

IMPROVING QUALITY, SAFETY AND EFFICIENCY OF HEALTHCARE: SECURITY BEST PRACTICES FOR HEALTH INFORMATION EXCHANGE

White Paper

Abstract:

Health Information Exchange (HIE) is the mobilization of healthcare information electronically across organizations within a region or community. Healthcare delivery networks are now faced with the challenge of deploying HIE solutions in community and enterprise environments. These care delivery networks need to achieve interoperability across the landscape of diverse stakeholders while meeting the needs of the patient by ensuring clinical and financial data is transmitted privately and securely. This paper discusses the challenges and regulatory requirements healthcare delivery networks are facing and highlights the security best practices recommended to achieve high quality, safe and efficient healthcare services while maintaining the privacy, security and confidentiality of personal health information (PHI).

Authored By:



TABLE OF CONTENTS

1	EXECUTIVE OVERVIEW	1
2	THE HEALTH INFORMATION EXCHANGE (HIE) LANDSCAPE	2
3	REGULATIONS AND COMPLIANCE DRIVING SECURITY	3
3.1	DATA BREACH DISCLOSURE LAWS	3
3.2	INFLUENTIAL REGULATIONS; NOT SPECIFICALLY HEALTHCARE RELATED.....	3
3.3	PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS).....	4
3.4	COMMON SECURITY COMPLIANCE THREADS.....	4
3.5	CONSEQUENCES OF NON-COMPLIANCE.....	4
4	INTEGRITY, SECURITY AND CONFIDENTIALITY OF HIE	5
4.1	STEPS TO PROTECT PERSONAL HEALTH INFORMATION (PHI)	5
4.1.1	<i>Inventory PHI</i>	5
4.1.2	<i>Risk Assessment and Management</i>	5
4.1.3	<i>Implement Security Measures</i>	6
4.2	CONFIDENTIALITY & PRIVACY PROTECTION.....	6
4.2.1	<i>Protected Health Information According to HIPAA Privacy Rule</i>	6
4.2.2	<i>Access Controls</i>	7
4.3	ENCRYPTION FOR DATA PROTECTION.....	8
4.3.1	<i>The Basics of Encryption Technology</i>	8
4.3.2	<i>Public Key Infrastructure (PKI) for Encryption Key Management</i>	9
4.3.3	<i>Encryption of Data ‘At Rest’</i>	9
4.3.4	<i>Encryption of Data ‘In Transit’</i>	10
4.3.5	<i>Virtual Private Networks (VPNs)</i>	11
4.3.6	<i>Minimum Requirements for Encryption of PHI</i>	11
4.4	INTRUSION DETECTION AND PREVENTION SYSTEMS (IDS/IPS).....	13
4.5	INTEGRITY PROTECTION	14
4.5.1	<i>Endpoint Protection</i>	14
4.6	ACCOUNTABILITY, AUDIT, & OVERSIGHT	15
4.6.1	<i>Security Information and Event Management (SIEM)</i>	15
4.6.2	<i>Data Leak Prevention</i>	15
4.7	AVAILABILITY CONTROLS	17
4.7.1	<i>Security Contingency Plan</i>	17
5	CONCLUSION	18
6	ABOUT THE AUTHORS	19
6.1	CONCORDANT	19
6.2	THIRD BRIGADE.....	19
6.3	TREND MICRO.....	19



1 Executive Overview

"Harvard Medical School networks are attacked every few seconds 24 hours a day, 7 days a week. These attacks come from such diverse locations as Eastern Europe and Eastern Cambridge (MIT students). In general, protecting the privacy of 3 million patient records is a Cold War. Hackers innovate, Information Technology departments protect, Hackers innovate and the process continues. Providing security is a journey and we have been on the path to security best practices for many years." **John Halamka, CIO, Harvard Medical School**¹

The adoption of health IT has been slow due to a number of well-documented factors including concerns about privacy and confidentiality of electronic personal information. With the passing of the Health Information Portability and Accountability Act (HIPAA) in 1996, regulatory compliance has been a driving factor behind security and privacy controls for the healthcare industry.

This paper is intended to assist the following groups in determining how they can best apply security best practices while developing HIE strategies and implementations:

- Healthcare Providers – doctors, hospitals, community practices...
- Healthcare Payers – billing services and health management systems
- Health Plans – insurance providers, third-party administrators (TPAs), health medical organizations...
- Healthcare Practice Management Vendors and Service Providers – practice management software (PMS), stand-alone claims submission engines, and attachment submission engines

The paper discusses the challenges and regulatory requirements healthcare delivery networks are facing and highlights the security best practices recommended to achieve high quality, safe and efficient healthcare services while maintaining the privacy, security and confidentiality of personal health information (PHI).

"HIPAA has far-reaching implications for information protection in many organizations. Not only do care providers need to pay close attention, but also enterprises that handle employee or client health information. Computer system security will be a key element of the compliance program. But other forms of information handling—even discussions over the telephone—will also require scrutiny."

Trent Henry, Vice President and Research Director,
Security and Risk Management Strategies, Burton Group

¹<http://geekdoctor.blogspot.com/2007/10/top-10-things-cio-can-do-to-enhance.html>

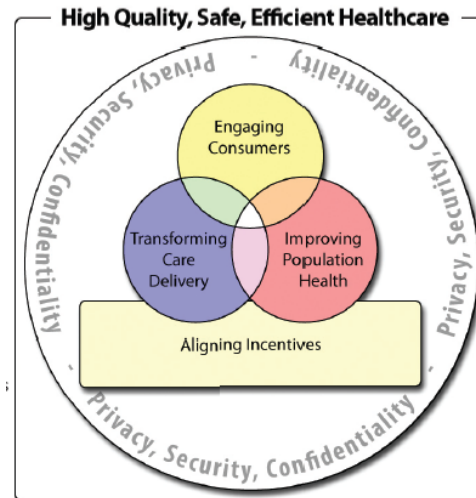
2 The Health Information Exchange (HIE) Landscape

The [eHealth Initiative](#) (eHI) defines Health Information Exchange (HIE) as the mobilization of healthcare information electronically across organizations within a region or community. The ability to provide interoperable health information technologies within a fragmented care delivery system, allows for the mobilization of pertinent clinical data — providing safe, timely, efficient, effective and equitable patient-centered care.

Healthcare delivery networks are now faced with the challenge of deploying HIE solutions in community and enterprise environments. These care delivery networks require a solution that provides interoperability across the landscape of diverse stakeholders while meeting the needs of the patient by ensuring clinical and financial data is transmitted privately and securely.

Developed with the input of nearly 200 organizations, the eHI Blueprint² outlines the vision, strategies and actions for utilizing health information technology (HIT) and health information exchange for improving health and healthcare. This is in line with the eHI's focus to improve quality, safety and efficiency of the healthcare system. The eHI Blueprint has five key focus areas:

1. Engaging Consumers
2. Transforming care delivery
3. Improving population health
4. Aligning financial and other incentives
5. Managing privacy, security, and confidentiality



The focus area 'Managing Privacy, Security and Confidentiality' is a critical success factor to the utilization of HIT and HIE to transform healthcare. If consumers are not confident that these areas are properly addressed, then the impact and adoption of the enabling technologies will be significantly reduced. In many ways privacy, security and confidentiality are driven by regulatory requirements, but this is only the starting point. The application of best practices, to manage the associated risks to the patient information that is exchanged over new and ever-changing technologies is critical to meeting the goals of transforming healthcare through technology.

What are the technologies required to meet the goals of an HIE? **Electronic Health Records** (EHR) are one key element. In order to exchange data you need a mechanism to collect it in the first place — widespread implementation and adoption efforts are under way to accomplish this crucial first step to data exchange. **Record locator services** are the next key element. The authors believe these services should provide a mechanism to locate the required data, but not store the data, or any personally identifiable information, centrally. Many other critical elements are required or may feed these systems including connectivity to external data sources like lab providers, external provider partners, and healthcare payer organizations. Each source needs to manage and maintain the privacy, security, and confidentiality of the data as it is stored, sent or received. The only way to accomplish this is through applying a best practices model.

²<http://www.ehealthinitiative.org/blueprint/eHiBlueprint-BuildingConsensusForCommonAction.pdf>

3 Regulations and Compliance Driving Security

With the passing of the Health Information Portability and Accountability Act (HIPAA) in 1996³, regulatory compliance has been the driving factor behind security and privacy controls for the healthcare industry. On a federal level the HIPAA privacy rule (finalized in 2002) and the security rule (finalized in 2003) provide guidance and standards that health care entities are required to meet in order to protect Personal Health Information (PHI).

In addition to federal laws like HIPAA, state and local governments have also adopted laws specific to protecting the privacy and security of patient records. Laws vary from state to state but are cumulative in relation to HIPAA and continue to apply. In order to try and reach common ground on the state level, in 2006 the National Governors Association (NGA)⁴ formed the State Alliance for e-Health, an initiative designed to improve the nation's health care system through the formation of a collaborative body that enables states to increase the efficiency and effectiveness of the health information technology (HIT) initiatives they develop. The State Alliance for e-Health was developed under a cooperative agreement with the U.S. Department of Health and Human Services' Office of the National Coordinator (ONC) for Health Information Technology. It provides a forum through which state governors, elected state officials and other policymakers can work together to identify inter- and intrastate-based HIT policies and best practices. They also will explore solutions to programmatic and legal issues related to the exchange of health information.

In addition, under a federal grant from the U.S. Agency for Healthcare Research and Quality (AHRQ) and the U.S. Office of the National Coordinator for Health IT, a collaboration of 33 states and 1 territory created the Health Information Security and Privacy Collaboration (HISPC). These 34 subcontractors assessed the variations that exist across states with respect to privacy and security practices and policies. The goals of HISPC were to identify best practices and challenges, develop consensus-based solutions for interoperable electronic health information exchange (HIE) that protect the privacy and security of health information, and develop detailed implementation plans to implement solutions.⁵

3.1 Data Breach Disclosure Laws

In 2003, California enacted the first in the nation, seminal data breach disclosure law (⁶SB 1386) which requires companies to notify consumers whose personal information has been violated. Since then more than 40 states have enacted similar legislation. In 2007, the California legislature added medical information and health insurance information (⁷AB1298) to the definition of personal information. So far Delaware and Arkansas are among the few to also include medical information but it would seem to be just a matter of time before the rest of the states follow suit.

3.2 Influential Regulations; Not Specifically Healthcare Related

Federal and state regulatory and compliance requirements are not limited to the Healthcare industry. Federal laws such as the Gramm-Leach-Bliley Act (GLBA) which covers financial service providers (FSP), the Sarbanes Oxley Act (SOX) which covers publicly traded companies and the Federal Information Security Management Act (FISMA) which covers all information systems used or operated by a US government agency or by a contractor or other organization on behalf of a US agency. All of these laws detail requirements and guidance relating to the appropriate security controls and safeguards that should be implemented to protect critical assets and information.

³ <http://aspe.hhs.gov/admsimp/pl104191.htm>

⁴ <http://www.nga.org>

⁵ <http://healthit.ahrq.gov>

⁶ http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

⁷ http://info.sen.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_cfa_20070905_200232_asm_floor.html

3.3 Payment Card Industry Data Security Standard (PCI DSS)

Unlike HIPAA, SOX or GLBA, the PCI DSS⁸ is not a government initiated law or regulation, but is a series of guidelines created and endorsed through the association of Payment Card Industry companies including: American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa Inc. The PCI DSS requires organizations that store, process or transmit customer payment card data to adhere to information security controls and processes that ensure data integrity. Failure to comply with the PCI DSS may result in fines or restrictions imposed by the affected credit card company. Protection from fines is typically provided to organizations that have been compromised but found to be compliant at the time of the security breach.

3.4 Common Security Compliance Threads

From a security perspective, all of these regulations and guidelines follow the basic fundamentals and industry best practices of security which are to protect the confidentiality, integrity and availability of electronic information. Creating a best practices security environment will result in a compliant environment. A better approach to enabling security compliance is to identify and address the common compliance threads that exist in most of the key laws, rules, or guidelines, which are applicable to any specific organization; then adopt a technology infrastructure that meets the intent of these compliance mandates. Common among these laws and rules are mandates for all companies to be proactive in strategically managing business and IT processes, applications, information, technology, facilities, and security. These are the “common compliance threads.” By focusing on the common compliance threads, organizations can help reduce cost and duplication of effort.

Organizations should perform a risk analysis of their environment. This will identify where vulnerabilities exist and the potential risk associated with them. Administrative, technical and physical safeguards should be implemented to ensure the integrity and confidentiality of the health information and to protect against any reasonably anticipated threats or hazards to the security or integrity of the information.

3.5 Consequences of Non-Compliance

The consequences of non-compliance could range from civil and criminal penalties, to compromising the actual safety of the patient, to loss of reputation and litigation. HIPAA has specific civil and criminal penalties for violations; civil penalties vary from state to state for breach violations but usually require notification to compromised parties. The credit card brands also impose fines and penalties on organizations causing breaches of payment card information.

In 2005, Kaiser Foundation Health Plan Inc, a division of Kaiser Permanente, was fined \$200,000 by the California Department of Managed Health Care (DMHC) for exposing the confidential health information of about 150 people. The DMHC said the data had been available on a publicly accessible Web site for as long as four years. "Patients must be assured that health plans will, at all costs, do everything possible to protect confidential information," Cindy Ehnes, director of the DMHC, said in a statement. "Health plans must make security of confidential information a top priority."⁹ Medical identity theft could have serious consequences to patient safety in the form of inaccurate medical charts which could lead to serious physical injury or death. But the real threat of liability is from potential civil lawsuits and the harm to an organization's reputation as a result of negative publicity and scrutiny.

In August of 2006, the office of Veterans Affairs (VA) discovered that a computer was missing from Unisys, a subcontractor that provides software support to the Pittsburgh and Philadelphia VA Medical Centers. The computer contained insurance claim data for some patients treated in these two facilities or their community clinics. For the veterans affected, the information included name, and some or all of the following: date of birth, Social Security Number, address, insurance

⁸ <http://www.pcisecuritystandards.org/>

⁹ <http://www.pcwelt.de/news/englishnews/114650/>

carrier and other insurance claim related information.¹⁰ Several lawsuits have been filed against VA pertaining to the data theft. All of these lawsuits have been filed as class actions.

4 Integrity, Security and Confidentiality of HIE

The adoption of health IT has been slow due to a number of well-documented factors including concerns about privacy and confidentiality of electronic personal information. The eHI Blueprint dictates that “measures should be implemented to protect the integrity, security and confidentiality of each individual’s personal health information (PHI), ensuring that it cannot be lost, stolen, or accessed or modified in an inappropriate way.” Organizations must, therefore, implement safeguards to protect PHI against reasonably anticipated threats, hazards, and impermissible uses and disclosures. These safeguards can be categorized as administrative, technical and physical (as per the HIPAA Security Rule¹¹).

4.1 Steps to Protect Personal Health Information (PHI)

4.1.1 Inventory PHI

The first step in a program to protect PHI is to identify all the applications, systems, storage devices, computing devices, and networks that process, stores or transmits PHI in the form of EHR or otherwise. This inventory should also include any existing controls and safeguards in use.

4.1.2 Risk Assessment and Management

In order to determine what measures are necessary to protect PHI, organizations must do an assessment of the potential threats, vulnerabilities and resulting risks to the confidentiality, integrity, and availability of electronic PHI on the systems, storage devices and networks. Threats may be categorized as natural, human, and environmental. *Natural threats* may include windstorms, floods, earthquakes, wild fires, and landslides. *Human and technology threats* are enabled or caused by humans and may include intentional threats such as network and computer-based attacks, malicious software upload, and unauthorized access to personal health information or unintentional threats such as system crashes, errors in data entry or deletion and disclosing information to unauthorized persons. *Environmental threats* may include power failures, chemical spills, and liquid leakage.

There are two types of vulnerabilities: technical and non-technical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include gaps, flaws or weaknesses in the development of information systems or incorrectly implemented or configured information systems. There are automated tools that scan systems and applications for vulnerabilities. These should be run frequently as new vulnerabilities are continuously being discovered.

Risk is the likelihood of a given threat triggering or exploiting a particular vulnerability and the resulting impact on the organization. Risk, therefore, is not a single factor or event, but rather a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization. Once the risks have been evaluated as to their impact, then appropriate administrative, technical, and physical safeguards must be identified to prevent or mitigate the risks to privacy and security. Any residual risk must be documented and accepted by management. The next step is to manage these risks and implement the safeguards. (See NIST Special Publication 800-30 for detailed explanation of risk assessment and management and

¹⁰ <http://www.usa.gov/veteransinfo.shtml#happened-Aug06>

¹¹ <http://www.hhs.gov/ocr/hipaa/bkgrnd.html>

NIST Special Publication 800-53 for a list of safeguards and controls that can be selected to manage the identified risks.)¹²

It is important that the scope of this risk assessment include all forms and locations of electronic media. Formal documentation of the process including the analysis, decisions and the rationale for its decisions must be kept for six years and periodically updated, typically once a year or more often as changes in the threat and business environment occur.

4.1.3 Implement Security Measures

The next step is to implement the security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule and state privacy laws. The risk management plan documents the implementation of the security safeguards and specifies how to test and maintain these safeguards.

The following sections cover the policies, procedures and technologies that organizations can implement to protect PHI and the systems used to process PHI.

4.2 Confidentiality & Privacy Protection

According to the U.S. Department of Health and Human Services (HHS) the first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the HHS, these standards (the Privacy Rule) provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this rule. HIPAA includes provisions designed to encourage electronic transactions and also requires new safeguards to protect the security and confidentiality of health information. Health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., enrollment, billing and eligibility verification) electronically are required to comply with the provisions of the Privacy Rule.¹³

4.2.1 Protected Health Information According to HIPAA Privacy Rule

The following is an excerpt from the "Summary of HIPAA Privacy Rule" provided by the HHS.

Protected Health Information. The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

De-Identified Health Information. There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either: 1) a formal determination by a qualified statistician; or 2) the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Source: <http://www.hhs.gov/ocr/privacysummary.pdf>

¹² <http://www.nist.gov/>

¹³ <http://www.hhs.gov/>

4.2.2 Access Controls

User Identification, Authentication and Authorization

Speaking plainly, **identification** is the declaration of who you are, **authentication** is the steps you take to prove that identity, and then once proven, **authorization** outlines what that identity (an individual or entity) is allowed to do.

Individual or entity (such as a business associate) **identity** may be verified using one or more of three means:

- One-factor authentication: something you know (a secret such as a password, Personal Identification Number (PIN), or cryptographic key);
- Two-factor authentication: something you know and something you have (a token such as an ATM card, smart card or security device);
- Multi-factor authentication: something you know and something you have and/or something you are, or can do (a biometric such as physical characteristics such as a voice pattern, iris image or fingerprint).

HIPAA requires only one-factor authentication, but there is a general industry trend toward the use of at least two-factor authentication methodologies for access to more sensitive data. For example, the Indiana Health Information Exchange uses two factor authentication, as does the Tennessee-based Mid South eHealth Alliance. CareEntrust, an HIE in Kansas City, Missouri, currently uses single factor authentication but is moving toward two-factor authentication.¹⁴

The HIPAA privacy rule restricts access to PHI to those individuals who and entities that are authorized due to their role in the healthcare treatment, payment or operation, or those who have been granted permission by the patient. The minimum necessary standard requires that a covered entity limit who within the entity has access to protected health information, based on who needs access to perform their job duties. If a hospital employee is allowed to have routine, unimpeded access to patients' medical records, where such access is not necessary for the hospital employee to do his job, the hospital is not applying the minimum necessary standard.

Role-based access control (RBAC) restricts access to applications and data based upon the users pre-defined role in the organization. Roles are defined in advance with associated job descriptions and pre-determined system and application access parameters. The goal of RBAC is to minimize "exceptions" and ease the administrative burden of managing the access of multiple users. Rules are applied to deal with exceptions and make it possible to apply greater and more granular access control to resources and information. For example, roles in a hospital might include: doctor, resident, nurse practitioner, orderly, administrator, technologist, etc. Rules might be applied to restrict access based on time of day, tenure or contract, status of individual (practicing, suspended, restricted), the condition or type of patient (emergency versus non-emergency, surgical versus out patient), or the method of connecting to information (remote, wireless, local).

Putting Authentication and Authorization Into Practice

A doctor on call at a hospital, visiting a patient that they are not familiar with, would have access to that patient's records pertinent to the current visit and applicable medical information. They would not necessarily need, or have access to for example i) medical history from most recent physical examination, ii) psychological medical history from previous visits to family practitioner, iii) financial information used to pay for medical services, or iv) family medical history. However, if an emergency situation were to arise, the doctor might be granted increased access to information (such as family medical history, but not financial information) by applying an emergency Rule to the Role already allocated to this doctor. In this emergency, the doctor would

¹⁴ <http://toolkit.ehealthinitiative.org/Interoperable%20Digital%20ID%20Management%20Report.pdf>

have access to more and different information than a nurse practitioner and a hospital administrator.

4.3 Encryption for Data Protection

Encryption has been receiving increasingly wide-spread acceptance and recognition as best practice for protecting the confidentiality and privacy of personally-identifiable information including PHI and personal financial data. The purpose of encryption is to make information unreadable by individuals or systems that do not have the appropriate cryptographic keys which grant access to this information. PHI needs to be maintained over a long period — indeed a lifetime. This presents unique challenges to healthcare organizations to achieve the balance of availability and confidentiality of this information. Specifically, the success of any encryption strategy is hinged on the ability to access and protect and manage the cryptographic keys used for encryption over PHI, for the duration of time that the information needs to be protected.

4.3.1 The Basics of Encryption Technology

Encryption can be performed symmetrically (using a single key to encrypt and decrypt) or asymmetrically (using different keys for encryption and decryption -- also known as public-key cryptography). The primary feature of public-key cryptography is that it removes the need to use the same key for encryption and decryption. With public-key cryptography, keys come in pairs of matched “public” and “private” keys. The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secret by its owner.

Prior to the invention of public-key cryptography, it was essentially impossible to provide key management for large-scale networks. With symmetric cryptography, as the number of users increases on a network, the number of keys required to provide secure communications among those users increases rapidly. For example, a network of 100 users would require almost 5000 keys if it used only symmetric cryptography. Doubling such a network to 200 users increases the number of keys to almost 20,000. Thus, when only using symmetric cryptography, key management quickly becomes unwieldy even for relatively small-scale networks.¹⁵

Encryption Algorithm Choices: Type, Length, Strength and Speed

Strength and speed of encryption is dependent on the algorithm type and length of cryptographic keys used for encryption. The purpose of the encryption will also impact the choice of algorithm implemented in a cryptographic system. Due to the extremely confidential and sensitive nature of PHI, HIE solutions should implement cryptographic algorithms that have been vetted through the [Federal Information Processing Standards \(FIPS\) 140-2 certifications](#) which is run by the [National Institute of Standards and Technology \(NIST\)](#) or through a similar certification process. Other standards bodies which have cryptography related standards include: American National Standards Institute ([ANSI](#)), International Organization for Standardization ([ISO](#)), Institute of Electrical and Electronics Engineers ([IEEE](#)), and Internet Engineering Task Force ([IETF](#)).

Depending on the nature and purpose of encryption, different algorithms may be used.

The following excerpt and table details the most commonly known algorithms and comes from the [Burton Group](#)¹⁶ research report titled “Encryption”, December 5, 2007:

“The choice of algorithm will also depend on the function that cryptography is providing for the system. Secret key algorithms (also known as private key algorithms) provide confidentiality. Depending on how they are used, public key algorithms can provide both authentication and confidentiality or a mechanism to exchange keys. Secret key algorithms tend to be faster than public key algorithms; therefore, they are normally used to encrypt the information after some type of authentication or key exchange is performed using public

¹⁵ [Entrust, Inc.](#), “Introduction to Cryptography and Digital Signatures”, March, 2001.

¹⁶ [Burton Group](#), Dan Blum et al., “Encryption”, December 5, 2007.

key algorithms (as is done in SSL). Secure Hash Algorithms (SHAs) are used to create a message digest that can be used to determine if a message or file has been modified. Table 1 shows a listing of the most well-known algorithms in each category.”

Secret key algorithms	Public key algorithms	Secure Hash Algorithms
<ul style="list-style-type: none"> • 3DES (NIST SP800-67) • AES (FIPS PUB 197) • Rivest Cipher 4 (RC4) (used in SSL) • CAST • IDEA • SEED • GOST 	<ul style="list-style-type: none"> • RSA (American National Standards Institute [ANSI] X9.31 and Public Key Cryptography Standards [PKCS]#1) • Diffie-Hellman (ANSI X9.42 and NIST SP800-56—for key exchange only) • ECC (ANSI X9.62 and X9.63) • Digital Signature Algorithm (DSA) (FIPS PUB 186-3—for authentication only) 	<ul style="list-style-type: none"> • Message Digest 5 (MD5) • SHA-1 • SHA-256

Table 1: Well-Known Algorithms

4.3.2 Public Key Infrastructure (PKI) for Encryption Key Management

Understanding the algorithms, though academically challenging, is not necessary and is not the cause for difficulty in a cryptographic implementations. The challenge lies in managing the encryption keys (which are typically stored in digital IDs or x.509 certificate formats within a hardware encryption device, on a hard disk, in the memory of a computer system, or on external security tokens/USB devices) for as long as the information that they are protecting needs to be maintained protected. Maintaining a secure key history, key back up and recovery, key renewal, key issuance and revocation are functions typically managed and performed by a Public Key Infrastructure (PKI).

4.3.3 Encryption of Data ‘At Rest’

A general best practice for personal information of any kind, including PHI, is that if it does not need to be kept, do not store the data. Using this as a starting point in HIE strategies, will significantly minimize potential exposure of PHI. For that information which does need to be maintained, it is important to consider the available options and challenges to protect that data, or the systems on which that data is ‘at rest’ on laptop computers and mobile devices, storage disks, databases and repositories, email and web servers — any of the locations that PHI is stored, either temporarily or permanently.

The PCI DSS¹⁷, due to significant risk of personal information for the purpose of identity fraud, does an excellent job documenting the practices and technologies that enable encryption of data at rest. This guidance is applicable across industries and can be used as a benchmark to strive towards best practice of data protection.

Encryption, Like All Security Mechanisms, Will Be Attacked

In February 2008, a team of researchers from Princeton University announced that they had discovered a way to gain access to encryption keys stored in the dynamic random access memory (DRAM) found in all computers by effectively “freezing” the hardware using cold compressed air. According to PGP, the Cold Boot Attack approach could potentially impact users

¹⁷ https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

of a broad range of encryption products that store their key(s) in DRAM and don't proactively delete those keys when not in use on systems that are left unattended while powered on or during the first few minutes after the computer is shut down.¹⁸

What can be done to prevent this type of attack? Most simply, protect access to a computer system until it is completely shut down and for several minutes after shut down. Do not allow systems to run, unattended in "stand-by" mode; choose to "hibernate" the system instead. Implement tools and products that prevent encryption keys from being stored in DRAM.

The Cold Boot Attack, February 2008

In a paper published Thursday February 21st, a team of security researchers affiliated with Princeton University announced they had discovered a way to leverage the inherent characteristics of DRAM found in all computers to circumvent various disk encryption products. **It is significant to note that this is a hardware attack, not an attack on the encryption tools themselves.** The "Cold Boot Attack," as its known, is dependant upon the attacker having physical access to the computer either while it is running or within a few minutes of shutting down. The attack centers on compromising encryption products that store their key(s) in DRAM. The details of how the Cold Boot Attack works are well summarized on C|Net and can be viewed on YouTube.

...all security tools and techniques, from firewalls to physical security methods, are designed to address specific threat models. Achieving comprehensive security in any given environment requires using a combination of security measures that addresses all of the potential threats to which the information in question may be subject. This is particularly true when protecting confidential information that is resident on complex modern computing devices.

Obviously information that is stored on desktop or laptop systems that are powered on and left unattended are vulnerable to a broad range of attacks far simpler than the Cold Boot Attack technique. What is unique about the Cold Boot Attack is that it also works during the period between powering off a computer and a few minutes after shut-down when the information stored in DRAM is actually gone. The attack is based on the insight that information stored in modern DRAM chips does not disappear the instant a computer is powered off.

Source: http://www.pgp.com/newsroom/cold_boot_attack_response.html

4.3.4 Encryption of Data 'In Transit'

SSL — stands for Secure Sockets Layer and is protocol which was renamed to TLS (Transport Layer Security) but it is most commonly known as SSL — is likely the most widely and possibly the most unnoticed form of encryption in use today. Support for SSL is in all major browsers and web servers making it universally accepted as a means to secure information in transit over the internet or within intranets. The strength of the encryption is actually a function of the version of the browser and the capabilities of the Web server. If a browser is limited to 128-bit encryption, then only a 128-bit session will be established, even if the Web server supports 256-bit sessions. If both the browser and server support 256-bit encryption, then a 256-bit session can be established. Since 2000, U.S. export regulations have permitted the export of 128-bit encryption-enabled browsers and upgrades for existing browsers to all countries except those under U.S. embargo.¹⁹

Advancements in Web browser and server technology have taken steps to protect the integrity of SSL security by offering extended validation capabilities. This is an anti-phishing measure that gives additional visible security cues to help individuals have confidence in identity of the web server they are visiting.

¹⁸ http://www.pgp.com/newsroom/cold_boot_attack_response.html

¹⁹ http://www.entrust.net/ssl-resources/pdf/understanding_ssl.pdf

4.3.5 Virtual Private Networks (VPNs)

A VPN is a virtual network, built on top of existing physical networks, which can provide a secure communications mechanism for data and other information transmitted between two endpoints. There are two basic types of VPNs: SSL VPN and IPsec-based VPN. The two VPN technologies are complementary and address separate network architectures and business needs. SSL VPNs offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so the client usually does not require configuration by the user. SSL VPNs offer granular control for a range of users on a variety of computers, accessing resources from many locations.²⁰

VPN Use for HIE

The obvious benefit of VPN is the protection of PHI as it travels over public networks such as the internet. It creates an encrypted “tunnel” to prevent PHI from being modified or intercepted. Many healthcare organizations take advantage of VPN for a variety of different applications. For example, **Saint Barnabas Health Care System**, the largest healthcare system in New Jersey, provides secure remote access to hospital resources using a SSL VPN appliance with a thin-client application used by physicians from home offices, on-site hospital medical and administrative staff and traveling caregivers.²¹

Winslow Health Care Center in Arizona combines VPN technology with **broadband satellite internet access** to receive and transmit protected PHI communications between the health care center and remote traveling caregivers providing medical services in a mobile health van.²²

The **Visiting Nurse Service of New York** (VNSNY) has nearly 10,000 care providers that make more than 2.2 million home visits per year and they spend the majority of their day providing in-home healthcare to patients and traveling between patient locations. VNSNY use hand-held pen operated tablet PCs or laptop computers, and use a **Mobile VPN** to secure the wireless connectivity to clinical records, applications and email. The mobile VPN enables application stability as users move in and out of wireless coverage areas and seamless roaming between Wi-Fi and wide-area cellular networks.²³

Though the benefits to VPN may be obvious, the risks of VPN are not as apparent. An encrypted tunnel serves the purpose to protect PHI while in transit; however, a VPN can also be used maliciously to hide an encrypted attack. This reinforces the requirement to have defense-in-depth as a best practice in any HIE strategy. Defense-in-depth requires many layers of protection to prevent attack of critical systems using tools such as network-level and host level intrusion prevention systems which will be discussed later in this paper.

4.3.6 Minimum Requirements for Encryption of PHI

HIPAA provides guidance on the nature of security — for example, encryption must be addressed as a means to protect information flowing over open networks — but does not indicate specific encryption algorithms, key strengths or technologies. Industry best practices can be gauged by an assessment of cryptography and security protocols implemented by industry leading security vendors, as well as by referring to [NIST Publications \(FIPS or Special\)](#).

For example, the following is an excerpt from NIST Special Publication Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations. Note the guidelines detail exact encryption algorithms and key lengths, and indicate certification levels such as FIPS-approved status.

²⁰ <http://csrc.nist.gov/publications/drafts/SP800-113/Draft-SP800-113.pdf>

²¹ http://www.aepnetworks.com/products/downloads/StBarnabas_CaseStudy.pdf

²² http://www.aepnetworks.com/products/downloads/satellite_business_solutions.pdf

²³ http://www.netmotionwireless.com/company/press/2_27_2008.aspx

2.2.2 Confidentiality

The following symmetric encryption algorithms are used in various cipher suites to provide confidentiality:

IDEA – IDEA is a block cipher that operates on 64 bit plaintext blocks. The key is 128 bits long. The same algorithm is used for encryption and decryption. IDEA is not FIPS-approved.

RC4 – RC4 is a stream cipher that uses a variable length key of anywhere between 8 and 2048 bits long. RC4 is not FIPS-approved.

3DES-EDE – The Data Encryption Standard (DES) is the most widely used symmetric block cipher. It uses 64 bit blocks and a 56-bit key. Triple DES (also known as 3DES) super-encrypts by running the data through the DES algorithm 3 times with different keys. The first time it Encrypts with key 1, the second time it Decrypts with key 2 and the third time it Encrypts again with key 3; hence the acronym 3DES-EDE. 3DES-EDE is FIPS-approved.

AES – The Advanced Encryption Standard is a FIPS-approved symmetric block cipher encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive but unclassified information. AES uses 128, 192, or 256 bit keys, however cipher suites have only been defined for 128 and 256 bit keys to reduce the over proliferation of cipher suites. The blocksize in AES is 128 bits. The AES algorithm [FIPS197] is designed to replace DES and 3DES. AES is FIPS-approved.

Note that RC4 is currently the most commonly used confidentiality algorithm in SSL/TLS. However, RC4 is not FIPS-approved.²⁴

The above recommendation is an example of the best practice implementation recommendations that are made by NIST. However, the evolutionary nature of security technology makes vigilance and persistence requirements in maintaining a best-practices level of security implementation. It is recommended that an organization regularly and directly consult these and other security guidelines to ascertain the latest security recommendations.

“Most real-world cryptographic systems are compromised by attacking the environment in which they operate rather than the algorithms they use. This includes the systems they run in, the users that use them, and a host of other related issues. For example, many enterprises trust cryptographic systems that run in personal computers operating under very insecure operating systems. In most cases, the operating system has to get involved in order to display the data, perform calculations, or otherwise make use of anything that is encrypted. If these systems can be defeated, the cryptographic system as a whole can also be defeated.”

Source: Burton Group, “Encryption”, December 5, 2007

²⁴ <http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf>

4.4 Intrusion Detection and Prevention Systems (IDS/IPS)

The threat landscape for healthcare organizations, like most enterprises and governments, now includes financially motivated attackers that steal and sell valuable data — including PHI and computing resources. Cyber-criminals are able to penetrate or bypass most perimeter security systems and now target software vulnerabilities in critical e-Health systems, including web-based applications such as EHR/EMR systems, as well as the underlying enterprise servers and operating systems.

“SecureWorks, an Atlanta-based security services firm, has recorded an 85% increase in the number of attempted attacks directed toward its healthcare clientele by Internet hackers, with these attempts jumping from 11,146 per healthcare client per day in the first half of 2007 to an average of 20,630 per day in the last half of last year through January of this year.” Source: Network World Magazine, February 2008²⁵

Intrusion prevention is a preemptive approach to IT security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the security administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, would be forwarded to the recipient with no apparent disruption or delay of service.²⁶

IPS can be implemented at the network (network-based intrusion prevention – NIPS) or on the host (host-based intrusion prevention – HIPS). NIPS are hardware devices, while HIPS are software solutions. HIPS solutions have an advantage over NIPS devices because they make it possible to gain fine-grained control and visibility on a unique host resource. IDS/IPS can be integrated with SIEM for improved visibility and control over network traffic.

When considering host-based IDS/IPS, these key features provide the best protection against known and zero-day attacks:

- *Blended approach:* Combine host-based stateful firewall with a high performance deep packet inspection engine to examine all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.
- *Intrusion detection/prevention filters:* A system that can operate in detection and prevention mode at the filter, host and profile (for example a laptop profile versus web server profile) level.
- *Application protection:* An IDS/IPS should include a wide array of out-of-the-box vulnerability protection for readily available commercial applications and operating systems.
- *Security updates:* Filters that shield newly discovered vulnerabilities need to be automatically delivered, and be able to be pushed out to thousands of hosts, without system reboot.
- *Virtual patching:* A system that can protect against known and zero-day vulnerabilities as a compensating control before vendor issued patches can be received, tested and deployed.
- *Logs, alerts and notifications and SIEM Integration:* Detailed logs need to provide information on who attacked, when they attacked and what they attempted to exploit. Administrators need to be automatically notified when an incident has occurred. If an organization has a SIEM system in place, the IPS needs to pass alerts, notifications and reports through web services or other interfaces.

²⁵ <http://www.networkworld.com/news/2008/022708-healthcare-cyberattacks.html>

²⁶ <http://searchsecurity.techtarget.com>

- *SSL inspection*: The IPS needs to be able to inspect encrypted traffic looking for malicious code and other anomalies that might signal an attack.
- *Custom and smart filters*: Specific applications such as a VoIP call-processing server—or unique challenges like protecting custom healthcare applications and EHR systems—should be able to be protected using custom filters or smart filters to log or block additional application security events.
- *Recommend security profiles*: To simplify and streamline management and performance of the IPS, the system should be able to identify applications running on hosts and recommend which IPS filters should be applied to the hosts, enabling automatic management of filters to ensure the correct protection is in place, with minimal effort.
- *Risk ranking*: Security events can be viewed based on asset value as well as vulnerability information.
- *Role-based access*: Allows multiple administrators, each with different levels of permission, to operate different aspects of the system and receive information appropriate to them.

4.5 Integrity Protection

PHI must also be protected from improper alteration or deletion. Based upon a risk assessment, an organization must implement policies, procedures and technical integrity safeguards to prevent or detect unauthorized alteration or deletion of PHI data and critical system and network files. Some policies and procedures include the following:

- Using access control auditing for files or file types containing PHI or determined to be critical.
- Assigning staff responsibility for reviewing the results of integrity checking, handling discrepancies, and escalating problems.
- Establish in-house standard procedures for change control, testing, documentation, approval and rollback requirements, and procedures for all software and hardware changes, firewall configuration and rules changes, and emergency fixes.
- Establish policies and procedures for moving systems from development into production.
- Maintain a copy of tested production software and control files in a secure location preferably in a geographically separate facility.
- Establish authentication procedures for software updates and patches. Verify all new programs before installation.

Some technical safeguards include:

- Automated file integrity checking mechanism.
- Digital signatures for file integrity.
- Reconciliation routines, such as hash totals and record counts.
- Consistency checks and reasonableness testing.
- Anti-virus software on servers, and endpoints including PCs, PDAs and network devices.
- Data leak prevention across the enterprise.

4.5.1 Endpoint Protection

Better protection and safeguards leads to overall better system availability. Today's corporate endpoints — PCs, PDAs and more — are increasingly mobile and often connect to the Internet outside the enterprise network where they are no longer protected by multiple layers of security. These endpoints require a blended approach to protection that secures data and applications from hacking attempts, Web, messaging, and network threats, and the increasing threat of

vulnerabilities being exploited. Combining a high-performance network-level **host intrusion prevention system** (HIPS) with client-server security that includes integrated **antivirus, anti-spyware, Web threat protection** and **firewall** provides strong endpoint protection.

Integrated, coordinated protection in the cloud, at the gateway, and on the endpoint, combined with messaging security capabilities such as anti-spam, provides multi-layered, multi-threat protection with the following capabilities:

- **Dynamic:** Delivers optimum Web security by analyzing the reputation of the source as well as the content being accessed.
- **Multi threat:** Provides comprehensive protection by combining antivirus, anti-spyware, anti-phishing and anti-spam.
- **Multi layer:** Maximizes protection with multiple techniques — including Web reputation, URL filtering, and HTTP traffic scanning — applied as appropriate within multiple network layers.
- **Integrated:** Coordinates defenses for malware detection, infection removal, and cleaning.

4.6 Accountability, Audit, & Oversight

Among the most important security safeguards for protecting PHI are those relating to oversight and audit. These ensure accountability for patients who entrust their information to electronic health record systems and provide a strong incentive to users of such systems to conform to the policies on the acceptable use of these systems. Effective accountability and audit can help to uncover misuse of PHI and systems and can assist organizations and patients to obtain redress against those who abuse their access privileges. Organization should implement the following:

- Create a secure audit record each time a user accesses, creates, updates, or archives personal health information via the system. The audit log should uniquely identify the user, uniquely identify the data subject (i.e., the patient), identify the function performed by the user (record creation, access, update, etc.), and the time and date that the function was performed.
- Retain a record of the former contents of the data and the associated audit record (i.e. who entered the data on what date) when patient data is updated,
- Keep a log of message transmissions when PHI is transmitted (such a log should contain the time, date, origin and destination of the message, but not its content).
- Monitor systems and network logs for indications of misuse. Consider implementing a security information and event management system (SIEM) to aid in monitoring.
- Consider implementing automated intrusion detection and prevention systems (IDS/IPS) as previously discussed.

4.6.1 Security Information and Event Management (SIEM)

Security information and event management (SIEM) systems provide a clear view of an enterprise's true IT security position, and improve management by enabling quick, decisive responses to real security threats. SIEMs also provide auditable proof of IT compliance with corporate governance and legislated requirements. Increasingly, organizations that have deployed a SIEM, or are planning to invest in one, are implementing host-based security as part of their defense-in-depth strategy. Host intrusion detection and prevention systems (IDS/IPS) shield mission critical hosts, applications and data from attacks that increasingly bypass or penetrate perimeter defenses. Host IDS/IPS provides a powerful and compelling complement to a SIEM.

4.6.2 Data Leak Prevention

Protecting the privacy of electronic patient records guaranteed under HIPAA and organizational governance policies is critical to the legal and economic standing of all healthcare organizations.

However, with the explosion of messaging systems, wireless networking and USB storage devices, and the promise of expanding health care delivery networks, protecting critical enterprise data has become even more difficult. And as verified by recent research, care delivery organizations (CDOs), health insurance providers, and other healthcare-related organizations have been victims of theft or loss of critical company data — often by legitimately authorized insiders — employees who maliciously or accidentally cause data leaks.

“The greater the value or usefulness of data outside of an organization, the more likely it is that someone will try to steal it. If the data can be sold, then it clearly has economic significance. If it can be used for competitive advantage, then it has an indirect economic significance. However, information doesn't have to be economically valuable to be of high interest to outsiders — it can also have social or political significance that would be harmful to the organization if the information became available to someone motivated to publicize it or use it for blackmail.”

Source: Gartner, Inc., “Understanding Data Leakage” Jay Heiser, August 21, 2007

What should healthcare organizations do to protect against data leaks? To prevent data leaks, organization can take advantage of emerging technologies that monitor and detect these leaks at the point of use, or as records are in motion transferred in wider networks, or at rest as they simply reside on a computer that can be accessed. A Data Leak Prevention (DLP) system will prevent leaks at every port, endpoint in the organization, and on any network whether it is the corporate, public, or WAN. This is a critical as an organization's drive to move patient data to disparate networks as envisioned in the new HIE landscape.

Additionally, since a high percentage of breaches are accidental, healthcare organizations have an opportunity to better protect sensitive data by educating employees on the proper handling of information. Data leak prevention technology should not only monitor and prevent leaks, but it should help educate and raise awareness of employees about companies' policies and procedures for handling sensitive patient data.

When evaluating a DLP solution, consider the following:

- Do you know what sensitive PHI needs to be protected, and where it currently resides, and where and how this data will be transported under HIE initiatives?
- Do you know who needs the sensitive data, and what if any, third parties may be receiving, using or handling this data?
- Do you have acceptable use policies governing the use and handling of PHI?
- Does the DLP solution offer management capabilities that allow an administrator to identify, define and classify organizations' sensitive information?
- Can the administrator easily define specific security policies according to the sensitive information classifications?
- Does the system effectively prevent PHI from disclosure or theft based on security policies that are defined at fine-grained levels?
- Once sensitive information and security policies have been defined, does the system have capabilities to determine if transmitted information is sensitive by inspecting it against sensitive information definitions?

- Can the system take necessary actions according to policies in real time when information is about to leave the organization? For example, if a document is being copied to a USB drive or sent out via the network, the system detects the activity, finds out if the file contains sensitive information, and logs and/or blocks the activity.
- Once sensitive records or documents are identified and registered within the system, is it able to inspect outbound transmission of the sensitive document (and its derivatives) by comparing outbound transmissions against signature files representing the registered document?
- Are there templates used to present sensitive structured data such as patient info, account numbers, credit card number, social security number?
- Are there mechanisms to discover sensitive information that is sitting at rest on a computer?

4.7 Availability Controls

Availability and business continuity are arguably more important in HIE than in any other industry due to risks associated with patient safety if appropriate PHI is not available in a timely and secure manner.

Each security practice and measure previously discussed in this paper plays an important role in maintaining the availability of systems and quality and protection of PHI.

4.7.1 Security Contingency Plan

“A contingency plan is the only way to protect the availability, integrity, and security of data during unexpected negative events. Data are often most exposed in these events, since the usual security measures may be disabled, ignored, or not observed.” (HHS Security Rule Preamble, pg. 8351). Using the risk assessment and impact analysis (including recovery time objectives) organizations must assess the relative criticality of specific applications and data in support of other contingency plan components. Organizations will need to determine the frequency and scope of testing and the process to revise and update disaster recovery and emergency mode operation plans. The contingency plan must include procedures to:

- Create and maintain retrievable exact copies of electronic PHI.
- Restore any lost data.
- Enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
- Respond to applicable breach disclosure requirements.

5 Conclusion

Health Information Exchange (HIE) is the mobilization of healthcare information electronically across organizations within a region or community. Healthcare delivery networks are faced with the challenge of deploying HIE solutions to achieve interoperability across the landscape of diverse stakeholders while meeting the needs of the patient by ensuring clinical and financial data is transmitted privately and securely.

In many ways privacy, security and confidentiality are driven by regulatory requirements, but this is only the starting point. If consumers are not confident that these areas are properly addressed then the impact and adoption of the enabling technologies will be significantly reduced. The application of best practices, to manage the associated risks to the patient information that is exchanged over new and ever-changing technologies, is critical to meeting the eHI stated goals of transforming healthcare through technology.

From a security perspective, all of the regulations and guidelines such as HIPAA, GLBA and PCI follow the basic fundamentals and industry best practices of security which are to protect the confidentiality, integrity and availability of electronic information. Creating a best practices security environment will result in a compliant environment. A better approach to enabling security compliance is to identify and address the common compliance threads that exist in most of the key laws, rules, or guidelines, which are applicable to any specific organization; then adopt a technology infrastructure that meets the intent of these compliance mandates.

Organizations must implement safeguards to protect PHI against reasonably anticipated threats, hazards, and impermissible uses and disclosures. The first step in a program to protect PHI is to identify all the applications, systems, storage devices, computing devices, and networks that process, stores or transmits PHI in the form of EHR or otherwise. This inventory should also include any existing controls and safeguards in use.

In order to determine what measures are necessary to protect PHI, organizations must do an assessment of the potential threats, vulnerabilities and resulting risks to the confidentiality, integrity, and availability of electronic PHI on the systems, storage devices and networks. Once the risks have been evaluated as to their impact, then appropriate administrative, technical, and physical safeguards must be identified to prevent or mitigate the risks to privacy and security. Any residual risk must be documented and accepted by management. An organization must then manage these risks and implement the safeguards and security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA Security Rule and state privacy laws.

6 About the Authors

6.1 Concordant

Concordant (www.concordant.com) is an eHealth Services firm that engages with healthcare organizations to plan, implement, and manage their HIT (Health Information Technology) infrastructure. Our unique methodology combines an ideal balance of tools, talents, techniques, and cost management. Healthcare IT leaders who are responsible for creating and maintaining a dynamic HIT infrastructure have a reliable partner in Concordant. Hundreds of healthcare organizations rely on our advanced techniques and experienced staff to provide reliable and optimized services for the entire HIT lifecycle to ensure that they have well-designed, efficiently operated technical environments.



6.2 Third Brigade

Third Brigade (www.thirdbrigade.com) specializes in providing host intrusion defense systems to organizations that need to detect and prevent attacks that exploit vulnerabilities in mission critical systems. Third Brigade Deep Security allows businesses to apply comprehensive security profiles to hosts that protect against known and zero-day attacks using deep packet inspection. It helps ensure compliance and the 24-7 availability of critical systems, provides a virtual patch for software vulnerabilities, and allows organizations to deliver Internet-based services with greater security and confidence. Unlike other host intrusion detection and prevention systems, Third Brigade Deep Security provides broader, faster and simpler protection. Third Brigade. That's control.



6.3 Trend Micro

Trend Micro Incorporated (www.trendmicro.com) is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit www.trendmicro.com.

