • IP addresses of successful and unsuccessful connections. • Changes to network security configuration (e.g. firewalls).
Content of audit trails	<ul style="list-style-type: none"> • Date, time, type, and any applicable error condition of event. • The ID of the user who caused the event. • The application that created the audit event. • The application(s) responsible for executing the event. • The component or workstation that initiated the event, and where the event happened. • Description of the event, which may include before and after images.
Monitoring	<ul style="list-style-type: none"> • Follow-up on suspicious events such as intrusion attempts, authorized accesses at unusual times, and unusual changes to infrastructure devices.

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

Risks or Control Objectives	Requirement
	<ul style="list-style-type: none"> • Identify, investigate, report, and respond to inappropriate activity. • Ensure that audit requirements and activities do not unduly disrupt critical business processes. • Identify the individuals performing event analyses. Each shall be independent from those setting audit trail rules. Ensure they are available and that they record who, what, when, where, and why sensitive information is released. Rules-of-evidence integrity must be maintained. • Document all event capturing and analysis procedures, requirements, and responsibilities, including when to involve inforensics specialists. • Develop a process to ensure that users comply with access control procedures, including strong password creation and protections. • Audit all user activity where risk levels warrant. • Employ event analysis support tools and/or e-intelligent methods of correlating log data to detect suspicious activity and reduce volume.
<p>Maintenance and storage of audit trails</p>	<ul style="list-style-type: none"> • Audit trails must be managed only by authorized staff. • Audit trail retention will vary depending upon legal requirements and business need. PHI and audit trails must be archived for six years. Other federal laws and regulations may stipulate other retention periods; always use the most stringent guideline when the data is covered by more than one policy, law, or regulation. • Audit trail records management retention and disposal rules must be documented.

3.2 Activity Review

The activity review process shall include an audit of system activity logs and reports at a level commensurate with a particular system's profiled data criticality category. This process may include a review of the following types of system activity information:

- Review of Security Incident Response reports
- System user privileges system grants and changes logs
- User-level system access logs, if available
- User-level system activity logs, if available
- User-level transaction log reports, if available
- Exception reports

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

- The required level of system activity logging and reporting capabilities, and the actual scope of the activity review for each risk profile should differ based upon a system's assigned data criticality level.

IT Security and Privacy and/or Internal Audit will carry out a full review or spot checks of user-level access, activity, and transaction and exception logs.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
-------------	-------------------

6.0 Revision History

Be sure to document any modifications and effective dates in the policy's Revision History.

Appendix VI - Glossary of Acronyms and Terms

Acronyms

Acronym	Phrase or Organization
ACH	Automated Clearing House
ARRA	American Recovery and Reinvestment Act
BA	Business Associate
BAA	Business Associate Agreement
CE	Covered Entity
EFT	Electronic Funds Transfer
EHNAC	Electronic Healthcare Network Accreditation Commission
EOB	Explanation of Benefits
EOP	Explanation of Payment
ERA	Electronic Remittance Advice
FACTA	Fair and Accurate Credit Transactions Act of 2003
HE	Hybrid Entity
HIMSS	Health Information and Management Systems Society
HIMSS MBProject	HIMSS Medical Banking Project
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IIHI	Individually Identifiable Health Information
PHI	Protected Health Information
WEDI	Workgroup for Electronic Data Interchange

Terms

835 (X12 835)

The X12 Healthcare Claim Payment & Remittance Advice transaction. Version 4010 of this transaction has been included in the HIPAA mandates. (<http://www.cms.hhs.gov/HIPAAGenInfo>)

837 (X12 837)

The X12 Healthcare Claim or Encounter transaction. This transaction can be used for institutional, professional, dental, or drug claims. Version 4010 of this transaction has been included in the HIPAA mandates. (<http://www.cms.hhs.gov/HIPAAGenInfo>)

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

837D

X12 837 for Dental Entities

837I

X12 837 for Institutional Entities

837P

X12 837 for Professional Entities

ACH

An ACH is an acronym that stands for Automated Clearing House. In the banking environment, this term is used in a number of ways:

- Refers to electronic transactions/payments routed through the national ACH network.
- Refers to the entire ACH network itself (“the ACH”).
- Refers to specific services a given financial institution provides .
- Is not the same as a healthcare clearing house.

Business Associate Agreement

Contract that specifies the obligations of a business associate to a covered entity (Payer, Provider or clearing house), usually specifically covering obligations related to the protection of private health information the business associate may encounter while performing functions or activities on behalf of a covered entity.

ARRA (American Recovery and Reinvestment Act)

Commonly referred to as **the Stimulus** or **The Recovery Act**, ARRA is an economic stimulus package enacted by the 111th US Congress in February 2009. The Act followed other economic recovery legislation passed in the final year of the Bush presidency including the Economic Stimulus Act of 2008 and the Emergency Economic Stabilization Act of 2008 which created the Troubled Assets Relief Program (TARP).

Claim

The document used by providers to invoice payers for services provided to a patient.

EDI (Electronic Data Interchange)

The exchange of routine business transactions from one computer to another in a standard format, using standard communications protocols. (<http://www.cms.hhs.gov/HIPAAGenInfo>)

EFT (Electronic Funds Transfer)

Defined in the Federal Regulation E as “any transfer of funds that is initiated through an electronic terminal, telephone, computer or magnetic tape for the purpose of ordering, instructing or authorizing a financial institution to debit or credit a consumer’s account.” For

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

practical purposes, this definition is used to cover all ACH transactions, whether or not the underlying account is a consumer, business, commercial or government account. In the financial services environment, the term “EFT” is increasingly replaced by the more generic phrase “electronic banking.”

EHNAC (Electronic Health Network Accreditation Commission)

EHNAC is a federally recognized standards development organization, a non-profit accrediting body designed to improve transactional quality, operational efficiency and data security in healthcare.

EOB (Explanation of Benefits)

Explanation to patient of what has been paid, adjusted or denied. Also an explanation to the provider, more commonly known as an EOP (Explanation Of Payment).

EOP (Explanation of Payment)

Explains to the provider how monies have been allocated per patient.

ERA (Electronic Remittance Advice)

ANSI X12 835 remittance format standard. Other electronic formats are used to capture remittance data but NONE are sanctioned by HIPAA. (<http://www.cms.hhs.gov/HIPAAGenInfo>)

FACTA (Fair and Accurate Credit Transactions Act of 2003)

FACTA is a United States federal law, passed by the United States Congress on November 22, 2003, and signed by President George W. Bush on December 4, 2003, as an amendment to the Fair Credit Reporting Act. The act allows consumers to request and obtain a free credit report once every twelve months from each of the three nationwide consumer credit reporting companies (Equifax, Experian and TransUnion). In cooperation with the Federal Trade Commission, the three major credit reporting agencies set up the annualcreditreport.com website to provide free access to annual credit reports.

The act also contains provisions to help reduce identity theft, such as the ability for individuals to place alerts on their credit histories if identity theft is suspected, or if deploying overseas in the military, thereby making fraudulent applications for credit more difficult. Further, it requires secure disposal of consumer information.

HIMSS (Health Information Management Systems Society)

The Healthcare Information and Management Systems Society (HIMSS) is a comprehensive healthcare-stakeholder membership organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare.

HIMSS Medical Banking Project

The HIMSS Medical Banking Project (HIMSS MBProject) is a civil society organization that helps financial institutions and health care organizations to form dynamic, efficient and sustainable

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

partnerships that improve global health using "medical banking" principles. HIMSS MBProject fosters the advancement of an efficient, consumer-centric and global healthcare financial network using an industry leading and neutral educational platform.

HIPAA

Enacted by the US Congress in 1996, HIPAA was originally sponsored by Sen. Edward Kennedy (D-Mass.) and Sen. Nancy Kassenbaum (R-Kan.). According to the Centers of Medicare and Medicaid Services (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

HITECH (Health Information Technology for Economic and Clinical Health Act)

On February 17, 2009 a \$787 Billion, the American Recovery and Reinvestment Act of 2009 aka "the Stimulus Bill," was signed into law by the federal government. Included in this law is \$19.2 Billion which is intended to be used to increase the use of Electronic Health Records (EHR) by physicians and hospitals; this portion of the bill is called, the Health Information Technology for Economic and Clinical Health Act, or HITECH Act. The government firmly believes in the benefits of using electronic health records and is ready to invest federal resources to proliferate its use.

NACHA -The Electronic Payments Association

The not-for-profit national association that governs and administers the ACH Network, creates and enforces ACH Network rules, protects and supports the ACH Network, and provides educational services. NACHA works closely with all types of ACH participants. NACHA does not operate the ACH Network.

Red Flag Rules

The Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Transactions Act of 2003 (also called the Identity Theft Red Flag Rules) is designed to hold businesses more accountable in their management of consumer information through guidelines and legislation that address technology and procedural issues affecting how that information is handled.

WEDI (Workgroup for Electronic Data Interchange)

WEDI was established to provide multi-stakeholder leadership and guidance to the healthcare industry on how to use and leverage the industry's collective technology, knowledge, expertise

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

and information resources to improve the administrative efficiency, quality and cost effectiveness of healthcare information.

Appendix VII - References

1. Cash, J. I. And Benn R. Konsynski, "IS Redraws Competitive Boundaries," Harvard Business Review, March-April 1985, pp.134-142.
2. HITECH Act: <http://www.boisestate.edu/research/recovery/HITECHlegislation.pdf>
3. HIPAA: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf>
4. Department of Health and Human Services. "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act; Proposed Rule." July 14, 2010.
<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/nprmhitech.pdf>
5. Healthcare Payments Glossary:
<https://admin.nacha.org/userfiles/File/Healthcare%20Resource/Healthcare%20Glossary%2004%2009%2010.pdf>
6. Healthcare Resources for Financial Institution:
<http://www.nacha.org/c/HealthcarePaymentsResources.cfm>
7. HIMSS Medical Banking Project: <http://www.mbproject.org/mbtoolkit.php>
8. NACHA – The Electronic Payments Association:
<http://www.nacha.org/c/HealthcarePaymentsResources.cfm>
9. The Office for Civil Rights (OCR) is responsible for issuing periodic guidance on the provisions in the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) On May 7, 2010 they published a document entitled "HIPAA Security Standards: Guidance on Risk Analysis", which can be found at:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf>

Appendix VIII 2004 NCVHS letter to HHS

June 17, 2004

The Honorable Tommy G. Thompson

Secretary

U.S. Department of Health and Human Services

200 Independence Avenue, S.W.

Washington, D.C. 20201

Dear Secretary Thompson:

As part of its responsibilities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the National Committee on Vital and Health Statistics (NCVHS) monitors the implementation of the Administrative Simplification provisions of HIPAA, including the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule).

The NCVHS Subcommittee on Privacy and Confidentiality held hearings in Washington, DC on February 18-19, 2004. The hearings, the second of several to be held on HIPAA implementation, were intended to gather information about the effect of the Privacy Rule in three areas: banking, law enforcement, and schools. Additional hearings will address other aspects of HIPAA implementation. This letter conveys the Committee's findings and recommendations for action by the Department regarding banking. Separate letters contain findings and recommendations regarding law enforcement, and schools.

Representatives from a broad range of backgrounds testified about the effect of the Privacy Rule on banking, including representatives with extensive technical knowledge of health care information and bank processing, health care clearinghouses, electronic privacy issues, and confidentiality provisions contained in federal laws applicable to financial institutions.

HIPAA provides that its standards shall not apply to financial institutions engaged in banking functions, including functions that might involve use or disclosure of information about patients (see Social Security Act, Section 1179, 42 U.S.C. 1320d-8). Although the vast majority of health care information processing activities performed by financial institutions fall under this exception, there are circumstances under which financial

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

institutions perform services not covered by the exception. For example, a small number of banks are clearinghouses as a result of services provided in addition to processing payments in their financial institution capacity, and are thus covered entities under HIPAA.

A critical issue is whether other privacy laws adequately protect health information held by financial institutions exempt from HIPAA under Section 1179. A witness from Georgetown University's Health Policy Institute testified that other laws do not adequately protect personal health information held by financial institutions. Neither the Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act), nor the recent amendments to the Fair Credit Reporting Act made by the Fair and Accurate Credit Transactions Act (FACT Act) provide protection. The Gramm-Leach-Bliley Act was intended to facilitate the integration of banks and other financial institutions, which involves sharing consumer information. Generally, the FACT Act prohibits a bank and other creditors from obtaining and using health information for consumer-credit decision purposes. Regulations for the FACT Act are under development.

A witness from the American Bankers Association (ABA) testified that financial institutions are very diligent about protecting consumers' personal financial and medical information. The ABA and the National Automated Clearinghouse Association (NACHA) developed educational materials to help financial institutions prepare for the implementation of the HIPAA Privacy Rule. The ABA has recommended to financial institutions that they participate in and execute business associate agreements when they are engaged in health care processing. The Medical Banking Project (Project) testified that a number of financial institutions have inquired about HIPAA business associate agreements and thus it is the sense of the Project that financial institutions are executing and signing the agreements when asked to do so.

A witness from the Electronic Privacy Information Center (EPIC) expressed several concerns about financial institutions and the privacy of personal health information. EPIC does not support the Section 1179 exception for financial institutions that handle protected health information (PHI) contained in premium payment and remittance advice transactions. EPIC believes such entities should have covered entity status as health care clearinghouses under the Privacy Rule. EPIC does not believe that business associate agreements provide the same level of protection for health information as covered entity status. Also, the EPIC witness discussed the problems associated with transmitting PHI through the banking system's automated clearing house (ACH) network. EPIC suggested that when PHI moves through the ACH, it be encrypted so that it is accessible only by the final recipient. Encryption also would help provide protection in the event of network security breaches as well as prevent potential data mining for marketing purposes.

NCVHS notes that the banking industry is evolving and diversifying its services for the processing of personal health information. For example, financial institutions have begun

Compliance Guidelines for Financial Institutions in the Healthcare Sector: HITECH and the HIPAA Privacy and Security Rules

to acquire health care clearinghouses, and they provide value-added services that potentially involve personal health information. Financial institutions face new privacy challenges and responsibilities in today's environment and with that in mind, the NCVHS recommends the following:

HHS should clarify the nature of the Section 1179 exception for financial institutions when engaged in processing health care transactions. Specifically, clarification is needed from HHS about whether the exception applies to consumer-initiated transactions (e.g., credit card or check payments), covered entity-initiated payment transactions, or both.

Until HHS clarifies the Section 1179 exception, HHS should recommend to health care providers and payers that they use business associate agreements with financial institutions.

Regardless of the technical status of financial institutions under the law and the regulation, HHS should consider whether encryption should be required for PHI moving through the ACH, to ensure that it is available only to final recipients.

We appreciate the opportunity to offer these comments and recommendations.

Sincerely,

/s/

John R. Lumpkin, M.D., M.P.H.

Chairman, National Committee on Vital and Health Statistics

Cc: HHS Data Council Co-Chairs