WEDI - Strategic National Implementation Process (SNIP)

December 2006 CMS HIPAA Security Guidance

SNIP
December 2006 CMS HIPAA Security Guidance White Paper
Working Draft Version 1.0 – September 2007

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange
12020 Sunrise Valley Drive., Suite 100, Reston, VA 20191
(t) 703-391-2716 / (f) 703-391-2759

Contents

Disclaimer 2

White Paper Background and Overview 3

Outline CMS HIPAA Security Guidance 4

To Whom Does This Apply? 4
Why Is This Important? 4
What Does The Guidance Document Cover? 4

Risk Management Strategies 8

Remote Access Questions- Getting Started 11

Types of Remote Access 13

Summary 14

Other Sources of Information 15

Acknowledgments 15

Disclaimer

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

White Paper Background and Overview

In December 2006 the Centers for Medicare and Medicaid Services [CMS] released a guidance document on HIPAA Security for remote use of ePHI. This first draft white paper is an outline of the guidance document, the risk management strategies suggested in the document, and some basic questions that a covered entity will need to consider before implementing the suggestions in the document. This first draft was used at the WEDI 16th Annual Meeting in Baltimore in May 2007 in a breakout session to brainstorm types and parameters of remote access. This white paper will be revised on an ongoing basis.

Outline CMS HIPAA Security Guidance

To Whom Does This Apply?

This guidance document reinforces the ways a covered entity or its business associates may protect ePHI (outside the organization's secured physical or logical perimeters) when data is;

a) remotely *accessed / transmitted* via mobile or offsite devices or
b) *stored / transported* on portable devices or removable media

While this Guidance is an augmentation to the rule, it is directly written for HIPAA Covered Entities. However many non-covered entities have chosen to adopt HIPAA Security standards in order to demonstrate a level of security administration, physical and technical safeguards and controls. As such, the CMS Guidance Document and this white paper may be helpful to any organization choosing to enhance the security of its data.

Why Is This Important?

CMS has made the following statement about the use of this Guidance document.

> **"The Centers for Medicare & Medicaid Services [CMS] … may rely upon this guidance 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. section 160.508(c)(1), the HIPAA Enforcement Rule."[1]**

This raises the bar for those accessing information from remote locations and may directly affect those business promoting off-site workers. As a result, CMS/OESS has stated that this document may be used to measure compliance- as of the December 2006 publication.

What Does The Guidance Document Cover?

Over recent months, an increasing number and frequency of security incidents related to mobile devices and removable media have been reported by covered entities. These are mobile assets that access, process, store, or transmit ePHI outside the protected perimeter of the organization. This is particularly relevant for covered entities that allow remote access to ePHI via;

- Laptops, PDAs, and Smartphones
- Home-based computers
- Business Associate computers (alliances, partners, software and hardware vendors, etc.)
- Public workstations (hotel, library, internet café, etc.)

Equally important, is the proper use and handling of removable media commonly used in devices for storing and backing up ePHI such as;

- USB External Flash Drives
- External Hard Drives
- Memory Cards (SD, CF, MiniSD, MicroSD, Memory Sticks, etc.)

[1] Page 1, *CMS HIPAA Security Guidance, December 26, 2006*

- CDs, DVDs, Floppy Disks and DAT (digital tape cartridges)

These devices and media are most vulnerable in high threat areas such as;

- airports
- parked cars
- hotels
- high traffic public areas
- public wireless access areas
- unsecured areas within the organization itself

Likelihood of actual data compromise can be realized through various events and practices such as;

- theft or accidental loss of mobile devices, removable media, or backup media
- business associate remote access to ePHI
- service repairs of equipment containing ePHI
- decommissioning and disposal of equipment containing ePHI
- eaves dropping of transmitted ePHI
- shipping devices or backup media containing ePHI

The guidance document sets forth strategies that may be reasonable and appropriate for organizations that conduct some business activities through:

- Transmitting ePHI with mobile or remote devices via FTP file transfers, HTTP (web), SMTP/MIME/Web (email), or WAP (wireless) protocols.
- Storing ePHI on the mobile device's internal or removable media in the form of emails, data backups, browser cache, temporary files, etc.
- Accessing ePHI via portable devices, external systems or hardware not owned or managed by the covered entity.

"In general, covered entities should be extremely cautious about allowing the offsite use of, or access to, ePHI."[2]

"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]

A covered entity must evaluate its own need for offsite use of, or access to, ePHI and when deciding which security strategies to use. The HIPAA covered entity must consider the factors identified in 45 C.F.R. section 164.306(b)(2):
(i) The size, complexity, and capabilities of the covered entity.
(ii) The covered entity's technical infrastructure, hardware, and software capabilities.
(iii) The costs of security measures.
(iv) The probability and criticality of potential risks to [ePHI].

With respect to remote access to or use of ePHI, covered entities should place significant emphasis and attention on:

[2] Ibid
[3] Ibid

- Risk analysis and risk management strategies
- Policies and procedures for safeguarding ePHI
- Security awareness and training on the policies and procedures for safeguarding ePHI

Risk Analysis and Risk Management Drive Policies

The covered entity's analysis of the risks associated with accessing, storing and transmitting ePHI will form the basis for the policies and procedures designed to protect this sensitive information. Each area should be individually addressed.

1. Complete analysis of potential threats and vulnerabilities and their associated risks with remote access to, and offsite use of, ePHI.

2. Implement risk management measures that reduce the overall impact and likelihood of vulnerabilities being exploited to a reasonable and appropriate level in compliance with 45 C.F.R. Section 164.306(a).

3. CMS groups risks related to remote use into three area:
    a. Access
    b. Storage
    c. Transmission.

Summary of Policy and Procedure Considerations

Remote data access policies and procedures focus on ensuring that users only access data for which they are appropriately authorized.

1. Remote access to ePHI should only be granted to authorized users based on their role within the organization and their need to access ePHI. Storage policies and procedures address the security requirements for media and devices that move beyond the covered entity's physical control and contain ePHI. This includes media and devices such as; Laptops, PDAs, smart phones, hard drives, backup media, USB flash drives or any other storage items which could potentially be removed from the organization's facilities.

2. Transmission policy and procedures focus on ensuring the integrity and safety of ePHI transmitted over networks. This includes:

    a. direct exchanges of data (i.e. trading partner relationships)
    b. appropriate use of encryption and decryption and
    c. The provisioning of remote access to applications hosted by the organization (i.e. provider's home access to ePrescribing systems or "web mail" in organizations where ePHI might be included in internal communications).

Policies Require Training

Workforce must have appropriate awareness and training that specifically address threats and vulnerabilities associated with remote access and use of ePHI.

" …covered entity must make reasonable efforts to ensure that any such use or access is authorized

and limited as required by the HIPAA Security Rule at 45 C.F.R. 164.308(a)(4) and the HIPAA Privacy Rule."[4]

1. Training should provide, *at minimum clear and concise instructions* for remotely accessing, storing and transmitting ePHI.
2. Training should provide procedures for transporting stored ePHI (i.e. shipping laptops for repair, transporting backup tapes to offsite locations, etc.)
3. If applicable, training should include;
    a. Password management procedures (for changing and safeguarding passwords)
    b. Remote device / media protection guidelines (i.e. unattended assets)
    c. Prohibition of ePHI transmission over open network (including email)
    d. Prohibition of downloading ePHI to public or remote computers
    e. Prohibition of transmitting or accessing ePHI via open wireless networks unless transmission is through a secure web site

Addressing Security Incidents and Non-compliance

A covered entity's security incident procedures must specify the actions workforce members take to manage harmful effects of the loss.

1. Procedures may include:
    a. Securing and preserving evidence (i.e. data forensic procedures)
    b. Managing the harmful effects of improper use or disclosure
    c. Notification to affected parties

2. Incidents should be evaluated as part of the covered entity's ongoing risk management initiatives. Previous or historical incidents may increase the likelihood of certain events re-occurring unless controls are augmented. These incidents should be considered during the required risk analysis.

3. A sanction policy must be in place, and be effectively communicated to the workforce members so that they understand the consequences of failure to comply with the Remote Access and Usage Policy and Procedures.

4. A covered entity should consider at least requiring employees to sign a statement of adherence to Policy and Procedures (P&Ps) as a prerequisite to employment.

[4] Ibid, page 4

Risk Management Strategies[5]

It is important to continually build on your initial HIPAA Security compliance activities. Go back to your original or most recent compliance review and consider adding the following threats and vulnerabilities to your risk analysis and cross reference your policies and procedures to consider adding the following technical and policy solutions. Consider reviewing other national standards for solutions as well (such as NIST, ISO, OCTAVE, etc...)

1. Assessing ePHI *(45 C.F.R. section 164.308(a)(4) and section 164.508)*

***Risk #1*:** Log-on / password (user authentication) information is lost or stolen resulting in potential unauthorized or improper access to or inappropriate viewing or modification of ePHI

- Implement two-factor authentication (employ the use of two distinct methods of authenticating the user) for granting remote access to systems that contain ePHI. Some "thin client" terminal services / remote access software products have this functionality built in
- Implement a technical process for creating unique user names and perform authentication when granting remote access to a workforce member.
- Disable or change default user accounts
- Do not establish a common password for all new user accounts when they are set up or reset

Risk #2: Workforce member access ePHI when not authorized to do so while working offsite

- Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access
- Establish remote access roles specific to applications and business requirements
- Implement appropriate audit trails that log inappropriate system and ePHI access by unauthorized workforce members and regularly review audit trails
- Ensure that the issue of unauthorized access of ePHI is addressed in the required sanction policy

Risk #3: Home or other offsite workstations left unattended risking improper access to ePHI

- Establish appropriate procedures for session termination [time-out] on inactive portable or remote devices
- Establish procedures to automate device logoff after a period of inactivity (such as password protected screen savers)

Risk #4: Contamination of systems by malicious code introduced from an infected external device used to gain remote access to systems that contain ePHI

- Install personal firewall software on all laptops and mobile devices that store or access ePHI or connect to networks on which ePHI is accessible
- Consider the use of Virtual Machines that assist in partitioning potentially harmful code from infecting areas of ePHI within remote devices
- Consider using secured thin client technology that transmits screen shots of remote data and not actual data
- Consider using Virtual Machines that provide a secured working environment partitioned from potential harmful code

[5] Ibid, paraphrased from pages 4 -- 6

- Install, use and regularly update anti-virus and anti-spyware software on all portable or remote devices accessing ePHI
- Implement manual or automated procedures requiring regular updates of virus and spyware signature
- Implement manual or automated procedures requiring regular complete full virus and spyware scans of devices and associated media before allowing access to systems containing ePHI

2. *Storing ePHI*

Risk #1: Mobile devices or media lost or stolen resulting in potential unauthorized / improper access to or modification of ePHI housed on or accessible through the device

- Identify the types of hardware or electronic media that must be tracked, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards, and security equipment. Develop an inventory control system that tracks the vital assets of the enterprise
- Implement process for maintaining a record of movements of, and person(s) responsible for, or permitted to use hardware and electronic media containing ePHI
- Require use of lock-down or other locking mechanisms for unattended laptops
- Password protect and encrypt files, mobile devices, and removable media containing ePHI with appropriate strength and complexity
- Develop a patch management processes to ensure security updates are deployed to portable devices
- Consider two factor authentication on mobile devices (i.e. biometric fingerprint readers)
- Implement policies that prohibit leaving portable devices or media unattended (i.e. vehicles, hotels, at home, etc.)

Risk #2: Use of external device to access corporate data resulting in the loss of operationally critical ePHI on the remote device

- Develop manual or automated processes to ensure timely backup of all ePHI entered into and/or stored on remote devices and media
- Deploy policy to encrypt backup and archival media; backup storage is secure; ensure that policies direct the use of encryption technologies of the appropriate strength

Risk #3: Un-authorized access of ePHI left on devices and media after inappropriate disposal by the organization

- Establish ePHI data shredding policies and media disposal procedures
- Use data shredding programs that overwrites data
- Use media shredding equipment for CDs, DVDs, etc. containing ePHI

Risk #4: Data is left on an external device or media, such as in a library or a hotel business center

- Prohibit or prevent downloading ePHI into remote systems, devices or storage media without operational justification
- Ensure workforce is appropriately trained on policies that require users to search for and overwrite any ePHI saved to an external device. Minimize use of browser-cached data in web based applications which manage ePHI, particularly those accessed remotely
- Consider using secured thin client technology that transmits screen shots of remote data and not actual data
- Consider using portable virtual machines that provide a secured encrypted working environment partitioned from the host computer

Risk #5: Contamination of systems by malicious code introduced from a portable storage device

- Install anti-virus and anti-spyware software and automate the use on all portable or remote devices that store ePHI

3. Transmitting ePHI

Risk #1: Data intercepted or modified during transmission

- If possible, create a secure channel where information exchange takes place. The use of VPN or a secure wireless network are just two examples that can be configured for secure trading of information
- Prohibit transmissions of ePHI via open networks such as the Internet, where appropriate
- Prohibit the use of offsite devices or wireless access points, such as hotel workstations that allow non-secure access to e-mail Use more secure connections for e-mail via SSL and the use of message-level standards such as S/MIME, SET, PEM, PGP, etc.
- Implement and mandate appropriate strong encryption solutions for transmission of ePHI, such as SSL, HTTPS, etc. 128 bit SSL should be a minimum requirement for all Internet-facing systems which manage ePHI in any form, including corporate web-mail systems

Risk #2: Contamination of systems by malicious code introduced from an external device used to transmit ePHI

- Install anti-virus and anti-spyware software on portable devices that can be used to transmit ePHI. Require regular automated or manual full scans of devices and media as well as automated frequent virus signature files updates

Remote Access Questions- Getting Started

1. How many workforce members have remote access to ePHI?

2. Does your organization have an inventory of all ePHI?

3. Make a list of the names of the staff members and vendors who have remote access
   - What is the purpose for workforce member remote access?
   - What is the type of access permitted the workforce member?
   - What type of ePHI is the workforce member permitted to access?
   - What is the role of the workforce member granted remote access?
   - What software applications do each identified workforce member access?

4. Has your organization conducted a data flow analysis to determine the origination and destination of ePHI and the supporting devices it flows between?

5. What type of remote access devices and tools are permitted within your organization?
   - Laptops
   - Home-based personal computers
   - PDAs
   - Smart phones
   - Hotel, library or other public workstations and Wireless Access Points [WAPs]
   - USB flash drives (Jump drives)
   - Memory cards
   - Floppy disks
   - CDs
   - DVDs
   - Back-up media
   - Email
   - Smart cards
   - Remote access devices
   - Other: _____

6. What current security controls are in place for remote access within your organization?
   - Have they been tested?
   - Do these need to be updated?
   - List what needs to be updated

7. What are the current policies and procedures in place for remote access within your organization?
   - Do these need to be updated?
   - List what needs to be updated
   - Does it include access to ePHI and access management P&Ps?
   - Does it include ePHI storage P&Ps?
   - Does it include transmitting ePHI P&Ps?
   - Does it include data backup and recovery procedures?
   - Does the sanctions policy adequately address remote access?
   - Are they being audited for compliance and enforced by sanctions?

8. What current workforce training is in place for remote access?
   - Does it need to be updated?
   - List what needs to be updated

9. What are your business cases for remote access to ePHI?
   - Include in your analysis the requirements found in 45 C.F.R. section 164.306(b)(2)

10. Has your organization performed a risk analysis for remote access?
    - Has the results been documented and communicated to upper management?
    - Have the identified risks been verified through penetration testing?
    - Does include remediation strategies?

11. Do current Disaster Recovery and Emergency Mode Operation Plans address the use of portable devices, removable media and remote access?

12. Do current Disaster Recovery Plans address loss or corruption of data stored on portable media or devices?

Types of Remote Access

1. Telecommuting / Home Office
2. Off Site Storage
3. Traveling Workforce
4. Business Associates
5. Off Shore

Summary

The December 2006 CMS HIPAA Security Guidance document prods covered entities to review who has, and what types of remote access is used by their office or facility. It recommends that a covered entity needs to review its risk analysis work and update it as necessary. It recommends that a covered entity needs to review its workforce training and update as necessary. It recommends that a covered entity need to review its policies and procedures that deal with remote access, and update as necessary.

Other Sources of Information

Other sources of HIPAA privacy and security information can be found on the WEDI/SNIP Web site at http://www.wedi.org

Acknowledgments

WEDI SNIP SPWG Co-Chair
Susan A. Miller, JD
COO, CPO, HealthTransactions.com

WEDI SNIP Co-Chair and SPWG Co-Chair
Lesley Berkeyheiser
Principal, The Clayton Group

WEDI SNIP SPWG Co-Chair
Mark Cone
Principal, N-Tegrity Solutions Group

Larry C. Eighmy, CISSP, CISM, PMP
President / CEO, The Halo Group, Inc.