

## INTRODUCTION

**Eagle Associates Background** - Eagle Associates, Inc. was founded in 1988 as a consulting and educational company specializing in regulatory compliance (OSHA and later CLIA) and staff training for medical and dental practices. Eagle Associates' services now include OSHA, CLIA, OIG and HIPAA compliance. The programs provided by Eagle Associates are designed for the healthcare practice setting (i.e., medical and dental practices) and are equally effective for individual sites as well as networks and associations of practices.

**Your Seminar Presenter** - Joseph Suchocki, President of Eagle Associates, Inc., has over 37 years experience in the health-care industry and is a nationally recognized speaker and consultant for compliance issues in the healthcare practice setting. Eagle Associates currently provides services to over 1,600 practices for OSHA, CLIA, OIG, and HIPAA compliance.

### ***Seminar Objectives***

The objectives of the seminar are:

1. An overview of HIPAA and the HITECH Act.
2. Enhanced HIPAA Enforcement.
3. A review and explanation of the Privacy Breach Notification requirements (including investigation of a potential breach to determine a harm threshold).
4. A review of additional HITECH Act elements and how they affect privacy and security compliance:
  - Enhanced Enforcement for Privacy and Security
  - Out of Pocket Payment in Full Requested Restriction;
  - Business Associates Agreement Modifications;
  - Disclosure Accountability Changes for EHR;
  - Agreements for Electronic Exchange of Information and PHR;
  - Access to PHI in Electronic Format; and
  - HHS Periodic Compliance Audits.
5. A review of the Red Flags Rules and required policies for an Identity Theft Program.

## HIPAA and the HITECH Act

---

The Health Information Technology for Economic and Clinical Health Act (The HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (also known as the Stimulus Bill). HITECH presented a number of changes for healthcare ranging from monetary incentives for implementation of EHR to Privacy Rule enhancements and onto tougher enforcement for compliance with HIPAA's privacy and security requirements.

Effective Dates - Elements of HITECH have different implementation or effective dates.

- **February 17, 2009** - HITECH Act enacted with enhanced penalties and State Attorney Generals have authority to bring civil action
- **August 18, 2009** - Implementation of Privacy Breach Notification requirements;
- **September 18, 2009** - Effective date for Privacy Breach Notification requirements;
- **December 31, 2009** - Adoption of new rules for accounting disclosures;
- **February 18, 2010** - First annual report on HIPAA enforcement;
  - Application of rules, enforcement, and penalties to business associates;
  - Patient's right to restrict disclosures to health plans;
  - Patient's right to Electronic access to , and an electronic copy, of their health record;
  - Clarification regarding marketing provisions;
  - Imposition of criminal penalties against individuals;
  - Civil monetary penalties and settlements flowing to OCR;
  - OCR to begin mandatory audits of covered entities and business associates;
  - Prohibition on resale of PHI;
- **January 1, 2011** - Required compliance with new accounting for disclosure rules for covered entities with EHR;
- **February 18, 2011** - Initial guidelines for patients to obtain percentage of HIPAA penalties that OCR collects;
  - OCR is required to impose monetary penalties for "willful neglect".
- **February 18, 2012** - Implementation of awarding percentage of collected HIPAA penalties to patients.

## Enhanced Enforcement

---

Prior to the HITECH Act, HIPAA allowed the Secretary of HHS to impose civil monetary penalties on persons violating the HIPAA rules of not more than \$100 per violation up to a maximum of \$25,000 for all violations occurring during a calendar year. HIPAA also limited the Secretary's authority to impose such penalties under various circumstances.

The HITECH Act strengthens the Secretary's enforcement authority by establishing four categories of violations that reflect increasing levels of negligence on the part of the covered entity, by defining tiers of increasing civil monetary penalties that the Secretary can impose, and by requiring that the Secretary base penalties on the nature and extent of the violation as well as the nature and the extent of the harm resulting from the violation.

HITECH's tiered penalty structure represents a significant increase in the liability of covered entities for civil monetary penalties. After February 18, 2009, the Secretary can impose civil monetary penalties for each violation ranging from at least \$100 to a maximum of \$50,000 for the lowest category violation. Under the highest category violation, the Secretary can impose a \$50,000 penalty per violation. Additionally the HITECH Act increases the maximum penalty that the Secretary can impose for all such violations of the same HIPAA provision in a calendar year from \$25,000 to \$1,500,000.

The new rule also eliminates certain defenses which were previously available to covered entities. For example, under the prior rule, a covered entity had an affirmative defense if the entity did not know and reasonably should not have known that a violation occurred.

Under the HITECH provisions of this new rule, this will only be an affirmative defense if the covered entity also corrects the violation during the 30-day period beginning on the first date of such knowledge or during the period determined by the Secretary to be appropriate based on the nature and extent of the covered entity's failure to comply. The new rule also does not alter affirmative defenses with respect to violations due to willful neglect.

All enforcement and penalties now apply directly to business associates as well as covered entities.

**State Attorney General** - Since the early days of HIPAA implementation and compliance there has largely been a lack of real enforcement efforts. The new provisions under HITECH allowing state attorney generals to file HIPAA enforcement actions on behalf of the public bring a new era of enforcement against covered entities who have a health data breach and fail to properly respond to such breach in a timely manner.

The Attorneys General are authorized to bring civil suit in federal district court (on behalf of state residents) if they believe their residents are threatened or adversely affected by HIPAA violations.

The Attorneys General can sue for injunctive relief, and/or for damages.

Damages are limited to \$25,000 in a calendar year, at up to \$100 per violation.

States must notify the Secretary of Health and Human Services before bringing such a suit; a pending federal suit bars any such state action.

Attorney fees may be awarded the states. Nothing in the amended federal law may be construed to prevent a state Attorney General from exercising powers granted under state law.

**Awarding the Patient a Percentage of Collected Penalties** - HHS will develop and implement a method that will award a percentage of monetary penalties collected by OCR. The awards will be implemented on February 18, 2012.

### **Privacy Breach Notification**

---

On August 18<sup>th</sup> HHS published an interim final rule for Notification in the Case of Breach of Unsecured Protected Health Information (PHI) and the requirements went into effect on September 18<sup>th</sup>. HHS has stated that the notification requirements will apply for any breach of PHI on or after September 18<sup>th</sup>.

**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.

**New Definitions** - The following new definitions will help clarify their use within the 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.

**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.

**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.

**Potential Breach** - The term “potential breach” will be used in this information to identify a discovered or reported breach that has not been investigated by the practice.

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

Examples of unsecured PHI would include electronic data (i.e., files, data on a server, data being transmitted), films, fax messages to wrong numbers, misplaced or lost charts, and other printed documents containing PHI.

**Work Force Members** – The breach requirements use the term “workforce members” instead of “staff members” to create a broader reach for identifying who may have caused a breach. Staff members would be limited to employees of the practice. Workforce members include employees, volunteers, trainees, consultants, business associates and other individuals performing work on behalf of the practice.

### **Breach Verification**

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.

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.

Was there a Breach and is Notification Required? Upon discovery of a potential breach a practice needs to:

- (a) Determine if the incident was an unauthorized disclosure of unsecured protected health information (PHI); and
- (b) If the breach warrants notification.

The following steps will help your practice make these determinations.

**Step 1** – Create and Maintain an Incident File - Upon learning of a potential breach (this establishes the date of discovery), a practice should develop an incident file for all of the documentation required to meet the practice's burden of proof that appropriate actions were completed. This is a simple file folder that will identify a specific potential breach and the actions taken by the practice

The definition of a breach is 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.

HHS has clarified the meaning of "compromises the security or privacy of such information" to mean that a breach poses a significant financial, reputational, or other harm to the patient. This clarification will be helpful in determining if a harm threshold has been met (see below).

**Step 2** – Conduct an Investigation – Immediately after the discovery of a potential breach, a practice should conduct an investigation to determine if a breach of unsecured PHI has occurred. The immediate focus is to determine if the potential breach involved unsecured or secured PHI. If a practice determines that the information was secure, the investigative process stops and the incident file closed with documentation maintained for a minimum of six years.

**Step 3** – Determine Harm Threshold - If it is determined that the disclosed PHI was unsecure, the practice should make a risk assessment to see if the potential breach meets the test for a "harm threshold" (i.e., does the breach present a significant financial, reputational or other harm to the patient) and thus requires appropriate notifications. The use of a harm threshold is intended to limit unnecessary notifications for breaches that pose no threat to the security or privacy of the patient's information or, alternatively, may cause unwarranted panic in individuals, and the undue costs and other resources by individuals in any remedial action.

Risk Assessment - A risk assessment for a potential breach will be the final step in determining if notifications are required. A risk assessment should include the following three elements:

**a. Determine Use and/or Disclosure** - The practice should determine what member of the practice's workforce used PHI in an unauthorized manner or to whom (what person or entity outside of the practice) was the PHI disclosed in an unauthorized manner.

If for example the PHI was disclosed to another covered entity (i.e., another practice, hospital, etc.) governed by HIPAA's Privacy Rule and Security Standard, there may be less risk or harm to the patient since the recipient is obligated to protect the privacy and security of the PHI it received in the same manner as the practice. In contrast, if the disclosure was made to a person or entity not governed by HIPAA's requirements, the risk of harm to the patient is significantly greater.

According to the breach notification requirements, there may be circumstances where a covered entity takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. If such steps eliminate or reduce the risk of harm to the individual to a less than "significant risk," then we interpret that the security and privacy of the information has not been compromised and, therefore, no breach has occurred.

In addition, there may be circumstances where impermissibly disclosed protected health information is returned prior to it being accessed for an improper purpose. For example, if a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, such a breach may not pose a significant risk of harm to the patients whose information was on the laptop. Note, however, that if a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.

The example of a lost or stolen laptop can be applied to a lost or misplaced patient record (i.e., printed materials, film, or other physical documentation of patient treatment). If a missing record is located (locating a record should take no more than 48 to 72 hours – if longer, it should be considered a breach) and the practice be assured that the PHI has not been disclosed in an unauthorized manner and that none of the PHI is missing then it may not be a breach.

Lost, stolen, or misplaced items that contain PHI present a significant risk to the patient because the practice does not know who has the PHI and what might be done to create a risk of harm to the patient.

**b. Consider Type and Amount of PHI** - In performing a risk assessment, practices should also consider the type and amount of PHI involved in the unauthorized use or disclosure. If the nature of the protected health information does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach.

For example, if a practice improperly discloses PHI that merely included the name of an patient and the fact that he/she received services from the practice, then this would constitute a violation of the Privacy Rule, but it may not constitute a significant risk of financial or reputational harm to the individual.

In contrast, if the information indicates the type of services that the individual received (specific description of services), that the patient from a specialized facility (such as a substance abuse treatment program<sup>8</sup>), or if the protected health information includes information that increases the risk of identity theft (such as a social security number, account number, or mother's maiden name), then there is a higher likelihood that the unauthorized use or disclosure compromised the security and privacy of the information.

The risk assessment should be fact specific, and the practice should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of the risk of reputational harm – especially in light of fears about employment or insurance discrimination.

**c. Number of Affected Patients** - The number of affected patients may require notification because the types of information disclosed may affect individuals differently.

When in Doubt – A risk assessment may not provide the practice with a clear determination due to the information involved, the relationship with the patient, or the cause of the breach. A practice should implement appropriate notification procedures if there is a doubt as to the potential for significant risk of harm for the patient.

It is critical to develop and maintain documentation for all potential breaches. There may be instances where the practice could receive inquiries from the Office for Civil Rights (OCR) regarding a reported breach (it can be made by an employee or ex-employee as well as a patient). Documentation of what was investigated and determined would be critical in responding to an inquiry from OCR.

### **Other Examples of Breaches and Non-Breaches**

**Faxes to a Wrong Number** – The risk is determined by what wrong number was used. If PHI was faxed to another covered entity (as previously discussed in disclosure to another covered entity) there may be no significant risk or harm as other covered entities are required to maintain the confidentiality of PHI. The practice should obtain reasonable assurances of confidentiality from the recipient because a breach may still occur if a member of the other practice's workforce were to use or disclose the PHI in an unauthorized manner. A practice should conduct and document immediate training for appropriate workforce members to ensure the use of accurate fax numbers.

**A fax sent to an individual** (other than the patient), an employer of the patient, or an unknown recipient may or may not result in a significant risk or harm to the patient.

**Business Associates and the 60 - Calendar Day Clock** – A practice must ensure that it has a good level of communication with its business associates and that business associates monitor PHI for potential unauthorized disclosures. Communication between practices and business associates becomes critical when considering that the practice has 60 - calendar days to notify patients from

the date of the discovery of a breach (whether the breach is discovered by the practice or the business associate). A business associate must notify the practice within 60 - calendar days of discovery. The practice's 60 - calendar day clock also begins on the date of discovery by the business associate.

### **Breach Notification to Individuals**

(notification may be concurrent with investigation) 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 by the practice (the 60 calendar days begin on the day a breach is discovered – see definition “discovery of a breach”). This means that the practice must begin a series of processes (i.e., investigation, sanction, documentation) as soon as possible. While the requirements provide a window of 60 days, the reality is to make notification 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 for individuals.

### **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, 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
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. Plain Language – 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 information. 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 written request 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.

**Substitute Notice**

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 for 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 for 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 web site ([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 associates 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 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 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 the information it can to the practice.

### **Modification of Business Associate Agreements**

Practices should review existing business associate agreements to ensure 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 also 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 "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.

**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 for 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.

### **Restrictions on Certain Disclosures of PHI**

---

**Payment in Full with Patient Requested Restrictions** - While a patient has always had the right (under the Privacy Rule) to request restrictions (with the practice having the option to agree to or deny a requested restriction), HITECH introduces a new type of requested restriction that removes a practice's option to deny a requested restriction. Here is an example of the new type of restriction and how it applies to a patient that has some form of insurance coverage.

Under the new requirement, a patient can pay a practice out of pocket in full for a treatment or procedure and then request that the practice not notify or disclose the information to the insurance carrier about the treatment or procedure (such a request would be a requested restriction under Privacy Rule provisions).

A practice will, under the new requirement, be required to agree to and honor the request if:

- (1) The disclosure or information would have been for the purposes of the practice obtaining payment from the insurance carrier or for other healthcare operations; and
- (2) The information that would have been disclosed to the insurance carrier pertains solely to a healthcare item or service (treatment or procedure) for which the practice has been paid out of pocket in full.

**Disclosures Required to be Limited to the Minimum Necessary** - A covered entity will be considered to be in compliance only if they limit disclosures to the minimum necessary information needed to accomplish the intended purpose of a use, disclosure, or request respectively. Until further defined, the covered entity or business associate shall determine what constitutes the minimum necessary information to accomplish the intended purpose.

BIOHAZARD

**Accounting Disclosures if Covered Entity Uses EHR**

---

**Disclosure Accountability** - The Privacy Rule provides patients with a right to request and obtain an accounting (listing) of their PHI disclosures a practice has made except that the accounting does not have to include disclosures that were made:

- (1) To carry out treatment, payment, and healthcare operations;
- (2) To patients about their PHI;
- (3) Made as stipulated in an authorization signed by the patient;
- (4) For a facility's directory or to persons involved in the patient's care;
- (5) For national security or intelligence purposes;
- (6) To correctional institutions;
- (7) As part of a limited data set; or
- (8) Prior to the compliance date of the Privacy Rule.

HITECH changes the disclosures a practice has to account for if the practice uses electronic health records (EHR). Under the new requirements, a practice using EHR would have to account for or provide a listing of all disclosures to carry out treatment, payment, and healthcare operations.

**Agreements for Electronic Exchange of Information and PHRs**

---

The use of a Regional Information Organization (RIO), Health Information Organization (HIO) or other entity for electronic exchange of information will require the covered entity to establish a business associate agreement with such entities. Vendors of Personal Health records (PHRs) will also require the implementation of a business associate agreement before a covered entity can begin disclosing information with the PHR vendor.

### **Access to Certain Information in Electronic Format**

---

If the covered entity uses or maintains an electronic health record with respect to the protected health information of a patient:

(1) The patient shall have the right to obtain a copy of their protected health information in an electronic format and, if the patient chooses, to direct the covered entity to transmit such copy to an entity or person designated by the patient, provided that the patient's choice is clear, conspicuous, and specific; and

(2) Any fee that the covered entity may impose for providing a patient with a copy of their protected health information (or a summary explanation if agreed to by the patient) if such copy is in an electronic form. The fee shall not be greater than the covered entity's labor costs in responding to the request for such copy of protected health information.

### **HHS Periodic Audits**

---

**Periodic Audits** - HHS will be conducting mandatory periodic audits to ensure that covered entities and business associates comply with privacy and security requirements. Audits shall address all requirements within the Privacy Rule and SecurityRule.

### **OCR's Mission and Vision**

As the Department's civil rights and health privacy and security rights law enforcement agency, OCR promulgates regulations, develops policy, investigates complaints, conducts compliance reviews, and provides technical assistance and public education to ensure understanding of and compliance with Federal non-discrimination and health information privacy and security laws and regulations, including:

- Ensuring that the more than 500,000 recipients of Federal financial assistance comply with the nation's civil rights laws.
- Ensuring that the practices of several million health care providers, health plans, healthcare clearinghouses, and their business associates adhere to Federal privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA).
- Implementing and enforcing new privacy protections under the Health Information Technology for Economic and Clinical Health Act (HITECH) contained in the American Recovery and Reinvestment Act of 2009 (ARRA).
- Annually resolving more than 10,000 citizen complaints alleging discrimination or a violation of HIPAA.

## Red Flags Rule and Identity Theft

---

On November 9, 2007, the Federal Trade Commission (FTC), the federal bank regulator agencies, and the national credit Union administration jointly issued regulations called the Red Flag Rules. The rules implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). The purpose of the red flag rules or the rules is to combat identity theft.

The rules require each financial institution and creditor that holds any consumer account, or other program for which there is a reasonably foreseeable risk of identity theft, to develop and implement an identity theft program for combating identity theft in connection with new and existing accounts. These rules apply to hospitals, clinics and other healthcare organizations **if** the organizations meet the rules definition of a creditor and if the organizations offer or maintain covered it counts.

The red flag rules have an unexpectedly broad application because the definition of creditor includes any entity that regularly accepts deferred payments for its goods and services. If a hospital, for example, regularly offers payment plans or allows patients to pay in installment payments, the hospital would be considered a creditor within the meaning of the rules. Many in the healthcare industry have been surprised that the broad application of these rules to healthcare organizations because healthcare organizations typically do not think of themselves as creditors. However, the FTC, in a business alert, specifically stated, *where nonprofit and government entities defer payment for goods and services, they, too, are to be considered creditors. This alert from the FTC sets out the test for determining whether an organization is subject to the red flag rules.*

Organizations that are subject to the rules, must implement written, identity theft programs and procedures by the effective date of the regulation. For healthcare organizations, red flag programs will most likely include policies and procedures for detecting, preventing and mitigating medical identity theft that affects accounts such as patient billing accounts and the related medical records. To a large degree, policies and procedures implemented under HIPAA's Security Standard address issues for protecting patient identities from being stolen.

## Identity Theft Program Elements

The final rules list the four basic elements that must be included in the identity theft program. The program must:

1. **Be Written** - As with all programs required for compliance with regulations, an identity theft program must be in writing and contain reasonable policies and procedures that address the practice's potential risk. Reasonable means that the policies and procedures should be easily understood by the staff to ensure compliance. The rules also call for a program to be appropriate to the size and complexity of the practice that means most practices can keep the program simple.

2. Identify Relevant or Potential Red Flags for Covered Accounts – This means that a practice should evaluate the type of covered accounts that it maintains and could be subject to possible identity theft. As discussed earlier, practices would have two types of covered accounts to evaluate, patient billing accounts and patient medical records (even if such accounts are maintained in a paper-based system).

Second, a practice should evaluate the methods that are available to open such accounts, as well as the methods for accessing the accounts. Access to such accounts could occur through patient registration and through updates to a patient's medical record. For the vast majority of practices, the opening and access to patient billing and medical records is under the control of its employees and therefore limits unauthorized access for identity theft.

Third, a practice should review any past experiences with identity theft or possible identity theft regarding patient billing and/or medical records. This should include any notices or incidents relative to patients that may have stolen the identity of another person and used that stolen identity to become a patient of the practice.

3. Detect Red Flags – A practice must identify instances where Red Flags would likely be detected in connection with the opening or accessing of covered accounts. For example, a missing or altered photo ID or insurance card presented at registration could be a Red Flag, and would trigger action, such as refusal to register the patient, in order to control risks of identity theft. Another example of a Red Flag may be an instance or pattern of unusual medical care that appears on a patient's medical chart. In that case, it may be appropriate to contact the patient to confirm with the patient that they are truly the one receiving the care.
4. Respond Appropriately to Red Flags – This means implementing policies and procedures that will limit the potential for identity theft. Prevention measures may include, as appropriate, a policy that requires patients to present photo identification upon registration into the practice. Further, an organization could require verification of the validity of address changes or authentication measures for insurance coverage, such as placing calls to third-party payers.

According to the Federal Trade Commission (FTC), appropriate responses may include monitoring the covered account for evidence of identity theft; contacting the patient to tell them about the suspicious activity; reopening a covered account with a new account number; not opening a new covered account if identity theft is suspected; closing an existing covered account; not attempting to collect on the covered account, refunding amounts already collected, or not selling the covered account to a debt collector; or notifying law enforcement or Medicaid Fraud Control Units, as appropriate. In some cases, after monitoring the activity associated with the account, or verifying information, an appropriate response will be no response at all.

5. Be Updated – A practice must ensure that the identity theft program is updated on a regular basis. The rules require a practice to periodically conduct risk assessments, similar to what is being done annually for HIPAA's Security Standard, to determine whether the practice offers or maintains covert accounts. The risk assessment must take into consideration the methods that the practice provides for opening and accessing its accounts, as well as the practices previous experiences with identity theft, if any.
6. Be Approved - The regulations further define that the program must be documented and have oversight from a board of directors, a committee of the Board, or an employee at senior management level.

**What If No Rule?** Should the FTC change its mind and not require healthcare providers to comply with the Red Flags Rule, the case for verifying a patient's identity is still called for under the Privacy Rule as verification. And with the implementation of the Privacy Breach Notification Requirements, it is critical to ensure you are providing information and data to the correct person.