McGraw Wentworth

SPECIAL Alert

Volume Three, Issue Two January 2007

In This Issue

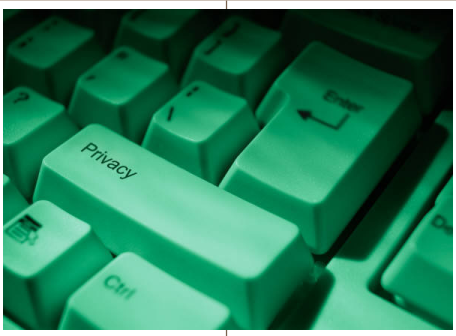
In this second Special Alert for 2007, we will discuss guidance recently released by the Department of Health and Human Services. The guidance addressed the Health Insurance Portability and Accountability Act's (HIPAA's) Security Rule. The Security Rule impacts all covered entities that use, store, create or transmit Electronic Protected Health Information (EPHI).

The Security Rule outlined broad parameters that covered entities needed to address to protect EPHI. The lack of specifics was quite intentional as covered entities needed to design compliance steps that worked with their activities and systems. However, with the prevalence that EPHI is compromised in remote work situations, the Department felt compelled to provide more details on how to protect EPHI in remote work situations or during data transmissions.

We welcome your comments and suggestions regarding this issue of our Special Alert. For more information on this article, please contact your Account Manager or visit the McGraw Wentworth web site at www.mcgrawwentworth.com.

"Additional Guidance of HIPAA Security"

It is not uncommon to hear that personal information has been stolen from major organizations across the United States. The Department of Health and Human Services is concerned with the number of thefts of Electronic Protected Health Information (EPHI) reported by entities covered under the HIPAA's Security Rule.



All covered entities must comply with HIPAA's Security Rule. Covered entities include health care providers, health information clearinghouses and group health plans. The Security Rule protects the confidentiality, integrity and availability of EPHI. EPHI is information on an individual's physical or mental health condition, or information on the payment of care for that individual that is stored or transmitted electronically. For more information on HIPAA's Security Rule, please read our Advisor at http://www.mcwent.com/Benefit_ Advisor/2003/Issue%20Six.pdf.

The Department of Health and Human Services recently released additional guidelines for protecting EPHI when the information is accessed or used in locations outside a covered entity's direct control. The additional guidance sets forth reasonable and appropriate strategies for protecting EPHI in the following two situations:

1. When workforce members use portable media or devices that store EPHI, such as USB flash drives.
2. When workforce members access data offsite or transport EPHI via laptops, personal digital assistants (PDAs), home computers or any non-corporate equipment.

Because the use of portable media devices may compromise EPHI, the Department has established guidelines to ensure the data is protected. Portable media devices include laptops, home-based personal computers, personal digital assistants (PDAs), smart phones, public computer workstations (at hotels, libraries, and other public workstations), Wireless Access Points, USB drives, memory cards, CDs, and so on.

In general, covered entities should be extremely cautious about allowing or encouraging employees to use, or access EPHI offsite. The Department discourages offsite use unless it is required for business reasons. Limiting offsite access for only necessary situations is a good strategy for protecting data. When covered entities need to allow remote access, they should

Continued on Page 2

completely review their current security policies and procedures and conduct a risk analysis to ensure EPHI is adequately protected.

The guidelines separate offsite use and transport risks into three areas of concern: access, storage and transmission. Risk management strategies should encompass all three of these areas as well as the specific vulnerabilities identified as a potential concerns:

- Data access policies and procedures should ensure remote users have access only to EPHI they need for work purposes. Remote access should be granted only to employees who need it.
- Storage policies and procedures should ensure EPHI contained in media and devices beyond the direct control of the covered entity remains protected. Laptops, hard drives, back up media and any other devices must be secure.
- Policies and procedures for transmitting data should ensure the integrity and safety of EPHI sent over networks in both direct data exchanges and remote access to the organization's applications.

The new guidance also offers suggestions for improving remote security. Covered entities are strongly encouraged to adopt the suggested strategies. The government strongly recommends using passwords to protect access to systems that house EPHI as well as to protect data files sent from a media device or over the Internet.

The table to the right shows examples of potential risks that covered entities may identify during their risk analysis and possible strategies to manage the risks.

Continued on Page 3

Possible Risks	Potential Risk Management Strategies
Log-on / password information is lost or stolen resulting in the potential for unauthorized or improper viewing and potentially altering EPHI.	- Implement a two-factor authentification process for granting remote access to systems containing EPHI. This process adds an extra layer of security. It may be as simple as asking a security question related to the user, such as first pet's name or the name of the street the user lived on as a child. - Implement a technical process for granting access to remote users and authenticating the remote access to a workforce member. This process may require using a Remote Authentication Dial in User Service (RADIUS) or a similar technological tool.
Employees working offsite access EPHI when not authorized to do so.	- Develop and use a proper clearance procedures and verify the employee has been trained before allowing remote access. - Establish remote access roles specific to applications and business requirements. Different users may be assigned different user rights for various levels of EPHI according to the needs of the specific job functions. - Ensure that your sanction policy appropriately addresses the unauthorized use of EPHI. The orginization needs to police and punish employees for unauthorized use of EPHI.
Home or other offsite workstations are left unattended, risking the potential of improper access to EPHI.	- Establish appropriate procedures for terminating sessions after a period of inactivity. If the system accessed is a software product, check with your vendor to activate the automatic logoff after a period of inactivity.
Virus contamination from an infected external device used to gain remote access to systems that contain EPHI.	- Install personal firewall software on all laptops that store or access EPHI and for any connections to networks storing EPHI. - Install, use and regularly update virus-protection software on all portable or remote devices used to access EPHI.
Lost or stolen laptop or other portable device resulting in potential unauthorized use or disclosure of EPHI.	- Inventory all types of hardware and electronic media used with EPHI, such as hard drives, magnetic tapes, digital memory cards and so on. - Implement a process to keep records of when these devices are moved or used including the employee responsible for maintaining and using any of these devices. - Require lock down procedures for any of these devices when they are not in use. - Password protect any files containing EPHI. - Password protect all portable media devices . - Require that all portable or remote devices containing EPHI have appropriate encryption technology. - Develop a process to make sure all these devices receive any required security updates. - Consider using biometric identifiers, such as fingerprint readers on portable devices.
Loss or theft of EPHI left on an improperly discarded device.	- Create procedures for deleting EPHI from electronic devices. Simply deleting a file does not adequately ensure the file is removed. Use special tools to ensure EPHI is completely deleted or, if appropriate, physically destroy the storage media or device.
Data is left on an offsite external device such as a computer in a library or hotel business center.	- Prohibit employees from downloading EPHI on remote systems without operational justification. - Ensure employees are properly trained on procedures to search for and delete any saved files on the external device. - Minimize the use of browser-cached data in a web-based application that manages EPHI, particularly those accessed remotely.

Additional Security Rule Resources	URL
Detailed Review of HIPAA Security Rule	www.cms.hhs.gov (follow the link under "Regulations and Guidance" for HIPAA educational materials)
Discussion of HIPAA Security Rule Topics	www.cms.hhs.gov/EducationMaterials/ (this section will provide access to the "Security Series of Papers" which are numerous white papers written to address specific aspects of the Security Rule)
Feedback or questions on the just issued remote access guidance?	RemoteAccessGuidance@cms.hhs.gov (Address your questions to Michael Phillips in the office of eHealth Standards and Services.)

The new guidelines also offer strategies to prevent data transmitted over a network from being intercepted or altered. Suggested risk management strategies include:

- Prohibit the transmission of EPHI over an open network, such as the Internet, whenever possible.
- Prohibit the use of offsite devices or Wireless Access Points for non-secure access to e-mail.
- Use more secure connections for e-mail.
- Implement and mandate appropriately strong encryption solutions for transmitting EPHI.

Training is a key to keeping EPHI secure. A covered entity can develop the best policies and procedures, but if employees do not understand the security provisions, the procedures will not be effective. Employees need to be trained on the vulnerabilities of accessing data remotely and risks associated with transporting data on portable media devices or memory devices. According to the Department, many of the reported security breaches were created by individuals who were unaware of the risks associated with accessing data remotely. Employees need to be trained to recognize potential problems that may be well known to IT personnel but not common knowledge to remote users.

The new guidance also expands the discussion on how covered entities should handle a security incident. Employees working remotely must be ready to resolve a security incident if the EPHI is compromised. Procedures for dealing with a remote security breach may include:

1. Securing and preserving evidence.
2. Managing any potential harmful effects of improper use or disclosure.
3. Notifying appropriate parties.

The covered entity must establish sanction policies. Employees need to understand the consequences of failing to comply with the security policies and procedures. In fact, the new guidelines recommend employees be required to sign a document stating they will adhere to the security policies and procedures as part of employment. This requirement should add weight to the necessity of following policies and procedures at all times.

Concluding Thoughts

This additional guidance on the Security Rule certainly provides more specifics than the Department of Health and Human Resources has offered in the past. Until now, the Department was reluctant to provide specifics for two reasons. First, since technological advances happen every day, the guidelines were kept technologically neutral to keep the regulations current. Second, an organization's ability to meet the security requirements varies depending on its size. A large employer group health plan can ensure security more easily than a mid-size employer.

Most organizations will welcome the glimpse of the procedures the government thinks are adequate to protect EPHI. Although the government procedures are probably more conservative than the procedures your organization has already implemented, it makes sense to review the protections you have in place for using the data remotely. It may be wise to reduce the use of EPHI offsite if possible, and implement procedures to protect this information if necessary.

Please contact your McGraw Wentworth Account Manager with any questions. MW

McGraw Wentworth Team

ACCOUNT DIRECTORS

DIRECTOR OF TECHNICAL SERVICES

MANAGER, CLIENT SERVICES

ASSISTANT MANAGER, CLIENT SERVICES

SR. ACCOUNT MANAGERS

ACCOUNT MANAGERS

CONTROLLER

PRINCIPAL PLAN ANALYST

SR. PLAN ANALYSTS

PLAN ANALYSTS

DIRECTOR OF INFORMATION TECHNOLOGY

SYSTEMS SUPPORT SPECIALIST

ADMINISTRATIVE SUPPORT

HUMAN RESOURCE DIRECTOR

MARKETING MANAGER

MARKETING DEPARTMENT

McGraw Wentworth, Inc.
3331 West Big Beaver Road, Suite 200
Troy, MI 48084
Telephone: 248-822-8000 Fax: 248-822-4131
www.mcgrawwentworth.com