

Special points of interest:

- HIPAA SECURITY
- HIPAA PRIVACY

## HIPAA SECURITY

### HIPAA Security

In previous Newsletters we've addressed the implementation of the HIPAA Security requirements for small group health plans by April 20, 2006. The HIPAA Security requirements only apply to protected health information (PHI) in electronic form. Electronic media includes storage media such as hard drives, magnetic tapes or disks, and digital memory cards, and it also includes transmission media such as the Internet, extranets, leased lines, dial-up lines, private networks and the physical movement of electronic storage media. The security regulations require Plan Sponsors to implement safeguards to protect PHI in electronic form from unauthorized access, alteration, deletion or transmission.

The preambles to the regulation clarifies that the definition of electronic PHI does not include "employment records" held by the Plan Sponsor in electronic form even though such records may include individually identifiable health information. For example, individually identifiable health information in electronic form received from a source other than the health plan (such as workers' compensation health records, FMLA health data, health information to administer "reasonable accommodation" requests under the ADA and drug testing results) is not electronic PHI in the hands of the employer. The security regulations also clarify that de-identified information is not subject to the security requirements.

The following are the 4<sup>th</sup>, 5<sup>th</sup>, 6<sup>th</sup> and 7<sup>th</sup> a series of 8 articles prepared by The Clayton Group, a HIPAA consulting company, to assist in HIPAA Security compliance. These articles are designed to provide a process overview and are not meant to provide legal advice. You should seek your own legal counsel or consulting service for HIPAA Security compliance.

The below list of articles will address electronic data technologies, operational reengineering (policy and procedure development), strategic planning.

- Article #1 - Getting Started
- Article #2 - Completing Your Risk Analysis
- Article #3 - The Remediation Process (technical vs. policy)
- Article #4 - The Controversial Issues: Email and Encryption
- Article #5 - Sanctions
- Article #6 - Handling Security Incidents
- Article #7 - Training
- Article #8 - Ongoing Compliance & Evaluation

Source: The Clayton Group, 2/20/06, [www.theclaytongroup.org](http://www.theclaytongroup.org)

### **Email And Encryption (No. 4 in series of 8 articles)**

#### **Email And Encryption**

Email is a powerful communication tool making our lives easier and our ability to do business faster. However, the very features that allow it to be easily used can also establish a potential security risk. As a result, email usage and monitoring should be reviewed as part of your HIPAA risk assessment.

- *Internally*, an organization has various levels of controls (from a technical and administrative policy perspective) that can make sue of email within the organization's firewall more secure.
- *Externally*, an organization has fewer options to control the level of risk outside the firewall. One of the best methods available today is the use of encryption.

Finding the right solution for your organization includes balancing the confidentiality, integrity and availability of protected health information.

## Decreasing the Risk of Email Misuse

### Technical considerations:

- Based on the results of your risk analysis; consider implementing strong encryption for open network emails.
- Ban use of instant messaging (as it is inherently insecure).
- Consider using other safe email applications/products.
- Implement a technical mechanism to authenticate the sender and receiver.
- Compress large files using a tool like WinZip before attaching an email message.
- Backup your email on a regular basis. Only allow access to the backup file to those with a "need to know".
- Actively monitor and manage email accounts and usage.

### Workforce considerations

- Expect your workforce to be your weakest link in your organization's security protection as it relates to email.
- Take steps to comprehensively define policies and train users.
- Only use the "reply all" feature when you know the identity of each recipient.
- Do not allow distribution groups or keep all email addresses and distribution groups up to date to avoid misdirection of information.

Email usage is an area where the technology and workforce cannot accomplish the end goal working alone. The best solution will only be successful when the two work hand-in-hand balancing the confidentiality of the data, with its availability to support your business needs.

Even if you have subcontracted much of your operations to a TPA, you still need to consider YOUR direct workforce members and the TPA should be providing you proof that they have implemented policies and procedures to adhere to HIPAA on your behalf!

Next week's feature will provide information about the use of workforce sanctions as the major tool for ongoing HIPAA compliance.

## **Sanctions (No. 5 in series of 8 articles)**

### Sanctions

Sanctions are the glue that holds HIPAA compliance together. In order to be compliant with HIPAA Privacy and Security, your organization must assure that all workforce members receive role-specific, detailed training regarding

the organization's protected health information safeguards.

Think of sanctions as the lever that encourages a workforce member to carry out your organization's chosen procedures.

In order to institute a strong sanctions program, an organization must also be sure it clearly defines what a breach is. Providing levels such as the following can help make the importance of the issue clear in the workforce members mind:

Level of Breach	Example	Penalty
Improper and/or unintentional breaches	Workforce member unintentionally sends fax to restaurant as a result of careless keying of fax number	* Verbal warning for first offense. Increased workforce training on subject * Recurring violation warrants written warning with period of days to cure.
Unauthorized use or misuse	Workforce member uses [ENTITY] computer to download executable files (.exe) or screen savers found on the internet.	* Written warning with clear direction that repeat offense will result in suspension and/or termination
Willful and/or intentional disclosures	Workforce member shares his/her password that allows someone else to view or search for PHI in [ENTITY] system to release it to the public	* Termination of employment * Other appropriate legal recourse

### **Big picture steps to assure compliance as it relates to your workforce including the following:**

- Be clear and comprehensive in organizational policies and procedures.
- Train the workforce members according to his/her job functions. Use clear examples of what kinds of behavior constitute a breach that may result in sanctions.
- Document that the workforce member has been trained on the required policies and procedures (some organizations tie yearly reviews and competency levels to specific policies and procedures).
- Encourage the workforce to report when things go wrong. Be clear so that they know intentional breaches will be dealt with swiftly.
- When you do apply sanctions, clearly define why, and what is being applied. Consider implementing a period of time for the workforce member to be on "probation" to assure they are closely watched to facilitate a positive behavior change.

- Examine why sanctions occurred, revise policies and redo training to other workforce members if necessary. Remember that HIPAA compliance is only as good as the written proof your organization can provide to demonstrate that compliance is occurring. Make sure your sanctions policy and employee training is documented as part of your HIPAA compliance program.

### **Handling Security Incidents (No. 6 in series of 8 articles)**

#### **Handling Security Incidents**

HIPAA Security work will not be over on Friday, April 21, 2006, the day after the compliance effective date for small group health plans. Covered entities are responsible to constantly monitor “high-risk” occurrences by first defining and then implementing a reporting process to identify and report security incidents. Reports can be both technical and related to the workforce.

Before you can tell your workforce what and how to report as a security incident, the organization must define what it considers as a Security Incident.

#### **Occurrence Suggestions**

Specific occurrences which will trigger the completion of the *Security Incident Reporting* form may include, but not be limited to, the following:

- Any suspicious or known breach of security by any workforce member for any reason known to be a violation or contradiction of [ENTITY's] philosophy of protecting and safeguarding PHI.
- Any suspicious or known breach of security by an external third party for any reason known to be a violation or contradiction of [ENTITY's] philosophy of protecting and safeguarding PHI.
- Any suspicious activity uncovered as a result of a review of routine or random audit trail.
- Request for audit log review of user activity (special authorization required).
- Suspected or proven violation of protection of malicious software (introduction of malicious software).
- Violation of Login Attempt (Using or attempting to guess another users log in and/or password).
- Sharing of passwords.
- Inappropriate access to the internet.
- Improper network activity.
- Improper email activity.
- Inappropriate access by customer, client, patient, contractor or business associate.

### **Training: A Core Ingredient of HIPAA remediation and compliance**

#### **(No. 7 in series of 8 articles)**

#### **Training: A Core Ingredient of HIPAA remediation and compliance**

HIPAA compliance is measured by how well your organizations workforce members carry out the policies and procedures which have been implemented.

If a formal training program has already been implemented in response to HIPAA Privacy, or for some other reason, start by reviewing the current program and revising it to include the following:

- **Awareness training:** Teach the workforce how to identify threats to the privacy and security of protected health information. Failure to protect against these threats can harm patients/members.
- **Protection from Malicious Software:** Many organizations control updates for antivirus software and other related software via central technical controls. Others allow for the software programs to be bypassed by the end user. It is important to teach the workforce members how the systems are protected, and teach good “systems hygiene” to prevent the introduction of a worm, spyware or malware.
- **Login Attempt Monitoring.** Your organization may actively monitor “Log-In Attempts” and report discrepancies as a result. Workforce should be trained to be vigilante in watching other workforce members and reporting suspected or known breaches of confidentiality to management immediately.
- **Password Management.** Consider procedures for creating, changing and safeguarding passwords. A good Password Management methodology would include protocols and direction on creating and maintaining login passwords.
- **Details of applicable policies and procedures:** This includes how privacy and security policies affect the job of each member of the workforce and how they define what is expected of each workforce member.
- **Periodic Reminders:** Periodic reminders are helpful ways to assure the workforce continues to focus on security measures.
- **Policy and Procedure Changes:** Timely information about changes in policies and procedures that affect workforce members must be communicated in accordance with job function.
- **Information about Sanctions:** Workforce members should be reminded about their role in carrying out compliance on behalf of the organization.

- **Make sure training has been and is documented.**
- **Make sure there is a retraining process for existing workforce members,** and to assure new workforce members whether they are full time, temporary or volunteer are trained as necessary in accordance with their job function.

*HINT:* Many organizations are using HIPAA as an opportunity to further define appropriate systems usage, email usage, password and other technical policies and to re-fresh users by having them sign statements that they understand and will abide by such procedures.

Source: EBIA Weekly 3/16/06 [www.ebia.com](http://www.ebia.com)  
 NEW FAQ EXPLAINS WHEN A HEALTH PLAN IS ALLOWED TO DISCLOSE PHI TO A PERSON WHO CALLS ON BEHALF OF A COVERED PERSON

[HHS Frequently Asked Questions (FAQs) on HIPAA Privacy (Updated March 14, 2006)] For a copy: <http://www.hhs.gov/ocr/hipaa/>

The HIPAA privacy rule prohibits health plans from disclosing protected health information (PHI) unless there is a provision in the regulations that specifically permits the disclosure. In this new FAQ, HHS explains that the regulations permit health plans to disclose PHI to callers who are family members, relatives, or close personal friends of persons who are covered by the plan, as well as to others who have been identified by the covered person as being involved with his or her care or payment. However, the PHI that may be disclosed is limited to that which is directly relevant to the caller's involvement with the covered person's care or payment for care. HHS reminds health plans that such disclosures may be made only if the covered person does not object or if the health plan can reasonably infer from the circumstances that the covered person does not object. However, HHS notes that if the covered person is not present or is incapacitated, the health plan is allowed to make the disclosure if, in the exercise of professional judgment, the health plan believes that the disclosure is in the best interests of the covered person.

The FAQ includes several examples that demonstrate permissible disclosures. One example illustrates that a health plan may disclose relevant PHI to a covered person's daughter who calls to assist her hospitalized, elderly mother in resolving a claim or other payment issue. Another example shows that a health plan may disclose relevant PHI to a human resources (HR) representative who calls the plan with the covered person also on the line, if the covered person confirms that the HR representative is calling to assist the covered person.

EBIA Comment: The provision in the HIPAA privacy rule that permits disclosures to family members, relatives, close personal friends, and others who have been identified by the covered person can be very helpful to group health plans, which often receive phone calls from spouses and the adult children of retirees seeking information to help answer questions and resolve problems related to claims. This FAQ is especially welcome because the example involving the HR representative clarifies that the covered person does not need to be in the physical presence of the health plan representative in order for the covered person to indicate that he or she agrees to the disclosure.