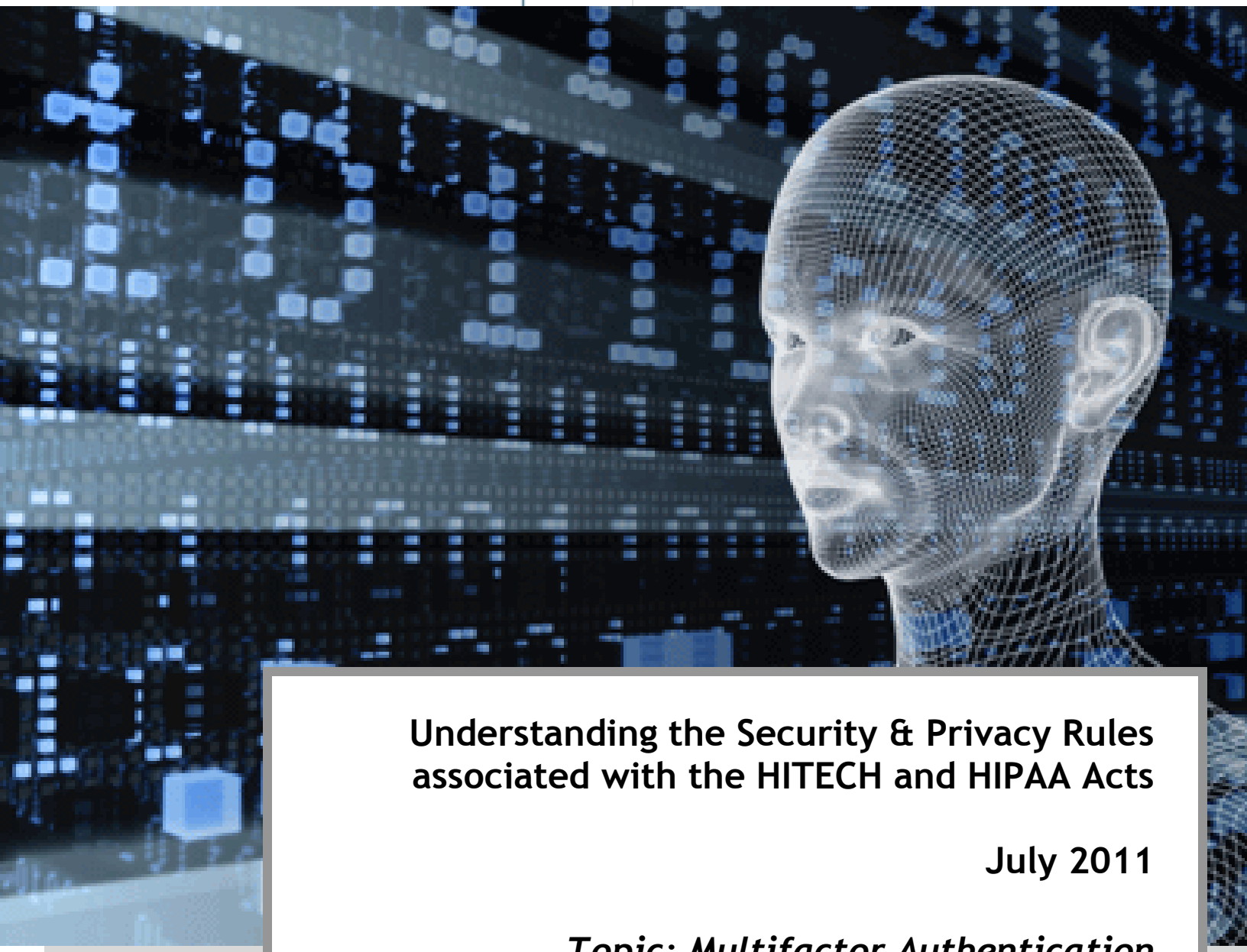
SECURE IT



Understanding the Security & Privacy Rules associated with the HITECH and HIPAA Acts

July 2011

Topic: Multifactor Authentication

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires covered entities and their business associates to comply with new guidance related to security and privacy of Protected Health Information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) was recently strengthened via Security and Privacy Rules issued by the Centers of Medicare and Medicaid Services (CMS).

The purpose of this paper is to examine the regulations, rules and guidelines for one aspect of security and privacy, multifactor authentication. The goal of this paper is to aid organizations in decisions regarding implementation of security and privacy protections to support access to health information or electronic health records (EHR).

Introduction

The Federal Government has issued a series of regulations and supporting rules which specify security and privacy requirements for organizations that provide healthcare services or information technology solutions that contain Electronic Personal Health Information (EPHI). This paper provides the reader an overview of the information security and privacy requirements and guidance of the Health Insurance Portability and Accountability Act (HIPAA and the Health Information Technology for Economic and Clinical Health (HITECH acts. Additionally, since many healthcare organizations interface to Federal government systems, a brief overview of the Federal Information Security Management Act (FISMA) is also provided.

Purpose

The purpose of this paper is to examine one specific aspect of these regulations and associated rules and guidance --- pertaining to the factors and requirements for multi-factor authentication. This paper examines the applicable regulations and supporting rules, controls and implementation guidance to aid system implementers and service providers to determine applicability based on their situation of:

- Commercial/non-profit organization providing IT services/solutions to another commercial/non-profit organization involving EPHI or otherwise subject to HIPAA
- Commercial/non-profit organization providing IT services/solutions to a Federal Government agency involving EPHI or otherwise subject to HIPAA
- Commercial/non-profit organization providing IT services/solutions via a Federal Government grant involving EPHI or otherwise subject to HIPAA

Intended Audience

This paper is intended for Chief Information Officers, Chief Information Security Officers, Risk and Compliance Officers, Chief Privacy Officers and individuals responsible for developing and implementing information technology solutions that support Healthcare organizations.

Background

The Department of Health and Human Services (HHS) issued an interim final rule which increases penalties for violations of HIPAA . HITECH Act increased the penalties that HHS can issue for violations of HIPAA rules. Section 13410(d) of the HITECH Act creates ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision. A covered entity can no longer bar the imposition of a civil money penalty for an unknown violation unless it corrects the violation within 30 days of discovery. This rule became effective on Nov 30, 2009.

On July 27, 2009, Kathleen Sebelius (Secretary HHS) delegated authority for the administration and enforcement of the Security Standards for the Protection of EPHI Security Rule to the Office for Civil Rights (OCR). This action combines the authority for administration and enforcement of the Federal standards for health information privacy and security (HIPAA).

Healthcare organizations, covered entities and their business associates are pursuing improvements to Health IT (HIT) to increase access to critical health information and improve the quality of care while creating efficiencies and reducing costs. Organizations must examine the security and privacy provisions of these acts and implement the necessary security, controls and protections or risk fines and penalties.

Implications of these regulatory changes:

- Business Associates (BA) are now held to the same standards as Covered Entities for safeguarding, use and disclosure of PHI. The American Recovery and Reinvestment Act of 2009 (ARRA) extends application of civil and criminal penalties, and the new obligations that are enacted as part of the legislation to Business Associates.
- Addresses new types of entities as Business Associates, including Health Information Exchange (HIE) Organizations, Regional Health Information Organization, E- prescribing Gateways, and Personal Health Vendors contracting with Covered Entities.
- Permits the HHS Secretary to conduct audits of both covered entities and business associates.
- Creates a temporary presumption that "minimum necessary" data is equivalent to the "limited data set" where an entity will be treated as being in compliance with the minimum necessary standard only if it limits disclosure to a "limited data set" or to the "minimum necessary" data that is required to accomplish the intended purpose of the use or disclosure.
- Effective date for entities that currently have electronic medical record systems is January 1, 2014. For entities that begin using electronic medical record systems after January 1, 2009, the effective date is the later of January 1, 2011, or the date upon which they begin using such systems. These dates can also be changed by the Secretary through regulation, but in no event can they be later than 2016 or 2013 (two years later than specified by statute)

Definitions and Abbreviations

Covered Entity	A health care provider that conducts certain transactions in electronic form (called here a "covered health care provider"), a health care clearinghouse or a health plan
Breach	the unauthorized acquisition, access, use or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information
Business Associate	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.
Personal Health Record	an electronic record of "PHR identifiable health information," that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.
Vendor of PHR	an entity, other than a covered entity, that offers or maintains a PHR identifiable health information --- individually identifiable health information on an individual including information that is provided by or on behalf of the individual; and that identifies the individual or there is a reasonable basis to believe that the information can be used to identify the individual.
EPHR	Electronic version of the Personal Health Record
EPH	Electronic Protected Health Information
Unsecured PHI	Information not secured through use of technology or methodology specified by the Secretary of HHS in the guidance document; or not protected by a technology standard that renders PHI unusable, unreadable, or indecipherable that is developed or endorsed by a

standards developing organization accredited by American National Standards Institute

FISMA ..... Federal Information Security Management Act included in the eGovernment Act of 2002 which specifies information security requirements for all Federal Government agencies which has been extended to other organizations that contract with or connect to Federal Government agencies.

Current Threat Environment

Verizon issued the "2009 Verizon Business Data Breach Investigation Report"[1] that provides analysis and trends from more than 280 million records that were compromised worldwide in 90 separate security breaches. While the incidents were performed by both internal and external sources, it is noteworthy to mention that the three (3) leading types of compromised information were:

1. Compromised Data;
2. Personal Information; and
3. Authentication Credentials.

Computer criminals utilize a wide array of methods to obtain sensitive information ranging from social engineer to malicious software. However, the 2009 Data Breach Report indicates that the leading method used by hackers and computer criminals is by using unauthorized access accounts or shared credentials (See figure below).

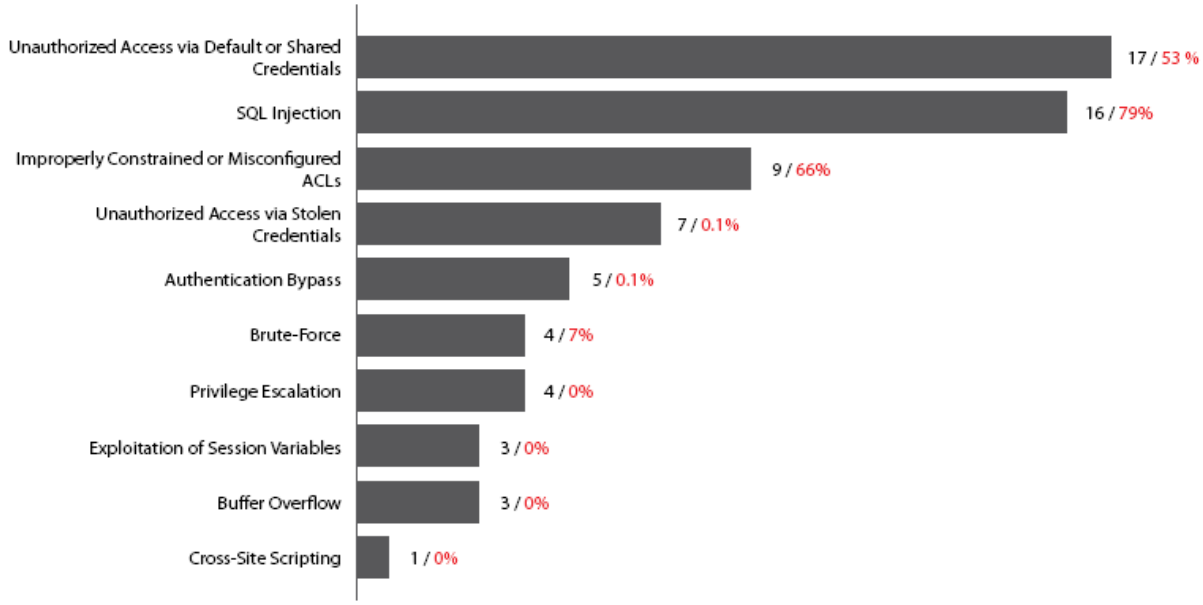


Figure 1 - Types and Frequency of Hacking by Number of Breach (courtesy Verizon)

In figure 1, the number of breached records is reported in (black) and percent of records breached reflected in (red)

[1] http://www.verizonbusiness.com/worldwide/products/security/risk/databreach/

In 2010, Verizon released the "2009 Data Breach Investigations Supplemental Report Anatomy of a Data Breach"[2]; Verizon reported that malware was by far the greatest threats to data security as indicated in the summary graphic below.

Table 1. Top 15 threat action types from 2009 DBIR

Threat Category	Threat Action Type	Legend	% of Breaches	% of Records
Malware	Keyloggers and Spyware	KEYLOG	19%	82%
Malware	Backdoor or Command/Control	BACKDR	18%	79%
Hacking	SQL injection	SQLINJ	18%	79%
Misuse	Abuse of system access/privileges	ABUSE	17%	1%
Hacking	Unauthorized access via default credentials[3]	DFCRED	16%	53%
Misuse	Violation of Acceptable Use and other policies[3]	POLICY	12%	<1%
Hacking	Unauthorized access via weak or misconfigured ACLs	WKACL	10%	66%
Malware	Packet sniffer[4]	SNIFFER	9%	89%
Hacking	Unauthorized access via stolen credentials	STLCRED	8%	<1%
Deceit	Pretexting (Social Engineering)	SOCIAL	8%	2%
Hacking	Authentication bypass	BYPASS	6%	<1%
Physical	Physical theft of asset	THEFT	6%	2%
Hacking	Brute-force attack	BRUTE	4%	7%
Malware	RAM scraper[4]	RAMSCR	4%	<1%
Deceit	Phishing (and *ishing variations)	PHISH	4%	4%

Figure 2 - Threat Action Types Corresponding to Breaches (courtesy of Verizon)

As evidenced from this analysis and trend, strong authentication control is; therefore, key to prevent some of the most pervasive types of attacks on systems containing sensitive information. This paper will explore the guidelines and regulations issued by the Federal government regarding the implementation of appropriate authentication mechanisms for information systems containing personal health information,

Analysis of the Regulations

Health Insurance Portability and Accountability Act (HIPAA)[3]

The CMS has delegated authority to enforce the HIPAA Security Standards, and may rely upon the guidance it prepares in determining whether or not the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity and availability of EPHI. CMS may be given deference in any administrative hearing pursuant to 45 C.F.R. § 160.508(c)(1), the HIPAA Enforcement Rule. Specifically, §164.312(d) states that the covered entity should "**implement procedures to verify**

[2] http://www.verizonbusiness.com/resources/security/reports/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf
[3] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

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

Health Information Technology for Economic and Clinical Health (HITECH) Act[4]

The HITECH Act, enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of this act specifies the privacy and security concerns associated with the electronic transmission of health information. The HITECH Act expands the HIPAA Security Rule (SR) requirements to all Business Associates (BA) responsible for processing, transmitting, and storing EPHI. The HITECH act also includes several provisions that expand the requirements for reporting security breaches and strengthen civil and criminal enforcement of the HIPAA rules.

As a result of expanding the HIPAA Security Rules to all business partners, the following standards for health information technology to protect health information created, maintained, and exchanged as defined by 45 CFR Subchapter D § 170.210 are also applicable:

(a) Encryption and decryption of electronic health information.
(1) General. A symmetric 128 bit fixed-block cipher algorithm capable of using a 128, 192, or 256 bit encryption key must be used.
(2) Exchange. An encrypted and integrity protected link must be implemented.

(b) Record actions related to electronic health information. The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, deleted, or printed; and an indication of which action(s) occurred must also be recorded.

(c) Verification that electronic health information has not been altered in transit. A secure hashing algorithm must be used to verify that electronic health information has not been altered in transit. The secure hash algorithm (SHA) used must be SHA-1 or higher.

(d) Cross-enterprise authentication. A cross-enterprise secure transaction that contains sufficient identity information such that the receiver can make access control decisions and produce detailed and accurate security audit trails must be used.

(e) (e) *Record treatment, payment, and health care operations disclosures.* The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.[5]

Federal Information Security Management Act (FISMA)

The FISMA specifies IT security requirements to all federal government agencies. FISMA requires agencies to inventory their systems, assign impact values for these systems, implement baseline security controls, develop a plan of actions and milestones (POA&M) to track remediation efforts, and formal authorization of systems with acceptance of residual risks (formerly called certification and accreditation (C&A)). FISMA also requires Federal agencies to ensure then when agencies contract for services or solutions from vendors, that FISMA requirements be specified in these contracts.

FISMA requires system boundaries to be defined, security plans, policies, procedures and controls implemented and subsequently assessed by an independent party. Organizations must demonstrate due diligence and put in place processes and technology to continually monitor security controls and vulnerabilities to demonstrate risk management and achieve compliance. Underlying FISMA is the standards issued by the National Institutes of Standards and Technology (NIST).

[4] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf
[5] http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=7fc34d36679e0fbef3091beca363b598&rgn=div5&view=text&node=45:1.0.1.4.73&idno=45#45:1.0.1.4.73.2.27.4

NIST has developed and continually updates and expands a suite of "special publications" that provide guidance for implementing risk management. Termed the Risk Management Framework (RMF), NIST prescribes an approach to be followed which is required of Federal agencies and oftentimes specified in contractual requirements/agreements with its vendors, suppliers and service providers. The figure below depicts the steps in the RMF and corresponding guidance from NIST.

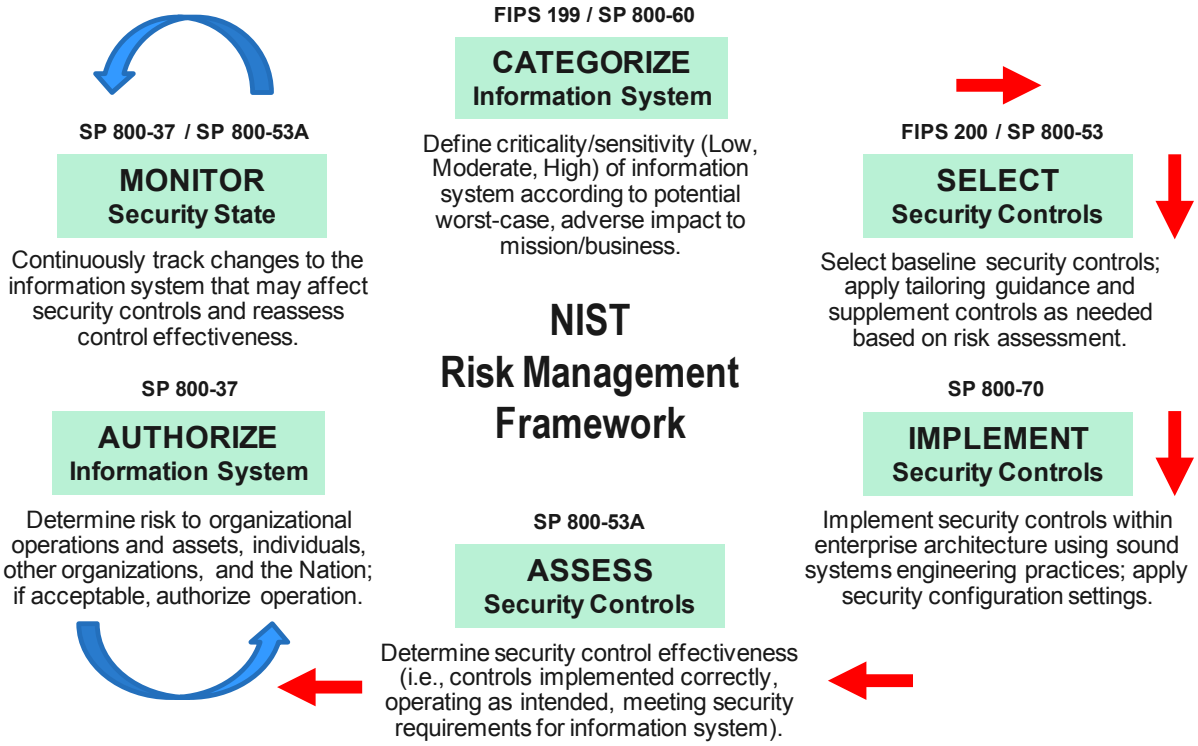


Figure 2 - NIST Risk Management Framework

NIST Special Publication 800-37 defines the overall process for security authorization of systems. NIST Special Publication 800-53 defines the minimum security controls which must be implemented based on the security impact level of the system (Low, Moderate or High). Figure 3 depicts a summary of the security control families. The applicable security controls are based on the security impact level (L, M, H) and a number of other factors such as environmental factors; the ability to tailor based on individual security values for confidentiality, integrity and availability; physical or policy-related factors.

As an agency of the U.S Federal government, CMS is subject to FISMA. CMS provides guidance and policy to contractors of CMS where contractor systems process CMS information or connect with CMS information systems. Through the Business Partner Systems Security Manual (BPSSM)[6], CMS defines security requirements and reporting processes for CMS contractors. The basis of BPSSM guidance is grounded in NIST. However, CMS has implemented agency-specific processes, standards and security controls. The control framework is based on NIST Special Publication SP 800-53 and is in the process of being updated to the current Revision 3 of these controls.

The following 800-53 Revision 3 security control is specified for Moderate Impact systems (which is the minimum impact level for processing EPHI):

[6] http://www.cms.hhs.gov/manuals/downloads/117_systems_security.pdf

IA-2 The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Enhancements:

(1) The information system uses multifactor authentication for network access to privileged accounts.

(2) The information system uses multifactor authentication for network access to non-privileged accounts.

(3) The information system uses multifactor authentication for local access to privileged accounts.

(8) The information system uses [Assignment: organization-defined replay-resistant authentication mechanisms] for network access to privileged accounts

Control Family	Control Family Title
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	Maintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

Figure 3 - NIST Security Controls

Organizations must determine if e-Authentication is applicable to the system. If it deemed applicable, then the assurance levels must be determined following NIST SP 800-63 guidance. Organizations with information systems defined as Moderate or High impact due to processing or storage of EPHI that are connected to the internet will most likely result at least a Level 3 Assurance. Level 3 assurance level is defined to require:

> *Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks.* ***A minimum of two authentication factors is required****. Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens and "one-time password" device tokens.*

Examination of the Security and Privacy Rules

HIPAA Privacy Rule[7]

The Privacy Rule, as well as all the Administrative Simplification rules, applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities").

[7] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

The Privacy Rule defines the requirements for Access and Use of EPHI as:

> *For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.*

HIPAA Security Rule[8]

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, is 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 Security Rule defines access in § 164.304 as

"the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition applies to "access" as used in this subpart, not as used in subpart E of this part [the HIPAA Privacy Rule])."

In addition, all covered entities are to review and modify, where necessary, security policies and procedures on a regular basis. For example, covered entities and business associates need to ensure their policies are up to date with regulations and guidance for ***remote access to EPHI through portable devices or on external systems or hardware not owned or managed by the covered entity***.

CMS Guidance for Complying with the Security Rule[9][10]

The CMS has provided the HIPAA Security Information Series which is a group of educational papers which are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. The security series includes guidance on "Technical Safeguards" for Access Control and Authentication. Provided below is guidance regarding access control:

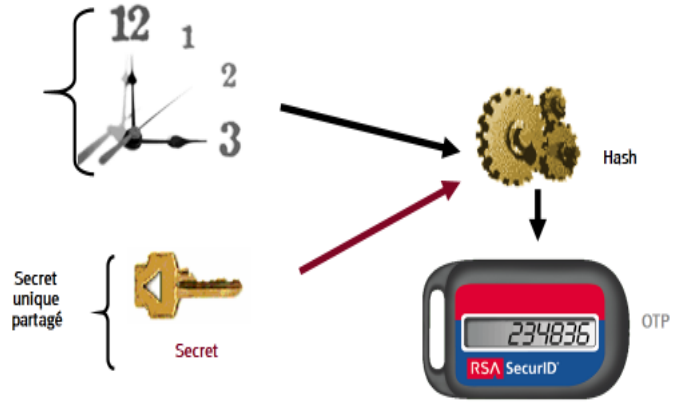
> *Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules that the covered entity is required to implement as part of § 164.308(a)(4), the Information Access Management standard under the Administrative Safeguards section of the Rule. Four implementation specifications are associated with the Access Controls standard:*
>
> - *Unique User Identification (Required)*
> - *Emergency Access Procedure (Required)*
> - *Automatic Logoff (Addressable)*
> - *Encryption and Decryption (Addressable)*
>
> *The Person or Entity Authentication standard is defined in § 164.312(d) and has no implementation specifications. This standard requires a covered entity to: "Implement procedures*

[8] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[9] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html
[10] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

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

In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to EPHI. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:

- *Require something known only to that individual, such as a password or PIN.*
- *Require something that individuals possess, such as a smart card, a token, or a key.*
- *Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.*



Most covered entities use one of the first two methods of authentication. Many small provider offices rely on a password or PIN to authenticate the user. If the authentication credentials entered into an information system match those stored in that system, the user is authenticated. Once properly authenticated, the user is granted the authorized access privileges to perform functions and access EPHI. Although the password is the most common way to obtain authentication to an information system and the easiest to establish, covered entities may want to explore other authentication methods.

Remote Use Guidelines, 12/28/2006[11]

CMS prepared this guidance document to reinforce ways covered entities can protect EPHI when it is accessed or used outside of the organization's physical control. This guidance presents strategies that may be reasonable and appropriate for organizations that conduct some of their business activities through:

- The use of portable media/devices (such as USB flash drives) that store EPHI
- Offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers or other non corporate equipment.

Covered entities must develop and implement policies and procedures for authorizing EPHI remote access in accordance with the HIPAA Security Rule at §164.308(a)(4) and the HIPAA Privacy Rule at §164.508. It is important that only those workforce members who have been trained and have proper authorization are granted access to EPHI. CMS has identified the following risk and provided suggested risk mitigation strategies:

Risk: Log-on/password information is lost or stolen resulting in potential unauthorized or improper access to or inappropriate viewing or modification of EPHI.

Possible Risk Management Strategies: Implement ***two-factor authentication for granting remote access to systems that contain EPHI****. This process requires factors beyond general usernames and passwords to gain access to systems (e.g., requiring users to answer a security question such as "Favorite Pet's Name"). Alternatively, implement a technical process for creating unique user names and performing authentication when granting remote access to a*

[11] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

workforce member. This may be done using Remote Authentication Dial-In User Service (RADIUS) or other similar tools.

Results of Analysis

Organization Situation	Requirement for Multi-Factor Authentication
Commercial/non-profit organization providing IT services/solutions to another commercial/non-profit organization that involves EPHI. • Covered entity • Business associate	Your organization is subject to the HIPAA and HITECH Acts and their respective security and privacy requirements. The use of multi-factor authentication is not explicitly required by the HIPAA or HITECH Act at the present time. However, these acts require CMS to provide and update implementation guidance. CMS has issued implementation guidance strongly encouraging organizations to deploy multi-factor authentication for access to systems containing EPHI on portable devices or to connect to external systems or hardware not owned by the covered entity.
Commercial/non-profit organization providing IT services/solutions to the CMS subject to BPSSM policy.	Organization must comply with CMS IT security guidelines specified in its contract with CMS. Typically, CMS specifies compliance with BPSSM which requires multi-factor authentication to protect system administration / privileged access to the system as well as remote access to the application.
Commercial/non-profit organization providing healthcare related services/solutions to a Federal Government agency involving EPHI. Commercial/non-profit organization providing IT services/solutions via a Federal Government grant involving EPHI. Federal Government agency providing services/solutions involving healthcare information and EPHI.	For commercial / non-profit organizations with a contract or a grant from a Federal government agency, examine contract/grant details for references to FISMA, FIPS 200, or NIST SP 800-53. For Federal government agencies, your organization is subject to FISMA, NIST Security Controls and the e-Authentication provisions of the eGovernment Act. Your organization is subject to HIPAA, HITECH and FISMA Act. FISMA regulation via NIST SP 800-53 security controls is the strongest with regard to multi-factor authentication. When involving healthcare information, a Moderate security impact level is the lowest encountered which requires: • Multifactor authentication for network access to privileged accounts. • Multifactor authentication for network access to non-privileged accounts. • Multifactor authentication for local access to privileged accounts. NIST security controls require the organization to conduct an e-Authentication determination and risk assessment to ascertain the required Assurance Level for the associated transactions. Level 3 is typically the minimum assurance level acceptable for systems processing EPHI. Assurance Level 3 requires: • Multi-factor remote network authentication • Identity proofing procedures require verification of

Organization Situation	Requirement for Multi-Factor Authentication
	identifying materials and information. • Authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. • Authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: "soft" cryptographic tokens, "hard" cryptographic tokens and "one-time password" device tokens.

Summary

A user ID and password alone are no longer considered adequate to prevent fraudulent or unauthorized access to private or sensitive information unless other protections are in place. Two-factor authentication (using two different types of authentication), provides a higher level of security and assurance. It is now widely held that two-factor authentication must be implemented in order to provide adequate security to protect remote access. The guidance provided by HHS and CMS addresses this requirement for remotely accessing EPHI for covered entities that must adhere to the HIPAA security regulations.

Organizations that are subject to HIPAA, HITECH or FISMA should examine their system architecture along with authentication and access control usage models to identify instances where multi-factor authentication is recommended based on the security control frameworks cited in this paper and considering the recommendations based on risk by CMS. The table below provides a summary of the authentication requirements based on the regulations and agencies discussed in this paper applicable to all business partners processing, transmitting or storing EPHI.

Regulation/Standard	Authentication Requirement
HIPAA and HITECH	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed
CMS Security Rule	A covered entity may: • Require something known only to that individual, such as a password or PIN. • Require something that individuals possess, such as a smart card, a token, or a key. • Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.
CMS Remote Access Requirement	Implement two-factor authentication for granting remote access to systems that contain EPHI
FISMA-NIST 800-53 Rev. 3	The information system uses multifactor authentication for network access to privileged accounts. The information system uses multifactor authentication for network access to non-privileged accounts. The information system uses multifactor authentication for local access to privileged accounts.

Regulation/Standard	Authentication Requirement
NIST 800-63 for eAuthentication systems at Level 3	Requires multi-factor remote network authentication. At least two authentication factors are required. Identity proofing procedures require verification of identifying materials and information. Authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks.

Figure 4- Federal Regulations and Standards Pertaining Authentication Mechanisms

SecureIT assists Healthcare organizations to understand and develop strategies to effectively and efficiently meet Healthcare and other Federal government security and privacy regulations and standards. SecureIT also provides independent security assessment services to support system security authorization (formerly known as Certification and Accreditation C&A).

About the Author

Jim Graham, Senior VP at SecureIT, has more than 25 years of experience providing IT solutions and cybersecurity professional services to Federal government agencies and commercial organizations. At SecureIT he directs Cybersecurity, Information Assurance, and Governance & Compliance services and solutions for the Federal Government market. Prior to SecureIT, Graham held leadership positions at LEADS Corporation, McDonald Bradley, DOMAIN Technologies and TRW. Mr. Graham earned his BS in Computer Science and Mathematics and maintains certifications for CISSP, CAP and NSA-IAM. He is active in industry associations including ACT-IAC where he is the chair for Cybersecurity.

About SecureIT

SecureIT helps private and public sector clients manage technology risks and implement secure and trusted information systems through effective practices in IT security. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT designs enterprise security programs, implements best practices and assesses technology implementation for security risk. SecureIT devises strategies and solutions to address the unique business needs and environments of our clients resulting in reduced risk and increased efficiency. Leveraging our knowledge and experience with industry regulatory and standards, we assist our clients to overcome the challenges of compliance with FISMA, FISCAM, HIPAA, HITECH, Privacy Act, SOX, and PCI. Founded in 2001 and located in Reston, VA, SecureIT serves clients in the U.S. Federal Government, Financial Services & Banking, and Healthcare markets.

SECURE IT

1902 Campus Commons Drive, Suite 100
Reston, VA 20191
info@secureit.com
www.secureit.com
703-464-7010