FIME MEDLAB AMERICAS

HIPAA Compliance

Dr. John Barker Ph.D., MIEEE

MEDICAL DEVICES BUSINESS SEMINAR

informa
life sciences exhibitions

A Novel Approach for the Implementation of HIPAA Compliant ePHI Access Control

Abstract

Storing and maintaining electronic Protected Health Information (ePHI) has associated risks: theft of records, databases held to ransom, fines imposed after a data breach and subsequent patient litigation.

Current technical solutions for ePHI access control are outside the budget of smaller healthcare entities, and require high-level technical expertise for their deployment.

This paper presents a novel approach to ePHI access control, built on a technical solution that is both economical to deploy, and can be managed by outsourced IT staff.

The technical solution is therefore appropriate for small and medium size healthcare entities that must deploy ePHI access control but are constrained by a limited budget. This presentation summarizes the HIPAA requirements for ePHI access control and describes the weak points where vulnerabilities might exist for ePHI attacks.

The methodology employed to develop an economical technical solution is described. The technical solution can be deployed by any smaller covered entity, from a physician or dental office, to a clinic or hospital. The deployment procedure and subsequent management of the technical solution is described.

PART 1:
HIPAA RULES OVERVIEW

PART 2:
SECURITY STANDARDS:
TECHNICAL SAFEGUARDS
Technical Implementation of the HIPAA Security Rule

PART 1:

HIPAA RULES OVERVIEW

1 Introduction

2 Security and Privacy

3 Risk Assessment and Data Breach

4 Attempted Intrusion

5 Supporting Documents

Health Insurance Portability and Accountability Act (HIPAA)

Title I of HIPAA regulates the availability and breadth of group health plans and certain individual health insurance policies. It amended the Employee Retirement Income Security Act, the Public Health Service Act, and the Internal Revenue Code.

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.

Health Insurance Portability and Accountability Act (HIPAA)

Title II of HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information, and sets civil and criminal penalties for violations. Title II also required the Department of Health and Human Services (HHS) to draft rules that would improve the efficiency of the health care system by creating standards for the use and dissemination of health care information

- The Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (health insurers, medical service providers, etc.)
- The Transactions and Code Sets Rule simplifies health care transactions by requiring all health plans to engage in health care transactions in a standardized way
- The Security Rule deals specifically with Electronic Protected Health Information (ePHI) and lays out three types of security safeguards required for compliance: administrative, physical, and technical
- The Unique Identifiers Rule (National Provider Identifier: NPI) requires that all covered entities using electronic communications (e.g., physicians, hospitals, health insurance companies) must use a single new NPI
- The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings regarding HIPAA violations

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

Under the HITECH Act, the United States Department of Health and Human Services promotes and expands the adoption of health information technology, to create a nationwide network of electronic health records.

Subtitle A – Promotion of Health Information Technology
Part 1 – Improving Health Care Quality, Safety, and Efficiency
Electronic health records (EHR): The HITECH Act sets meaningful use of inter-operable EHR adoption in the health care system as a national goal with incentives for EHR adoption.

Subtitle B – Testing of Health Information Technology

Subtitle C – Grants and Loans Funding

Subtitle D – Privacy
Part 1 – Improved Privacy Provisions and Security Provisions
The HITECH Act requires entities covered by the HIPAA to report data breaches, which affect 500 or more persons, to the United States Department of Health and Human Services. This subtitle extends the complete Privacy and Security Provisions of HIPAA to the business associates of covered entities. This includes the extension of updated civil and criminal penalties to the pertinent business associates. These changes are also required to be included in any business-associate agreements among the covered entities.

HIPAA Security Rule Technical Safeguard Standard

HIPAA Security Rule Technical Safeguard Standard has four implementation specifications:

Unique user identification

Emergency access procedure

Automatic logoff

Encryption and decryption

The first two are required; the last two are addressable. Addressable does not mean “optional.” Rather, an addressable implementation specification means that a covered entity must use reasonable and appropriate measures to meet the standard.

HIPAA Security Rule Access Control

There are four commonly used approaches to controlling who has access to information and when access is available. A covered entity will choose one of the following approaches based on outcomes of the covered entity's risk analysis.

Access Control List (ACL): The Security Official or designee (e.g., office manager or IT head) will control a workforce member's access to specific applications.

User Based Access Control (UBAC): The Security Official or designee will control a workforce member's access based on the workforce member's identity.

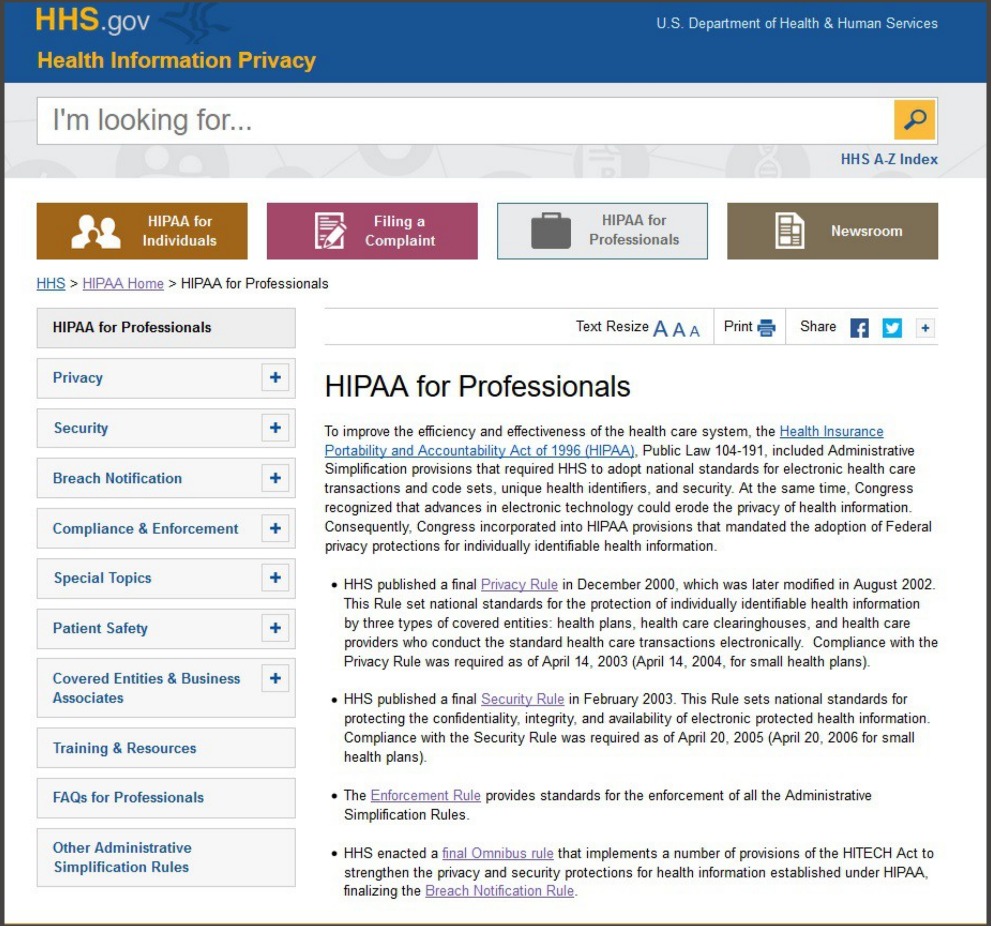
Role Based Access Control (RBAC): The Security Official or designee will control a workforce member's access based on the workforce member's work role. For example, a workforce member with multiple job functions would be assigned multiple roles and access rights.

Context Based Access Control (CBAC): The Security Official or designee will enhance control of a workforce member's access through context-based rights, such as restricting access to certain dates or times, or certain devices on the covered entity's electronic information system or network.

Note: Our technical design, described later, combines UBAC and RBAC

Information resource:

Consult the U.S. Department of Health and Human Services Website



HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).
- HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006 for small health plans).
- The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.
- HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.

https://www.hhs.gov/hipaa/for-professionals/index.html

HIPAA RULES OVERVIEW

PART 1:

1 Introduction

2 Security and Privacy

3 Risk Assessment and Data Breach

4 Attempted Intrusion

5 Supporting Documents

HIPAA Security Series: 1

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part1: Security 101 for Covered Entities

Administrative Simplification
Who Must Comply?
Why Security?
The Privacy Rule and Security Rule Compared
Implementation Specifications
Overview of the Process
Flexible and Scalable Standards
Technology Neutral Standards
Security Standards
Resources
Security Standards Matrix

DEPARTMENT OF HEALTH & HUMAN SERVICES-USA

HIPAA Security SERIES

Security Topics

☆1. Security 101 for Covered Entities

2. Security Standards - Administrative Safeguards

3. Security Standards - Physical Safeguards

4. Security Standards - Technical Safeguards

5. Security Standards - Organizational, Policies & Procedures, and Documentation Requirements

6. Basics of Risk Analysis & Risk Management

7. Implementation for the Small Provider

1 Security 101 for Covered Entities

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information”, found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule, and assistance with implementation of the security standards. While there is no one approach that will guarantee successful implementation of all the security standards, this series aims to explain specific requirements, the thought process behind those requirements, and possible ways to address the provisions. This first paper in the series provides an overview of the Security Rule and its intersection with the HIPAA Privacy Rule, the provisions of which are at 45 CFR Part 160 and Part 164, Subparts A and E.

Compliance Deadlines

No later than April 20, 2005 for all covered entities except small health plans which have until no later than April 20, 2006.

Administrative Simplification

Congress passed the Administrative Simplification provisions of HIPAA, among other things, to protect the privacy and security of certain health information, and promote efficiency in the health care industry through the use of standardized electronic transactions.

The health care industry is working to meet these challenging goals through successful implementation of the Administrative Simplification provisions of HIPAA. The Department of Health and Human Services (HHS) has published rules implementing a number of provisions, including:

Security Regulation

The final Security Rule can be viewed and downloaded from the CMS Website at: http://www.cms.hhs.gov/SecurityStandard/ under the “Regulation” page.

CMS CENTERS for MEDICARE & MEDICAID SERVICES

Volume 2 /Paper 1 1 11/2004:rev. 3/2007

HIPAA Security Series: 2

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part 2: Security Standards: Administrative Safeguards

What are Administrative Safeguards?

“administrative actions, and 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.”

The Importance of Risk Analysis and Risk Management
1. Risk Analysis
2. Risk Management
3. Sanction Policy
4. Information System Activity Review

Assigned Security Responsibility

Workforce Security
1. Authorization and/or Supervision
2. Workforce Clearance Procedure
3. Termination Procedures

Information Access Management
1. Isolating Clearinghouse Functions
2. Access Authorization
3. Access Establishment & Modification

Security awareness and Training
1. Security Reminders
2. Protection from Malicious Software
3. Login Monitoring
4. Password Management

Security Incident Procedures
Response and reporting

Contingency Plan
1. Data Backup Plan
2. Disaster Recovery Plan
3. Emergency Mode Operation Plan
4. Testing and Revision Procedures
5. Application and Data Critically Analysis

Business Associate Contracts

HIPAA **Security** SERIES

Security Topics

1. Security 101 for Covered Entities

★ 2. Security Standards - Administrative Safeguards

3. Security Standards - Physical Safeguards

4. Security Standards - Technical Safeguards

5. Security Standards - Organizational, Policies and Procedures and Documentation Requirements

6. Basics of Risk Analysis and Risk Management

7. Implementation for the Small Provider

2 Security Standards: Administrative Safeguards

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

Compliance Deadlines
No later than April 20, 2005 for all covered entities except small health plans, which have until no later than April 20, 2006.

CMS recommends that covered entities read the first paper in this series, “Security 101 for Covered Entities” before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This second paper in the series is devoted to the standards for Administrative Safeguards and their implementation specifications and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, “Security 101 for Covered Entities,” visit the CMS website at: *www.cms.hhs.gov/SecurityStandard/* under the “Regulation” page.

Background

An important step in protecting electronic protected health information (EPHI) is to implement reasonable and appropriate administrative safeguards that establish the foundation for a covered entity’s security program. The Administrative Safeguards standards in the Security Rule, at § 164.308, were developed to accomplish this purpose.

HIPAA Security Series: 3

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part 3: Security Standards: Physical Safeguards

What are Physical Safeguards?

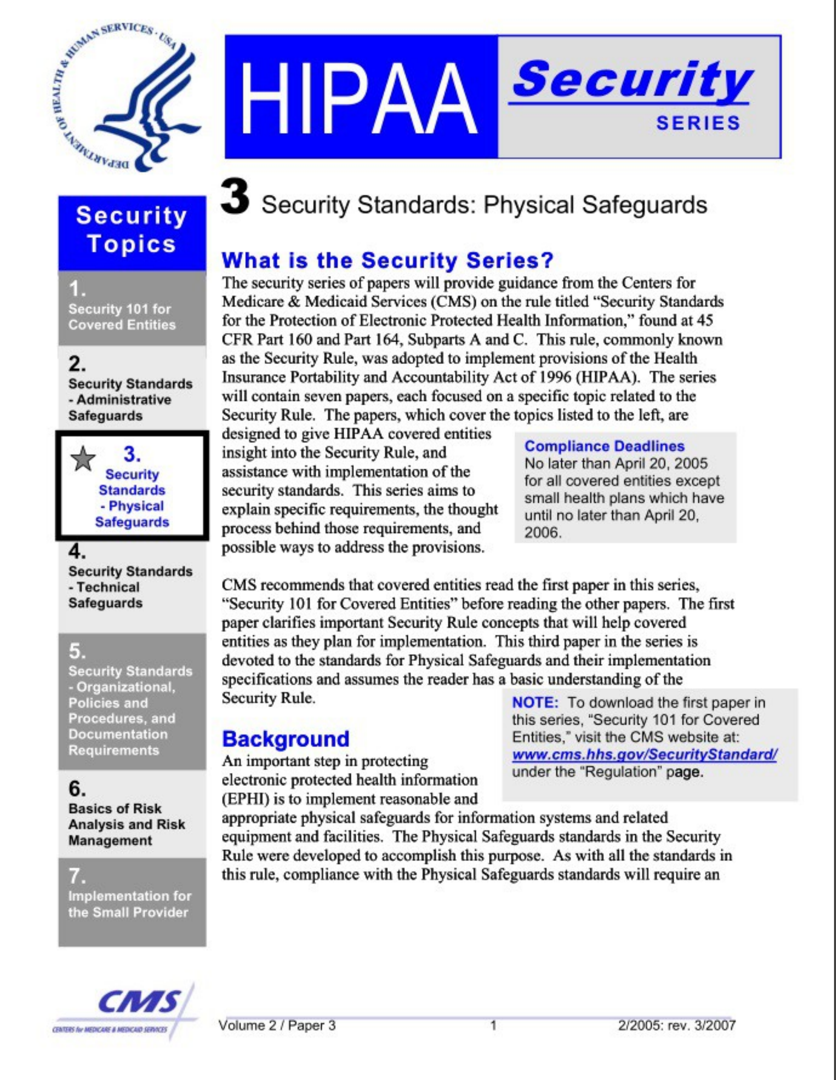
“physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

Facility Access Controls
1. Contingency Operations
2. Facility Security Plan
3. Access Control and Validation Procedures
4. Maintenance Records

Workstation Use

Workstation Security

Device and Media Controls
1. Disposal
2. Media re-use
3. Accountability
4. Data Backup and Storage



DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

HIPAA **Security** SERIES

Security Topics

1. Security 101 for Covered Entities
2. Security Standards - Administrative Safeguards
3. ★ Security Standards - Physical Safeguards
4. Security Standards - Technical Safeguards
5. Security Standards - Organizational, Policies and Procedures, and Documentation Requirements
6. Basics of Risk Analysis and Risk Management
7. Implementation for the Small Provider

3 Security Standards: Physical Safeguards

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule, and assistance with implementation of the security standards. This series aims to explain specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

Compliance Deadlines
No later than April 20, 2005 for all covered entities except small health plans which have until no later than April 20, 2006.

CMS recommends that covered entities read the first paper in this series, “Security 101 for Covered Entities” before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This third paper in the series is devoted to the standards for Physical Safeguards and their implementation specifications and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, “Security 101 for Covered Entities,” visit the CMS website at: ***www.cms.hhs.gov/SecurityStandard/*** under the “Regulation” page.

Background

An important step in protecting electronic protected health information (EPHI) is to implement reasonable and appropriate physical safeguards for information systems and related equipment and facilities. The Physical Safeguards standards in the Security Rule were developed to accomplish this purpose. As with all the standards in this rule, compliance with the Physical Safeguards standards will require an

CMS CENTERS for MEDICARE & MEDICAID SERVICES

HIPAA Security Series: 4

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part 4: Security Standards: Technical Safeguards

What are Technical Safeguards?

“the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

Access Control: *Implement technical policies and procedures for electronic information systems that allow access only to those persons that have been granted access rights.*

1. Unique User Identification
2. Emergency Access Procedure
3. Automatic Logoff
4. Encryption and Decryption

Audit Controls: *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems*

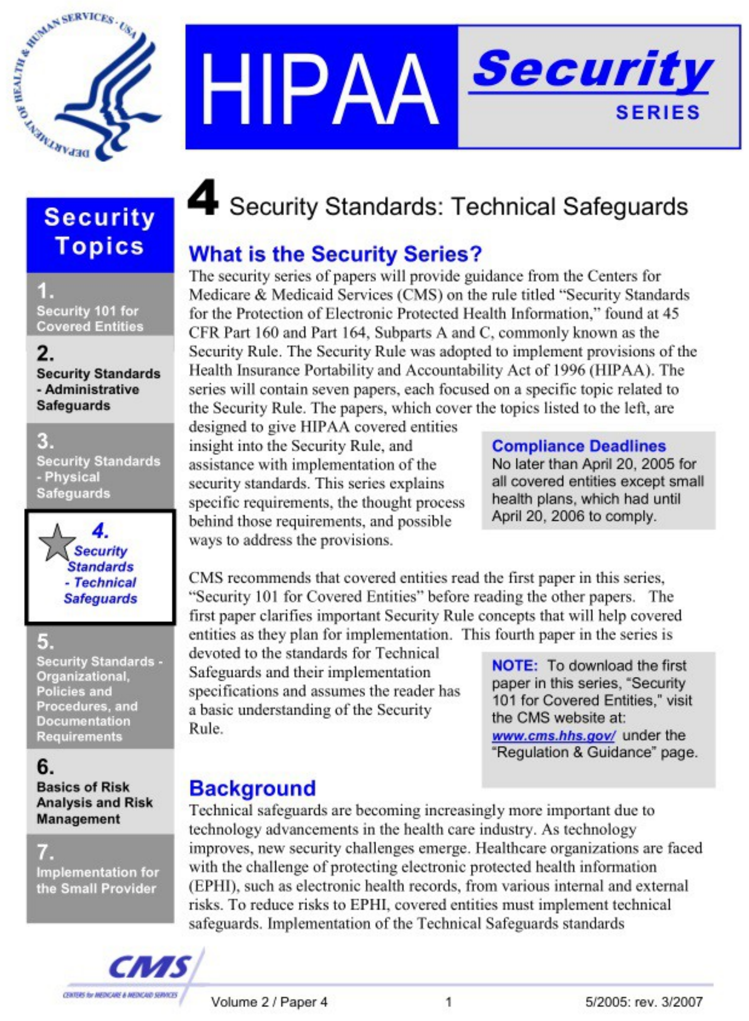
Integrity of Data: *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*

1. Mechanism to Authenticate ePHI

Person or Entity Authentication: *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*

Transmission Security: *Implement technical security measures to guard against unauthorized access*

1. Integrity Controls
2. Encryption



HIPAA Security SERIES

4 Security Standards: Technical Safeguards

Security Topics

1. Security 101 for Covered Entities
2. Security Standards - Administrative Safeguards
3. Security Standards - Physical Safeguards
4. ★ *Security Standards - Technical Safeguards*
5. Security Standards - Organizational, Policies and Procedures, and Documentation Requirements
6. Basics of Risk Analysis and Risk Management
7. Implementation for the Small Provider

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule, and assistance with implementation of the security standards. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

Compliance Deadlines
No later than April 20, 2005 for all covered entities except small health plans, which had until April 20, 2006 to comply.

CMS recommends that covered entities read the first paper in this series, “Security 101 for Covered Entities” before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This fourth paper in the series is devoted to the standards for Technical Safeguards and their implementation specifications and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, “Security 101 for Covered Entities,” visit the CMS website at: www.cms.hhs.gov/ under the “Regulation & Guidance” page.

Background

Technical safeguards are becoming increasingly more important due to technology advancements in the health care industry. As technology improves, new security challenges emerge. Healthcare organizations are faced with the challenge of protecting electronic protected health information (EPHI), such as electronic health records, from various internal and external risks. To reduce risks to EPHI, covered entities must implement technical safeguards. Implementation of the Technical Safeguards standards

HIPAA Security Series: 5

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part 5: Security Standards: Organizational, Policies and Procedures and Documentation Requirements

Business Associate Contracts or Other Arrangements

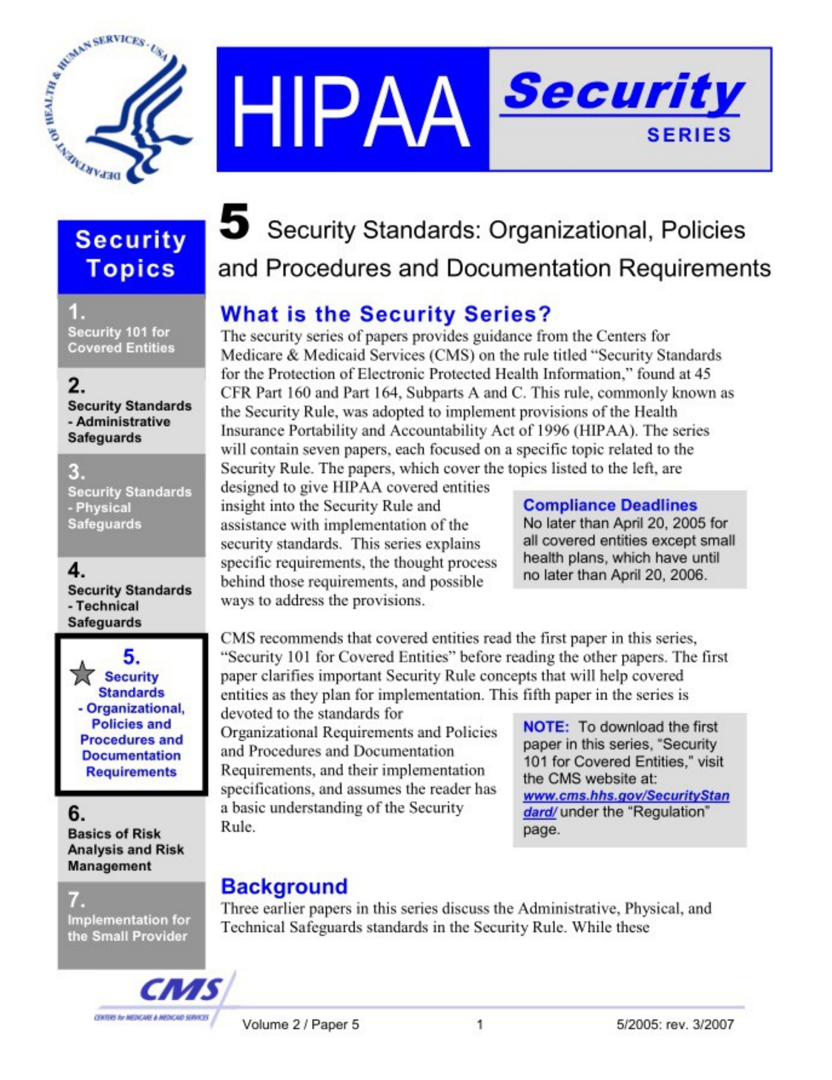
1. Business Associate Contracts
2. Other Arrangements

Requirements for Group Health Plans

Policies and Procedures

Documentation

1. Time Limit
2. Availability
3. Updates



HIPAA **Security** SERIES

5 Security Standards: Organizational, Policies and Procedures and Documentation Requirements

Security Topics

1. Security 101 for Covered Entities
2. Security Standards - Administrative Safeguards
3. Security Standards - Physical Safeguards
4. Security Standards - Technical Safeguards
5. ★ Security Standards - Organizational, Policies and Procedures and Documentation Requirements
6. Basics of Risk Analysis and Risk Management
7. Implementation for the Small Provider

What is the Security Series?

The security series of papers provides guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

Compliance Deadlines
No later than April 20, 2005 for all covered entities except small health plans, which have until no later than April 20, 2006.

CMS recommends that covered entities read the first paper in this series, “Security 101 for Covered Entities” before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This fifth paper in the series is devoted to the standards for Organizational Requirements and Policies and Procedures and Documentation Requirements, and their implementation specifications, and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, “Security 101 for Covered Entities,” visit the CMS website at: *www.cms.hhs.gov/SecurityStandard/* under the “Regulation” page.

Background

Three earlier papers in this series discuss the Administrative, Physical, and Technical Safeguards standards in the Security Rule. While these

HIPAA Security Series: 6

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part 6: Basics of Security Risk Analysis and Risk Management

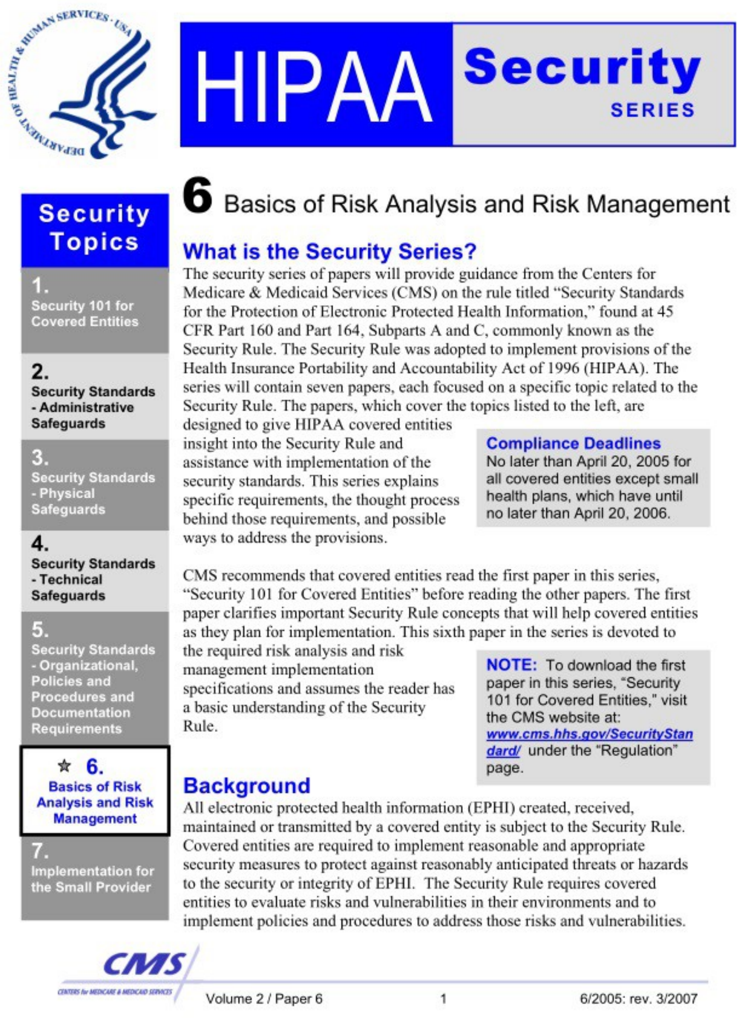
Security Rule Requirements for Risk Analysis and Risk Management

Important Definitions to Understand
- VULNERABILITY
- THREAT
- RISK

Example Risk Analysis and Risk Management Steps

Example Risk Analysis Steps
1. Identify the Scope of the Analysis
2. Gather Data
3. Identify and Document Potential Threats and Vulnerabilities
4. Assess Current Security Measures
5. Determine the Likelihood of Threat Occurrence
6. Determine the Potential Impact of Threat Occurrence
7. Determine the Level of Risk
8. Identify Security Measures and Finalize Documentation

Example Risk Management Steps
1. Develop and Implement a Risk Management Plan
2. Implement Security Measures
3. Evaluate and Maintain Security Measures



HIPAA Security SERIES

Security Topics

1. Security 101 for Covered Entities

2. Security Standards - Administrative Safeguards

3. Security Standards - Physical Safeguards

4. Security Standards - Technical Safeguards

5. Security Standards - Organizational, Policies and Procedures and Documentation Requirements

☆ 6. Basics of Risk Analysis and Risk Management

7. Implementation for the Small Provider

6 Basics of Risk Analysis and Risk Management

What is the Security Series?

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed to the left, are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

Compliance Deadlines
No later than April 20, 2005 for all covered entities except small health plans, which have until no later than April 20, 2006.

CMS recommends that covered entities read the first paper in this series, “Security 101 for Covered Entities” before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This sixth paper in the series is devoted to the required risk analysis and risk management implementation specifications and assumes the reader has a basic understanding of the Security Rule.

NOTE: To download the first paper in this series, “Security 101 for Covered Entities,” visit the CMS website at: www.cms.hhs.gov/SecurityStandard/ under the “Regulation” page.

Background

All electronic protected health information (EPHI) created, received, maintained or transmitted by a covered entity is subject to the Security Rule. Covered entities are required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. The Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities.

CMS CENTERS for MEDICARE & MEDICAID SERVICES

Volume 2 / Paper 6 1 6/2005: rev. 3/2007

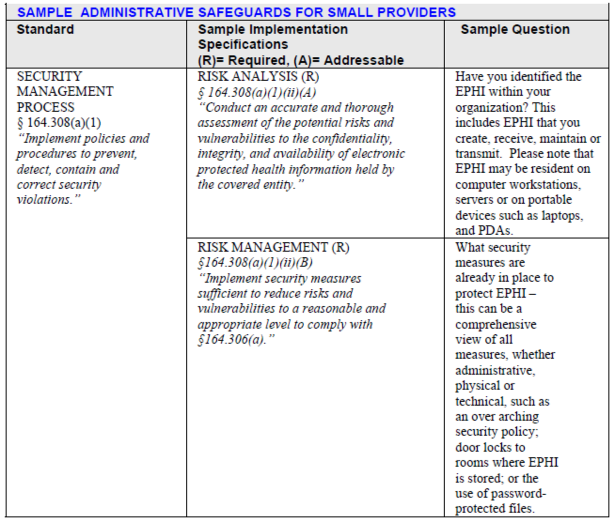
HIPAA Security Series: 7

Guidance from the Centers for Medicare and Medicaid Services (CMS) regarding the HIPAA rule “Security Standards for the Protection of Electronic Protected Health Information”

Part 7: Security Standards: Implementation for the Small Provider

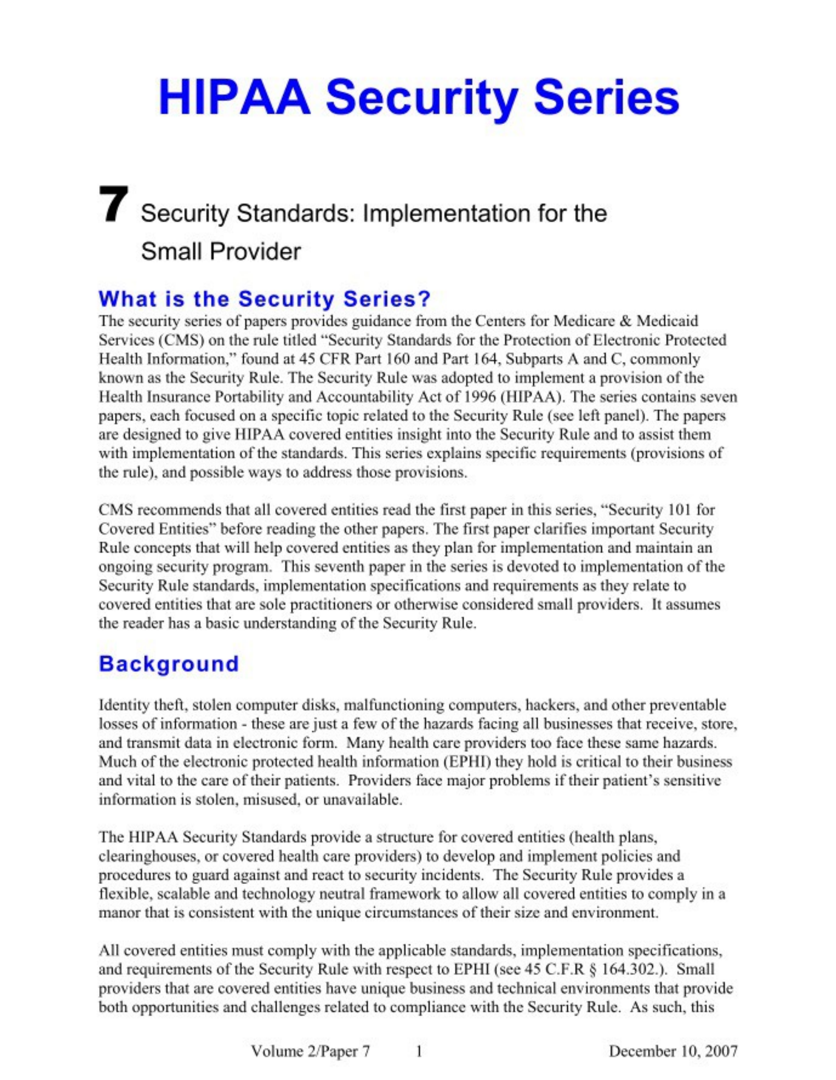
Security Rule Overview for Small Providers

Using This Resource
The tables and sample questions provided relate to the Administrative, Technical and Physical Safeguard requirements from the Security Rule, and are relevant for small providers seeking to evaluate and/or establish ePHI security practices.



SAMPLE ADMINISTRATIVE SAFEGUARDS FOR SMALL PROVIDERS

Standard	Sample Implementation Specifications (R)= Required, (A)= Addressable	Sample Question
SECURITY MANAGEMENT PROCESS § 164.308(a)(1) *“Implement policies and procedures to prevent, detect, contain and correct security violations.”*	RISK ANALYSIS (R) *§ 164.308(a)(1)(ii)(A)* *“Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”*	Have you identified the EPHI within your organization? This includes EPHI that you create, receive, maintain or transmit. Please note that EPHI may be resident on computer workstations, servers or on portable devices such as laptops, and PDAs.
	RISK MANAGEMENT (R) *§164.308(a)(1)(ii)(B)* *“Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).”*	What security measures are already in place to protect EPHI – this can be a comprehensive view of all measures, whether administrative, physical or technical, such as an over arching security policy; door locks to rooms where EPHI is stored; or the use of password-protected files.



HIPAA Security Series

7 Security Standards: Implementation for the Small Provider

What is the Security Series?

The security series of papers provides guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement a provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series contains seven papers, each focused on a specific topic related to the Security Rule (see left panel). The papers are designed to give HIPAA covered entities insight into the Security Rule and to assist them with implementation of the standards. This series explains specific requirements (provisions of the rule), and possible ways to address those provisions.

CMS recommends that all covered entities read the first paper in this series, “Security 101 for Covered Entities” before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation and maintain an ongoing security program. This seventh paper in the series is devoted to implementation of the Security Rule standards, implementation specifications and requirements as they relate to covered entities that are sole practitioners or otherwise considered small providers. It assumes the reader has a basic understanding of the Security Rule.

Background

Identity theft, stolen computer disks, malfunctioning computers, hackers, and other preventable losses of information - these are just a few of the hazards facing all businesses that receive, store, and transmit data in electronic form. Many health care providers too face these same hazards. Much of the electronic protected health information (EPHI) they hold is critical to their business and vital to the care of their patients. Providers face major problems if their patient’s sensitive information is stolen, misused, or unavailable.

The HIPAA Security Standards provide a structure for covered entities (health plans, clearinghouses, or covered health care providers) to develop and implement policies and procedures to guard against and react to security incidents. The Security Rule provides a flexible, scalable and technology neutral framework to allow all covered entities to comply in a manor that is consistent with the unique circumstances of their size and environment.

All covered entities must comply with the applicable standards, implementation specifications, and requirements of the Security Rule with respect to EPHI (see 45 C.F.R § 164.302.). Small providers that are covered entities have unique business and technical environments that provide both opportunities and challenges related to compliance with the Security Rule. As such, this

Volume 2/Paper 7 1 December 10, 2007

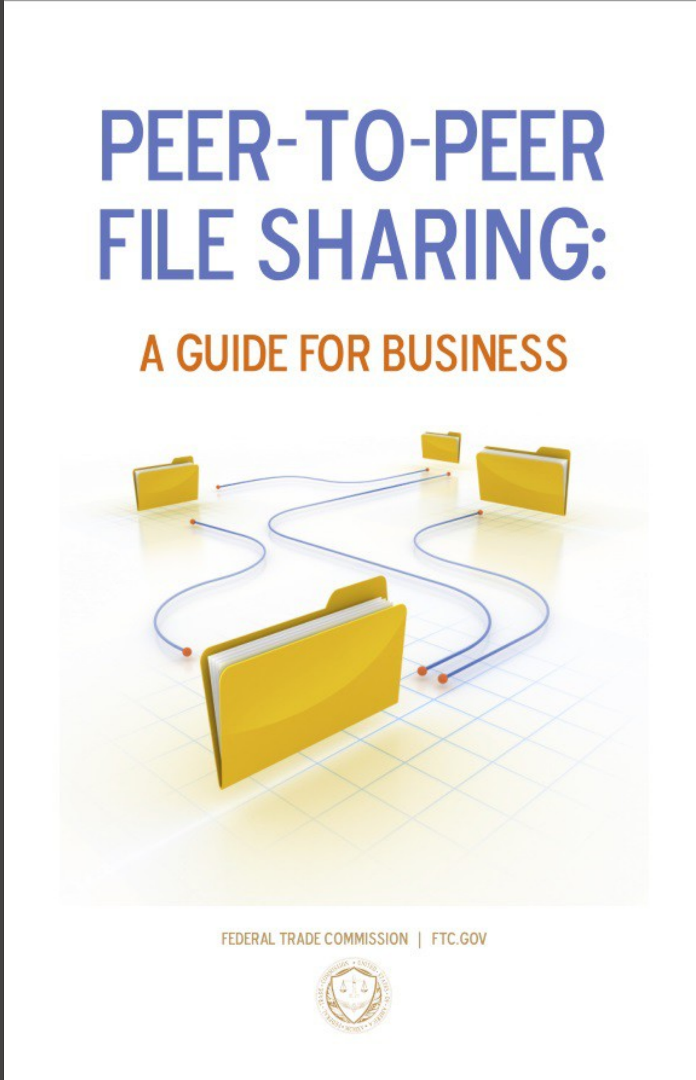
FTC: Peer to peer file sharing

ALL software products and computer devices that communicate and manipulate electronic Protected Health Information (ePHI) must have data encryption between end points of the link

This means that a computer, laptop, tablet or smartphone that is connecting to a network or cloud server to retrieve patient information must maintain an encrypted data link between the device and the server

All application programs that provide access to ePHI will include data encryption

Furthermore, all ePHI data stored on a device (network server, laptop, tablet, smartphone) must be held in an encrypted format, that will allow access to authorized personnel only



PEER-TO-PEER FILE SHARING:

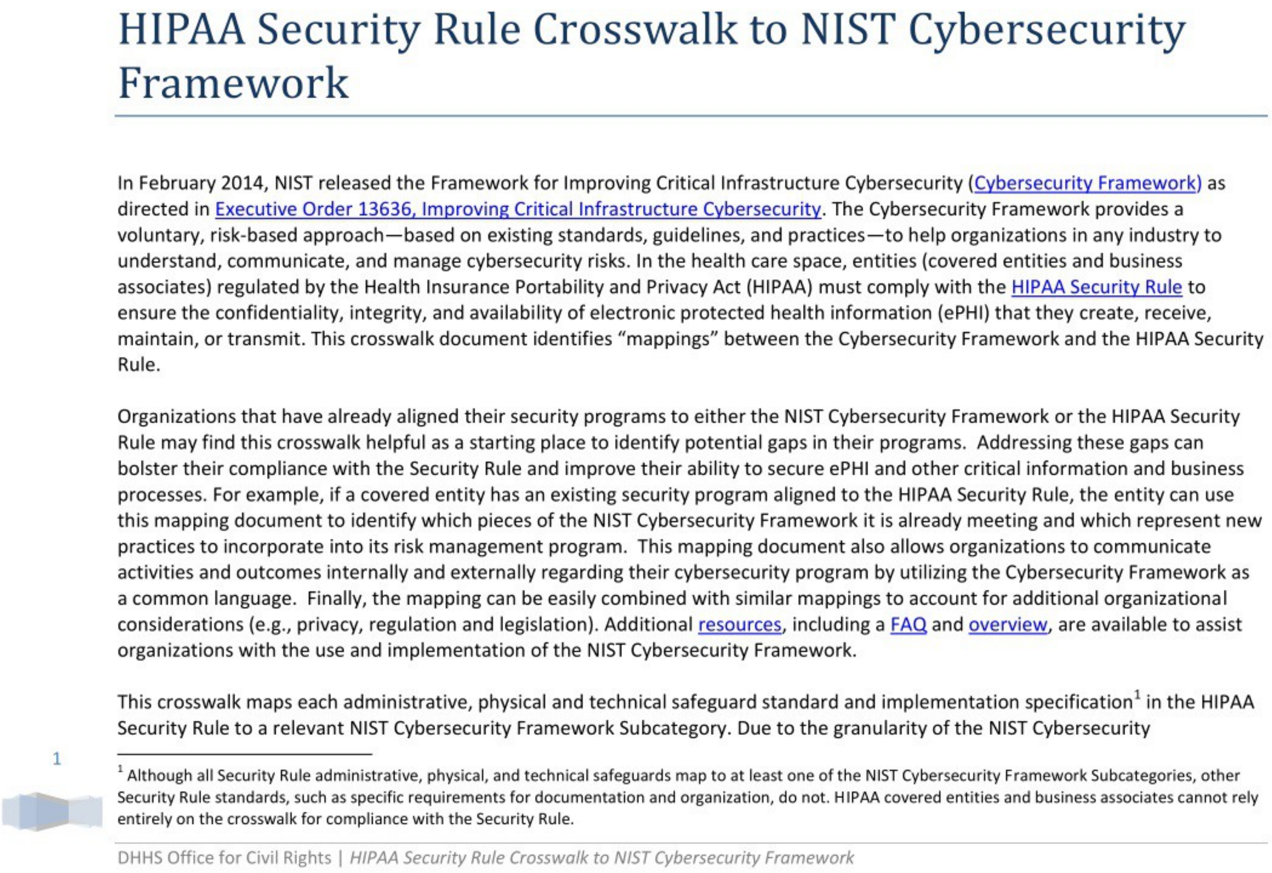
A GUIDE FOR BUSINESS

FEDERAL TRADE COMMISSION | FTC.GOV

HIPAA security alignment with NIST framework

The primary U.S. Government regulation for Critical Infrastructure Cybersecurity is the National Institute of Standards and Technology (NIST) Framework

The DHHS Office published a document that aligns the HIPAA security rules with the NIST Framework



HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a voluntary, risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Privacy Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that they create, receive, maintain, or transmit. This crosswalk document identifies “mappings” between the Cybersecurity Framework and the HIPAA Security Rule.

Organizations that have already aligned their security programs to either the NIST Cybersecurity Framework or the HIPAA Security Rule may find this crosswalk helpful as a starting place to identify potential gaps in their programs. Addressing these gaps can bolster their compliance with the Security Rule and improve their ability to secure ePHI and other critical information and business processes. For example, if a covered entity has an existing security program aligned to the HIPAA Security Rule, the entity can use this mapping document to identify which pieces of the NIST Cybersecurity Framework it is already meeting and which represent new practices to incorporate into its risk management program. This mapping document also allows organizations to communicate activities and outcomes internally and externally regarding their cybersecurity program by utilizing the Cybersecurity Framework as a common language. Finally, the mapping can be easily combined with similar mappings to account for additional organizational considerations (e.g., privacy, regulation and legislation). Additional resources, including a FAQ and overview, are available to assist organizations with the use and implementation of the NIST Cybersecurity Framework.

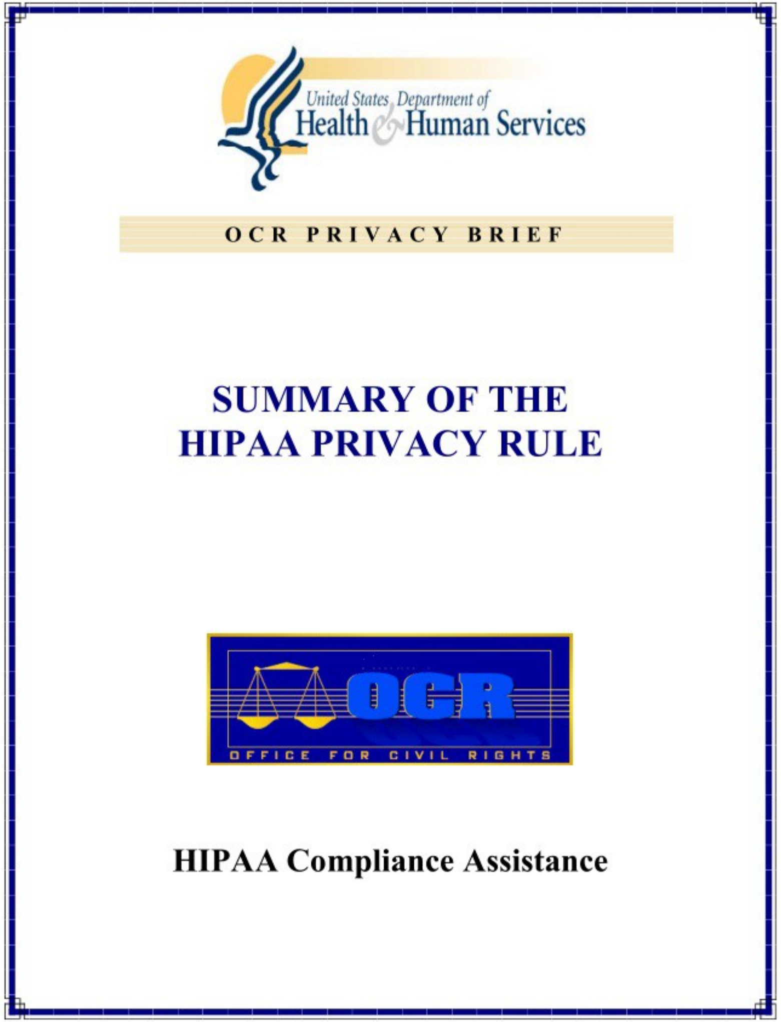
This crosswalk maps each administrative, physical and technical safeguard standard and implementation specification[1] in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework Subcategory. Due to the granularity of the NIST Cybersecurity

[1] Although all Security Rule administrative, physical, and technical safeguards map to at least one of the NIST Cybersecurity Framework Subcategories, other Security Rule standards, such as specific requirements for documentation and organization, do not. HIPAA covered entities and business associates cannot rely entirely on the crosswalk for compliance with the Security Rule.

U.S. Department of Health and Human Services: Office for Civil Rights

Summary of the HIPAA Privacy Rule

Introduction
Statutory & Regulatory Background
Who is Covered by the Privacy Rule
Business Associates
What Information is Protected
General Principle for Uses and Disclosures
Permitted Uses and Disclosures
Authorized Uses and Disclosures
Limiting Uses and Disclosures to the Minimum Necessary
Notice and Other Individual Rights
Administrative Requirements
Organizational Options
Other Provisions: Personal Representatives and Minors
State Law
Enforcement and Penalties for Noncompliance
Compliance Dates
Copies of the Rule & Related Materials
End Notes



United States Department of Health & Human Services

OCR PRIVACY BRIEF

SUMMARY OF THE
HIPAA PRIVACY RULE

OCR
OFFICE FOR CIVIL RIGHTS

HIPAA Compliance Assistance

PART 1:

HIPAA RULES OVERVIEW

1 Introduction

2 Security and Privacy

3 Risk Assessment and Data Breach

4 Attempted Intrusion

5 Supporting Documents

Guidance on Risk Analysis Requirements

Guidance to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI).

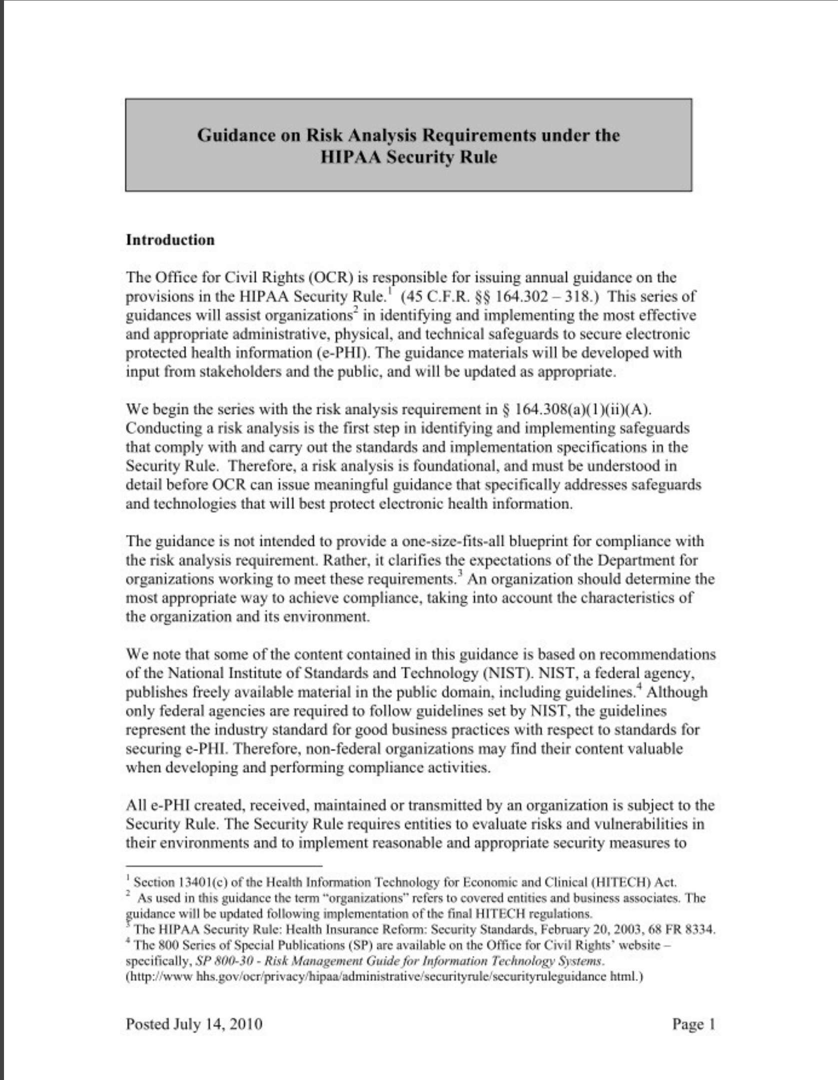
Risk Analysis Requirements under the Security Rule

Important Definitions

- Vulnerability Threat
- Threat
- Risk

Elements of a Risk Analysis

- Scope of the Analysis
- Data Collection
- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Measures
- Determine the Likelihood of Threat Occurrence
- Determine the Potential Impact of Threat Occurrence
- Determine the Level of Risk
- Finalize Documentation
- Periodic Review and Updates to the Risk Assessment



Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.[1] (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations[2] in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate.

We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.[3] An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.

We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.[4] Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to

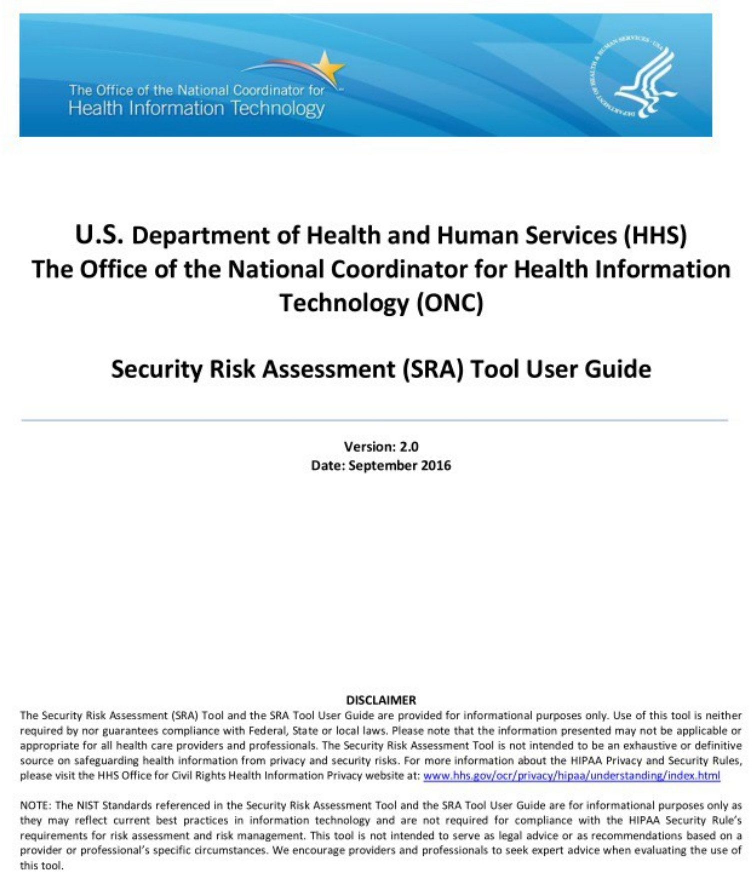
[1] Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.
[2] As used in this guidance the term "organizations" refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.
[3] The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
[4] The 800 Series of Special Publications (SP) are available on the Office for Civil Rights' website – specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems*. (http://www hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance html.)

Posted July 14, 2010 Page 1

Security Risk Assessment Tool (HHS)

A Covered Entity can evaluate the risk of a data breach using a software tool that is provide by HHS

Acronym Index
1.Introduction
 1.1. Purpose
 1.2. Audience
 1.3. What is the SRA Tool?
 1.4. The Role of the SRA Tool in a Risk Assessment
 1.5. What the SRA Tool Is Not
2.Downloading the SRA Tool
 2.1. Downloading the SRA Tool (Windows version)
 2.2. Downloading the SRA Tool (iPad version)
3.Using the SRA Tool
 3.1. Creating and Updating Users
 3.2. Adding Information About Your Practice
 3.3. Adding Information about Business Associates
 3.4. Adding Information about IT Assets
 3.5. SRA Tool Login and Question Window
 3.6. Answering SRA Tool Questions
 3.7. Reporting
 3.8. Using the Navigator
 3.9. Exporting Data from the SRA Tool
 3.10. Importing Data into the SRA Tool
 3.11. Logging Out of the SRA Tool
4.Uninstalling the SRA Tool
Appendix A. Addressable and Required Specifications



The Office of the National Coordinator for
Health Information Technology

U.S. Department of Health and Human Services (HHS)
The Office of the National Coordinator for Health Information Technology (ONC)

Security Risk Assessment (SRA) Tool User Guide

Version: 2.0
Date: September 2016

DISCLAIMER

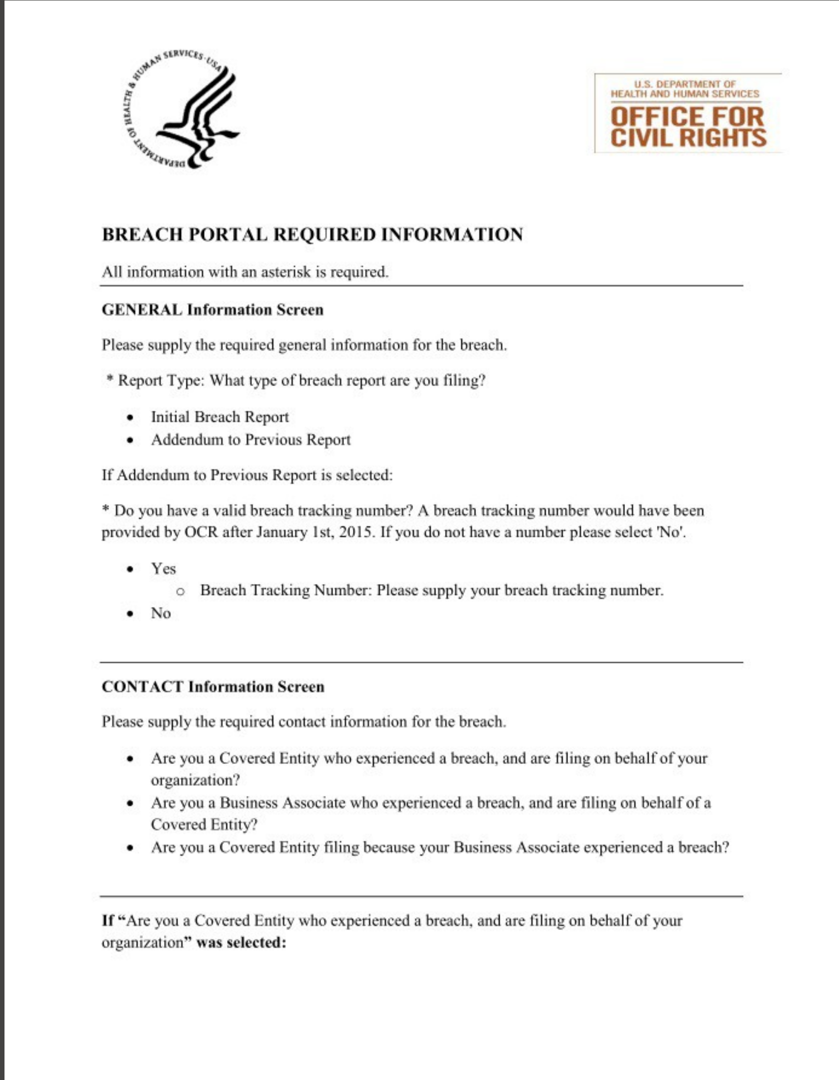
The Security Risk Assessment (SRA) Tool and the SRA Tool User Guide are provided for informational purposes only. Use of this tool is neither required by nor guarantees compliance with Federal, State or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and professionals. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks. For more information about the HIPAA Privacy and Security Rules, please visit the HHS Office for Civil Rights Health Information Privacy website at: www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

NOTE: The NIST Standards referenced in the Security Risk Assessment Tool and the SRA Tool User Guide are for informational purposes only as they may reflect current best practices in information technology and are not required for compliance with the HIPAA Security Rule's requirements for risk assessment and risk management. This tool is not intended to serve as legal advice or as recommendations based on a provider or professional's specific circumstances. We encourage providers and professionals to seek expert advice when evaluating the use of this tool.

BREACH PORTAL REQUIRED INFORMATION

After the occurrence of a data breach, a report must be filed immediately with the Department of Health and Human Services

Failure to do so can result in civil and criminal penalties



DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

BREACH PORTAL REQUIRED INFORMATION

All information with an asterisk is required.

GENERAL Information Screen

Please supply the required general information for the breach.

* Report Type: What type of breach report are you filing?

- Initial Breach Report
- Addendum to Previous Report

If Addendum to Previous Report is selected:

* Do you have a valid breach tracking number? A breach tracking number would have been provided by OCR after January 1st, 2015. If you do not have a number please select 'No'.

- Yes
  - Breach Tracking Number: Please supply your breach tracking number.
- No

CONTACT Information Screen

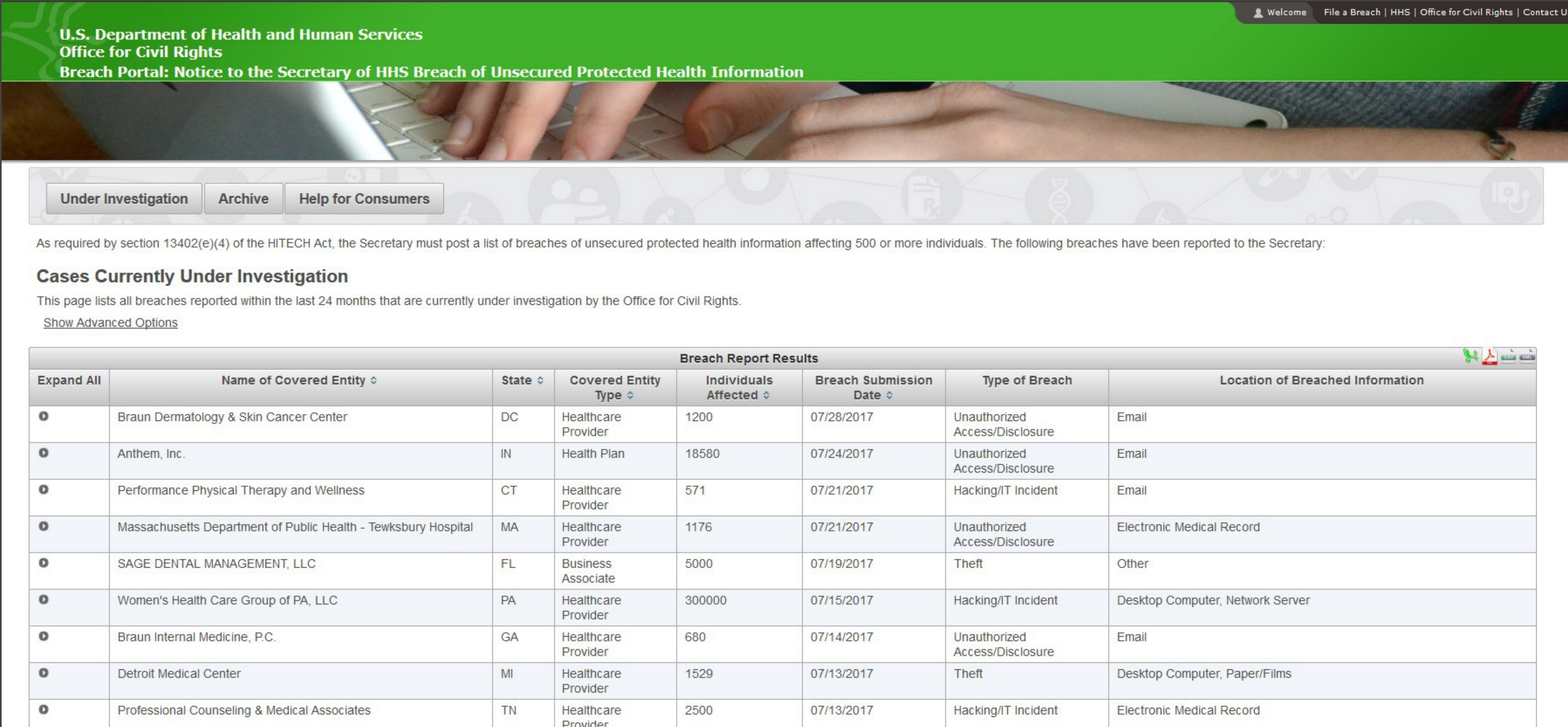
Please supply the required contact information for the breach.

- Are you a Covered Entity who experienced a breach, and are filing on behalf of your organization?
- Are you a Business Associate who experienced a breach, and are filing on behalf of a Covered Entity?
- Are you a Covered Entity filing because your Business Associate experienced a breach?

If "Are you a Covered Entity who experienced a breach, and are filing on behalf of your organization" **was selected:**

File the breach report using the HHS portal

View cases under investigation (public record)



U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

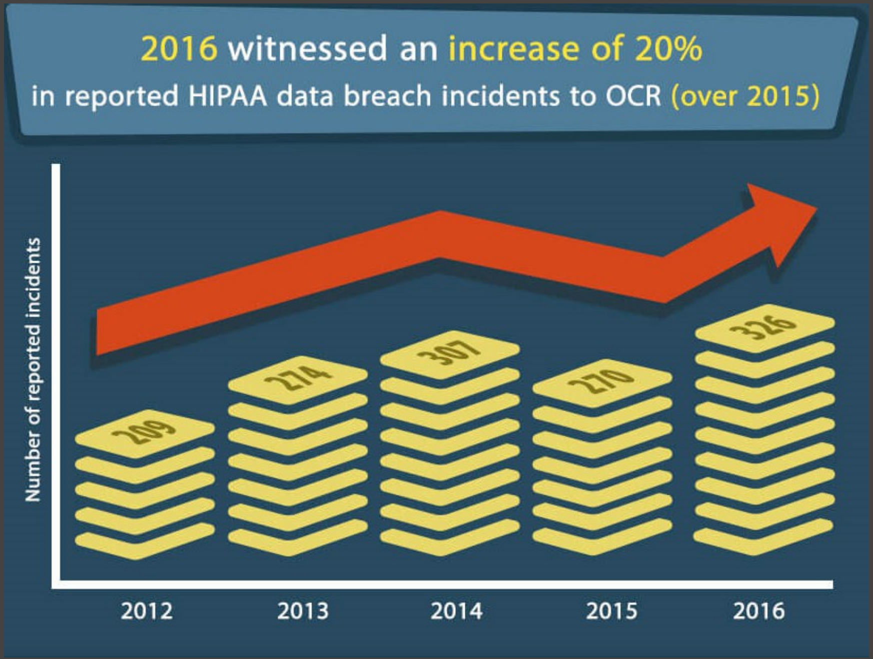
Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

Breach Report Results

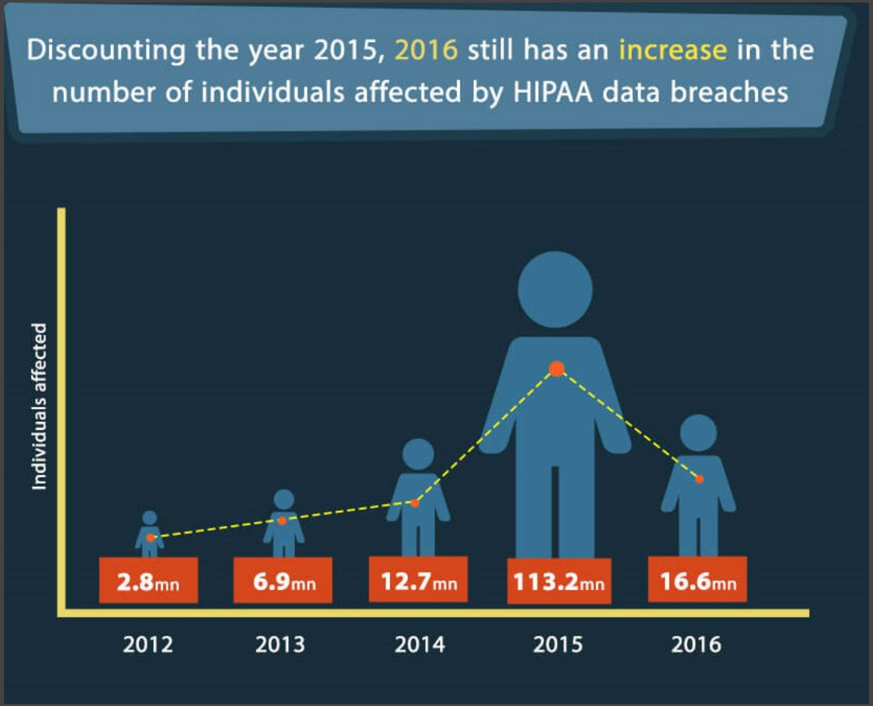
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	Braun Dermatology & Skin Cancer Center	DC	Healthcare Provider	1200	07/28/2017	Unauthorized Access/Disclosure	Email
●	Anthem, Inc.	IN	Health Plan	18580	07/24/2017	Unauthorized Access/Disclosure	Email
●	Performance Physical Therapy and Wellness	CT	Healthcare Provider	571	07/21/2017	Hacking/IT Incident	Email
●	Massachusetts Department of Public Health - Tewksbury Hospital	MA	Healthcare Provider	1176	07/21/2017	Unauthorized Access/Disclosure	Electronic Medical Record
●	SAGE DENTAL MANAGEMENT, LLC	FL	Business Associate	5000	07/19/2017	Theft	Other
●	Women's Health Care Group of PA, LLC	PA	Healthcare Provider	300000	07/15/2017	Hacking/IT Incident	Desktop Computer, Network Server
●	Braun Internal Medicine, P.C.	GA	Healthcare Provider	680	07/14/2017	Unauthorized Access/Disclosure	Email
●	Detroit Medical Center	MI	Healthcare Provider	1529	07/13/2017	Theft	Desktop Computer, Paper/Films
●	Professional Counseling & Medical Associates	TN	Healthcare Provider	2500	07/13/2017	Hacking/IT Incident	Electronic Medical Record

Data source: Kays Harbor™ Technologies, (c) 2017



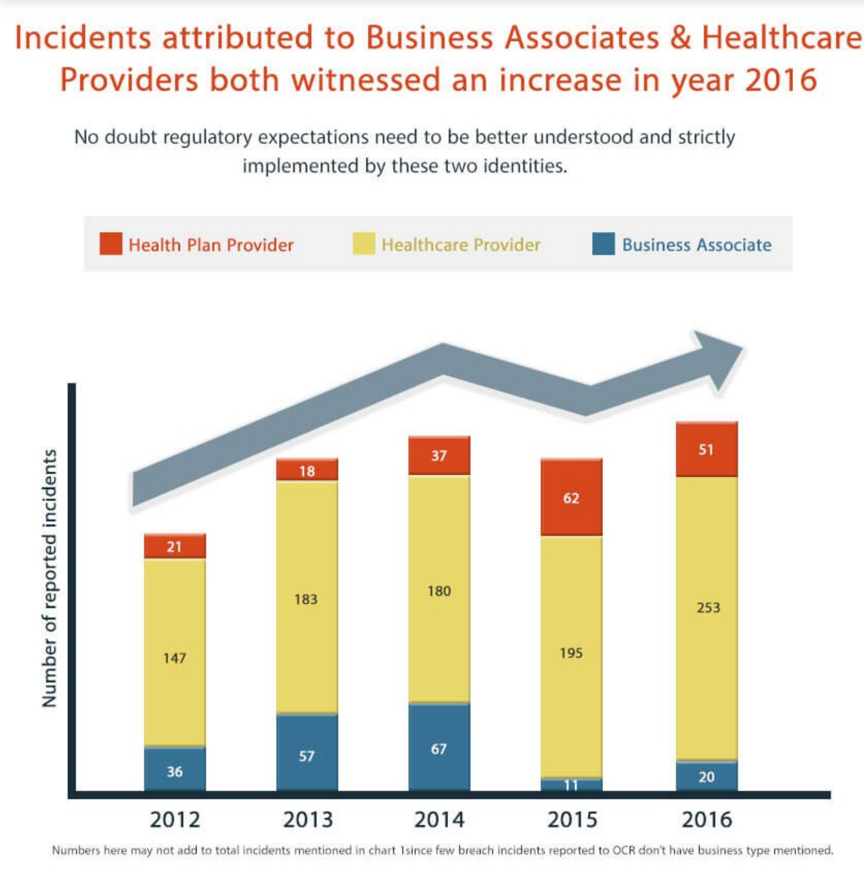
2016 witnessed an increase of 20%

in reported HIPAA data breach incidents to OCR (over 2015)



Discounting the year 2015, 2016 still has an increase in the number of individuals affected by HIPAA data breaches

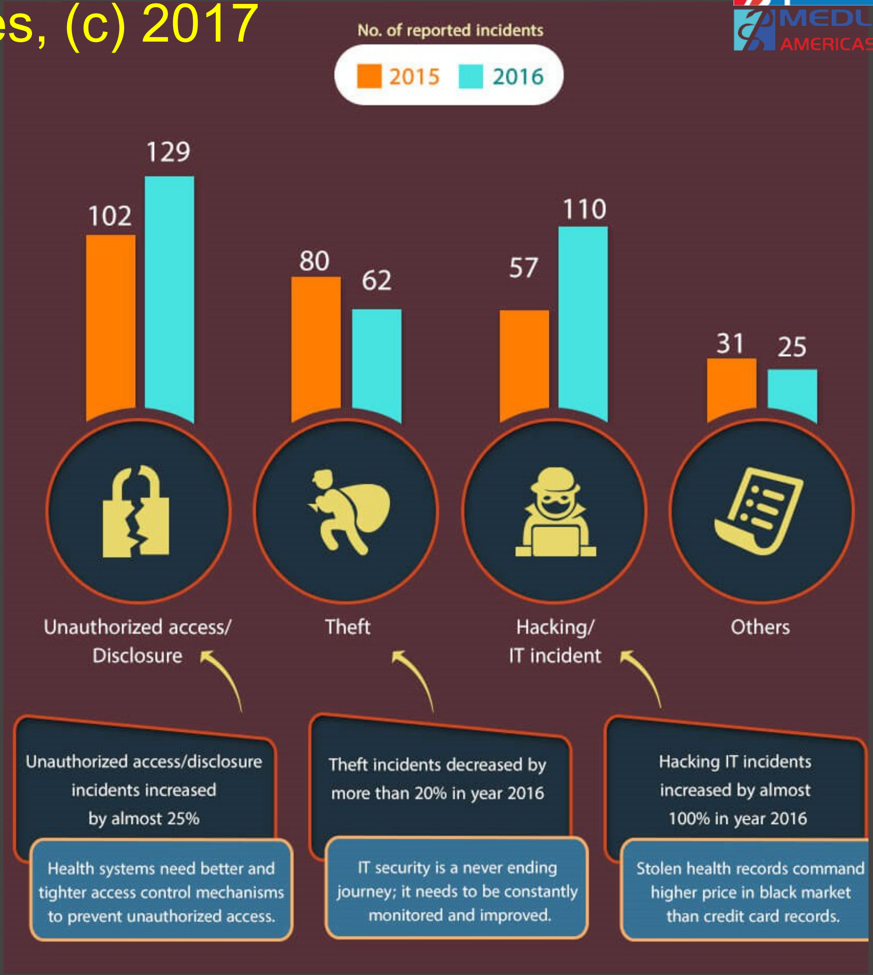
Data source: Kays Harbor™ Technologies, (c) 2017



Incidents attributed to Business Associates & Healthcare Providers both witnessed an increase in year 2016

No doubt regulatory expectations need to be better understood and strictly implemented by these two identities.

Numbers here may not add to total incidents mentioned in chart 1since few breach incidents reported to OCR don't have business type mentioned.



Unauthorized access/disclosure incidents increased by almost 25%

Health systems need better and tighter access control mechanisms to prevent unauthorized access.

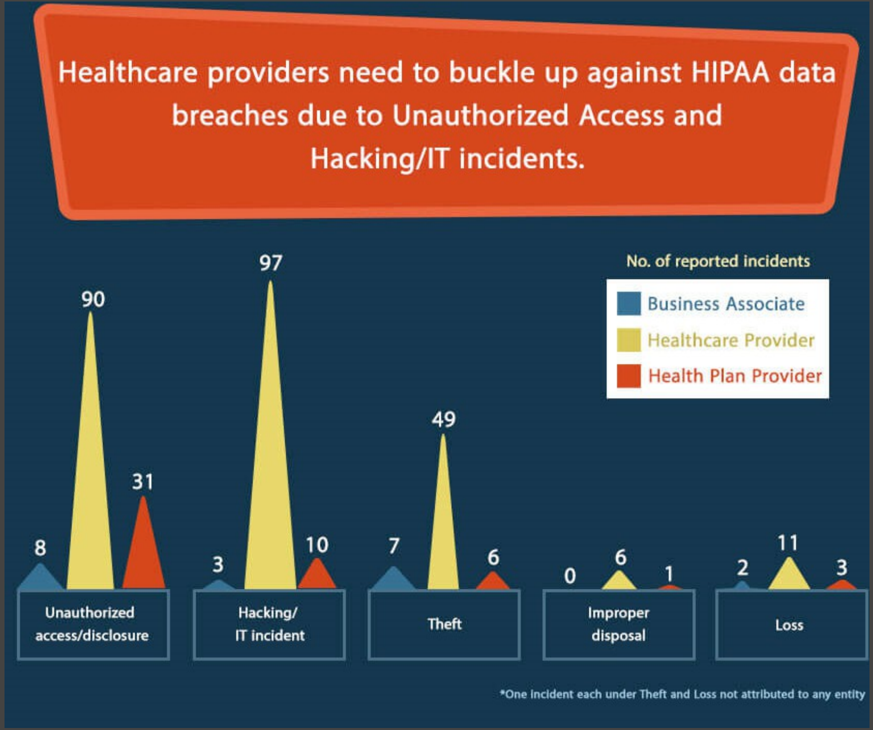
Theft incidents decreased by more than 20% in year 2016

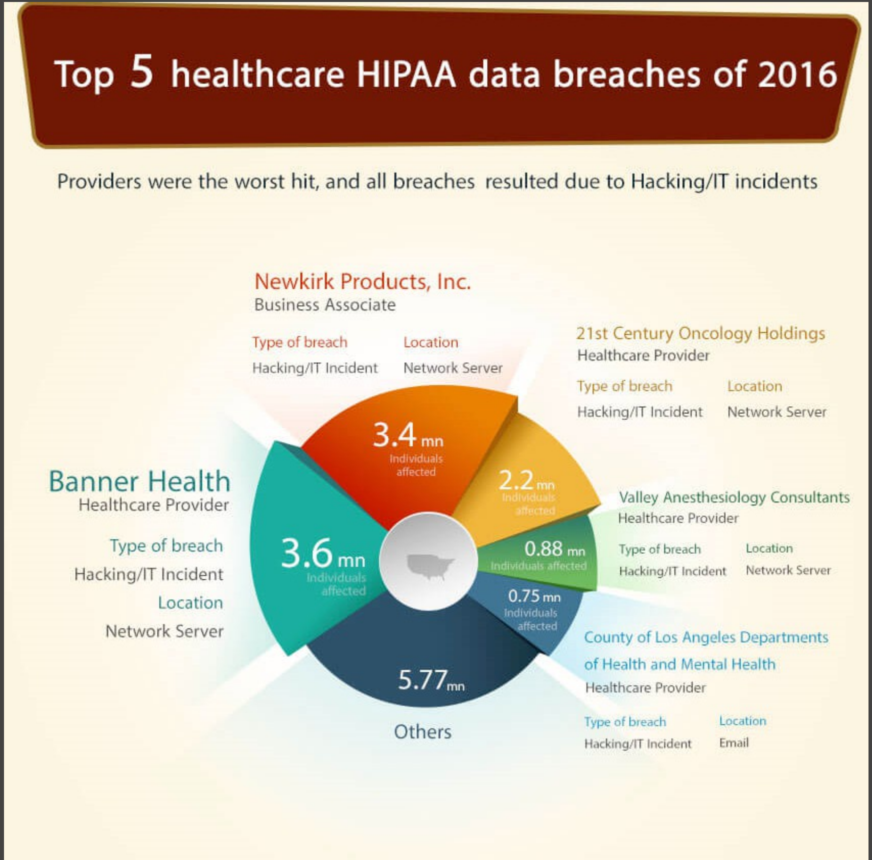
IT security is a never ending journey; it needs to be constantly monitored and improved.

Hacking IT incidents increased by almost 100% in year 2016

Stolen health records command higher price in black market than credit card records.

Data source: Kays Harbor™ Technologies, (c) 2017





PART 1:

HIPAA RULES OVERVIEW

1 Introduction

2 Security and Privacy

3 Risk Assessment and Data Breach

4 Attempted Intrusion

5 Supporting Documents

Cyber-attack!

A quick response checklist from the HHS

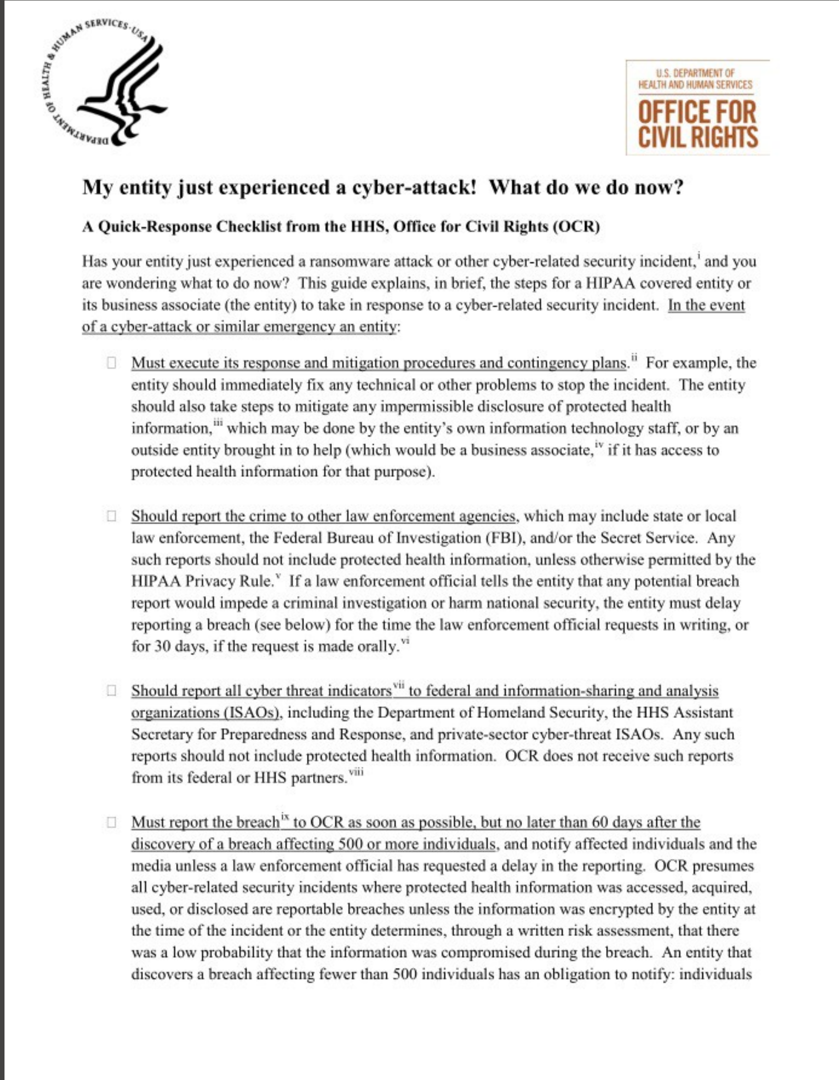
In the event of a cyber-attack or similar emergency an entity:

Must execute its response and mitigation procedures and contingency plans

Should report the crime to other law enforcement agencies

Should report all cyber threat indicators to federal and information-sharing and analysis organizations (ISAOs)

Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals



DEPARTMENT OF HEALTH & HUMAN SERVICES·USA

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

My entity just experienced a cyber-attack! What do we do now?

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

Has your entity just experienced a ransomware attack or other cyber-related security incident,[i] and you are wondering what to do now? This guide explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident. In the event of a cyber-attack or similar emergency an entity:

- □ Must execute its response and mitigation procedures and contingency plans.[ii] For example, the entity should immediately fix any technical or other problems to stop the incident. The entity should also take steps to mitigate any impermissible disclosure of protected health information,[iii] which may be done by the entity's own information technology staff, or by an outside entity brought in to help (which would be a business associate,[iv] if it has access to protected health information for that purpose).

- □ Should report the crime to other law enforcement agencies, which may include state or local law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service. Any such reports should not include protected health information, unless otherwise permitted by the HIPAA Privacy Rule.[v] If a law enforcement official tells the entity that any potential breach report would impede a criminal investigation or harm national security, the entity must delay reporting a breach (see below) for the time the law enforcement official requests in writing, or for 30 days, if the request is made orally.[vi]

- □ Should report all cyber threat indicators[vii] to federal and information-sharing and analysis organizations (ISAOs), including the Department of Homeland Security, the HHS Assistant Secretary for Preparedness and Response, and private-sector cyber-threat ISAOs. Any such reports should not include protected health information. OCR does not receive such reports from its federal or HHS partners.[viii]

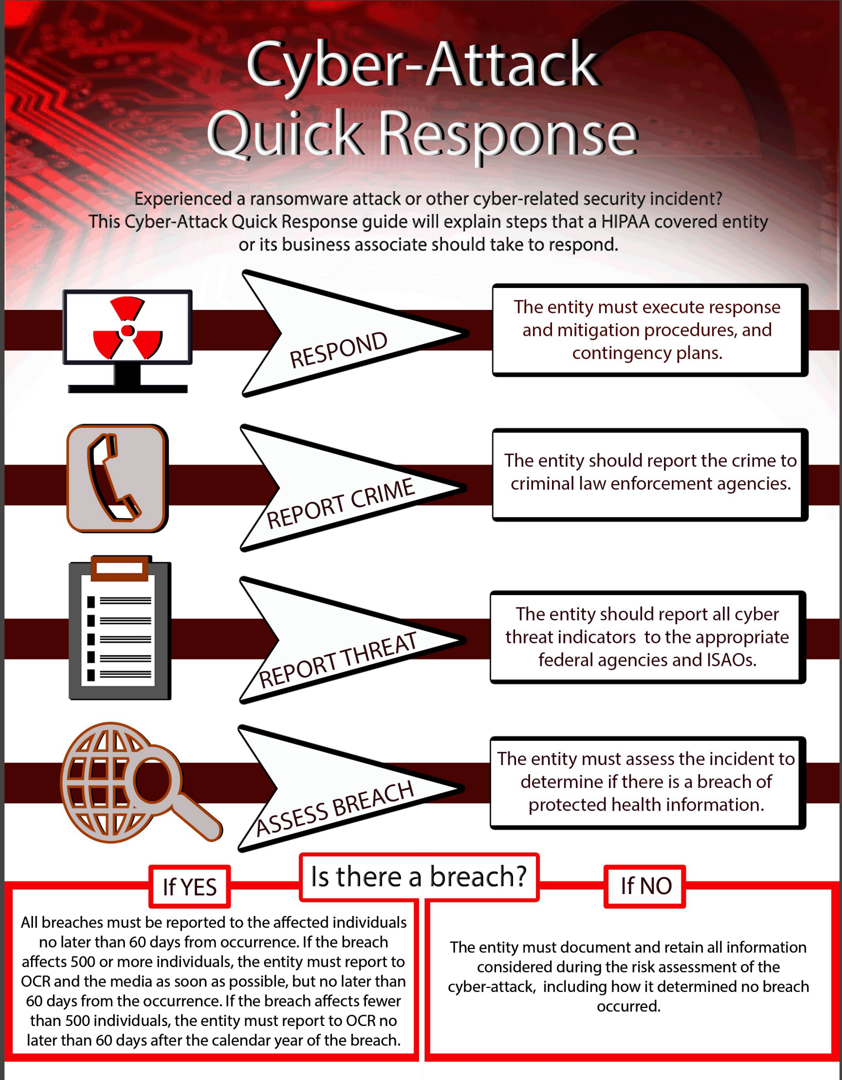
- □ Must report the breach[ix] to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach. An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify: individuals

Cyber-attack

Quick response infographic. Upon the occurrence of a cyber-attack, the following steps must be taken

- Response and mitigation procedures, contingency plans
- Report the crime to law enforcement (FBI)
- Report the threat to federal agencies
- Assess the data breach, and determine if ePHI has been compromised

Display the poster in a visible location so that staff are aware of the risks



Cyber-Attack Quick Response

Experienced a ransomware attack or other cyber-related security incident? This Cyber-Attack Quick Response guide will explain steps that a HIPAA covered entity or its business associate should take to respond.

RESPOND — The entity must execute response and mitigation procedures, and contingency plans.

REPORT CRIME — The entity should report the crime to criminal law enforcement agencies.

REPORT THREAT — The entity should report all cyber threat indicators to the appropriate federal agencies and ISAOs.

ASSESS BREACH — The entity must assess the incident to determine if there is a breach of protected health information.

Is there a breach?

If YES

All breaches must be reported to the affected individuals no later than 60 days from occurrence. If the breach affects 500 or more individuals, the entity must report to OCR and the media as soon as possible, but no later than 60 days from the occurrence. If the breach affects fewer than 500 individuals, the entity must report to OCR no later than 60 days after the calendar year of the breach.

If NO

The entity must document and retain all information considered during the risk assessment of the cyber-attack, including how it determined no breach occurred.

Ransomware Fact Sheet

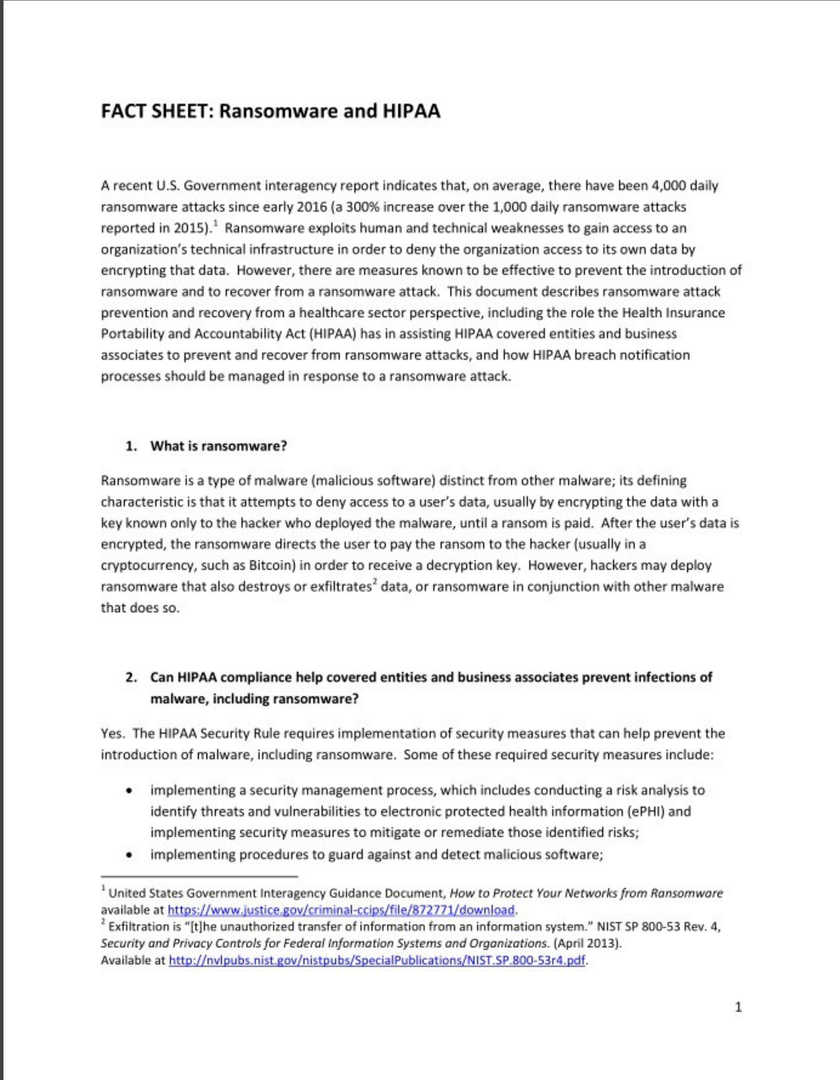
A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015). Ransomware exploits human and technical weaknesses to gain access to an organization’s technical infrastructure in order to deny the organization access to its own data by encrypting that data. The hacker demands a ransom (usually in untraceable Bitcoin) to unlock the data.

Ransomware hackers have a preference to attack healthcare entities because:

Healthcare entities have less cybersecurity protection than other entities (e.g. banks)

Healthcare entities will pay the ransom quickly due to the extreme urgency to access the patient data

Hackers can extort larger monetary values from healthcare entities compared with other segments due to the sensitive nature of the data



FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization’s technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. What is ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user’s data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user’s data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

2. Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;

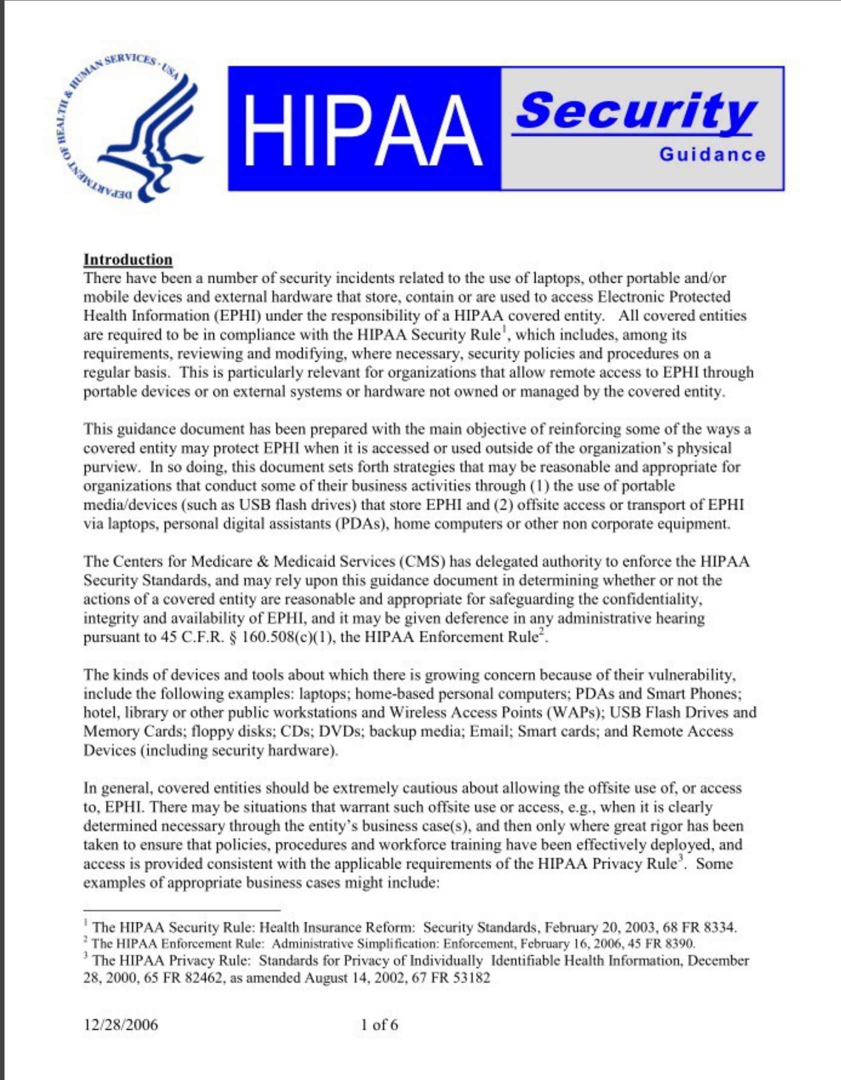
[1] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download.

[2] Exfiltration is “[t]he unauthorized transfer of information from an information system.” NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Mobile Devices and Remote Access

Guidance for the use of portable and mobile devices that access and store ePHI, the use of data storage media holding ePHI, and remote access to ePHI

Risk analysis and risk management drive policies
Policies require training
Addressing security incidents and non-compliance
Possible risk management strategies
Accessing ePHI
Storing ePHI
Transmitting ePHI



DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

HIPAA Security Guidance

Introduction

There have been a number of security incidents related to the use of laptops, other portable and/or mobile devices and external hardware that store, contain or are used to access Electronic Protected Health Information (EPHI) under the responsibility of a HIPAA covered entity. All covered entities are required to be in compliance with the HIPAA Security Rule[1], which includes, among its requirements, reviewing and modifying, where necessary, security policies and procedures on a regular basis. This is particularly relevant for organizations that allow remote access to EPHI through portable devices or on external systems or hardware not owned or managed by the covered entity.

This guidance document has been prepared with the main objective of reinforcing some of the ways a covered entity may protect EPHI when it is accessed or used outside of the organization's physical purview. In so doing, this document sets forth strategies that may be reasonable and appropriate for organizations that conduct some of their business activities through (1) the use of portable media/devices (such as USB flash drives) that store EPHI and (2) offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers or other non corporate equipment.

The Centers for Medicare & Medicaid Services (CMS) has delegated authority to enforce the HIPAA Security Standards, and may rely upon this guidance document in determining whether or not the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity and availability of EPHI, and it may be given deference in any administrative hearing pursuant to 45 C.F.R. § 160.508(c)(1), the HIPAA Enforcement Rule[2].

The kinds of devices and tools about which there is growing concern because of their vulnerability, include the following examples: laptops; home-based personal computers; PDAs and Smart Phones; hotel, library or other public workstations and Wireless Access Points (WAPs); USB Flash Drives and Memory Cards; floppy disks; CDs; DVDs; backup media; Email; Smart cards; and Remote Access Devices (including security hardware).

In general, covered entities should be extremely cautious about allowing the offsite use of, or access to, EPHI. There may be situations that warrant such offsite use or access, e.g., when it is clearly determined necessary through the entity's business case(s), and then only where great rigor has been taken to ensure that policies, procedures and workforce training have been effectively deployed, and access is provided consistent with the applicable requirements of the HIPAA Privacy Rule[3]. Some examples of appropriate business cases might include:

[1] The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
[2] The HIPAA Enforcement Rule: Administrative Simplification: Enforcement, February 16, 2006, 45 FR 8390.
[3] The HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information, December 28, 2000, 65 FR 82462, as amended August 14, 2002, 67 FR 53182

12/28/2006 1 of 6

HIPAA RULES OVERVIEW

PART 1:

1 Introduction

2 Security and Privacy

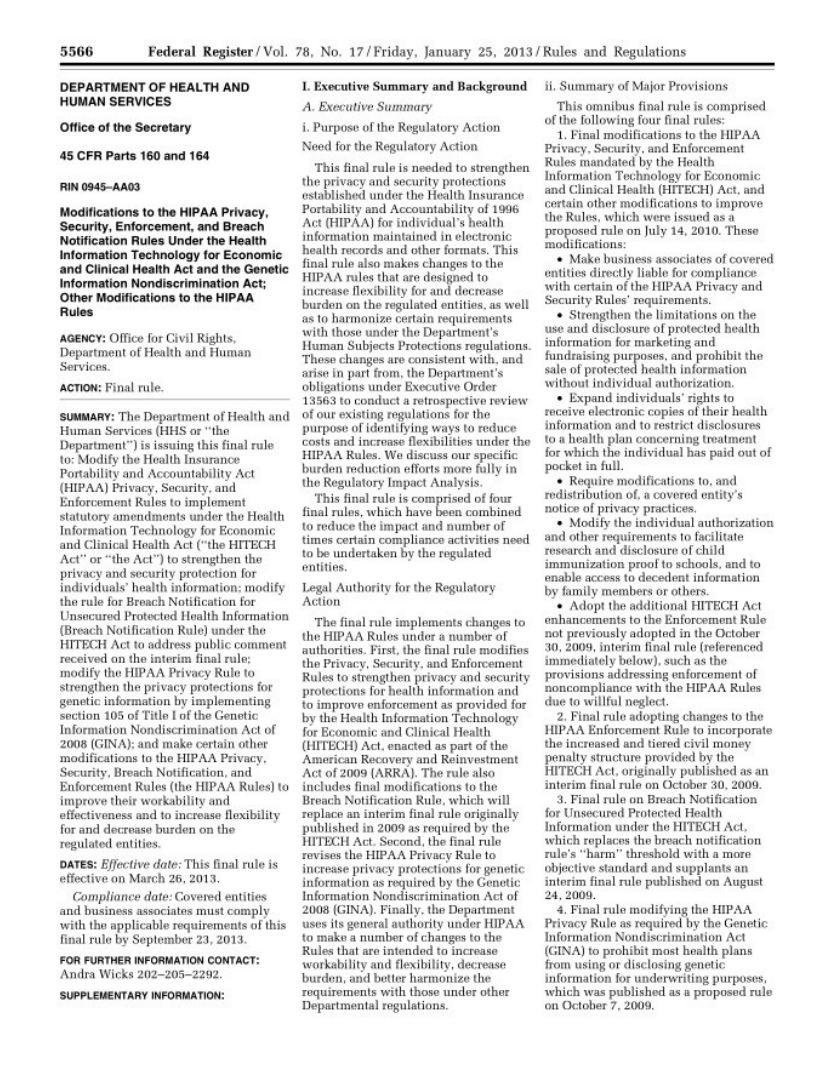
3 Risk Assessment and Data Breach

4 Attempted Intrusion

5 Supporting Documents

Federal Register

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule



5566 **Federal Register** / Vol. 78, No. 17 / Friday, January 25, 2013 / Rules and Regulations

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945–AA03

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

AGENCY: Office for Civil Rights, Department of Health and Human Services.

ACTION: Final rule.

SUMMARY: The Department of Health and Human Services (HHS or "the Department") is issuing this final rule to: Modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement statutory amendments under the Health Information Technology for Economic and Clinical Health Act ("the HITECH Act" or "the Act") to strengthen the privacy and security protection for individuals' health information; modify the rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) under the HITECH Act to address public comment received on the interim final rule; modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA); and make certain other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities.

DATES: *Effective date:* This final rule is effective on March 26, 2013.

Compliance date: Covered entities and business associates must comply with the applicable requirements of this final rule by September 23, 2013.

FOR FURTHER INFORMATION CONTACT: Andra Wicks 202–205–2292.

SUPPLEMENTARY INFORMATION:

I. Executive Summary and Background

A. Executive Summary

i. Purpose of the Regulatory Action

Need for the Regulatory Action

This final rule is needed to strengthen the privacy and security protections established under the Health Insurance Portability and Accountability of 1996 Act (HIPAA) for individual's health information maintained in electronic health records and other formats. This final rule also makes changes to the HIPAA rules that are designed to increase flexibility for and decrease burden on the regulated entities, as well as to harmonize certain requirements with those under the Department's Human Subjects Protections regulations. These changes are consistent with, and arise in part from, the Department's obligations under Executive Order 13563 to conduct a retrospective review of our existing regulations for the purpose of identifying ways to reduce costs and increase flexibilities under the HIPAA Rules. We discuss our specific burden reduction efforts more fully in the Regulatory Impact Analysis.

This final rule is comprised of four final rules, which have been combined to reduce the impact and number of times certain compliance activities need to be undertaken by the regulated entities.

Legal Authority for the Regulatory Action

The final rule implements changes to the HIPAA Rules under a number of authorities. First, the final rule modifies the Privacy, Security, and Enforcement Rules to strengthen privacy and security protections for health information and to improve enforcement as provided for by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The rule also includes final modifications to the Breach Notification Rule, which will replace an interim final rule originally published in 2009 as required by the HITECH Act. Second, the final rule revises the HIPAA Privacy Rule to increase privacy protections for genetic information as required by the Genetic Information Nondiscrimination Act of 2008 (GINA). Finally, the Department uses its general authority under HIPAA to make a number of changes to the Rules that are intended to increase workability and flexibility, decrease burden, and better harmonize the requirements with those under other Departmental regulations.

ii. Summary of Major Provisions

This omnibus final rule is comprised of the following four final rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:

- Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.
- Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
- Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
- Require modifications to, and redistribution of, a covered entity's notice of privacy practices.
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule (referenced immediately below), such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's "harm" threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.

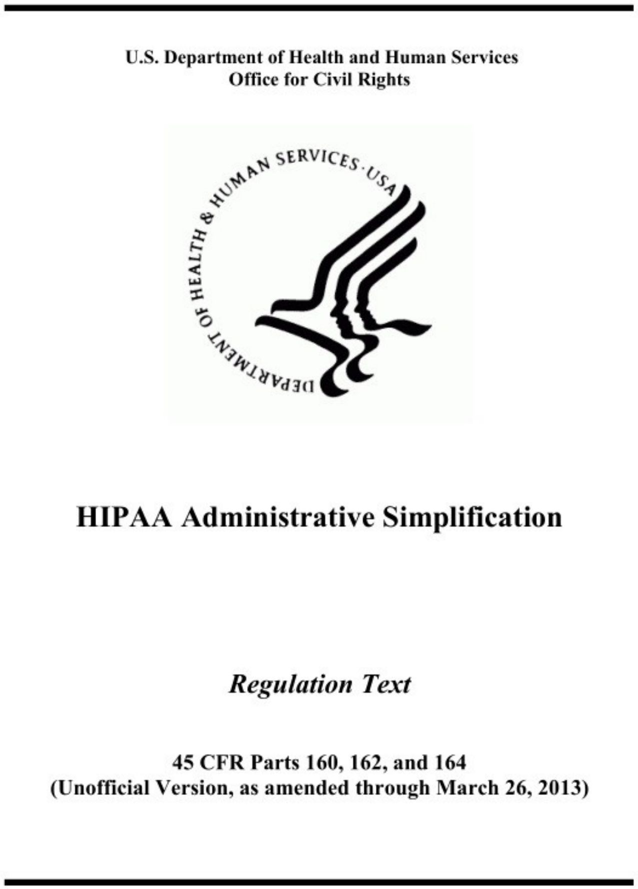
4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

HIPAA Administrative Simplification

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

PART 162—ADMINISTRATIVE REQUIREMENTS

PART 164—SECURITY AND PRIVACY



U.S. Department of Health and Human Services
Office for Civil Rights

HIPAA Administrative Simplification

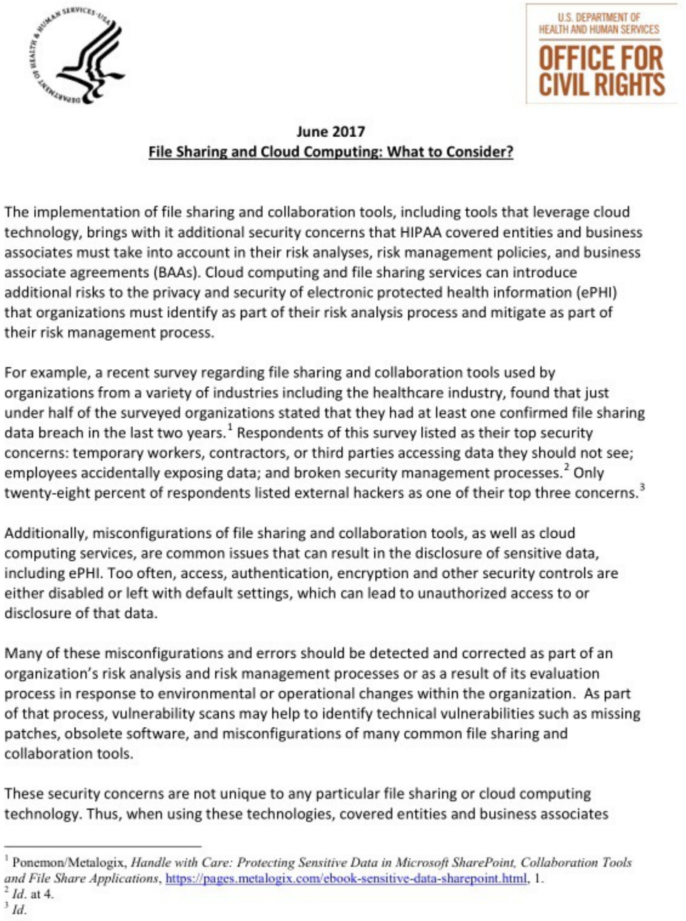
Regulation Text

45 CFR Parts 160, 162, and 164
(Unofficial Version, as amended through March 26, 2013)

Monthly Newsletter

U.S. Department of Health and Human Services (HHS)
Office for Civil Rights (OCR)

June 2017: File Sharing and Cloud Computing: What to Consider?



DEPARTMENT OF HEALTH & HUMAN SERVICES USA

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

June 2017
File Sharing and Cloud Computing: What to Consider?

The implementation of file sharing and collaboration tools, including tools that leverage cloud technology, brings with it additional security concerns that HIPAA covered entities and business associates must take into account in their risk analyses, risk management policies, and business associate agreements (BAAs). Cloud computing and file sharing services can introduce additional risks to the privacy and security of electronic protected health information (ePHI) that organizations must identify as part of their risk analysis process and mitigate as part of their risk management process.

For example, a recent survey regarding file sharing and collaboration tools used by organizations from a variety of industries including the healthcare industry, found that just under half of the surveyed organizations stated that they had at least one confirmed file sharing data breach in the last two years.[1] Respondents of this survey listed as their top security concerns: temporary workers, contractors, or third parties accessing data they should not see; employees accidentally exposing data; and broken security management processes.[2] Only twenty-eight percent of respondents listed external hackers as one of their top three concerns.[3]

Additionally, misconfigurations of file sharing and collaboration tools, as well as cloud computing services, are common issues that can result in the disclosure of sensitive data, including ePHI. Too often, access, authentication, encryption and other security controls are either disabled or left with default settings, which can lead to unauthorized access to or disclosure of that data.

Many of these misconfigurations and errors should be detected and corrected as part of an organization's risk analysis and risk management processes or as a result of its evaluation process in response to environmental or operational changes within the organization. As part of that process, vulnerability scans may help to identify technical vulnerabilities such as missing patches, obsolete software, and misconfigurations of many common file sharing and collaboration tools.

These security concerns are not unique to any particular file sharing or cloud computing technology. Thus, when using these technologies, covered entities and business associates

[1] Ponemon/Metalogix, *Handle with Care: Protecting Sensitive Data in Microsoft SharePoint, Collaboration Tools and File Share Applications*, https://pages.metalogix.com/ebook-sensitive-data-sharepoint.html, 1.
[2] *Id.* at 4.
[3] *Id.*

SECURITY STANDARDS: TECHNICAL SAFEGUARDS

PART 2:

1 Current challenges to meet HIPAA security compliance

2 HIPAA Security Rule requirements for e-PHI access control

3 HIPAA Security Rule solution providers

4 Medipriv implementation of e-PHI access control to meet the HIPAA Security Rule requirements

5 Beyond HIPAA: Hacking Risks and Multi-factor Authentication

Security Standards: Technical Safeguards

HIPAA Technical Safeguards are the most difficult section of the HIPAA regulations to implement

- The regulations do not describe a Technical Safeguard methodology for implementation: strong technical knowledge is required to determine how the regulations can be implemented

Government regulation has directed all healthcare entities to store patient information in electronic format to improve communications between entities, reduce errors and cut costs

- However the regulation provides only limited guidance to ensure that electronic protected health information is kept safe

Regulation requires that access to electronic protected information is restricted to only those people who are authorized

- The regulations describe rules, but do not describe how the ePHI access control should be implemented

The government imposes strict penalties for entities when a data breach has occurred

- Penalties are higher when the entity is not in compliance, and no attempt was made to implement technical safeguards

Security risks

When health records are stored on paper then physical access to archives is required, making protection of medical records easy, using a locked door

When health records are stored in the form of electronic Protected Health Information (e-PHI) then the risk of unauthorized access is much greater, with access through a number of different pathways:

- Information stored electronically is accessed through a computer network where the computer network can give a path of access to any non-authorized person if the path of access is not protected or that person has the necessary technical skills to gain access
- When e-PHI has poorly implemented access control then it can be easily circumvented by a non-authorized person with technical skills
- Theft of an authorized persons credentials, which permits a non-authorized person to have access to e-PHI
- Discovery of a network path to e-PHI that does not have access control
- Loss or theft of portable devices that store ePHI

Hacking Risks

Computer hacking has become an epidemic

- Inc.com estimates that hackers cost US companies $400B/year in 2015
- US Government estimates up to 4000 ransomware attacks per day in 2016

Healthcare entities are extremely vulnerable to ransom and theft of patient medical information

- Hackers have had great success with ransom extortion, with the threat of information disclosure

The hacker has several paths to access the electronic protected health information stored on protected servers

- Via the Internet public network, hacking into the protected network via the Internet router
- Via the staff network, installing a Trojan onto a staff computer via deception
- Hacking into the encrypted wireless network, then capturing logon information

Building a Secure Technical Environment

Highly skilled IT and network staff are required to build secure computer systems and networks that safeguard information and comply with HIPAA requirements

> Only larger healthcare IT environments have the infrastructure to support highly skilled technical staff (hospital groups, insurance companies, etc.)

The only path available to most smaller (practitioner) and medium size (clinic, small hospital) healthcare environments is to contract with a specialist networking company

> With current technical solutions, the cost can be in the $10K's to $100K’s for the design and Installation of a secure technical environment, plus the cost of on-going support and maintenance fees

Technology Solutions

Government regulation stipulates that entities holding e-PHI must control access to the information

- However there are limited technology options to implement access control, and the solutions that are available are very expensive

There is a lack of published information about the design of healthcare computer systems that will protect patient information

- The information published by Cisco, the largest network vendor, has an implementation cost in Excess of $100K

Network access control products are available from several vendors, however few completely implement the full HIPAA Security Rule requirements

- The solutions have to be emended using or or more additional pieces of equipment to meet the full HIPAA requirements specifications, which requires additional staff skills

SECURITY STANDARDS: TECHNICAL SAFEGUARDS

PART 2:

1 Current challenges to meet HIPAA security compliance

2 HIPAA Security Rule requirements for e-PHI access control

3 HIPAA Security Rule solution providers

4 Medipriv implementation of e-PHI access control to meet the HIPAA Security Rule requirements

5 Beyond HIPAA: Hacking Risks and Multi-factor Authentication

HIPAA Security Rule: Access Control Requirements Summary

Authorized users are permitted to have access only to that specific e-PHI for which they are authorized

Authorized users must be obliged to use strong passwords to access e-PHI

Authorized user passwords must be forced to change frequently

Any authorized user who has not interacted with e-PHI for a period of time must be ‘logged off’

Emergency access to e-PHI must be provided, with the system manager alerted each time that the emergency access is used

All accesses to e-PHI must be logged in an encrypted format and the log maintained for an extended period. The log will be required in the event of an e-PHI data breach to provide support for forensic experts who may identify the source of the data breach

Assumptions about e-PHI Storage and Access Control

e-PHI is stored on one or more local network connected devices (server computers) that can be accessed using personal computers, tablets and smart phones by authorized users only

e-PHI is stored on one or more remote Internet connected devices (cloud servers) that can be accessed using personal computers, tablets and smart phones by authorized users only

Each authorized user has access restricted to the e-PHI permitted for that user: User Based and Role Based access control (UBAC and RBAC)

Authorized medical devices can be permitted to directly access e-PHI for data storage and retrieval

Non-authorized personnel and non-authorized devices must be completely blocked from access to any e-PHI local or cloud storage device

Identity and Access Management

Overview

The principal requirement of the HIPAA Security Rule safeguards is the identity management of authorized users, and access controls of users/devices/systems to e-PHI using authentication, authorization, accounting (AAA) principles

Strong authorized user identity management and access control is critical for warranting an assessment of low risk under a covered entity's risk management program

Effective identity and access management is critical to a covered entity's ability to meet the HIPAA Disclosure Accounting Rule

Identity management

An identity record is maintained for each authorized user and authorized device, for the purpose of authentication, authorization and accounting

Access management

Authorized staff are permitted to access only the specific e-PHI servers for which they are authorized

Non-authorized individuals are blocked from accessing e-PHI servers

Logging, Auditing, and Monitoring

Overview

Logging, auditing, and monitoring are critical to a covered entity's ability to meet Accounting Rule 164.528

Logging, auditing, and monitoring is essential help identify when a compromise has occurred that may lead to a breach notification

Logging, Auditing, and Monitoring

Logging, auditing, and monitoring of access to e-PHI by authorized users and systems is a critical requirement of the HIPAA Security rule

Application, database and device access logging is important to effectively support a covered entity or business associate's breach management strategy and is an important support for auditing

Real-time intrusion detection and protective response is desired for the identification of any attempted non-authorized access before it becomes a data breach

e-PHI Data and Access Control Encryption

Overview

HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption states that the ability to encrypt and decrypt e-PHI is essential to prevent unwanted exposure of e-PHI data.

e-PHI encryption is end-to-end: data is encrypted between the e-PHI database and the application (app) on the authorized users computer device

Login connection between the authorized user computer and the e-PHI access controller is encrypted to prevent capture of passwords

Logged information of e-PHI accesses by authorized users is stored in an encrypted format to prevent unauthorized access

e-PHI Data Isolation through Computer Network Segmentation

Overview

- Covered entities that can effectively isolate e-PHI from other data are most effective at maintaining control over secure information.
- Administrative functions and clinical data should be isolated through network segmentation in order to limit the scope and depth of security controls that are applied to various forms of data

Segmenting clinical information from administrative information makes it possible to apply appropriate controls to effectively secure the protected information base

Enterprise networks are segmented by separating e-PHI onto its own IP address space as a protected subnet

Segregating data within a covered entity via segmentation permits the network to support HIPAA Security Rule safeguards, minimizing risks to e-PHI and critical medical systems

Network segmentation can also improve the speed of e-PHI data access by eliminating data traffic that is not related to e-PHI access

SECURITY STANDARDS: TECHNICAL SAFEGUARDS

PART 2:

1 Current challenges to meet HIPAA security compliance

2 HIPAA Security Rule requirements for e-PHI access control

3 HIPAA Security Rule solution providers

4 Medipriv implementation of e-PHI access control to meet the HIPAA Security Rule requirements

5 Beyond HIPAA: Hacking Risks and Multi-factor Authentication

Technical Solutions that Implement the HIPAA Security Rule, Either Partially or Completely

A number of manufacturers and integration companies offer technical solutions that implement the HIPAA security rule, either partially or completely. The following pages present a sample list of manufacturers and providers, as follows:

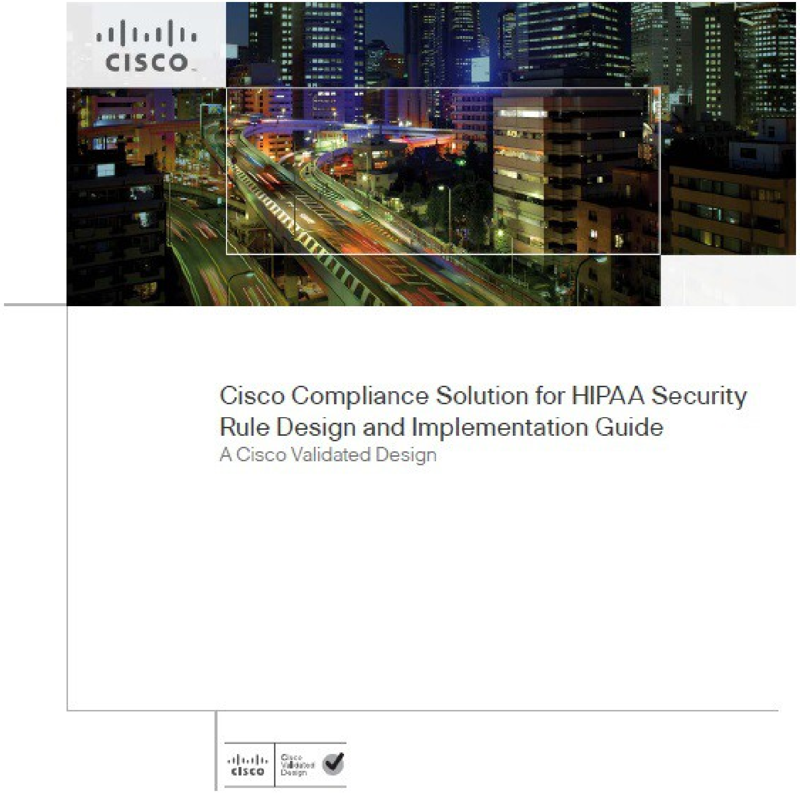
Cisco
Amazon
Bradford
Brocade
Forescout
Fortinet
Hexis
Juniper
Fortrix
Tyco
Medipriv

Cisco

Cisco has developed an industry reference design that implements the HIPAA Security Rule

This design has been implemented in many larger healthcare environments with success

The Cisco design is the reference to which other solutions are compared



Cisco Compliance Solution for HIPAA Security Rule Design and Implementation Guide

A Cisco Validated Design

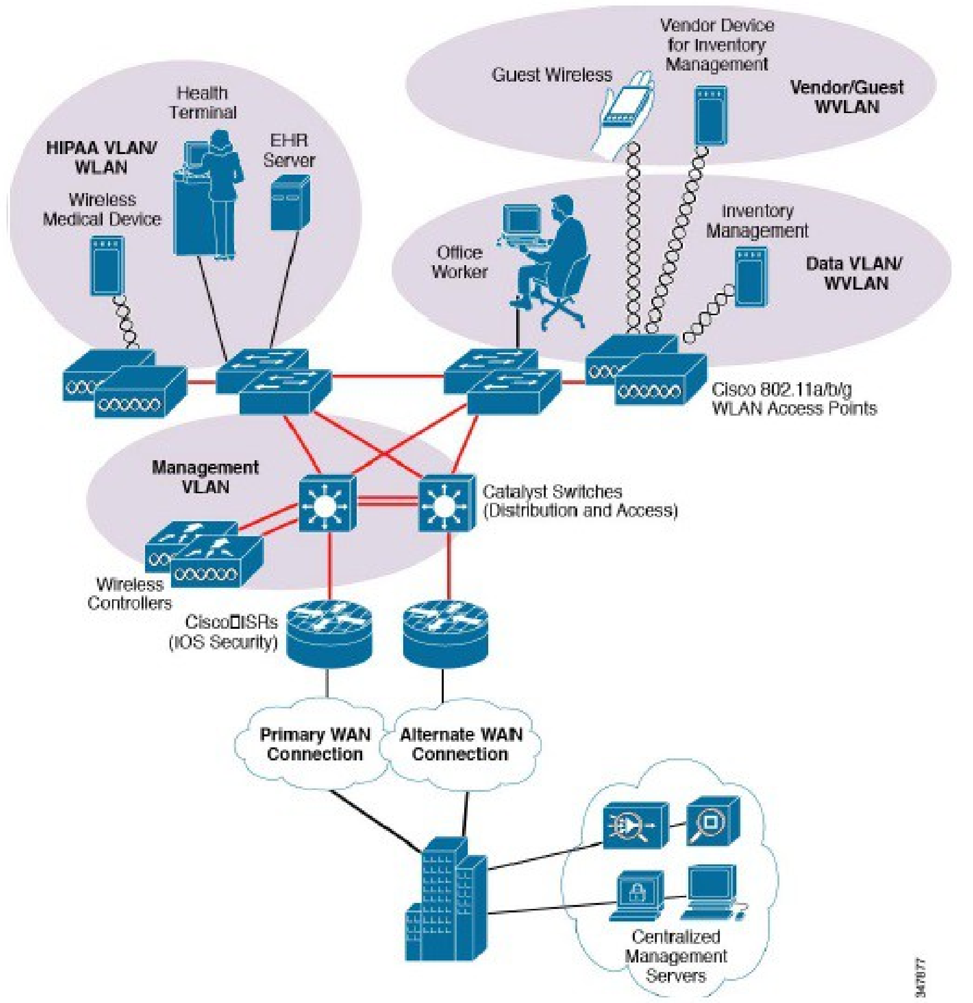
Cisco

The Cisco standard design is published as a very comprehensive document of 938 pages, which indicates the complexity of the solution

Implementation requires highly qualified personnel and can cost $100,000's +

The Cisco HIPAA Security Rule implementation design is considered to be a standard of excellence due to the level of integration and reliability

Figure 4-10 *Hospital Architecture*

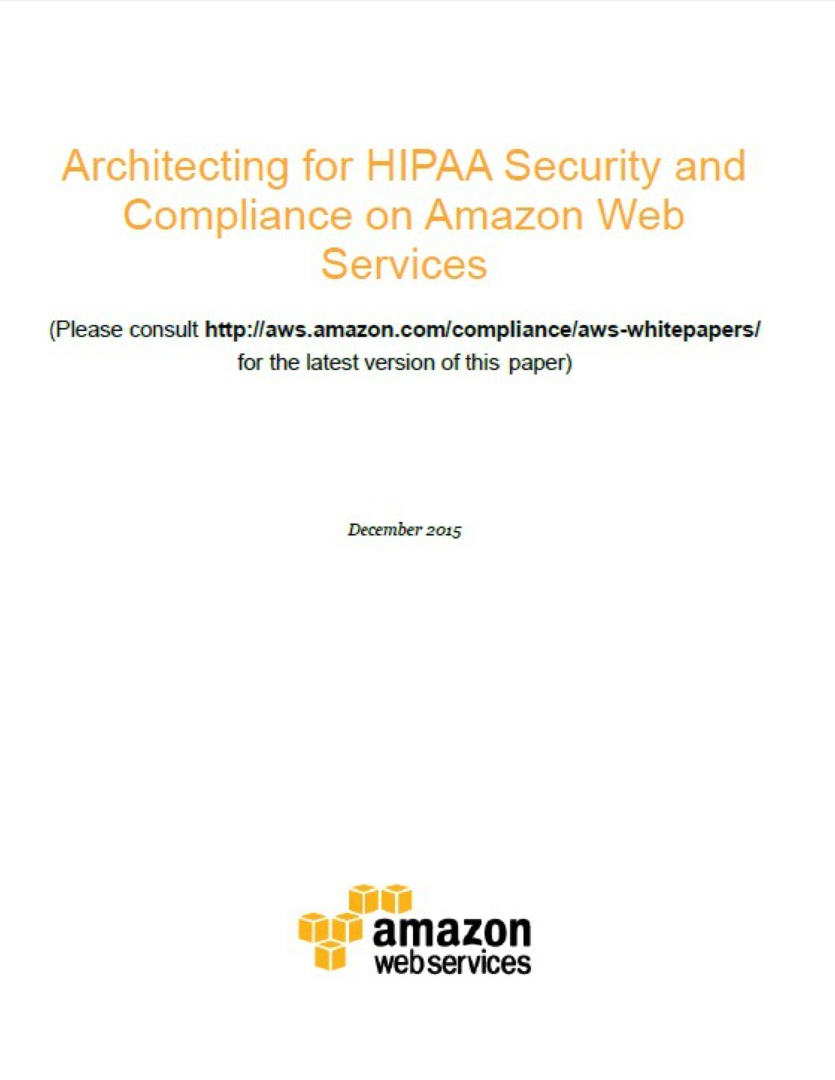


Amazon

Amazon offers a cloud data storage service that is compliant with the HIPAA Security Rule

Healthcare applications must implement all data storage in the Amazon cloud

The Amazon cloud storage does not implement the security rule for ePHI data stored at the covered entity site (e.g. X-ray database, MRI scanner database), therefore a second solution is required to implement the Security Rule for data stored at the entity site



Architecting for HIPAA Security and Compliance on Amazon Web Services

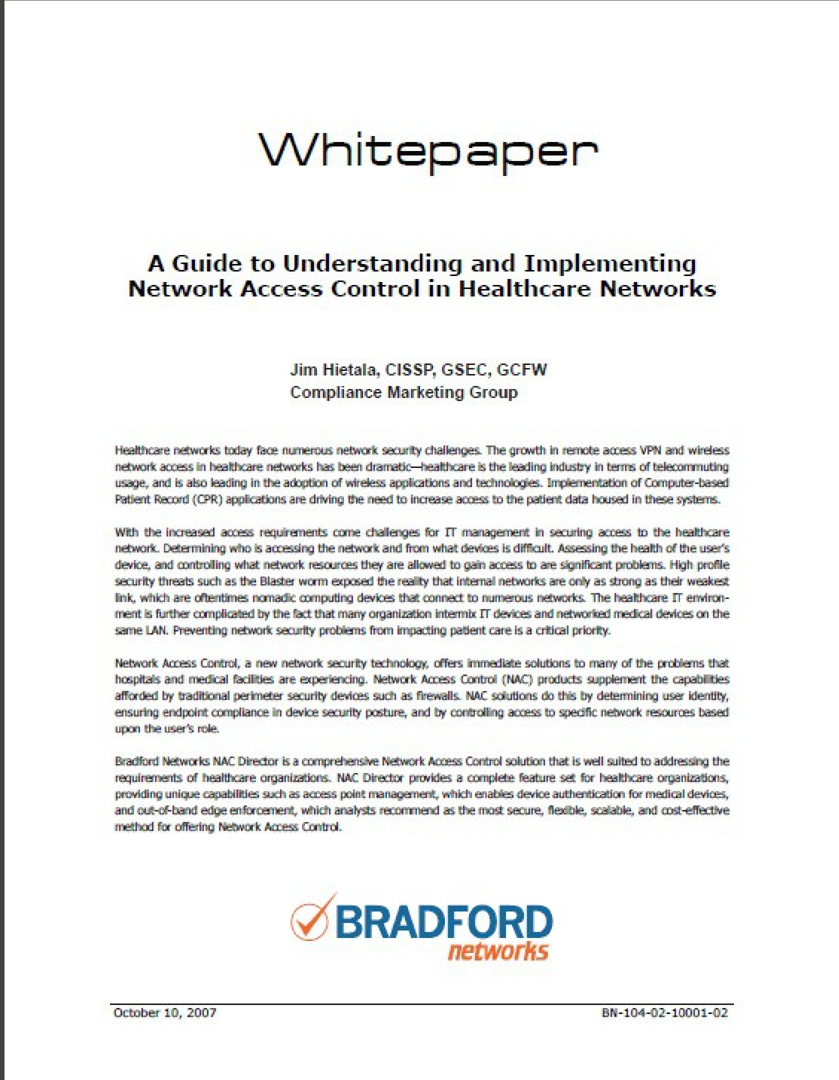
(Please consult **http://aws.amazon.com/compliance/aws-whitepapers/** for the latest version of this paper)

December 2015

amazon
web services

Bradford Networks

Bradford Networks manufactures products that implement access control



Whitepaper

A Guide to Understanding and Implementing Network Access Control in Healthcare Networks

Jim Hietala, CISSP, GSEC, GCFW
Compliance Marketing Group

Healthcare networks today face numerous network security challenges. The growth in remote access VPN and wireless network access in healthcare networks has been dramatic—healthcare is the leading industry in terms of telecommuting usage, and is also leading in the adoption of wireless applications and technologies. Implementation of Computer-based Patient Record (CPR) applications are driving the need to increase access to the patient data housed in these systems.

With the increased access requirements come challenges for IT management in securing access to the healthcare network. Determining who is accessing the network and from what devices is difficult. Assessing the health of the user's device, and controlling what network resources they are allowed to gain access to are significant problems. High profile security threats such as the Blaster worm exposed the reality that internal networks are only as strong as their weakest link, which are oftentimes nomadic computing devices that connect to numerous networks. The healthcare IT environment is further complicated by the fact that many organization intermix IT devices and networked medical devices on the same LAN. Preventing network security problems from impacting patient care is a critical priority.

Network Access Control, a new network security technology, offers immediate solutions to many of the problems that hospitals and medical facilities are experiencing. Network Access Control (NAC) products supplement the capabilities afforded by traditional perimeter security devices such as firewalls. NAC solutions do this by determining user identity, ensuring endpoint compliance in device security posture, and by controlling access to specific network resources based upon the user's role.

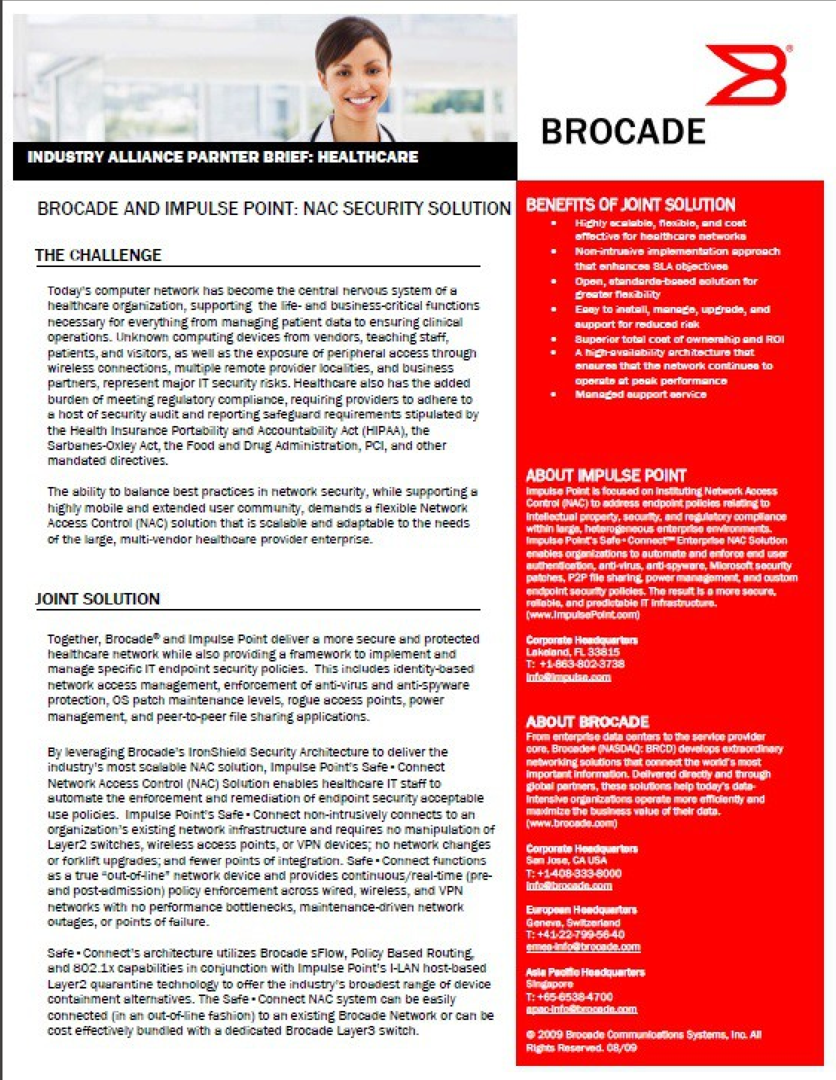
Bradford Networks NAC Director is a comprehensive Network Access Control solution that is well suited to addressing the requirements of healthcare organizations. NAC Director provides a complete feature set for healthcare organizations, providing unique capabilities such as access point management, which enables device authentication for medical devices, and out-of-band edge enforcement, which analysts recommend as the most secure, flexible, scalable, and cost-effective method for offering Network Access Control.

BRADFORD networks

October 10, 2007 BN-104-02-10001-02

Brocade

Brocade offers products as part of a partnership that implement network access control



BROCADE

INDUSTRY ALLIANCE PARNTER BRIEF: HEALTHCARE

BROCADE AND IMPULSE POINT: NAC SECURITY SOLUTION

THE CHALLENGE

Today's computer network has become the central nervous system of a healthcare organization, supporting the life- and business-critical functions necessary for everything from managing patient data to ensuring clinical operations. Unknown computing devices from vendors, teaching staff, patients, and visitors, as well as the exposure of peripheral access through wireless connections, multiple remote provider localities, and business partners, represent major IT security risks. Healthcare also has the added burden of meeting regulatory compliance, requiring providers to adhere to a host of security audit and reporting safeguard requirements stipulated by the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Food and Drug Administration, PCI, and other mandated directives.

The ability to balance best practices in network security, while supporting a highly mobile and extended user community, demands a flexible Network Access Control (NAC) solution that is scalable and adaptable to the needs of the large, multi-vendor healthcare provider enterprise.

JOINT SOLUTION

Together, Brocade® and Impulse Point deliver a more secure and protected healthcare network while also providing a framework to implement and manage specific IT endpoint security policies. This includes identity-based network access management, enforcement of anti-virus and anti-spyware protection, OS patch maintenance levels, rogue access points, power management, and peer-to-peer file sharing applications.

By leveraging Brocade's IronShield Security Architecture to deliver the industry's most scalable NAC solution, Impulse Point's Safe•Connect Network Access Control (NAC) Solution enables healthcare IT staff to automate the enforcement and remediation of endpoint security acceptable use policies. Impulse Point's Safe•Connect non-intrusively connects to an organization's existing network infrastructure and requires no manipulation of Layer2 switches, wireless access points, or VPN devices; no network changes or forklift upgrades; and fewer points of integration. Safe•Connect functions as a true "out-of-line" network device and provides continuous/real-time (pre- and post-admission) policy enforcement across wired, wireless, and VPN networks with no performance bottlenecks, maintenance-driven network outages, or points of failure.

Safe•Connect's architecture utilizes Brocade sFlow, Policy Based Routing, and 802.1x capabilities in conjunction with Impulse Point's I-LAN host-based Layer2 quarantine technology to offer the industry's broadest range of device containment alternatives. The Safe•Connect NAC system can be easily connected (in an out-of-line fashion) to an existing Brocade Network or can be cost effectively bundled with a dedicated Brocade Layer3 switch.

BENEFITS OF JOINT SOLUTION

- Highly scalable, flexible, and cost effective for healthcare networks
- Non-intrusive implementation approach that enhances SLA objectives
- Open, standards-based solution for greater flexibility
- Easy to install, manage, upgrade, and support for reduced risk
- Superior total cost of ownership and ROI
- A high-availability architecture that ensures that the network continues to operate at peak performance
- Managed support service

ABOUT IMPULSE POINT

Impulse Point is focused on Instituting Network Access Control (NAC) to address endpoint policies relating to intellectual property, security, and regulatory compliance within large, heterogeneous enterprise environments. Impulse Point's Safe•Connect™ Enterprise NAC Solution enables organizations to automate and enforce end user authentication, anti-virus, anti-spyware, Microsoft security patches, P2P file sharing, power management, and custom endpoint security policies. The result is a more secure, reliable, and predictable IT infrastructure. (www.ImpulsePoint.com)

Corporate Headquarters
Lakeland, FL 33815
T: +1-863-802-3738
info@impulse.com

ABOUT BROCADE

From enterprise data centers to the service provider core, Brocade® (NASDAQ: BRCD) develops extraordinary networking solutions that connect the world's most important information. Delivered directly and through global partners, these solutions help today's data-intensive organizations operate more efficiently and maximize the business value of their data. (www.brocade.com)

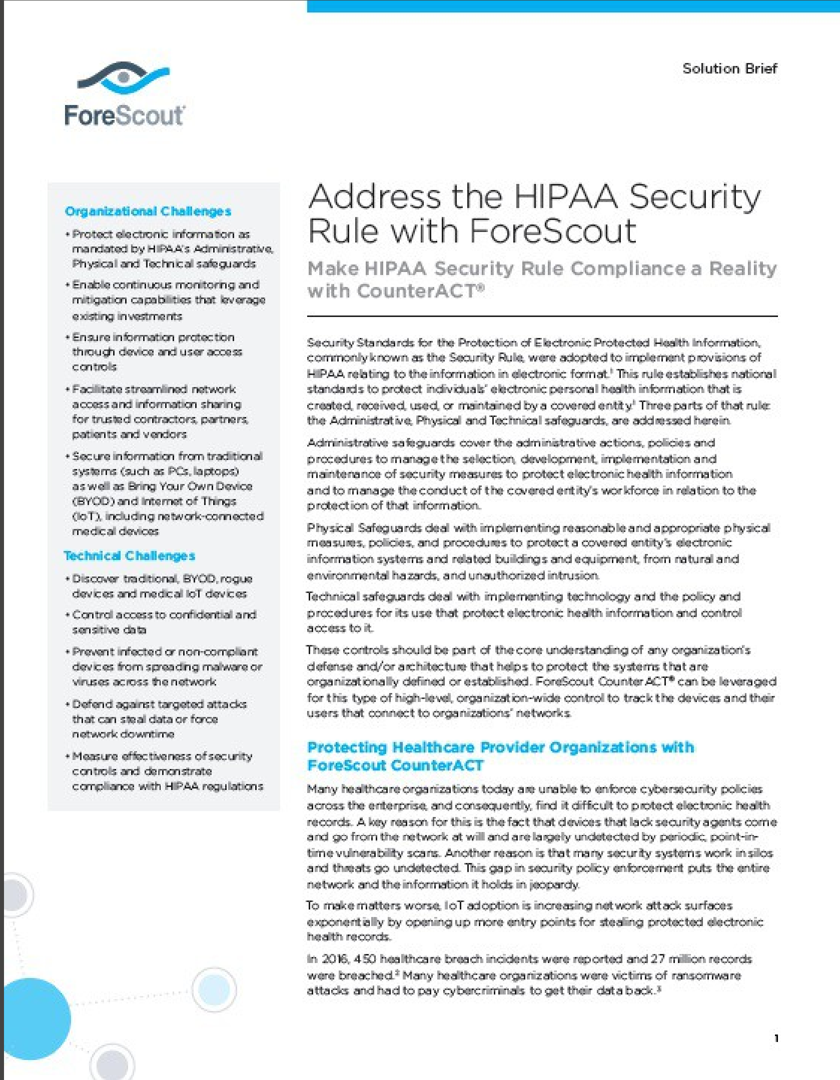
Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

Forescout

Forescout offers a technical solution that will implement the HIPAA Security Rule



ForeScout

Solution Brief

Address the HIPAA Security Rule with ForeScout

Make HIPAA Security Rule Compliance a Reality with CounterACT®

Organizational Challenges

- Protect electronic information as mandated by HIPAA's Administrative, Physical and Technical safeguards
- Enable continuous monitoring and mitigation capabilities that leverage existing investments
- Ensure information protection through device and user access controls
- Facilitate streamlined network access and information sharing for trusted contractors, partners, patients and vendors
- Secure information from traditional systems (such as PCs, laptops) as well as Bring Your Own Device (BYOD) and Internet of Things (IoT), including network-connected medical devices

Technical Challenges

- Discover traditional, BYOD, rogue devices and medical IoT devices
- Control access to confidential and sensitive data
- Prevent infected or non-compliant devices from spreading malware or viruses across the network
- Defend against targeted attacks that can steal data or force network downtime
- Measure effectiveness of security controls and demonstrate compliance with HIPAA regulations

Security Standards for the Protection of Electronic Protected Health Information, commonly known as the Security Rule, were adopted to implement provisions of HIPAA relating to the information in electronic format.[1] This rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.[1] Three parts of that rule: the Administrative, Physical and Technical safeguards, are addressed herein.

Administrative safeguards cover the administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Physical Safeguards deal with implementing reasonable and appropriate physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Technical safeguards deal with implementing technology and the policy and procedures for its use that protect electronic health information and control access to it.

These controls should be part of the core understanding of any organization's defense and/or architecture that helps to protect the systems that are organizationally defined or established. ForeScout CounterACT® can be leveraged for this type of high-level, organization-wide control to track the devices and their users that connect to organizations' networks.

Protecting Healthcare Provider Organizations with ForeScout CounterACT

Many healthcare organizations today are unable to enforce cybersecurity policies across the enterprise, and consequently, find it difficult to protect electronic health records. A key reason for this is the fact that devices that lack security agents come and go from the network at will and are largely undetected by periodic, point-in-time vulnerability scans. Another reason is that many security systems work in silos and threats go undetected. This gap in security policy enforcement puts the entire network and the information it holds in jeopardy.

To make matters worse, IoT adoption is increasing network attack surfaces exponentially by opening up more entry points for stealing protected electronic health records.

In 2016, 450 healthcare breach incidents were reported and 27 million records were breached.[2] Many healthcare organizations were victims of ransomware attacks and had to pay cybercriminals to get their data back.[3]

Fortinet

Fortinet manufactures network access control products that can be used to implement the HIPAA Security Rule

FERTINET.

SOLUTION BRIEF

SECURE ACCESS SOLUTION

Fortinet gives Health IT organizations a choice of three WLAN solutions which provide seamless mobility within and between healthcare facilities of all sizes, while assuring mission-critical apps perform flawlessly, and patient data, devices and applications are fully protected from the latest cyberthreats.

Secure Access for Healthcare

Reliable Wi-Fi for Uninterrupted Clinical Care

Healthcare professionals are the epitome of a mobile workforce: Constantly on the move, yet highly dependent on fast, accurate information. They need a secure wireless solution that performs flawlessly on the array of devices they rely on every day.

Hospitals, clinics and elder care facilities have countless ways to exploit wireless technology for better patient outcomes, and to improve operational efficiency. From accessing patient records with computers on wheels or handheld tablets, to getting telemetry from medical devices, nurse call and location tracking applications, Wi-Fi is now at the heart of patient care.

WLAN reliability is of course paramount. But there are a growing number of wireless devices accessing the network, many of them headless (with no user interface). That means that access control and application security are now critical success factors for any healthcare network.

Only Fortinet can offer Health IT organizations a choice of WLAN and security deployment models, without compromising the protection provided, with three distinctly different wireless offerings, each backed by world-class cyber-security.

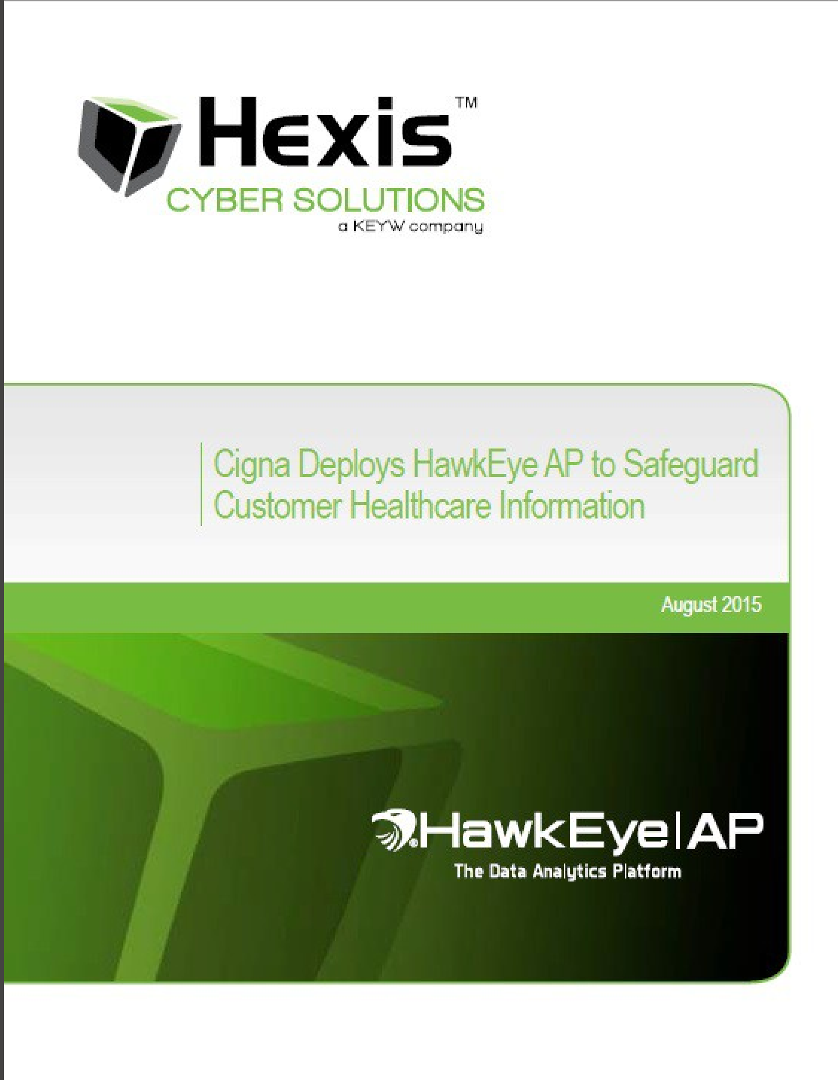
Fortinet's *Cloud-Managed* Secure Access solution provides quick and easy wireless deployment to any size facility without requiring on-premise wireless controllers. The *Integrated* Secure Access solution unifies network and security management through a "single pane of glass", and provides superior visibility and control of applications. And the *Infrastructure* Secure Access solution simplifies WLAN deployment and scaling, offering several unique reliability and traffic isolation advantages.

- Choice of cloud-managed, or two premise-managed WLAN deployment models to suit organizational preferences
- Rich set of options for guest access and BYOD onboarding
- Comprehensive threat protection consolidated on one appliance
- Full compliance with HIPAA and other health IT regulations
- Exceptional visibility and control of applications and utilization
- Security devices kept up-to-date through regular signature updates from FortiGuard Labs

www.fortinet.com 1

Hexis

Hexis offers a solution that controls access to healthcare information



Hexis™ CYBER SOLUTIONS
a KEYW company

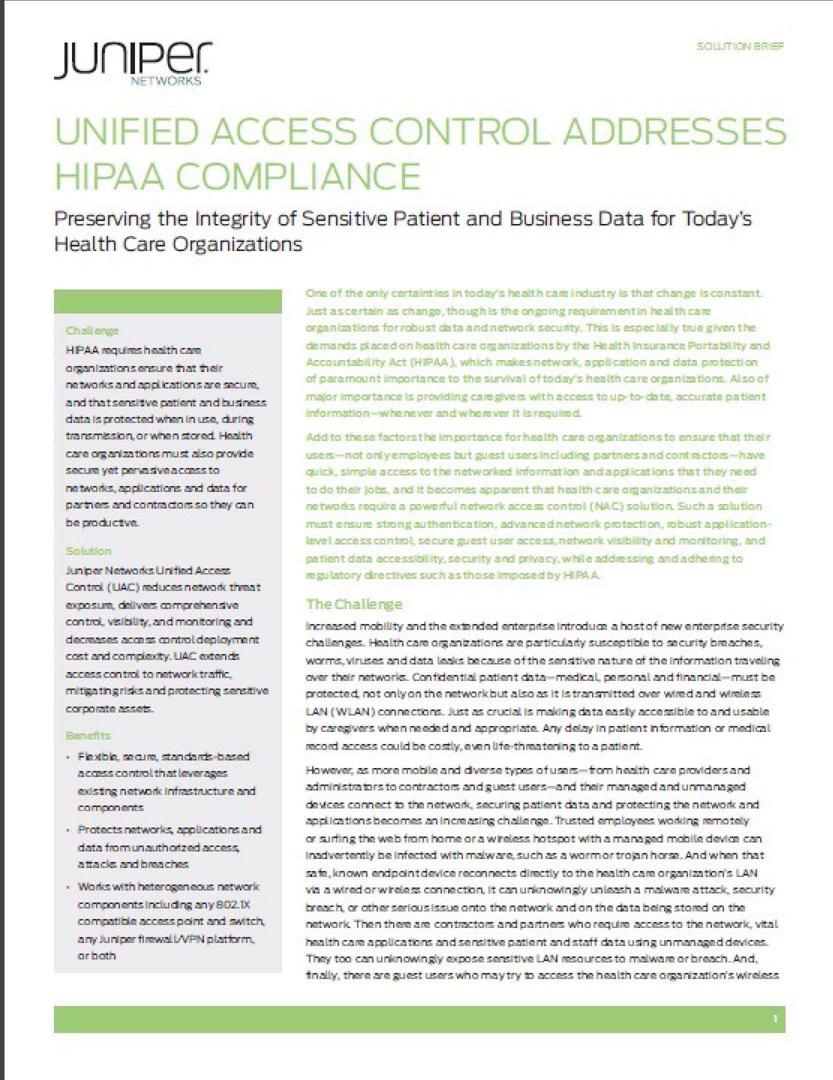
Cigna Deploys HawkEye AP to Safeguard Customer Healthcare Information

August 2015

HawkEye | AP
The Data Analytics Platform

Juniper

Juniper manufactures access control products that implement data access control



JUNIPer NETWORKS

SOLUTION BRIEF

UNIFIED ACCESS CONTROL ADDRESSES HIPAA COMPLIANCE

Preserving the Integrity of Sensitive Patient and Business Data for Today's Health Care Organizations

Challenge

HIPAA requires health care organizations ensure that their networks and applications are secure, and that sensitive patient and business data is protected when in use, during transmission, or when stored. Health care organizations must also provide secure yet pervasive access to networks, applications and data for partners and contractors so they can be productive.

Solution

Juniper Networks Unified Access Control (UAC) reduces network threat exposure, delivers comprehensive control, visibility, and monitoring and decreases access control deployment cost and complexity. UAC extends access control to network traffic, mitigating risks and protecting sensitive corporate assets.

Benefits

- Flexible, secure, standards-based access control that leverages existing network infrastructure and components
- Protects networks, applications and data from unauthorized access, attacks and breaches
- Works with heterogeneous network components including any 802.1X compatible access point and switch, any Juniper firewall/VPN platform, or both

One of the only certainties in today's health care industry is that change is constant. Just as certain as change, though is the ongoing requirement in health care organizations for robust data and network security. This is especially true given the demands placed on health care organizations by the Health Insurance Portability and Accountability Act (HIPAA), which makes network, application and data protection of paramount importance to the survival of today's health care organizations. Also of major importance is providing caregivers with access to up-to-date, accurate patient information—whenever and wherever it is required.

Add to these factors the importance for health care organizations to ensure that their users—not only employees but guest users including partners and contractors—have quick, simple access to the networked information and applications that they need to do their jobs, and it becomes apparent that health care organizations and their networks require a powerful network access control (NAC) solution. Such a solution must ensure strong authentication, advanced network protection, robust application-level access control, secure guest user access, network visibility and monitoring, and patient data accessibility, security and privacy, while addressing and adhering to regulatory directives such as those imposed by HIPAA.

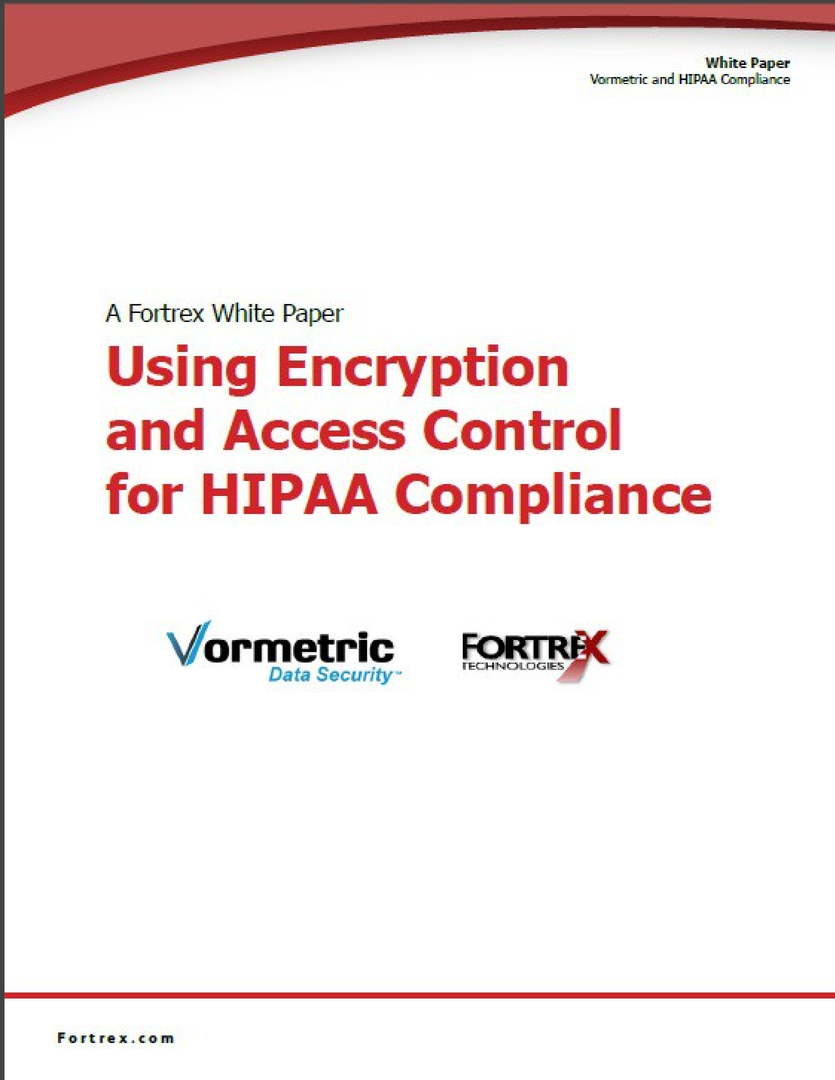
The Challenge

Increased mobility and the extended enterprise introduce a host of new enterprise security challenges. Health care organizations are particularly susceptible to security breaches, worms, viruses and data leaks because of the sensitive nature of the information traveling over their networks. Confidential patient data—medical, personal and financial—must be protected, not only on the network but also as it is transmitted over wired and wireless LAN (WLAN) connections. Just as crucial is making data easily accessible to and usable by caregivers when needed and appropriate. Any delay in patient information or medical record access could be costly, even life-threatening to a patient.

However, as more mobile and diverse types of users—from health care providers and administrators to contractors and guest users—and their managed and unmanaged devices connect to the network, securing patient data and protecting the network and applications becomes an increasing challenge. Trusted employees working remotely or surfing the web from home or a wireless hotspot with a managed mobile device can inadvertently be infected with malware, such as a worm or trojan horse. And when that safe, known endpoint device reconnects directly to the health care organization's LAN via a wired or wireless connection, it can unknowingly unleash a malware attack, security breach, or other serious issue onto the network and on the data being stored on the network. Then there are contractors and partners who require access to the network, vital health care applications and sensitive patient and staff data using unmanaged devices. They too can unknowingly expose sensitive LAN resources to malware or breach. And, finally, there are guest users who may try to access the health care organization's wireless

Fortrex

Fortrex offers a solution that implements the HIPAA Security Rule



White Paper
Vormetric and HIPAA Compliance

A Fortrex White Paper

Using Encryption and Access Control for HIPAA Compliance

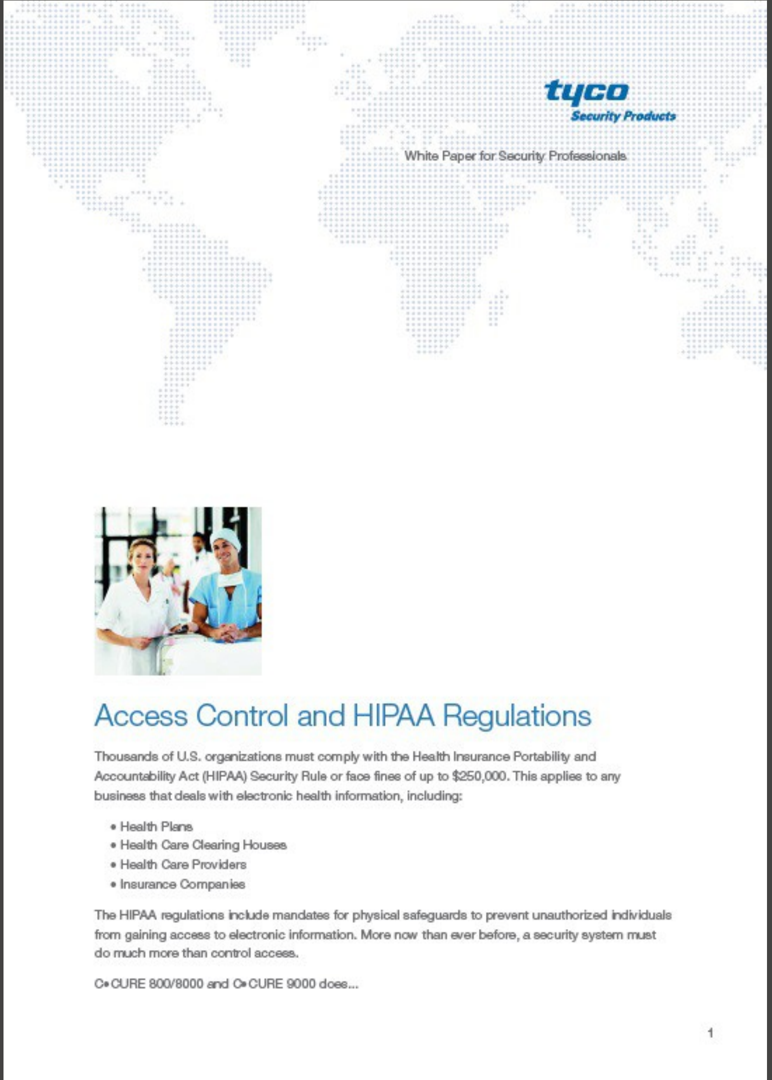
Vormetric Data Security™

FORTREX TECHNOLOGIES

Fortrex.com

Tyco

Tyco in an integrator that implements healthcare security solutions using products manufactured by other companies



tyco
Security Products

White Paper for Security Professionals

Access Control and HIPAA Regulations

Thousands of U.S. organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule or face fines of up to $250,000. This applies to any business that deals with electronic health information, including:

- Health Plans
- Health Care Clearing Houses
- Health Care Providers
- Insurance Companies

The HIPAA regulations include mandates for physical safeguards to prevent unauthorized individuals from gaining access to electronic information. More now than ever before, a security system must do much more than control access.

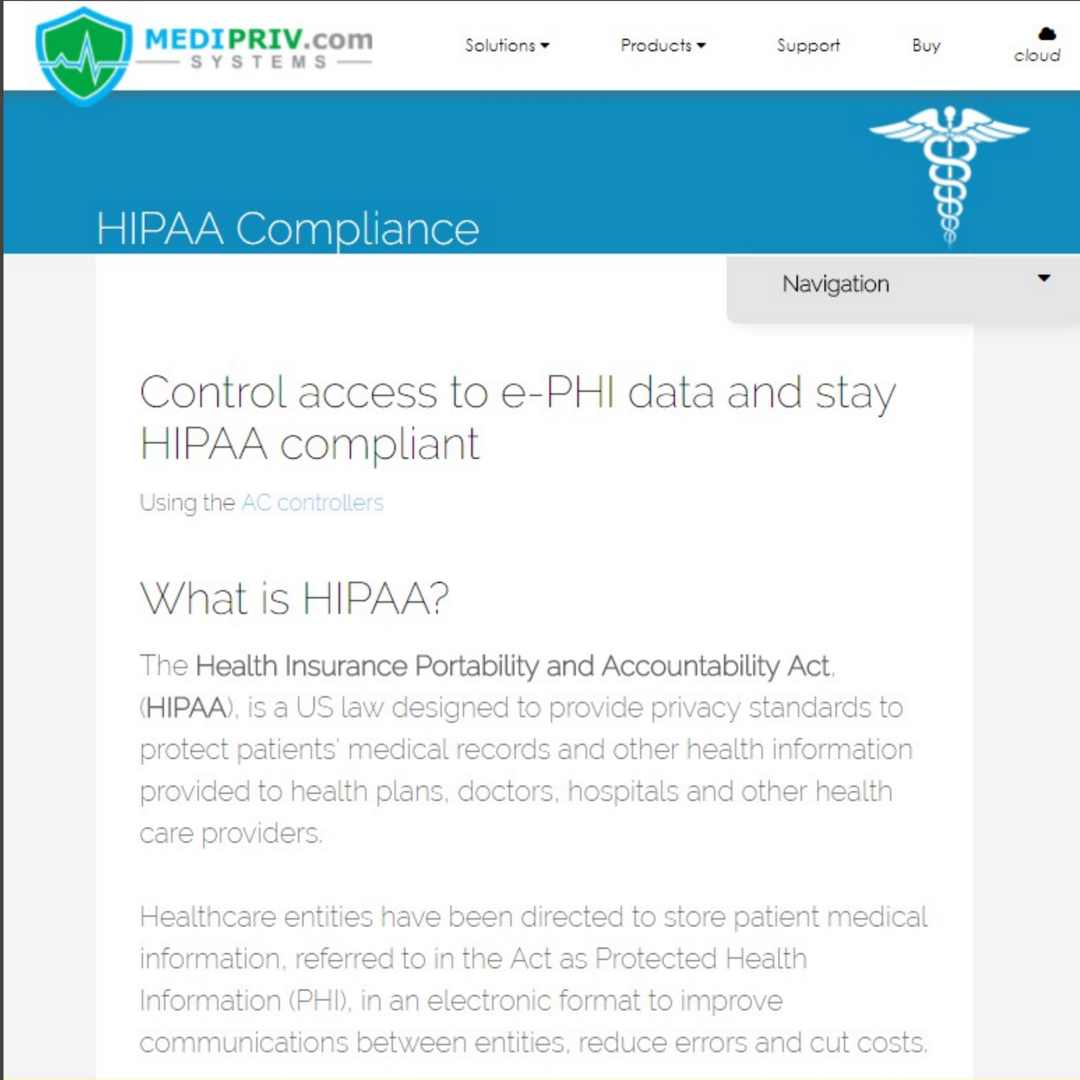
C•CURE 800/8000 and C•CURE 9000 does...

Medipriv

Medipriv (Medical Privacy Systems) has developed a family of products that implement the HIPAA Security Rule

Medipriv have been designed as a low cost solution for smaller medical offices and clinics, where other solutions exceed budget limitations

Medipriv products have been designed to be installed by IT staff (or an outsourced IT provider) who need not have specialist network skills (e.g. Cisco certification)



HIPAA Compliance

Control access to e-PHI data and stay HIPAA compliant

Using the AC controllers

What is HIPAA?

The Health Insurance Portability and Accountability Act, (HIPAA), is a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

Healthcare entities have been directed to store patient medical information, referred to in the Act as Protected Health Information (PHI), in an electronic format to improve communications between entities, reduce errors and cut costs.

HIPAA Security Rule: Implementation Decision Process

The choice of the technical solution is determined by seven factors:

Compliant with the HIPAA Security Rule

Meets reliability requirements

Meets cost requirements

Meets performance requirements

Budget availability

Time required to implement ensuring ePHI access during the transition

Availability of skilled personnel for deployment and staff training

SECURITY STANDARDS: TECHNICAL SAFEGUARDS

PART 2:

1 Current challenges to meet HIPAA security compliance

2 HIPAA Security Rule requirements for e-PHI access control

3 HIPAA Security Rule solution providers

4 Medipriv implementation of e-PHI access control to meet the HIPAA Security Rule requirements

5 Beyond HIPAA: Hacking Risks and Multi-factor Authentication

Medipriv Implementation of e-PHI access control to meet the HIPAA Security Rule Requirements

Medipriv has developed a network access control product that can be deployed as part of the healthcare entity technology infrastructure, that:

- Meets HIPAA Security Rule compliance requirements
- Economical compared with alternative solutions
- Can be installed by a technician with IT skills: advanced networking skills are not required

Medipriv has a full range of access control products, each with a price/performance level

- Meeting the requirements of a single practitioner, clinic, or hospital

Medipriv has a cloud-based management, support and maintenance tool that permits IT staff or an outsourced IT service firm to support the healthcare entity

Medipriv provides a product support service for IT staff to ensure operational continuity

Medipriv design and implementation methodology is described in the following pages

User Based Access Control (UBAC): Authorized user profile

The authorized user profile is a database stored on the access controller

- The profile is backed up daily, for redundancy and security

The authorized user profile is encrypted to prevent unauthorized access

- The encryption key is held by the system administrator

The authorized user profile can be created and updated via the access controller administrators console

User Based Access Control (UBAC): Authorized user profile entries

Name of user

Emergency contact information: email, mobile phone

Checkbox indication that the user is authorized to access e-PHI

Position or the user in the organization, numerical identification (employee number, SSN, etc)

Username and password, with frequency of password change

Emergency login credentials, date of birth, user supplied question/answer

List role-based groups of e-PHI servers that the user is permitted to access

- Select from a drop down menu of role-based groups
- Each user can be associated with multiple role-based groups

ID’s (fingerprints) of approved devices to be used

- MAC address + device type (optional) + operating system version (optional) + browser type (optional)
- Multiple devices can be associated with each user

Log of user authorized network accesses

- Date/time of login and logout, reason for logout, user logout or forced logout
- Server IP addresses accessed during the session
- Log of DNS requests with URL sent and IP returned
- Log of emergency accesses with username, date/time/duration and reason
- No password match, no device ID match flags

Role Based Access Control (RBAC): group records

Creation and management of role based groups, an association of ePHI databases (server IP addresses) associated with a specific role within the healthcare organization

e-PHI server IP's are selected from the e-PHI server list when configuring the server access permissions of each role-based group

List of all local e-PHI servers

- Server IP address
- Description of e-PHI on the server

List of all remote (cloud based) e-PHI servers

- Server IP address
- Description of e-PHI on the server

Administrator account and authorized user account creation procedure

Create an administrator account, providing authentication parameters and modes

- Configure network parameters (subnets, etc) as required for the network implementation

The administrator will create role-based access control groups, defined by the entity organization

The administrator will add the e-PHI server IP’s to each role-based access control group

- IP addresses and descriptions of local e-PHI servers in the protected LAN
- IP addresses and descriptions of remote e-PHI servers in one or more clouds

The administrator will add authorized users to the authorized user data base in the following sequence

- Enter the authorized user personal information (name, position, employee number etc.)
- Associate the role-based access control groups that the authorized user is permitted to access, from the drop-down list
- Create a username and password for the authorized user (a password change will be requested on the first login), give to the authorized user

Authorized user login procedure

Authorized and non-authorized users can access any server/website IP that is not on the e-PHI server list of IP’s

When any user attempts to access an IP address that is on the e-PHI server list then that user is presented with a login page requesting username and password credentials

An authorized user will provide login credentials that, once authorized, will allow that user to communicate with any of the e-PHI servers on that users role-based access control group list

If the authorized user attempts to access an e-PHI server that has an IP address which is not included in that users authorized list then that user is shown a login screen with the message “not authorized”

When the authorized user accesses an authorized e-PHI server then the browser based software application will request login credentials for that specific e-PHI data

Therefore, the authorized user will ‘login’ twice for any e-PHI access

Authorized user credentials 1

Each authorized user must provide a username and a strong password to access any of the e-PHI servers

Optionally the user computer device will be verified and approved (2-factor authentication)

Each e-PHI web based server software will also request user credentials when accessed by a Software application on the users computer

The access controller must apply a strong security layer because

The healthcare entity often relies on third-party (software companies) strength of access control to a specific e-PHI database, therefore having access control with known characteristics is beneficial

Authorized user credentials 2

The access controller password has three important characteristics to comply with the HIPAA Security Rules

- The authorized user must be forced to use a strong password, minimum length, special characters, etc (options can be selected by the administrator)
- The authorized user must be forced to change the password frequently, the period before change can be selected by the administrator
- The authorized user must be logged off after a period of inactivity, the period is set by the administrator

The access controller must provide emergency access for any authorized user

- Emergency access is made with the users surname, date of birth and the answer to a question provided by the user
- Any emergency access is logged and the administrator is informed immediately, the administrator is responsible to contact the authorized user and understand why the proper login credentials were not used

Authorized user credentials 3

The authorized user profile has information that identifies the device(s) being used to access the e-PHI

- Optional parameter selected by the administrator

Each authorized user may have several different devices that are used to access e-PHI

Devices can be shared between users

Each device must be identified by specific device characteristics

- Device MAC address (optional, selected by the administrator)
- Type of device (optional, selected by the administrator)
- Device operating system type/ version (optional, selected by the administrator)
- Device browser type (optional, selected by the administrator)

An authorized user can access e-PHI only when

- Correct login credentials are provided
- The authorized user is using an authorized device (optional, selected by the administrator)

Logging, Auditing, and Monitoring 1

HIPAA requires that a log is kept of all accesses to ePHI. In the event of a data breach this log will be used by forensic experts to identify the source of the data breach

Monitor the data communications of all staff and contractors of the covered entity and identify when any attempt is made to access a server or cloud based storage that contains e-PHI

> Logs are kept of access to Cloud based storage however HIPAA compliant cloud providers have to limit access only to authorized users and maintain a log of accesses
>
> To ensure that the covered entity is compliant, it may have to demonstrate that it has implemented access control for cloud storage as the HIPAA compliance status of the cloud storage may change with time

Logging, Auditing, and Monitoring 2

User access data logs are held on storage internal to the access controller, with a backup mechanism to external storage

Records of user accesses are encrypted, with access only by the administrator using a key

The user log records must be made available when a data breach occurs as specialists must perform a forensic analysis of the data

- The covered entity (hospital, etc) MUST report any data breach immediately, and at the earliest possible date provide data for forensic analysis, permitting identification of how and when the data breach occurred

Logging, Auditing, and Monitoring 3

HIPAA requires that an unauthorized attempt to access e-PHI should be logged and the administrator should be notified immediately

Attempts to access e-PHI can take one or more of the following forms

Repeated attempts to find a password for a specific username
Any MAC/IP that attempts logins with combinations of usernames/passwords
Any repeated access attempt from a device which is not listed as an approved device in the approved user database

What is logged in the event of an attempted unsuccessful access

The MAC and IP address of the attempting device
Time(s) and date(s) of occurrences
List what type of attempt(s) was being made

All of the above listed attempts are notified to the administrator via email

Steps to implement the technology infrastructure for HIPAA Security Rule deployment

Modify the local area network (LAN) design following the segmentation rules (see following pages) so that all servers containing e-PHI are connected to a protected isolated segment

Separate e-PHI databases that have a different set of authorized users, databases must be identified by unique IP addresses

Ensure that both authorized and non-authorized users are contained within the user network segment, this includes both wired and wireless devices

Create the Access Controller administrator account that will be used to log usage and send email messages regarding abnormalities such as attempted accesses from non-authorized users

Create the Access Controller authorized user database, specifying for each authorized user which e-PHI servers that each authorized user is permitted to access (using IP addresses)

Install the Access Controller between the user segment, and the e-PHI server (protected) segment

Network Segmentation Rules

Segmentation requires that all e-PHI servers be located in one isolated subnet

e-PHI databases that have different authorized users must be located with unique IP addresses in order to implement the access control methodology

The access controller routes authorized accesses to the appropriate local server(s) containing the e-PHI being requested

The access controller routes authorized accesses to remote cloud servers

Remote access to both local and cloud servers is made using a VPN to an end point server connected to the user local area network segment

Segmented Network Architecture

The secure network segment containing e-PHI servers is connected directly to the firewalled Internet router to permit a server application to have access to a remote server if necessary

The firewalled Internet router must block all incoming traffic, with the exception of a VPN service for remote users

Medical equipment which accesses e-PHI servers is connected directly to the secure network segment

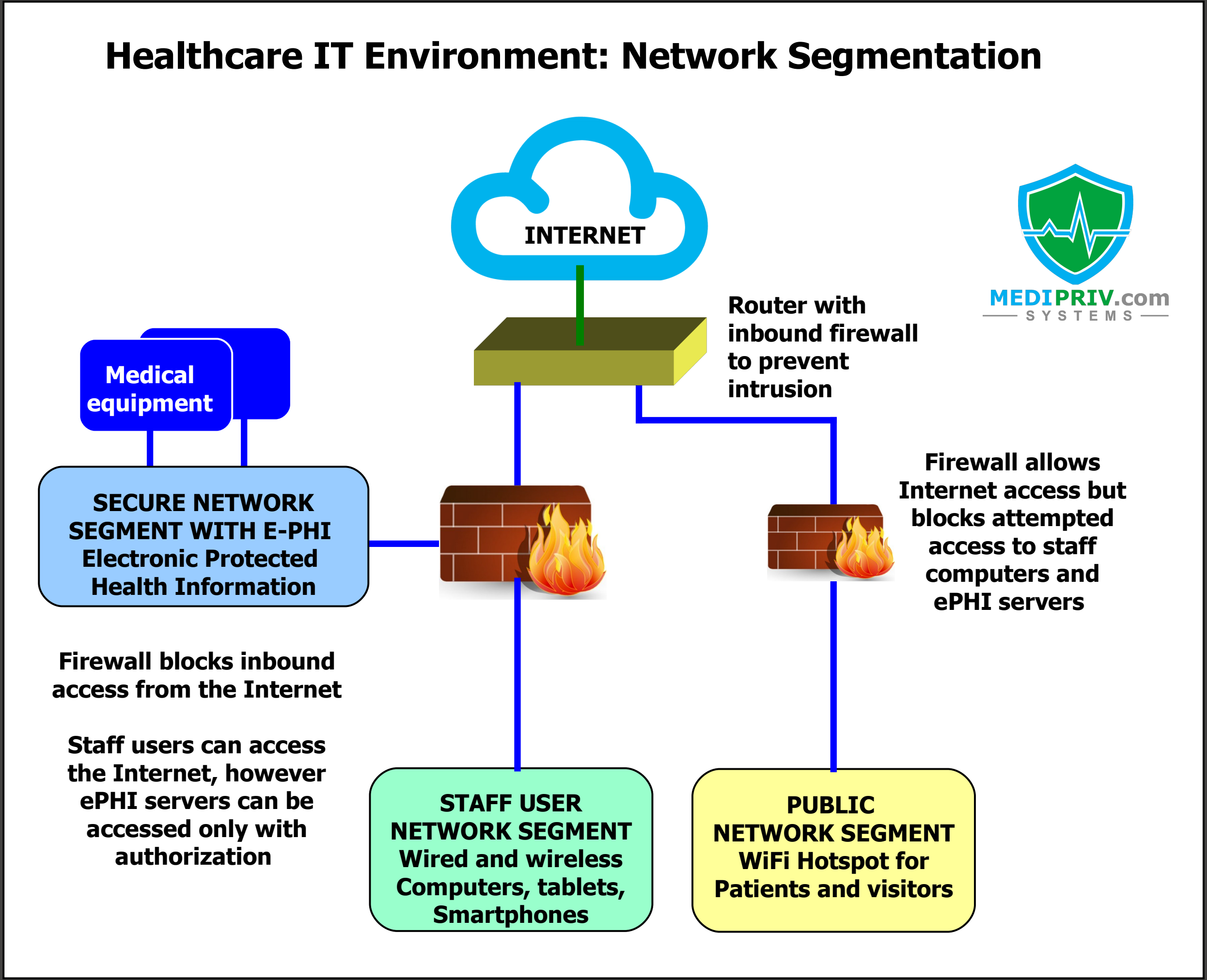
The remote access VPN gateway is connected to the user network segment, so that remote VPN users have to pass through access control

The user segment is connected to the secure segment through the access controller

All authorized and non-authorized user computers are connected to the user segment wired and wirelessly

Public Internet access (patients and visitors) is a separate network segment managed by the Internet access controller

The administrator connection to the access controller is a security weak point: the administrator can connect out-of-band (isolated network connection) or can manage via the Cloud


Healthcare IT Environment: Network Segmentation
INTERNET
Router with inbound firewall to prevent intrusion
MEDIPRIV.com SYSTEMS
Medical equipment
SECURE NETWORK SEGMENT WITH E-PHI Electronic Protected Health Information
Firewall allows Internet access but blocks attempted access to staff computers and ePHI servers
Firewall blocks inbound access from the Internet
Staff users can access the Internet, however ePHI servers can be accessed only with authorization
STAFF USER NETWORK SEGMENT Wired and wireless Computers, tablets, Smartphones
PUBLIC NETWORK SEGMENT WiFi Hotspot for Patients and visitors

Network Segmentation

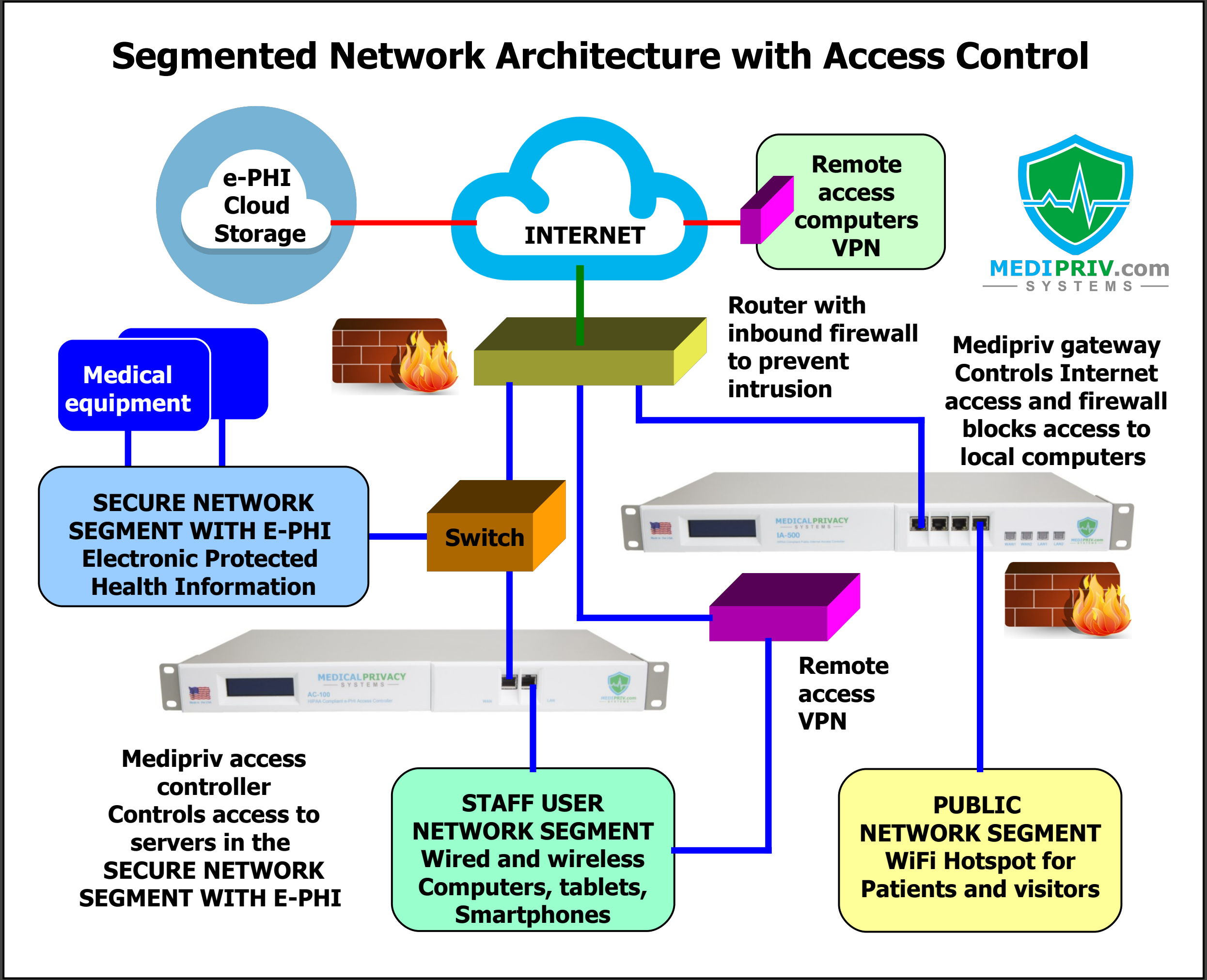
Three network segments are required by the healthcare entity, each with a firewall to control access:

Secure segment containing ePHI servers

Staff computer segment, desktop and laptop computers, tablets and smartphones

Public network for patients and visitors providing Internet access

Segmented Network Architecture



Segmented Network Architecture with Access Control
e-PHI Cloud Storage
INTERNET
Remote access computers VPN
MEDIPRIV.com SYSTEMS
Router with inbound firewall to prevent intrusion
Medipriv gateway Controls Internet access and firewall blocks access to local computers
Medical equipment
SECURE NETWORK SEGMENT WITH E-PHI Electronic Protected Health Information
Switch
MEDICAL PRIVACY SYSTEMS IA-500
MEDICAL PRIVACY SYSTEMS AC-100
Remote access VPN
Medipriv access controller Controls access to servers in the SECURE NETWORK SEGMENT WITH E-PHI
STAFF USER NETWORK SEGMENT Wired and wireless Computers, tablets, Smartphones
PUBLIC NETWORK SEGMENT WiFi Hotspot for Patients and visitors

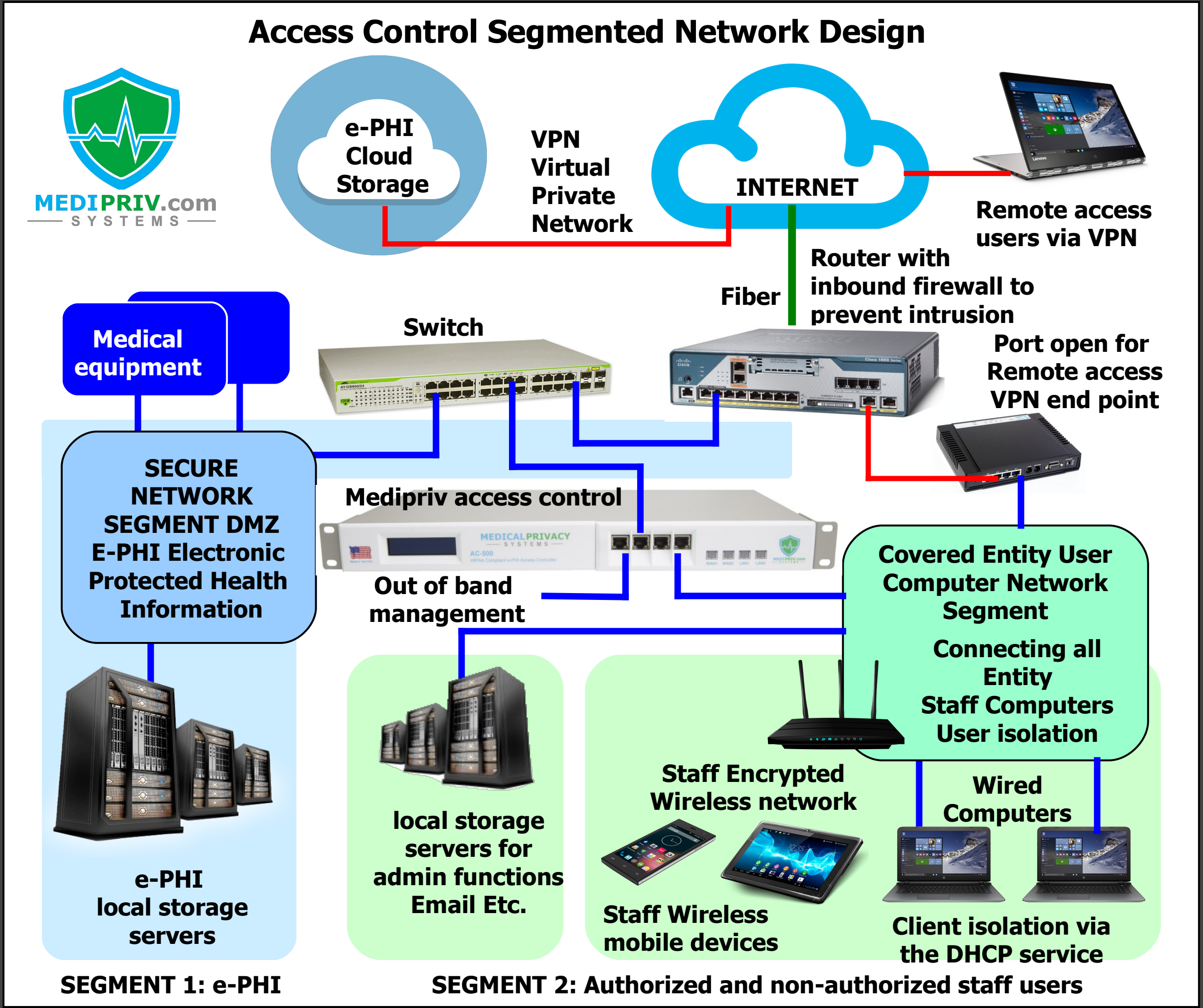
Inbound router/firewall blocks access to ePHI via the Internet

Access controller allows access to ePHI only from authorized users

Remote authorized users must access ePHI via the access controller

Public WiFi must have a firewall to prevent ePHI access by public users

Access Control Segmented Network Design


MEDIPRIV.com SYSTEMS
e-PHI Cloud Storage
VPN Virtual Private Network
INTERNET
Remote access users via VPN
Fiber
Router with inbound firewall to prevent intrusion
Port open for Remote access VPN end point
Switch
Medical equipment
SECURE NETWORK SEGMENT DMZ E-PHI Electronic Protected Health Information
Medipriv access control
Out of band management
Covered Entity User Computer Network Segment
Connecting all Entity Staff Computers User isolation
e-PHI local storage servers
local storage servers for admin functions Email Etc.
Staff Encrypted Wireless network
Wired Computers
Staff Wireless mobile devices
Client isolation via the DHCP service
SEGMENT 1: e-PHI
SEGMENT 2: Authorized and non-authorized staff users

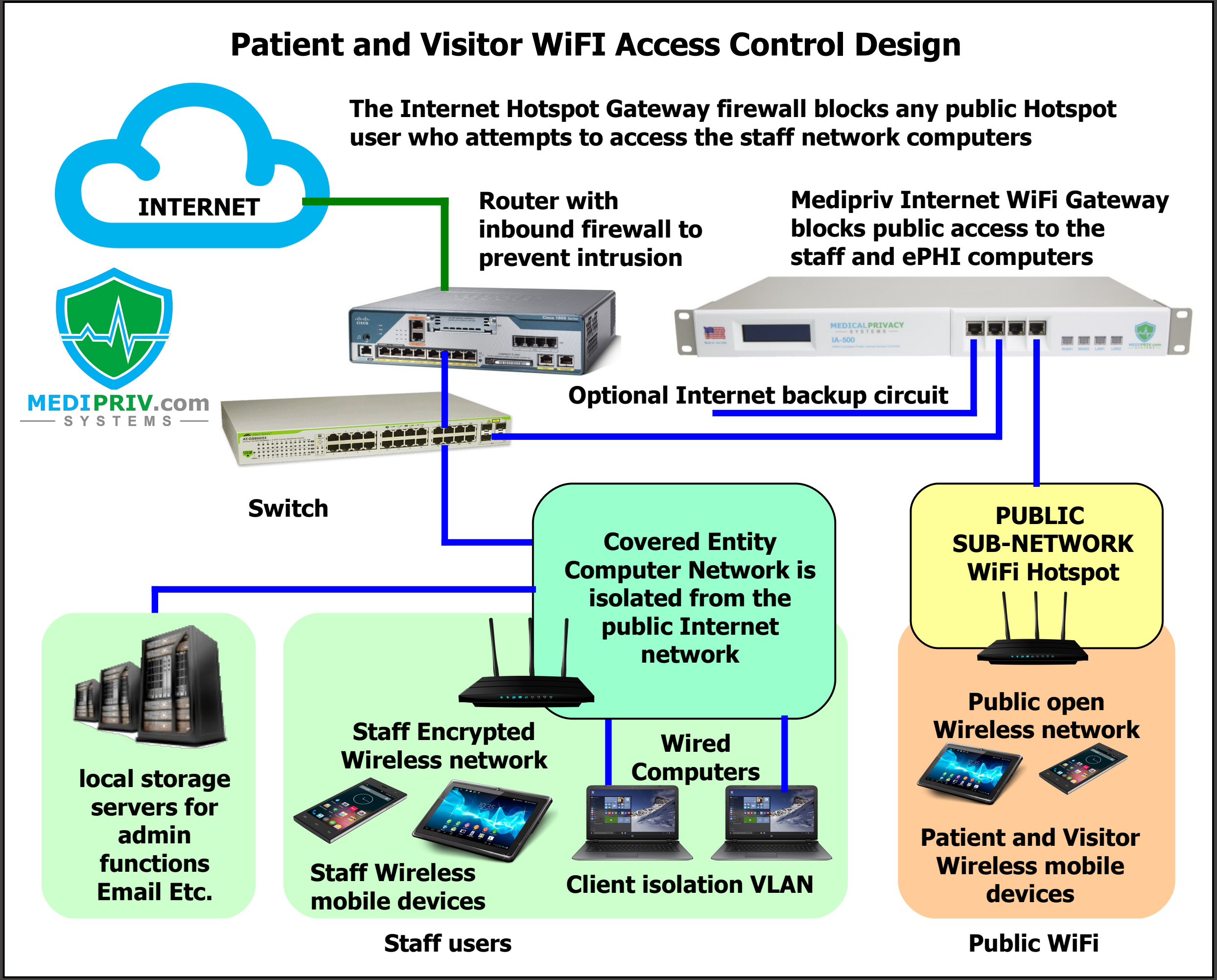
Segmented Network Design

Staff computers have access to non-ePHI network services and to the Internet, however authentication is required to access ePHI servers, both locally and in the cloud via VPN

Remote access is via VPN to the staff network and requires authentication to access ePHI

If possible the administrator connection to the access controller should be 'out-of-band' (not accessible via the staff network) for security

Patient and Visitor WiFi



Patient and Visitor WiFI Access Control Design
The Internet Hotspot Gateway firewall blocks any public Hotspot user who attempts to access the staff network computers
INTERNET
Router with inbound firewall to prevent intrusion
Medipriv Internet WiFi Gateway blocks public access to the staff and ePHI computers
MEDIPRIV.com SYSTEMS
Optional Internet backup circuit
Switch
Covered Entity Computer Network is isolated from the public Internet network
PUBLIC SUB-NETWORK WiFi Hotspot
Public open Wireless network
local storage servers for admin functions Email Etc.
Staff Encrypted Wireless network
Wired Computers
Staff Wireless mobile devices
Client isolation VLAN
Patient and Visitor Wireless mobile devices
Staff users
Public WiFi

The public WiFi network is a possible point of access to ePHI that a hacker will attempt to exploit

Patients and visitors using the public WiFi get routed to the Internet

Any attempt to access the entity computer network or ePHI data servers is blocked by the firewall

Secure Cloud Management

Security of the access controller is very important and two methods of management are available to minimize tampering

- Out of band administrator access, a secondary isolated network used for device management
- Administration via an encrypted cloud management connection

Medipriv Secure Cloud Management
MEDIPRIV.com
SYSTEMS
MEDICALPRIVACY
SYSTEMS
AC-500

Medipriv Cloud management features

Remote monitoring and management for one or many access controllers

Manage access controllers individually, or in groups

Performance stats for individual access controllers and for groups

Access controller failure monitoring

Central authentication for individual access controllers and for groups of access controllers

The ideal tool for IT firms who provide managed services for healthcare entities

SECURITY STANDARDS: TECHNICAL SAFEGUARDS

PART 2:

1 Current challenges to meet HIPAA security compliance

2 HIPAA Security Rule requirements for e-PHI access control

3 HIPAA Security Rule solution providers

4 Medipriv implementation of e-PHI access control to meet the HIPAA Security Rule requirements

5 Beyond HIPAA: Hacking Risks and Multi-factor Authentication

Security Strengths and Weaknesses

Hackers use several methods to attempt access of ePHI data, the two most common are:

Via the Internet: hack through the router/firewall to get access to the servers, then hack into the servers to get access to the data, finally encrypt the database to extort a ransom

Difficulty is high

Plant a 'Trojan' software onto a users computer by sending an email with a link, clicking the link installs the Trojan, the Trojan then lets the hacker take control of the computer. The hacker waits until the user authenticates access to the ePHI, then attempts to access the server to encrypt the data and extort a ransom

Difficulty is low if the computer has outdated operating software and the user is unaware of the risk (as in the case of the recent ransomware attack on the UK NHS service that used a security flaw in Windows XP)

Difficulty is high if (i) the computer has the latest operating software, (ii) the computer has anti-virus software installed, (iii) the entity has email virus/trojan detection, and (iv) the user is aware of the risk

SINGLE-FACTOR AUTHENTICATION: Recommended by HIPAA

The implementation of the HIPAA technical safeguards will provide a degree of security that will make access to ePHI difficult, but it will not stop determined malicious attacks

Hackers have discovered that healthcare entities are easy targets, due to the lack of security and sensitivity of the data, and the entities are willing to pay big ransom demands quickly, using untraceable bitcoin

HIPAA authentication requires SINGLE FACTOR AUTHENTICATION, however HIPPA specifies two important parameters that will strengthen the authentication method:

> Strong password, however HIPAA does not specify minimum character length, minimum letter caps and lower case, minimum numeric, and minimum non-alphanumeric. This is the decision of the IT manager
>
> Frequent password changes, however HIPAA does not specify the period, can be 30/60/90 days

Data security can be improved with MULTI-FACTOR authentication, methods are described on the following pages

TWO-FACTOR AUTHENTICATION: Device Verification

In addition to a strong password, 2-factor authentication requires the identification of a previously approved computer/tablet/smartphone for that user to gain access to ePHI

Identification is made using a number of parameters: MAC address + OS type + browser type etc.

Device authentication can ensure that only computers with the latest OS, and with the latest security patches can access ePHI.

For example, this method would have prevented the recent ransom-ware attack in the UK NHS healthcare system, which occurred because users had Windows XP computers with security vulnerabilities that were exploited

THREE-FACTOR AUTHENTICATION: OTP

In addition to the previous two factors, one-time password (OTP) authentication can be used

OTP is used by many banks (we safeguard our money better than our patients information)

Usually a smartphone app provides a pass code (4 to 6 numerical digits) that is valid for only a short period of time (1 minute) and has to been entered after the users password

The pass code can also be provided by a special credit card type of device with a numerical display

Three factor authentication improves security of data and reduces the probability of hacking, however it does not protect against the 'trojan horse' attack. With this method the hacker sends emails with links to the entity staff, if the user clicks on the link then software is installed that gives the hacker remote access to the computer. When the user logs in to the network using 3-factor authentication the hacker can start hacking the servers via the logged in computer

It is very important that any device connecting to the network has anti-virus software to minimize a Trojan being installed if the user clicks on the hackers link

FOUR-FACTOR AUTHENTICATION: Profiling

The Profiling authentication method is used by technology companies, like Google

The Profiling authentication method monitors the users constantly while the user is logged in to the network

A record is stored of all the types of data access made by the user, the longer the user is connected then the access information becomes more reliable

If the user deviates from the normal routine then that user is flagged and optionally the user can be blocked from the network

The deviation will occur when a hacker is using a Trojan installed on the users computer to access servers that are not normally accessed by the user. The hacker will attempt to gain access to the server, and subsequently encrypt the database to demand a ransom to unlock the data

Final:

1 SUMMARY

2 FURTHER READING

3 MEDIPRIV: Medical Privacy Systems

Summary

Consultants who assess HIPAA Security Rule compliance for healthcare entities state that a significant percentage of entities are not compliant with the HIPAA Security Rule

Implementation of the Security Rule is technically challenging and few specialists are available to implement a solution that covers all aspects of the Rule

The cost of non-compliance is very high in the event of a data breach, much higher than the cost of implementing the Security Rule

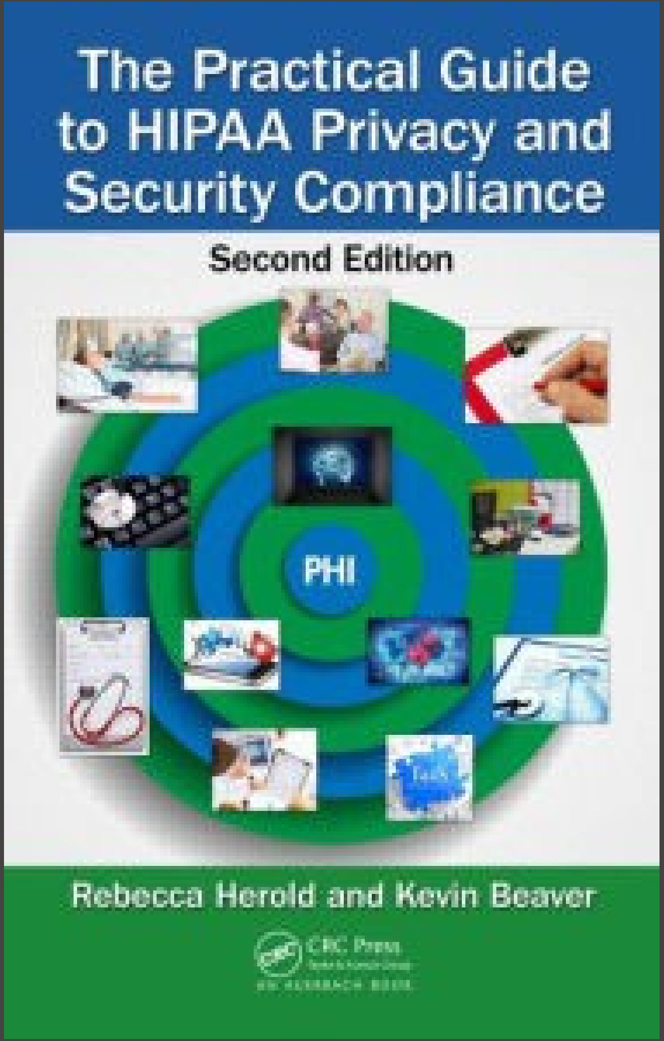
- Civil and criminal penalties
- Patient litigation
- Payment of ransom

Healthcare entities are especially targeted by hackers seeking to extort money, principally through ransomware attacks

- Healthcare entities in general have poor data security so are easy to hack
- Unavailability of data will pressure the entity to pay quickly due to urgency

Further Reading

See section 22, page 331
Building a HIPAA-Compliant
Technology Infrastructure



The Practical Guide to HIPAA Privacy and Security Compliance

Second Edition

Rebecca Herold and Kevin Beaver

CRC Press

FIME
MEDLAB
AMERICAS

Please visit our booth: **A.T81**

MEDIPRIV.com
SYSTEMS

Medical Privacy Systems
Part of the Fire4 Systems Inc. Group