



# Advisor<sup>®</sup>

American Practice

An Eagle Associates Publication

October 2009

## Compliance Training Privacy Breach Notification

**Employee Training Section**  
**Page A-D**

**Trainer's Plan**  
**Page 9**

Next scheduled employee training -- Training for Workplace Violence Protection, November 2009

### Privacy Breach Notification Requirements

page 2

New requirements effective September 18, 2009

### Pandemic Influenza Update

page 7

Vaccine, resources, and training information

### Secure Protected Health Information

page 6

Defining how PHI is secured

### Questions and Answers

page 8

Topics include: tuberculosis, workplace harassment, MSDSs, and Notice of Privacy Practices.

# HIPAA Compliance System Upgrade

Upgrade to the HIPAA Compliance System and save over 25%. You will have one **complete** system for HIPAA compliance at less than \$1 per day, approximately one-tenth the cost of doing it on your own.

## HIPAA Compliance System Features

- **Red Flags Rule** *New for 2009* – HCS includes policies for an Identity Theft Program to meet the Federal Trade Commission requirements under the Red Flags Rule.
- **Privacy Breach Notification** *New for 2009* – HCS includes policies for Privacy Breach Notification, as required by modifications to HIPAA's Privacy Rule as of September 18, 2009.
- **Compliance Manual** A complete policy manual is organized into individual sections, by regulation, for quick reference, and covers all HIPAA regulations.
- **Automatic Updates** HCS includes automatic updates as changes to regulations occur.
- **Annual HIPAA Planner** HCS includes an annual HIPAA planner of scheduled compliance activities to help you maintain compliance each year.
- **American Practice Advisor®** HCS includes an annual subscription to the *American Practice Advisor®*.
- **New Employee Training** HCS includes Employee HIPAA Orientation, which provides all of the initial training that new employees need to understand HIPAA regulations.
- **Annual Staff Training** Annual staff safety and HIPAA training is provided through training modules ("Compliance Training") included with the *American Practice Advisor®*.
- **Live Support** HCS includes unlimited consulting at no additional cost. Simply call or email Eagle for help as often as needed.
- **Free Webinars** Access to webinars is included to address new and existing compliance issues.
- **Guarantee** Eagle Associates guarantees your compliance. Should you receive a complaint from the Office for Civil Rights or Federal Trade Commission, we will guide you through the process and write necessary responses for you.

## 2009 UPGRADE SERVICES PACKAGE

Add HIPAA Compliance System to your existing *Advisor®* or Custom Safety Program subscription.

HIPAA Compliance System

\$240.00 (\$85 savings)

To upgrade your service, contact us at (800) 777-2337, or send an email to [eassoc@mac.com](mailto:eassoc@mac.com).

The Department of Health and Human Services recently published a privacy breach notification rule that went into effect September 18, 2009. Refer to the article on page 2 for full details.

An update pertaining to the new privacy breach notification requirements has been sent to current subscribers of the HIPAA Compliance System. See the shaded box on page 5 for more details.

Securing protected health information is necessary to avoid a privacy breach. For more information on properly securing both electronic and paper records, please refer to the article on page 6.

Refer to the article on page 7 for a variety of pandemic influenza information resources.

## Important Notice Regarding Training Schedule Change

DUE TO THE RECENT CHANGES TO THE PRIVACY RULE REQUIREMENTS FOR PRIVACY BREACH notification, we are changing our training schedule for Compliance Training in the *Advisor*. October normally provides training on Office of the Inspector General (OIG) requirements for fraud detection and prevention in Medicare and Medicaid programs.

The New requirements for Notification in the Case of Breach of Unsecured Protected Health Information (PHI), require training by the practice as identified in 45 CFR 164.414(b)(1):

*“A covered entity must provide training to all members of its workforce on the policies and procedures with respect to notification in the case of breach of unsecured PHI as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.”*

Because annual retraining for OIG is not specifically mandated, we are replacing it this year with training for the new privacy breach requirements. If you have a need to conduct OIG training, simply use the October 2008 materials, as the guidance has not changed. If you need a copy of the October 2008 *Advisor*, send an email request to [jcosey@mac.com](mailto:jcosey@mac.com), and a PDF copy will be emailed to you. Also, Test Registry On-Line subscribers can use the new hire OIG Orientation module any time for employees to complete OIG training.

As always, we are please to bring you the latest regulatory information and training. ●

# Privacy Breach Notification Requirements

ON AUGUST 18TH, 2009, THE DEPARTMENT OF HEALTH and Human Services (DHHS) published an interim final rule for Notification in the Case of Breach of Unsecured Protected Health Information (PHI). These new requirements went into effect on September 18th, 2009. With only 30 days notice to develop and implement applicable policies, many covered entities (i.e., medical and dental practices, health insurance companies, etc.) have been out of compliance since the effective date. HHS has stated that the notification requirements will apply for any breach of PHI on or after September 18th, 2009.

The following information provides an overview of the notification requirements, along with actions a practice must take to achieve compliance.

## Applicability

The notification requirements apply to all covered entities under HIPAA's Privacy Rule. While vendors of personal health records (PHRs) are not currently covered by HIPAA, the Federal Trade Commission (FTC) has implemented similar notification requirements for such vendors.

The purpose of the breach notification requirements is to ensure that affected persons (i.e., patients) will be informed, in a timely manner and method, of any unauthorized breach of unsecured PHI.

## New Definitions

The following new definitions will help clarify their use within this article explaining notification requirements.

**Breach** – A breach is defined as an unauthorized acquisition, access, use, or disclosure of unsecured PHI (that compromises the security or privacy of such information) by a member of the practice's workforce, person working under the authority of the practice, or a business associate of the practice.

**Breach Exceptions** - Exceptions to this definition include disclosures where the recipient of the information would not reasonably have been able to retain the information, certain

unintentional acquisition, access, or use of information by employees or persons acting under the authority of a covered entity or business associate, as well as certain inadvertent disclosures among persons similarly authorized to access protected health information at a business associate or covered entity.

**Discovery of a Breach** - For the purposes of the breach notification policies and procedures, a breach shall be considered discovered as of the first day on which a breach is made known to the practice, or, by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is a workforce member or agent of the practice.

**Individual** – For privacy and breach notification purposes, the term individual means a patient and or his/her authorized representative (i.e., a Personal Representative).

**Law Enforcement Official** – A law enforcement official is defined as an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian Tribe, who is empowered to (a) investigate or conduct an official inquiry into a potential violation of the law; or (b) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of the law.

**Media** – The term media is used to identify “prominent media outlets” for a specific geographical area. Media notification requires notice of a breach being sent to a general interest newspaper with circulation in the area where the individuals involved in the breach may reside.

**Notification** – The term notification shall apply to appropriate notices to individuals, HHS, media, and from business associates regarding breaches of unsecured PHI.

**Unsecured and Secure PHI** - The Notification in the Case of Breach of Unsecured PHI requires a practice to provide notice to individuals, HHS, and media when an individual's unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as the result of a breach.

Unsecured PHI is the key phrase in the requirements and it applies to electronic PHI, printed information, films or any other format of PHI. PHI is considered secure if it has been

rendered unusable, unreadable, or indecipherable (using technologies and methods specified by HHS) to unauthorized individuals. See the companion article (“Secure Protected Health Information”) for a complete explanation on the accepted methods for securing PHI.

Examples of unsecured PHI would include electronic data, films, fax messages to wrong numbers, misplaced or lost charts, and other printed documents containing PHI.

## Investigation

Upon discovery of a breach, a practice should begin, and document, a complete investigation of the incident. An investigation enables a practice to confirm if a breach has occurred, identify the cause, eliminate any recurrence, and gather information it needs to provide to the individuals affected by the breach.

## Breach Notification to Individuals

Upon discovery of a breach, a practice is required to make notification to an individual as soon as is reasonable, but no later than 60 calendar days after the discovery of a breach (see definition) by the practice (the 60 calendar days begin on the day a breach is discovered). This means that the practice must begin a series of processes (i.e., investigation, sanctions, documentation) as soon as possible. The notification process may be concurrent with investigation. While the requirements provide a window of 60 days, notification(s) should be made as soon as possible. If necessary, information required in notices may be communicated in multiple notices (as it becomes known, rather than in a single notice) to individuals, HHS and media outlets. This use of multiple notices would allow for a more rapid initial notification of individuals.

Should an investigation identify that the PHI was secured or that a breach did not occur, there is no requirement to provide any notifications. As with all HIPAA documentation, records pertaining to a breach must be maintained for a minimum of six years by the practice.

**Notification Content** - Notification must be provided to all individuals involved in a confirmed breach. The notification must include the following elements:

1. A brief description of what happened, the date of the breach (if known) and the date of discovery of the breach;

2. A description of the types of unsecured PHI that were involved in the breach (i.e., individual’s full name, social security number, date of birth, home address, account number, diagnosis, disability code, and other types of PHI). Note – only the types of PHI will be listed, not the actual individual’s information;
3. Any steps an individual should take to protect themselves from potential harm resulting from the breach (i.e., recommendations for an individual to contact credit bureaus and how to make contact if credit card information was involved);
4. A brief description of what the practice is doing to investigate the breach, to limit harm to individuals, and to protect against any further breaches, including the imposition of employee sanctions, if appropriate; and
5. Contact procedures (i.e., the practice’s Compliance or Privacy Officer contact information) for individuals to ask questions or learn additional information, which will include a toll-free number, an email address, website, or postal address.
6. Breach notification requirements specify that the notice to individuals must be in plain language that the individual can easily understand.

**Notifying Individuals** - Again, it is more important to provide notification as soon as possible (once a breach has been confirmed) rather than wait for all of the investigative results. This is why the requirements allow for multiple notices to get all of the information out to affected individuals.

Notification for individuals must be made by first-class mail to the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by email. Note that a practice should have a signed authorization from the individual regarding the use of electronic mail.

If the practice knows that the individual is deceased and has the address of the next of kin or personal representative, written notification by first-class mail shall be made to the next of kin or personal representative. As with the individual, the required information can be provided in multiple notices, for next of kin and personal representatives, as information is available to the practice.

In cases where there is insufficient or out-of-date contact information that precludes written notification to an individual, a substitute form of notice must be provided. A substitute notice will be made as soon as possible after the practice becomes aware that it has insufficient or out-of-date contact information.

A substitute notice can be sent by alternative methods that include electronic mail or telephone. The practice should ensure that no sensitive information is left on answering machines or voice mail when using telephone contact as an alternative means for providing notification.

In cases where there is insufficient or out-of-date contact information for 10 or more individuals, the substitute notice must:

1. Be in the form of a conspicuous posting for a period of 90 days on the home page of the website of the practice (if the practice has a website), or conspicuous notice in major printed media (i.e., major newspaper) or broadcast media (i.e., television or radio) in geographic areas where the individual's affected by the breach are likely to reside.
2. Include a toll-free number that remains active for at least 90 days where an individual can learn whether his/her unsecured PHI was included in the breach.

In any breach situation that the practice identifies as urgent because of possible misuse of unsecured PHI, the practice may provide information to individuals by telephone or other means, as appropriate to ensure immediate notification to individuals.

### Notification to Media

A practice is required to provide notification to media for a breach that involves 500 or more residents of a State or jurisdiction. Following the discovery of a breach involving 500 or more residents, the practice is required to notify media outlets serving the State or jurisdiction. Notices to the media are additional notices to those provided for individuals and are not meant to replace the notice to individuals.

As with individuals, notification shall be made to the media as soon as is reasonable, but no later than 60 calendar days after the discovery of a breach by the practice. As with

notification to individuals, multiple notices may be used to provide applicable information. The content of a notification to media is the same as with individuals.

### Notification to HHS

A practice is required to notify Health and Human Services (HHS) of all confirmed breaches. Breaches involving 500 or more individuals will require immediate notification to HHS, while smaller breaches will be reported annually.

Notification to HHS for breaches of 500 or more individuals must be made concurrently with the notification to individuals. HHS will provide a posting on its website ([www.hhs.gov](http://www.hhs.gov)) regarding the method for immediate notification.

Additionally, a practice must maintain an annual log of all confirmed breaches. A copy of the log must be submitted to HHS no later than 60 calendar days after the end of each calendar year using the method specified on the HHS website. Copies of the annual privacy breach log have to be maintained for a minimum of six years.

### Notification to a Practice by a Business Associate

A business associate of the practice that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured PHI must immediately notify the practice when it discovers a breach of such information. Notification of a breach by the business associate can be reported to the practice by fax or electronic mail or other means as established between the practice and the business associate.

Business associates must provide notification of breaches to the practice as soon as is reasonable, but no later than 60 calendar days after the discovery of a breach by the business associate. Upon notification of a breach by the business associate, the practice must make appropriate notifications to individuals and HHS. The practice must make notice to individuals within 60 days of the discovery of the breach by the business associate.

A business associate is required to provide the practice with as much information about the breach as is possible including, if available, the identification of each individual and any other information that the practice is required to include in its notification to individuals. There may be situations where

Continued on page 5

# Compliance Training

## Privacy Breach Notification

A

### Privacy Breach Notification

#### Privacy and Security

THE GROWING CONCERN OVER CONFIDENTIALITY OF AN INDIVIDUAL'S PERSONAL information has raised an awareness of identity theft, and has resulted in a new HIPAA requirement for providing patients with notification in the event of a breach or unauthorized disclosure of PHI.

The Department of Health and Human Services (DHHS) published new requirements on August 18th, 2009 and made them effective on September 18th, 2009. Originally anticipated to be part of new HIPAA elements for 2010, Privacy Breach notification has become an immediate requirement for healthcare entities.

HIPAA's Privacy Rule has established the ground rules for maintaining the confidentiality of PHI. The Security Standard contains rules for maintaining the confidentiality of electronic PHI. The Privacy Breach requirements have now established actions that must be completed should a healthcare entity discover a breach of confidentiality involving PHI.

Understanding the notification requirements will help you to better understand the growing need for protecting the confidentiality of PHI, and the costs your practice may incur should you experience a breach.

How is a breach of PHI defined? First, the incident would have to involve unsecured PHI. Stolen, lost, or misplaced PHI that is in a secure format is not considered a breach. The key is determining whether the information was secured as defined below.

A breach is defined as an unauthorized acquisition, access, use, or disclosure of unsecured PHI (that compromises the security or privacy of such information) by a member of the practice's workforce, person working under the authority of the practice, or a business associate of the practice.

A breach of PHI could include a lost or stolen device (i.e., computer, smart phone, etc.) that would have unsecured patient information stored on it. An unsecured flash drive or other mobile media, such as a CD or DVD containing patient information, would also present a possible breach. A lost chart or other printed material containing patient information would also be considered a potential breach, because you cannot encrypt or otherwise protect such

#### THIS TRAINING SESSION IS RECOMMENDED FOR:

All personnel (administrative and clinical).

#### Training Objectives

The training objective is to address new requirements under the Privacy Rule known as Notification in the Case of Breach of Unsecured Protected Health Information (PHI) or Privacy Breach. This objective is met by understanding the following topics:

- Privacy Breach definition;
- Staff responsibility and sanctions;
- Notification process; and
- HHS and media notifications.

#### Interactive Training Reminder

Compliance Training is an interactive training program in which you can address questions with other staff members or supervisors to obtain clarification for situations in your work setting.

Write down any questions that you have about the training topic and address them with your Privacy Manager or supervisor.

information. Faxing a patient's information to the wrong fax number also constitutes a breach of unsecured PHI.

What is secured and unsecured PHI? PHI is considered secure if it has been rendered unusable, unreadable, or indecipherable (using technologies and methods specified by HHS) to unauthorized individuals. This means that the information has been encrypted (if in electronic format) or, in the case of printed hard copy materials such as medical records, shredded or otherwise destroyed so that it can neither be read nor reassembled.

The term unsecured PHI means PHI that (using technologies and methods specified by HHS) has not been rendered unusable, unreadable, or indecipherable to unauthorized persons or entities.

### Staff Responsibility

The major requirement of HIPAA regulations is protection and safeguarding of patient information to ensure its privacy. While the regulations impose the primary responsibilities on the practice, they place a responsibility on all of the practice's workforce members, and business associates, to fulfill the responsibility for confidentiality. Employers are required to impose sanctions on workforce members involved in a breach of PHI.

### Discovery and Investigation of a Breach

For the purposes of privacy breach notification requirements, a breach is considered to be discovered as of the first day on which a breach is made known to the practice, or, by exercising reasonable diligence would have been known to any person, other than the person committing the breach, who is a workforce member or agent of the practice. This carries a continuation of staff responsibility, in that every member of the workforce should be alert and notify the practice if they have reason to believe that a privacy breach has occurred.

Upon discovery of a breach, a practice is required to begin and document a complete investigation of the incident. An investigation enables a practice to determine whether a breach has occurred, identify the source or cause, take corrective

actions to limit any recurrence, and gather information it needs to provide to patients affected by the breach.

Should an investigation identify that the PHI was secured, or that a breach did not occur, there is no requirement to provide any notifications.

### Patient Notification

Upon discovery of a breach, a practice is required to make notification to the patient(s) as soon as is reasonable, but no later than 60 calendar days after the discovery of a breach by the practice (the 60 calendar days begin on the day a breach is discovered). This does not mean that a practice can wait to make notification of the breach to a patient. The intent is to make a notification as soon as possible (i.e., as soon as there is confirmation of the breach). If needed, a practice can provide all of the required information (see below) to the patient in multiple notices, as the practice obtains the information.

Notification must be provided to all patients involved in a confirmed breach. The notification must include the following elements:

1. A brief description of what happened, including the date of the breach (if known) and the date of discovery of the breach;
2. A description of the types of unsecured PHI that were involved in the breach (i.e., individual's full name, social security number, date of birth, home address, account number, diagnosis, disability code, and other types of PHI). Note – only the types of PHI will be listed, not the actual individual's information;
3. Any steps an individual should take to protect themselves from potential harm resulting from the breach (i.e., recommendations for an individual to contact credit bureaus and how to make contact if credit card information was involved);
4. A brief description of what the practice is doing to investigate the breach, to limit harm to individuals, and to protect against any further breaches, including the imposition of employee sanctions, if appropriate; and

- Contact procedures (i.e., the practice's Compliance or Privacy Officer contact information) for individuals to ask questions or learn additional information, which will include a toll-free number, an email address, website, or postal address.

Breach notification requirements specify that the notice to individuals be in plain language that the individual can easily understand.

Notification to patients must be made by first-class mail to the last known address of the individual or, if the patient agrees to electronic notice and such agreement has not been withdrawn, by email.

If the practice knows that the patient is deceased and has the address of the next of kin or personal representative, written notification by first-class mail shall be made to the next of kin or personal representative. As with the patient, the required information can be provided in multiple notices, for next of kin and personal representatives, as information is available to the practice.

What if the patient's contact information is out-of-date and the practice cannot make contact?

In cases where there is insufficient or out-of-date contact information that prevents written notification to a patient, a substitute form of notice must be provided. A substitute notice will be made as soon as possible after the practice becomes aware that it has insufficient or out-of-date contact information.

A substitute notice can be sent by alternative methods that include electronic mail or telephone. The practice should ensure that no sensitive information is left on answering machines or voice mail when using telephone contact as an alternative means of providing notification.

In cases where there is insufficient or out-of-date contact information for 10 or more individuals, the substitute notice must:

- Be in the form of a conspicuous posting for a period of 90 days on the home page of the website of the practice

(if the practice has a website), or conspicuous notice in major printed media (i.e., major newspaper) or broadcast media (i.e., television or radio) in geographic areas where the individuals affected by the breach are likely to reside.

- Include a toll-free number that remains active for at least 90 days from which an individual can learn whether his/her unsecured PHI was included in the breach.

In any breach situation that the practice identifies as urgent because of possible misuse of unsecured PHI, the practice may provide information to individuals by telephone or other means, as appropriate to ensure timely notification.

### Notification to Media

A practice is required to provide notification to media (print or broadcast) for a breach that involves 500 or more residents of a State or jurisdiction. Notices to the media are in addition to those provided for individuals, and are not meant to replace the notice to individuals.

### Notification to DHHS

A practice is required to notify DHHS of all confirmed breaches. Breaches involving 500 or more individuals will require immediate notification to DHHS, while smaller breaches will be reported annually.

Notification to DHHS for breaches of 500 or more individuals must be made concurrently with the notification to individuals. Additionally, a practice must maintain an annual log of all confirmed breaches. A copy of the log must be submitted to HHS no later than 60 calendar days after the end of each calendar year using the method specified on the HHS website. Copies of the annual privacy breach log must be maintained for a minimum of six years.

### Notification by a Business Associate

Business associates of the practice could also experience a privacy breach. Should this occur, the business associate is required to immediately notify the practice. Upon notification of a breach by a business associate, the practice will then begin the entire notification process. ●

# Compliance Training Test

## Privacy Breach Notification

NAME: \_\_\_\_\_

DATE: \_\_\_\_\_

SIGNATURE: \_\_\_\_\_

STAFF POSITION: \_\_\_\_\_

*There are 10 questions to the test for Privacy Breach Notification. Return your test to your supervisor or Privacy Manager upon completion. Individual tests will be maintained with the training log to document participation and understanding of the information. There is no pass or fail grade to the test. Review the training information to find the correct answers to any questions that may have been missed.*

**Select One 1**

HIPAA's Privacy Rule has established the ground rules for maintaining the confidentiality of PHI.

T F

**Select One 2**

A privacy breach is defined as an unauthorized acquisition, access, use, or disclosure of unsecured PHI.

T F

**Select One 3**

The practice has sole responsibility for maintaining the confidentiality of PHI.

T F

**Select One 4**

PHI is considered secure if it has been rendered unusable, unreadable, or indecipherable (using technologies and methods specified by HHS) to unauthorized individuals.

T F

**Select One 5**

Employers are required to impose sanctions on workforce members involved in a breach of PHI.

T F

**Select One 6**

A breach is considered to be discovered as of the day a notification is sent to the affected patient.

T F

**Select One 7**

Upon discovery of a breach, a practice is required to make notification to the patient(s) as soon as is reasonable, but no later than 60 calendar days after the discovery of a breach by the practice.

T F

**Select One 8**

Notification to patients must be made by first-class mail to the last known address of the individual or, if the patient agrees to electronic notice and such agreement has not been withdrawn, by email.

T F

**Select One 9**

The Privacy Breach requirements have now established actions that must be completed should a healthcare entity discover a breach of confidentiality involving PHI.

T F

**Select One 10**

A practice is required to notify the Department of Health and Human Services (HHS) of all confirmed breaches.

T F

**Test Code ID: 10200901**

## Continued from page 4

the business associate may not know the identification of affected individuals, as with a box of stored medical records being stolen from a storage facility. The business associate must report all available information to the practice.

**Modification of Business Associate Agreements** – Practices should review existing business associate agreements to ensure that language regarding breach notification requirements (i.e., timeliness of notification and notification content) is included in the agreement.

## Law Enforcement Delay

Should a law enforcement official notify the practice or business associate that a notification, notice, or posting required by the regulation would impede a criminal investigation or cause damage to national security, the practice or business associate shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay notification, notice, or posting for the period of time specified by the official; or
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during the 30-day time period.

## Burden of Proof

In the event of a breach of unsecured PHI, the practice or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required, or that the discovered use or disclosure did not constitute a breach. It is advised that the practice maintain a file for all documentation of reported breaches (including those that the practice does not consider a breach) to meet the burden of proof that required actions were taken.

## Administrative Requirements

The breach notification requirements also require a practice to ensure continued compliance with the Privacy Rule and Security Standard. A practice must ensure that it maintains a complaint system with appropriate documentation for handling privacy and security problems.

**Training** - The practice must also provide training to all members of its workforce on the policies and procedures with respect to notification in the case of breach of unsecured PHI as necessary and appropriate for the members of the workforce to carry out their functions within the practice. This month's edition of "Compliance Training" provides training materials to meet this requirement.

**Sanctions** - The practice must have and apply sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the practice. Sanction requirements have already been in place under both the Privacy Rule and Security Standard, and those same sanctions can be used for breaches of unsecured PHI.

**No Retaliation or Waivers** - The practice may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process for notification in cases of an unsecured PHI breach, including the filing of a complaint. Additionally, the practice may not require individuals to waive their rights to file a complaint with the practice or HHS as a condition of the provision of treatment or payment of services from the practice.

**Policies and Procedures** - The practice must implement policies and procedures that are designed to comply with the requirements of notification in the case of breach of PHI. The practice must also change its policies and procedures as necessary to comply with changes in the law, including the standards, requirements, and implementation specifications for notification in case of breach of PHI. ●

## Privacy Breach Notification Update

An update to the Privacy Rule policies of the HIPAA Compliance System (HCS) has become necessary due to the new privacy breach requirements. Complete written policies have been provided, so that your practice will be ready to meet the requirements.

The written policies have been sent via email to subscribers of the HIPAA Compliance System. If you did not receive the policies, but are a current HCS subscriber, please contact us so that we can arrange for provision of the policies through a method that is convenient for you. You may email [eassoc@mac.com](mailto:eassoc@mac.com) or call us at (800) 777-2337.

# Secure Protected Health Information

WHILE THE NEW PRIVACY BREACH REQUIREMENTS focus on unsecured PHI, just what will be considered secured PHI? A portion of the answer has existed in part of the Security Standard for several years. The complete answer is explained in the rest of this article.

The Security Standard already requires practices to safeguard electronic PHI, and allows the use of any security measure that reasonably and appropriately secures the information. One of the Security Standard implementation specifications identifies the use of encryption as an acceptable method for safeguarding electronic PHI. Because the encryption specification is addressable, a practice can use another method (other than encryption) as long as it appropriately secures the information (see “Technologies and Methodologies” below).

Note that when using encryption, a practice should ensure that encryption keys are maintained on a separate device from the data that they encrypt or decrypt. The definition of encryption (from 45 CFR 164.304, definitions from the Security Standard for the Protection of Electronic Protected Health Information) states Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

If a practice uses encryption to comply with the Security Standard, and subsequently discovers a breach, the practice would not have to make any notifications, because the breach involved secured PHI. The same applies to the use of other acceptable methods for securing PHI, because a breach of secured PHI does not require notifications. This is because secured PHI is indecipherable.

The new breach requirements establish specific methods for securing PHI, as published in guidelines from the National Institute of Standards and Technology (NIST). It is important to understand the difference between “data in motion,” “data at rest,” “data in use,” and “data disposed.”

*Data in motion* includes data that is moving through a network, including wireless transmission, whether by electronic mail or structured electronic interchange. *Data at rest* includes data that resides in databases, file systems, flash drives, memory, and any other structured storage environment. *Data in use* includes data in the process of being created, retrieved, updated, or deleted. *Data disposed* includes discarded paper records or recycled electronic media.

Access control methods (i.e., firewalls) are not considered acceptable methods for securing PHI, because they fail to meet the requirement for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. If access controls are compromised, the underlying PHI is still usable, readable, or decipherable to unauthorized individuals, and thus constitute unsecured PHI for which breach notification would be required.

## Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

*PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:*

1. *Electronic PHI has been encrypted using an algorithmic process to transform the data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key. To avoid a breach of the confidential process or key, these encryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption process has been tested by NIST and judged to meet the requirements for securing data at rest or in motion (check with software or hardware manufacturers to ensure NIST guidelines can be met).*
2. *Media on which PHI is stored or recorded has been destroyed by one of the following methods:*
  - a. *Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed (redaction is specifically excluded as a means of data destruction).*
  - b. *Electronic media have been cleared, purged, or destroyed consistent with NIST guidelines for media sanitization such that the PHI cannot be retrieved.*

The need for security of PHI is becoming more and more critical for all healthcare providers. The use of the Internet, electronic mail, mobile devices, and a variety of media have raised concerns that were not relevant when HIPAA first arrived on the healthcare scene.

While these new requirements may seem a burden, the key is good security for all PHI (electronic and hard copy). Securing PHI will limit the potential need for making burdensome notifications to individuals, HHS, and media. ●

## Pandemic Influenza Update

### Vaccination

ON PAGE 1 OF THE SEPTEMBER 2009 ISSUE OF THE *Advisor*, an article included information about Centers for Disease Control and Prevention (CDC) recommendations for the H1N1 vaccine (still in development). We strongly advise you to read the article, so that you are apprised of the most recent vaccine recommendations.

Remember that the seasonal influenza vaccine will be administered separately from the H1N1 vaccine, and should be offered to employees as soon as it becomes available in your area.

### CDC Resources

The CDC has an excellent web page titled “CDC Novel H1N1 Influenza: Resources for Clinicians.” The page is available at <http://www.cdc.gov/h1n1flu/clinicians/>.

Topics on the CDC clinicians’ page include:

- Guidance for Patient Management;
- Guidance for Specific Settings;
- Guidance for Specific Populations;
- Treatment Guidance;
- Vaccine Resources
- Additional Resources for Clinicians

- Patient Information and Education
- Laboratories
- Training

### Advisor Articles

Refer to the other *Advisor* articles we’ve published on influenza this year as listed below:

- June 2009 - page 1  
“CDC Guidance for H1N1 Flu Patient Care”
- August 2009 - page 4  
“Employee Influenza Vaccination”
- August 2009 - page 5  
“Infection Control for Pandemic Influenza”

### Staying Informed

As the situation with novel influenza A H1N1 continues to develop, we will work to keep you informed. The *Advisor* will continue to provide articles that will inform and assist you in responding to the pandemic situation.

In the case of important news that breaks after an issue of the *Advisor* goes into production, we will issue notices through our monthly e-mail service “Compliance Bulletins.” To subscribe to “Compliance Bulletins,” email a request to [hprochaska@mac.com](mailto:hprochaska@mac.com). Note that “Compliance Bulletins” are sent via email only, and are not available via fax or regular mail (USPS).

We will also post information at our online News Site, which can be reached by clicking the yellow box titled “News Site” on our home page at <http://www.eagleassociates.net>.

### Training

The August 2009 issue of the *Advisor* featured Influenza Safety as the “Compliance Training” topic. Look for the training material on pages A – D. If you have not already done so, be sure to train employees using this year’s material, as it has been updated with information on novel influenza A H1N1, and also addresses seasonal influenza. In addition, “Trainer’s Plan” on the inside back cover provides notes for the individual in charge of the training, along with a handy checklist of reminders. ●

# Questions & Answers



**We have a policy in our facility that we do not treat patients with active TB. However, if a person comes into the office, and exhibits signs and symptoms consistent with TB, we do perform a chest x-ray on the patient to either rule out TB, or to suggest that further testing is needed. What precautions are to be taken in such cases?**

First, administrative personnel need to be trained to recognize signs and symptoms of TB, so that they can alert clinical personnel. Second, persons exhibiting signs and symptoms of TB should be separated from the general waiting area, and their treatment should be expedited to get them out of the practice as soon as possible (to reduce exposure in case they do indeed have active TB). Third, instruct the patient to wear a surgical mask throughout their stay in your practice. This helps to reduce respiratory secretions that enter the air. Finally, if the chest x-ray seems to suggest possible TB activity, refer the patient to a collaborating facility, which is equipped to properly diagnose TB, and protect employees from exposure to TB. Be sure that employees are aware of the selected collaborating facility, including the contact name, facility name, address and phone number.



**What is the difference between workplace harassment and workplace violence, and is separate training required for each?**

Workplace harassment is essentially a subset of workplace violence. It can lead to a hostile work environment for employees, and can come from sources inside or outside the practice (an example of an outside source would be a vendor who harasses employees when he/she visits your practice). Workplace harassment does not need to be sexual in nature. It includes abusive language or actions as well. Your workplace violence training should include information on workplace harassment. Separate training for each is not specifically required.



**Our office is attempting to reduce its use of paper, and would like to have our employees look up Material Safety Data Sheets on-line when they need to access them. Is this acceptable?**

No, because you have no way of ensuring that your internet connection is always on. Even the most stable of Internet Service Providers (ISP) experience occasional outages. However, you could have MSDSs stored on a computer or computers. As long as you have a backup of the data, which could be accessed if the computers are disabled, or the original data becomes corrupted, you could do away with paper copies of MSDSs. The key lies in ensuring that MSDSs are accessible in an emergency situation.



**If a patient refuses to sign an acknowledgement that he/she received our Notice of Privacy Practices, what should we do? Are we permitted to provide services to that patient, or should we discharge him/her?**

The Privacy Rule requires a practice to make a “good faith effort” to obtain a signed acknowledgement of receipt for your Notice of Privacy Practices (NPP). You should make a notation in the patient’s record if he/she chooses not to sign an acknowledgement of receipt. There is no need to deny treatment or dismiss a patient for such a refusal.

# Trainer's Plan

## Privacy Breach Notification

### THIS SECTION IS RECOMMENDED FOR: Privacy Manager or Compliance Officer Only

Privacy breach notification is the topic for this month's "Compliance Training." The following information will provide reminders on supplemental information that you may need to provide for staff members. The supplemental information provides specific information that is unique to your practice site.

#### Interactive Training Reminder

It is required that the staff be provided with an interactive training program. This means that they must be able to address questions on the training material and information to gain clarification on how their tasks and assignments within the workplace may be affected. An interactive training reminder has been included in the training test to encourage your staff to address their concerns with the Privacy Manager, Compliance Officer, or supervisor.

To accomplish an interactive training program when utilizing "Compliance Training," have staff members write down their concerns and bring them to your attention for clarification. This process also helps you, as the Privacy Manager or Compliance Officer, to become aware of situations in the practice that may need to be reviewed to ensure compliance

and maintain a compliant working environment. Remember to call Eagle Associates if you need assistance with specific issues.

#### Training Reminders for Privacy Breach Notification

To ensure compliance by your practice, the following elements should be clarified for staff members:

- Identify the person in your practice that should be notified if a staff member has reason to suspect that a breach of unsecured PHI has occurred.
- Review the information that must be included in a notification for patients (see article "Privacy Breach"), and use it as a guide to ensure that patients are adequately notified.
- Review your existing business associate agreement to ensure it has been modified to include language regarding breach notification requirements. If needed, contact business associates to begin the process of signing modified or new agreements.
- Review your most current Security Risk Assessment to ensure you have appropriate safeguards in place for devices and data storage. ●

#### Employee Test

- Photocopy the test page for each staff member to complete.
- Review questions answered incorrectly with staff to ensure proper understanding of the training information.
- Establish a date for return of the training test to ensure its completion.
- Prepare a training file folder or log book (if you do not already have one) for storage of training documentation.
- Maintain safety training records for a minimum of three years, and HIPAA training records for a minimum of six years from the date of training.

#### Answers to the October 2009 Privacy Breach Notification Training Test

- |      |       |
|------|-------|
| 1. T | 6. F  |
| 2. T | 7. T  |
| 3. F | 8. T  |
| 4. T | 9. T  |
| 5. T | 10. T |

Eagle Associates, Inc.  
P.O. Box 1356  
Ann Arbor, MI 48106

PRESORTED  
STANDARD  
U.S. POSTAGE PAID  
ANN ARBOR, MI  
PERMIT NO. 885

**DATED MATERIAL - PLEASE DELIVER IMMEDIATELY**



# Advisor<sup>®</sup>

American Practice

1992-2009 Eagle Associates, Inc.

All rights reserved. No part of this publication may be reproduced or transmitted in any form without prior written permission of the publisher. American Practice Advisor<sup>®</sup> is published monthly by Eagle Associates, Inc., P.O. Box 1356, Ann Arbor, MI 48106. Telephone (800) 777-2337 or (734) 662-8002 Fax (734) 662-0651, Electronic Mailbox: eassoc@mac.com.

Due to the constantly changing nature of government regulations, it is impossible to guarantee the absolute accuracy of the material contained herein. The Publisher and Editor, therefore, cannot assume any responsibility for omissions, errors, misprinting, or ambiguity contained within this publication and shall not be held liable in any degree for any loss or injury caused by such omission, error, misprinting, or ambiguity presented in this publication.

This publication is designed to provide healthcare practices and their staff with regulatory and practice management information and is sold with the understanding that neither the Editor nor the Publisher is engaged in rendering legal, accounting, or other professional service or advice. If legal or other expert advice is required, the services of a competent professional should be sought.

For more information on Eagle Associates' programs and services, visit our website at [www.eagleassociates.net](http://www.eagleassociates.net).