

## Chapter II Federal Privacy and Security Laws (HIPAA, ARRA, HITECH, Prevention of Medical Identity Theft)

Disclaimer: The information contained in this manual is not intended to be used as legal advice. Please refer to the most current specific state statutes and your own legal counsel when warranted. Some statutes will be referred to throughout this manual.

**WHAT IS HIPAA?** The Health Insurance Portability and Accountability Act (1996) established a minimum federal protection or "privacy floor" for the privacy and security of "protected health information "(PHI) as well as established rules for the transmission of electronic claims (administrative simplification). It is very important to note that state law in many cases is stricter than the HIPAA privacy and security.

The American Recovery and Reinvestment Act (ARRA) and its HITECH Act (Health Information Technology for Economic and Clinical Health) component became federal law in 2009. There are various portions pertaining to the privacy and security of information, and while some of these are still being determined (as of June, 2011), the changes we know about are incorporated into this chapter. It is important to recognize, as the push for electronic records continues, that tightening and expanding the rules protecting the privacy and security of PHI are evolving. Consult other resources to be sure you have the most up to date information.

Volumes have been written on HIPAA compliance. In this chapter we will outline the basic steps which each covered entity (CE) must take to achieve compliance as well as provide a list of resources you can turn to when implementing or evaluating your HIPAA compliance program.

**WHO MUST COMPLY?** Any organization that submits PHI electronically, such as providers, hospitals, pharmacies, nursing homes, home health agencies, health care plans, employer benefit plans, etc. must comply with the HIPAA provisions. And, the HITECH act expanded the concept of covered entities to include health care business associates. Business associates who access PHI (for instance, transcription companies, coding consultants, HCIS vendors and more) are now also required to follow HIPAA and can suffer criminal and civil penalties if they do not.

**THE HISTORY OF HIPAA** President Clinton ran for office in 1996 on the promise that Americans would have portable insurance to take with them from job to job that would not penalize them for preexisting conditions. Congress was charged with developing Privacy and Security regulations, with a time line that defaulted this responsibility to the Department of Human Services if Congress failed to act. DHS also failed to act, and the regulations were issued as part of Clinton's acts in his final days as president, and finalized in the early days of the G.W. Bush Administration. Most recently, The American Recovery and Reinvestment Act (ARRA) has expanded and

clarified some of these original privacy and security rules with the Health Information and Technology Provisions (HITECH), issued in 2009.

A number of factors contributed to the federal privacy focus at the time HIPAA was first proposed, including gene mapping, genetic and DNA testing, the emergence of the Internet and associated identity thefts. There were also some very well publicized breaches of confidential medical information in both electronic and paper media.

There was a great deal of consternation expressed by providers, insurers, patients, privacy advocates, drug companies and others in response to the proposed regulations. In total more than 50,000 written comments were received by DHS during two open comment periods. The final Privacy Rules, effective in 2003 and still the subject of debate, are considerably less protective of PHI than the original regulations were. Supporters say that the final rules have struck a balance between patient privacy rights and the needs of providers and insurers to have essential information necessary to conduct health care operations and to provide quality patient care.

As mentioned, 2009 brought ARRA (and HITECH) and with it an emphasis on healthcare information technology and more stringent rules for protecting PHI. Patient access is also expanded, and the “breach notification rules” require the notification of patients whose PHI is breached, as well as an annual report to DHS. (If more than 500 breaches occur, the media must also be notified).

Healthcare reform, called the *Patient Protection and Affordable Care Act*, was signed into law in March, 2010. While provisions of the bill are not entirely clear or implemented at this time, again, the Obama administration is placing much emphasis on the value of electronic health care records in improving patient safety, quality of care, and importantly, reducing the cost of care. Convincing consumers and others that their information will be appropriately secure and private is a major prerequisite for the widespread adoption of electronic records and Health Information Exchanges the Obama administration envisions.

### **General HIPAA Concepts**

HIPAA and the subsequent privacy and security regulations outlined in ARRA and HITECH have a set of unique terms HIM directors and those charged with compliance should know. The major acronyms, and their meanings, are listed below to hopefully help you make sense of the information which follows.

<b>Abbreviation</b>	<b>Meaning</b>
<b>ACE</b>	Affiliated Covered Entity
<b>ARRA</b>	The American Recovery and Reinvestment Act (2009)
<b>BA</b>	Business Associate
<b>CE</b>	Covered Entity
<b>CMS</b>	Centers for Medicare and Medicaid Services
<b>FTC</b>	Federal Trade Commission, responsible for the Red Flag Rules

<b>DHHS</b>	Department of Health and Human Services (both Maine and US)
<b>DRS</b>	Designated Record Set
<b>Health Info Net</b>	Health Info Net- Maine's HIE
<b>HIE</b>	Health Information Exchange- refers to shared records in a geographic area
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>HITECH</b>	These are provisions of ARRA which pertain to record privacy and security
<b>LAR</b>	Legally authorized representative
<b>MH</b>	Mental health
<b>MHA</b>	Maine Hospital Association
<b>NPP</b>	Notice of Privacy Practices
<b>OCR</b>	Office of Civil Rights
<b>OHCA</b>	Organized health care arrangement
<b>PHI</b>	Protected Health Information
<b>SA</b>	Substance abuse
<b>TPO</b>	Treatment, payment and health care operations

### COMPLIANCE DEADLINES

- ◆ **Transaction and Code Set Standards**- effective October 2002. With an extension form filed and accepted by DHS, extended to October 2003
- ◆ **Privacy Standards**- effective April 14, 2003
- ◆ **Security Standards**- effective April, 2005
- ◆ Breach Notification Rules effective fall 2009, and must be reported by March of each year to DHS.
- ◆ Expansion of the accountability of Business Associates- effective 2/17/10
- ◆ Rules to prevent Medical Identity Theft
- ◆ Accounting for disclosures for TPO ( to be determined)

### ENFORCEMENT

HIPAA and ARRA are enforced by the federal government and criminal and civil penalties may apply. Although originally the focus was primarily educational, and that focus continues (the office of Health Info Technology, established in 2009, has as its primary focus the education of consumers and covered entities), there has been more effort directed at enforcement and penalties for non compliance. We can expect this to continue in the future, and there are hints that CEs may be subject to unannounced HIPAA compliance audits in the coming years.

Covered entities are responsible for demonstrating their compliance via documentation and monitoring. Written risk assessments should be done regularly, along with workforce

training which of course must also be done on hire. Policies and procedures must be written and kept current.

Complaints against covered entities may be registered directly with the entity and/or the Secretary of Health and Human Services (HHS). Consumers are educated regarding this process in the Notice of Privacy Practices which must be given to each new patient, and acknowledged in writing (or documented why not) as well as posted in waiting areas and on facility websites.

The law provides significant CRIMINAL and CIVIL penalties for non-compliance. Enforcement of these privacy rules has fallen to the Office of Civil Rights (OCR) under the Department of Human Services. Security Rules are enforced by CMS. With the addition of the HITECH rules, however, authority has been granted to state attorneys general to bring actions on behalf of consumers residing in the state if the privacy or security of information rules are not followed.

### **SECURITY STANDARDS**

The Security Standards became effective April 2003. Covered entities were required to comply with the requirements by April 14, 2005. A major focus of the HITECH Act has been the enhancement of the security of electronic information in order to increase the confidence level of the public regarding the safety of electronic record and health information exchanges.

The security standards define administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic PHI. The standards require covered entities to implement basic safeguards to protect electronic PHI from unauthorized access, alteration, deletion, and transmission.

The Privacy Rule applies to protected health information in any form, whereas the Security Standards apply only to protected health information in electronic form. It is very important for HIM Professionals to work closely with IS leadership to develop policies and procedures to protect electronic PHI. This should include regular monitoring to insure basic best practices such as disaster recovery, server back up, etc are completed and documented regularly.

The regulations specify that some security practices are required, while others are addressable (meaning can be assessed to determine if risk warrants implementation in a particular facility or setting) In deciding which addressable security measures to implement, a covered entity should take into consideration the following factors:

- The size, complexity, and capabilities of the covered entity.
- The covered entity's technical infrastructure, hardware, and software security capabilities.
- The costs of security measures.
- The probability and criticality of potential risks to electronic protected health information.

## **Administrative Safeguards:**

**Policies and Procedures:** Required. Covered entities must document and implement policies and procedures regarding confidentiality, integrity and availability of electronic PHI. Policies and procedures to prevent, detect, contain, and correct security violations must also be in place. The policies and procedures need to be reasonably designed, taking into account the size and type of activities of the covered entity. Note that the ARRA HITECH provisions of 2009 have added additional requirements for policies regarding notifying patients and others if PHI is breached.

**Risk Analysis:** Required. Covered entities must conduct a written risk analysis and develop a written security plan to ensure the confidentiality, integrity and proper accessibility of PHI. The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-ennial or every 3 years) depending on circumstances of their environment.

The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:  
*“Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [E PHI], that establishes the extent to which an entity’s security polices and procedures meet the requirements of [the Security Rule].”*

**Risk Management:** Covered entities must implement security measures to protect against any reasonably anticipated threats or hazards (as identified in the risk assessment) to the security or integrity of the information and unauthorized use or disclosure of the information.

**Sanction Policy:** Covered entities must apply appropriate sanctions against employees who fail to comply with the entity’s security policies and procedures. The regulations do not specify what the sanction policy must be; some organizations have elected to be very specific and others have chosen a more case by case process.

**Information System Activity Review 164.308(a) (1) (ii) (V)** Required Covered entities must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Documentation of these activities should be retained permanently, but the logs may be destroyed 90 days after the completion of the report.

**Security Officer:** Required. Covered entities must appoint a Security Official (as they also must have a Privacy Officer). This individual has the final responsibility for a covered entity's security.

**Training:** Required. Covered entities must implement a security awareness and training program for all of its employees. This should be done at hire and regularly. Best practice is at least annually. Documentation of these activities should be retained.

**Contingency Plan:** Required. Covered entities must develop a written contingency plan to protect the availability, integrity, and security of data during downtime or other unforeseen occurrences. Covered entities need to consider how natural disasters could damage systems that contain electronic PHI and develop policies and procedures for responding to such situations. A **data backup plan** must be developed as part of the contingency plan. The content of the data backup plan should be determined by the risk analysis and risk management process. The data backup plan should define exactly what information is needed to be retrievable to allow the entity to continue business “as usual” in the face of damage or destruction of data, hardware, or software. Covered entities must develop a **disaster recovery plan** that establishes procedures to restore any loss of data. An **emergency mode operation plan** needs to be established to provide procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode. As with any of the information management policies or plans, this should be reviewed and updated on a regular basis.

### **Physical Safeguards:**

**Facility Access Controls:** Required. Covered entities must implement policies and procedures to limit physical access to its electronic information systems and the facility in which they are housed, while ensuring that properly authorized access is allowed. Covered entities must also implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users and mitigate any possibility of tampering or theft.

**Device and Media Controls:** Required. Covered entities must also implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility as well as the movement of these items within the facility. This should include policies regarding portable electronic media (laptops, PDA/s, cell phones, cameras, flash drives etc.) which have been known to be the cause of numerous reportable breaches. Many employers have elected to block access to social media sites from staff computers, however risk from at home use remains. Policies and procedures must also address the final disposition and destruction of electronic protected health information and/or the hardware or electronic media on which it is stored and the removal of electronic protected health information from electronic media before the media can be re-used. Note this can include images retained on digital photocopiers and hard drives. This should be discussed with IT leadership and professional assistance obtained if necessary.

### **Technical Safeguards:**

**Access Control:** Required. Covered entities must establish policies and procedures for systems that contain electronic protected health information to allow access only to

authorized individuals. Procedures for obtaining necessary electronic protected health information during an emergency must also be developed. All users must be assigned a unique identifier for tracking and procedures need to be established to verify that a person seeking access to electronic protected health information is the one claimed. In addition, passwords should be changed regularly and be sufficiently complex to discourage potential hackers. As defined in the Privacy Rules, access to PHI in any form should be based on an individual's role in the institution and restricted to the minimum necessary to fulfill the obligations of that role.

**Audit Controls:** Required. Covered entities must implement mechanisms that record and examine activity in information systems that contain electronic protected health information and develop policies and procedures to protect electronic protected health information from improper alterations or destruction. These activities should be documented and the documents retained. The Security Rule does not identify data that must be gathered by the audits or how often the audit reports should be run or reviewed. A CE must consider its risk analysis and organizational factors, such as current technical infrastructure and hardware and software security capabilities to determine its own reasonable and appropriate audit controls. Facilities may want to review their own record retention policies and decide how long to retain audit reports.

**Transmission Security:** Addressable. Technical security measures must be implemented to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. The HITECH regulations have increased the emphasis on the importance of ensuring that any information sent electronically is protected through encryption and password, but the HITECH Act itself does NOT require the use of encryption. The HHS guidance specifies that if encryption solutions are used that meet the minimum specified standards, and PHI is encrypted using these standards, then any incident which occurs would not be considered a privacy breach, and therefore notification to HHS would not be required. As noted previously, each covered entity must consider its own risk analysis and organization factors to determine when and how electronic information is to be encrypted.

**Business Associate Contracts:** Required. The contract between a covered entity and a business associate must provide that the business associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity. Originally Business Associates themselves were not considered covered entities under HIPAA and the contracting covered entity retained accountability for any privacy or security lapses of the business associate. With the HITECH provisions, Business Associates themselves now also have criminal and civil liability for neglecting to protect PHI in any format.

## PRIVACY STANDARDS

- **EVERY COVERED ENTITY MUST HAVE A PRIVACY OFFICER\_ § 164.530 (a)(1):** Every CE must appoint a Privacy Officer who has responsibility for HIPAA Privacy compliance. In addition, an individual (the Privacy Officer or someone else) must be appointed as the point person to receive privacy complaints. For an excellent description of the role of privacy officer and a sample job description, consult AHIMA's website ([www.AHIMA.org](http://www.AHIMA.org)).
  
- **EVERY COVERED ENTITY MUST HAVE A NOTICE OF PRIVACY PRACTICES----- § 164.520** HIPAA requires that EVERY covered entity have a Notice of Privacy Practices which must be given to patients or their legally authorized representative (LAR) at the initiation of treatment. There are very specific statements which MUST be included and areas that must be covered in this notice, which is designed to inform patients about how covered entities may use their PHI. CEs are required to attempt to obtain written acknowledgement of receipt of the notice from the patient/LAR and maintain this documentation. If the patient refuses to acknowledge receipt, efforts to obtain acknowledgement must be documented, and in *some* cases providers may refuse to treat patients who refuse to sign. (Consult legal counsel on this point). The requirement is that the notice must be given at the initiation of treatment, and need not be repeated unless the Notice changes. It is also required that the complete notice be posted on walls in patient care areas and on a CEs website, if one exists.

Over time, some CEs have revised their Notice of Privacy Practices. The law is clear that while the fact that the notice has been revised must be posted, along with the revised notice, it is NOT required that the notice be reissued to every patient. However, many organizations do redistribute the notice, and some do it annually, combining it with the annual revision of consent process. This may be a best practice.

Note that under HITECH, CEs must respect a patient's right to request that their PHI not be released to their insurance company, as long as they agree to pay out of pocket. This is an extension of the HIPAA privacy rules which until recently stated that a CE is not required to adhere to any restrictions requested by the patient, and so strengthens patients' rights to restrict disclosure.

**EVERY COVERED ENTITY MUST HAVE A COMPLAINT PROCESS AND AN INDIVIDUAL DESIGNATED TO RECEIVE COMPLAINTS- § 164.530 (d)(1)** HIPAA requires a formal complaint process be in place for managing privacy complaints, and that documentation of investigations and outcomes be maintained. This information may be requested for review by the Office of Civil Rights or CMS, (and now States Attorneys General) all of which have roles in HIPAA compliance oversight. Complaint forms and policies must reflect that there will be no retaliation in response to complaints, and complainants must be told of their option to contact the federal government should they be unhappy with the outcome of the CE's complaint process.

**DESIGNATED RECORD SET- §164.501** The designated record set is defined as a group of records maintained by or for a covered entity that includes: Medical and billing records about individuals.

- The enrollment, payment, claims adjudication, and case or medical management record systems maintained and used to make decisions about patients.
- Information used in whole or in part to make decisions about an individual.
- Records maintained by a Business Associate (for instance, record storage facilities) that also manages the release of information instead of returning the records to the covered entity to respond to requests.

Covered entities need to define what they consider their “designated record set” (sometimes also called the legal health record). This becomes especially important as more and more organizations keep at least some of their documentation in electronic format. So called “Hybrid Records”, which are partly electronic and partly on paper, can be difficult for HIM Directors to manage. There should be a written policy and procedure which most importantly includes a process to alert the end user that he/she may have to look in more than one place in order to access the complete clinical record. Many covered entities may have “shadow records”. These are records that may be considered a duplicate of the original record that is kept in the originating department as a “working copy”. However, it is important to be sure that the “shadow records” do not contain data/information that is not in the original record defined in your designated record set. When possible, “shadow records” should be avoided.

In order to gain knowledge of possible “shadow records” an inventory of records should be completed. Every department that creates data for the original record should be a participant in this inventory. It may be helpful to have a committee consisting of these people. This committee should consider the type of records, the record content, the location of the records, and the accessibility or access demands for the records. With the increasing adoption of electronic medical records and the concept of “one patient, one record”, it is expected that there will be even less need for “shadow records”.

**MINIMUM NECESSARY STANDARD- § 164.502 (b)(1-2)** A key concept in HIPAA is that only the information absolutely necessary to accomplish the stated purpose of the request should be accessed by the user of PHI, whether an internal or external user. Thus, facilities must have policies in place delineating which types of employees have access to what PHI and for what reasons and for how long.

Outside the organization, it is a little more complicated to define minimum necessary, but again policies and procedures should spell this out. Patients may authorize copies of their entire record, but requesting covered entities, which are also bound by HIPAA, are required to ask for only the minimum necessary.

It is important to note that the HITECH provisions of ARRA address this concept and strengthen it. While not completely implemented as of this writing, CEs may be expected to determine what the minimum necessary is in a particular scenario, rather than

assuming that the requestor, if also a covered entity, will do so. This could become particularly complex when releasing information for operational or payment purposes.

**BUSINESS ASSOCIATES- § 164.504 (e)** A Business Associate is defined as a person or entity that performs certain functions or activities that involve the use or disclosure of PHI (protected health information) on behalf of, or provides services to, a covered entity that is not part of treatment, payment, or health care operations. A covered entity must have all business associate agreements complete by April 2004. These should be revised to make sure the new obligations of Business Associates as articulated in ARRA are included.

- A member of the covered entity's workforce is not a business associate.
- When a health care provider discloses protected health information to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network, the plan is not considered a business associate (A provider that submits a claim to a health plan, and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other).
- A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

Some examples of Business Associates include:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose legal services to a health plan involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist (or transcription vendor) that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.
- A covered entity's computer systems vendors.
- The Joint Commission (TJC)

The following elements must be contained in a Business Associate agreement or contract:

- It must describe the permitted and required uses of protected health information by the business associate.
- It must provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the agreement/contract or as required by law.

- It must require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the agreement or contract.

As of February 17, 2010 Under Section 13404, a Business Associate may only use or disclose PHI in a manner that complies with 45 C.F.R. §164.504 (e) which describes the requirements for business associate agreements. They must also comply with the applicable provisions of the HITECH Act and the following provisions of the security rule:

§164.308 Administrative Safeguards

§164.310 Physical Safeguards

§164.312 Technical Safeguards

§164.316 Policies and Procedures

They will be subject to the civil and criminal penalties if they violate these provisions.

Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the agreement or contract. If termination of the agreement or contract is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Sample Business Associate agreement or contract language is available on the HHS OCR Privacy of Health Information website at <http://www.hhs.gov/ocr/hipaa/contractprov.html>.

**MITIGATION- §164.530(f):** A covered entity must mitigate, to the extent practical, any harmful effect that is known of a use or disclosure of protected health information in violation of its policies and procedures by an employee or Business Associate. In addition, as of 2009, the Business Associate is also responsible for this. (However providers are ultimately (and equally) responsible for the privacy and security of their PHI and so should work with Business Associates to mitigate a breach should it occur. The BA will be generally looking to the provider for guidance in achieving compliance in this area. The following factors should be evaluated in determining whether or how to mitigate any damages:

1. Whether any damage occurred;
2. The damage that occurred, if any;
3. The type of damage, if any;
4. The amount of damage, if any;
5. The PHI that was used or disclosed;
6. The reasons for the use or disclosure; and
7. Whether the harm can be mitigated

**OHCAs , HIEs and ACEs** HIPAA recognizes that the world of healthcare is a world of networks. It is the rare provider's office or hospital, or even health plan, that stands

totally alone. Thus, organizations may elect to consider themselves part of an Organized Health Care Arrangement (OHCA) or an Affiliated Covered Entity (ACE) or a Health Information Exchange (HIE) to share NPPs, policies, procedures, PHI, and, of course, potential liability. There are also hybrid organizations where a part of the organization is a covered entity but the rest is not (for instance, the Walmart pharmacy is a CE, but the rest of the organization is not). These are all legal designations, and the decision to identify your organization as any of these should be made with legal advice.

**PSYCHOTHERAPY NOTES § 164.508 (a)(2)** There has been quite a lot of confusion about the special protection HIPAA gives to Psychotherapy notes and exactly what a "psychotherapy note" is. HIPAA clearly states that Psychotherapy notes are those kept separate from the traditional medical record. These cannot be used to substantiate billing, and if psychotherapy notes are kept, another note documenting the service must be kept for billing and legal purposes. These "case notes" or "raw data" are afforded special protection under HIPAA. Most CE's reading this chapter will have no such notes, or very limited ones (and should remember that ANY note is subject to discovery with a judge's order, even a psychotherapy note). It should also be noted that Maine has more stringent laws than HIPAA when it comes to protecting Mental Health information (see Chapter 7), and so these laws would apply.

**FUNDRAISING § 164.514 (f)(1-2)** Certain fundraising activities have been included in the definition of "health care operations", thus allowing covered entities to use and disclose PHI without patient authorization in support of limited fundraising activities. General administrative and business functions necessary for covered entities to remain a viable business are included as part of the definition of a covered entity's "health care operations". Covered entities may use or disclose an individual's demographic information and/or the dates that the individual received treatment.

These uses and disclosures are permissible as long as:

- ❑ the covered entity's notice of privacy practices states that individuals may be contacted for the purpose of raising funds,
- ❑ any and all fundraising materials include prominent instructions on how to opt-out of future communication, and the covered entity honors the request.

**RESEARCH § 164.512 (i)** The Privacy Rule recognizes that the research community has legitimate needs to use, access, and disclose Protected Health Information (PHI) to carry out a wide range of health research protocols and projects. The Privacy Rule protects the privacy of such information while providing ways in which researchers can access and use PHI when necessary to conduct research. See [http://privacyruleandresearch.nih.gov/pr\\_08.asp#8b](http://privacyruleandresearch.nih.gov/pr_08.asp#8b) for more information on research.

## **MARKETING**

**§ 164.514 (e)** The use or disclosure of PHI for marketing purposes is permissible without an authorization in three instances:

- Covered entities are permitted to use or disclose PHI without authorization to make marketing communications in face-to-face encounters. These communications may include discussion of any services or products, including the services or products of a third party.
- Communication about a product or service that encourages recipient to purchase or use product or service only will be considered “health care operations” if covered entity does not receive direct or indirect remuneration in exchange for the communication and the communication meets certain exceptions under “marketing” definition:
  - (i) to describe health-related product or service included in plan of benefits, such as entities participating in network, replacement of or enhancements to health plan, and services or products that add value to, but are not part of, plan of benefits;
  - (ii) for treatment; or
  - (iii) for case management or care coordination, or to direct alternative treatments, providers, or settings of care.
    - Remuneration is permitted if communication only describes drug or biologic currently being prescribed and payment is reasonable or if individual authorizes.
    - In order to fall under definition of “health care operations,” any written fundraising communication by covered entity shall, in clear and conspicuous manner, provide recipient opportunity to opt out of further communications. Opt out is treated as a revocation of authorization.
- PHI may be used or disclosed without authorization to make marketing communications involving products or services of nominal value. This would allow distribution of calendars, pens, and other merchandise that is generally considered to be of a promotional nature.
- No authorization is required for marketing communications about health related products or services of the covered entity or a third party, if the communication:
  - identifies the covered entity as the party making the communication
  - discloses any direct or indirect remuneration received by the covered entity for making the communication,
  - contains instructions on how to opt-out of similar future communications, and
  - explains why the individual has been targeted for the communication in those instances where PHI was used to target the communication to particular individuals based upon their health status or condition.

**PREEMPTION** As mentioned above, HIPAA sets a "Privacy Floor" and is by no means the strictest standard for the protection of PHI. Many states, including Maine, have confidentiality laws (1711C- *See Chapter 1*), which have stricter requirements, wholly or in part. In addition, Maine has the "*Rights of Recipients for Patients who Receive Mental Health Services*" and a state statute which affords higher protection to information related to HIV. The federal government has its own set of stricter laws with CFR 42. These provide a very high level of protection to information pertaining to substance abuse testing and treatment services.

The basic concept is that whatever is stricter, prevails. Whatever provides the greatest protection to PHI, stands. If HIPAA is silent on a point and the state law speaks to it, then part of HIPAA and part of the state law may both apply. Obviously, this has been a challenge for attorneys to parse out which aspects of which laws apply in which circumstances. An Arizona law firm was commissioned in 2003 to analyze HIPAA as it relates to Maine State law. The result is a comprehensive set of analyses, guidance, sample policies and forms which are available for purchase from the Maine Hospital Association. This document is several volumes long and is impossible to summarize here. Only the highlights are mentioned below:

**Consent.** Although not required by HIPAA, consent is legally required for mental health services, abortion, sterilization, and HIV testing, and is strongly advised in all cases prior to the initiation of treatment and for any invasive or potentially risky procedure (surgeries, invasive tests, even vaccinations and flu shots). MRSA 21 2905 states that having written informed consent may be protection from legal recovery. It is also an excellent way to educate patients about your practices and to be sure that they are told of your organization's practices in releasing information for Treatment, Payment and Operations (TPO). Many organizations include a line to acknowledge the receipt of the Notice of Privacy Practices on the same form, which may be more efficient. Best practice is to obtain general written consent for treatment for each episode of care (inpatient) or once a year in outpatient sites.

**Unauthorized disclosures.** Maine Law very specifically outlines the circumstances under which information may be released without written patient authorization. If a recipient is not listed in the Maine Statute, Maine providers should NOT disclose PHI to that recipient without patient/legally authorized representative (LAR) written authorization, even if HIPAA would permit the disclosure.

**Protections for substance abuse (SA), mental health (MH) and HIV still apply.** These various protections are complicated and are derived from state and federal laws which apply higher privacy protections for this extremely sensitive information. Generally, this type of information may NOT be released for TPO without specific patient written consent/authorization, unless there is a medical emergency or as otherwise allowed by law. See related chapters in this manual.

**Minors.** HIPAA very specifically leaves the handling of information regarding Minor's privacy rights to state laws. See Chapter 1 for further discussion of Minors.

### **PATIENT RIGHTS UNDER HIPAA**

- **RIGHT TO ACCESS PHI- §164.524:** Individuals have the right to inspect and obtain copies of their PHI contained in a designated record set, which includes the medical record, billing record and other records used to make decisions about an individual. The right to access is valid as long as the designated record set is available (see Chapter X for information regarding retention and destruction of PHI).

Rarely, a covered entity may deny an individual access to review in the following circumstances:

- The provider determines the information is reasonably likely to endanger the life or physical safety of the individual or another person;
- The request is made by a personal representative and it is determined that access to such PHI is likely to cause substantial harm to the individual or another person.

If access is denied, the individual must be informed in writing and the statement must include the basis for the denial, a statement of the individual's review rights, and how the individual may file a complaint. The individual has the right to request a review by a licensed health care professional who did not participate in the original denial process. If access is denied, a summary be provided instead.

If a request to access is approved, the covered entity must act upon the request within 30 days of receipt of the request (HITECH may impact this time frame when the final rules are released). (Note that per Mental Health Regulations in Maine, the patient must be permitted to review his/her records within 3 "working" days). If the records are stored offsite, the covered entity may take 60 days to comply with the request provided the individual is informed in writing of the delay.

The covered entity may impose a reasonable, cost-based fee, provided the fee includes *only* the cost of actual copying (supplies and labor) and postage. HIPAA specifically prohibits retrieval fees. However, Maine state law allows a charge of \$10 for the first page and \$.35 for each additional page.

Under the HITECH Act, keepers of PHI are encouraged to permit electronic access to patient information through a patient portal or similar technology. The HITECH rules require that if the requestor asks for the information in an electronic format that it be provided. Some facilities with hybrid records are satisfying this requirement by scanning information and downloading to a CD.

The covered entity must document the designated record sets that are subject to access and the titles of persons or offices responsible for receiving and processing requests for access.

**PATIENT REQUESTS TO AMEND PHI- §164.526:** An individual has the right to request to amend protected health information in a designated record set for as long as the PHI is maintained in the designated record set. A covered entity may deny a request for amendment on any one of the following bases:

1. The PHI in the designated record set is accurate and complete.
2. The PHI is not part of the designated record set.
3. The PHI was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act upon the request to amend.

Patients/LARs should submit the request for amendment in writing to the Privacy Officer. The covered entity must act upon the request within 60 days of the date of the request. If the covered entity grants the requested amendment, in whole or in part, the following requirements must be met (note that the original document must never be altered but additional information may be added):

1. The amendment to the PHI must be made to the records in the designated record set.
2. The individual requesting the amendment must be informed that the amendment was accepted. The covered entity should obtain the individual's agreement/request for the covered entity to notify relevant persons.
3. The covered entity must make reasonable efforts to notify relevant persons about the amendment, if authorized and requested.

If the covered entity denies the requested amendment, in whole or in part, a written notice of the denial must be provided to the individual. This written notice should contain:

1. The basis for the denial;
2. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
3. A statement that if the individual does not submit a statement of disagreement, the individual may request that the covered entity provide the individual's request for amendment and the denial with any future disclosures of PHI;
4. A description of how the individual may submit a complaint to the covered entity.

The covered entity should prepare a written rebuttal to the individual's disagreement statement that is forwarded to the individual. The request for amendment, notice of denial, individual's written statement and written rebuttal shall be included in the designated record set and included in all future disclosures of PHI, if authorized. (note that Maine Law requires that sharing an amendment with third parties be authorized by the patient or LAR).

**ALTERNATIVE MEANS OF COMMUNICATION §164.522(b)(1):** Covered entities must permit individuals to request an alternative means or location for receiving communications of PHI. For example, individuals may request a specific phone number for communication or the use of a closed envelope for communications instead of a post card.

A covered entity may require the request for alternative means of communication in writing. Under the HITECH rules, a covered entity is obligated to respond to the individual's request. A covered entity may not require an explanation from the individual as a condition of providing alternative communications.

**PATIENTS MAY REQUEST RESTRICTIONS ON USE/DISCLOSURE OF PHI §164.522(a)(1-3):**

- A covered entity must allow an individual to request restrictions on uses and disclosures of PHI/EPHI for treatment, payment or health care operations.

- ❑ Originally, a covered entity was not required to agree to a restriction and had to notify the individual of such refusal. Under HITECH, the covered entity must agree to the patient's request for a restriction. Note that if this involves payment, the patient must assume financial responsibility in advance for the care provided if he or she restricts the covered entity's ability to exchange PHI with the payer.
- ❑ The only exception to the request of use and disclosure is when the restricted PHI is needed for a health care emergency. The covered entity may release PHI to a health care provider if it is needed to provide emergency treatment to the individual. The covered entity must request that the recipient not further use or disclose the PHI.
- ❑ A covered entity may terminate the agreement to restrict use and disclosure of PHI if:
  1. The individual agrees to or requests the termination in writing; or
  2. The individual agrees orally to the termination and it is documented in the medical record;
- ❑ All requests and terminations of uses and disclosures of PHI should be documented in the medical record.

**REVOCAION OF AUTHORIZATION§ 164.508 (b)(5)** Patients have the right to revoke their authorization for release of PHI except to the extent that the CE has already taken action based on the release, or if the authorization was obtained as a condition of receiving insurance coverage. (Other laws provide the insurer with the right to contest a claim under this policy.)

Most CE's include this "revocation of authorization" notice on their Release of Information form and in their Notice of Privacy Practices. Most CE's will act immediately upon a verbal notice of intent to revoke and ask the patient to put the request in writing. This should be documented in the patient's record.

**RIGHT TO AN ACCOUNTING OF DISCLOSURES§ 164.528** Patients have the right to receive an accounting of disclosures of PHI made by covered entities and their business associates extending back six years prior to the date of the request. (HITECH is proposing 5 years for EPHI) This applies to disclosures for "non-routine" purposes. The accounting does not have to include disclosures made:

- ❑ for treatment, payment, or operations;
- ❑ to the patient or patient's representative;
- ❑ in the facility directory (patient census);
- ❑ to persons involved in the patient's care;
- ❑ for national security or intelligence purposes;
- ❑ to correctional institutions or law enforcement officials with custody of an inmate;
- ❑ as part of a limited data set;
- ❑ To any disclosure made pursuant to a properly executed authorization to release information

Note that under HITECH covered entities must be able to account for any electronic disclosure, for ANY purpose, including TPO, and including disclosures within your institution which can be tracked electronically (audit trails). As of June, 2011, HHS has yet to issue regulations on the information that must be collected as part of an accounting

audit, but this may include information shared within an organization or network as well as outside of it.

The disclosure (of external releases) must include:

- ❑ date of disclosure;
- ❑ name of entity or person who received the PHI and address, if known;
- ❑ a brief description of the PHI disclosed; and
- ❑ a brief statement of the purpose of disclosure or a copy of a written request for disclosure, if any.

If a covered entity has made multiple disclosures of PHI to the same person or entity for a single purpose or pursuant to a single authorization, provide a summary disclosure, which includes:

- ❑ for the first disclosure, the date, name of entity or person who received PHI and address, if known, a brief description of the PHI, and a brief statement of the purpose of the disclosure or copy of disclosure request;
- ❑ for later disclosures, the frequency, periodicity, or number of further disclosures; and
- ❑ the date of the last such disclosure.

If the disclosure was for research, and if during the period of the accounting the covered entity made disclosures for a particular research purpose that involved 50 or more individuals, and the requesting patient may have been included in the research, the covered entity may provide the following in the accounting;

- ❑ The name of the protocol or other research activity;
- ❑ A description of the research protocol or activity, including the purpose of the research and the criteria for selecting particular records;
- ❑ A brief description of the type of PHI that was disclosed;
- ❑ The date or period of time during which such disclosure occurred, or may have occurred, including the date of the last disclosure;
- ❑ The name, address, and telephone number of the entity that sponsored the research and the researcher to whom the information was disclosed; and
- ❑ A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

The entity must act on the request for an accounting no later than 60 days after the receipt of the request. This can be extended by no more than 30 days providing that the covered entity gives the patient a written statement briefly stating why more time is needed and the date by which the accounting will be provided. The first accounting in any 12 month period must be without charge. The entity can charge for any subsequent accountings within the same 12 month period provided that the patient is informed in advance of the fee. The entity must retain a copy of any accounting provided and must document the titles of the persons or offices responsible for receiving and processing requests for an accounting, for six years (5 years proposed under HITECH).

NOTE: A difficult aspect of the HIPAA accounting requirement is obtaining timely, complete, and accurate information from business associates. Covered entities need to

think carefully about how to track which business associates make disclosures and how to ensure these business associates keep track of information required to provide an accounting and to provide this information to the covered entity in a timely manner.

## **SUGGESTED/REQUIRED POLICIES AND PROCEDURES**

**POLICIES AND PROCEDURES TO PROTECT SECURITY AND PRIVACY OF PHI :** CEs should have policies and procedures regarding the protection and security of PHI in whatever form. These policies should include computer security, password security, record accessibility and security, destruction and retention of records, damage controls, back up files, audits, use of electronic media, including portable devices, use of email and social networking, etc

**PROTECTION FROM "INCIDENTAL DISCLOSURES" § 164.530** When HIPAA was first released, as with the first Maine State Confidentiality law, there was a lot of consternation and confusion about how far CE's are expected to go to protect patient privacy. Must all hospital rooms be private? Must walls take the place of curtains in the ER? The Office of Civil Rights and the Department of Human Services has published several series of frequently asked questions (FAQs) which readers should review. Written in simple language, these FAQs spell out what is considered reasonable and what is not. Key is that CEs should do a written assessment of privacy issues within their organizations, and take reasonable steps to correct or ameliorate them. Steps which do not cost much money (reconfiguring work stations, removing names from the front of records or at least keeping them turned over, eliminating white boards, moving fax machines to private locations etc.) will almost certainly be considered reasonable, and therefore expected, for an organization to be compliant with HIPAA. These written assessments should be reviewed and updated periodically.

**CLERGY §164.510(a)(1)(ii)(A):** The covered entity may disclose facility directory information which includes patient's name, room number and religious affiliation to clergy members, (as long as the patient has been given the opportunity to opt out) but not the patient's place of residence. The exception is if the clergy is a member of the covered entity's workforce and may have access to PHI as necessary to perform job functions.

**FACILITY DIRECTORIES:** Under HIPAA, patients must be given the opportunity to "opt out" of facility directories, keeping even their presence in the facility confidential.

**CONFIDENTIAL DESTRUCTION:** All CEs must have policies and procedures to safeguard PHI, whether in paper or electronic form. Thus, policies calling for all information with patient names on it to be shredded or otherwise confidentially destroyed or for PCs and other electronic devices to be expunged of any patient information prior to resale or recycling are essential. Pay particular attention to copy and fax machines where images may be permanently retained and get technical consultation prior to destroying or recycling. A major concern is documents (or electronic media) leaving the facility and becoming stolen or lost. Policies should also address this concern.

**ROLE BASED ACCESS:** Organizations should limit access to PHI by staff member role. Level of access is determined by the staff member's need to know PHI in order to perform his/her assigned duties. This should be documented in policy.

**TERMINATION PROCEDURES CHECKLIST § 142.308:** The covered entity must have documented instructions which include appropriate security measures when an employee's employment is terminated for any reason and when an internal or external user's access is terminated. The instructions must include procedures for the following implemented features (checklist):

- Changing of locks
- Removal from access lists
- Removal of user account(s)
- Turning in of keys, tokens, cards, or badges that allow access.
- Returning computers, PDAs, laptops or other electronic media

**EMAIL AND FAXING POLICIES:** Covered Entities must have policies and procedures to establish guidelines for the use of e-mail and for faxing and receiving faxed information to safeguard PHI. CEs must use encryption when transmitting PHI over an "open network." CEs must put in place certain other technical security mechanisms to guard against unauthorized access to data that is transmitted over a network:

- Integrity controls
- Message authentication
- Access controls or encryption
- An alarm
- Audit trail
- Entity authentication
- Event reporting.

Covered entities should consider carefully whether they will permit providers and patients to exchange emails or texts. Although seen as convenient by some, email can be forwarded, printed, altered, legally discovered, sent in error to the wrong address, etc. If email communication is permitted, clinically pertinent email should be printed and put in the patient record or retained electronically. New federal discovery rules make it clear that electronic media, including email and voice mail, is subject to legal discovery.

Fax machines must be located in a secure location accessible only by authorized staff/personnel. CEs should make sure their policies restrict faxing to situations in which there is a need for urgency and the fax is going to a secured location. If organizations allow preprogramming of fax machines, care should be taken to periodically verify the accuracy of the preprogrammed numbers, as these do change.

**INTERNET AND SOCIAL MEDIA POLICIES:** Social Networking sites such as Face Book and Twitter provide additional challenges to Privacy and Security Officers. Staff should be educated to never post work related information or photographs. In addition, "friending" patients is generally considered unethical by most professional groups.

**REMOTE ACCESS:** Many covered entities allow telecommuting. There should be policies and procedures and technical safeguards in place to minimize any privacy and security concerns.

**PHOTOGRAPHS, AUDIO and VIDEOTAPES:** See Chapter XIII of this manual for a full discussion of this topic.

**BREACH NOTIFICATION POLICY:** As mentioned, the American Recovery and Reinvestment Act's HITECH provisions require that patients be notified of any breach of unsecured PHI that, in the estimation of the investigator, could lead to "significant risk of financial, reputational or other harm to the individual." There are time limits from when the breach is first discovered to the notification (note that Maine state law requires notification within 7 days if electronic information is breached (Title 10, part 3, Chapter 210-B, 1346-1348) and so is stricter than these federal requirements). The notification must be in writing. In addition, by March first of each year, the Covered Entity must file a written report with the Department of Human Services listing each breach. Information on how to report breaches can be found at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.

If you should have a breach involving 500 patients or more, there are additional steps you must take. You must notify DHS immediately (same website) and also notify your local media and put the information on your website. Of course a breach this significant should also be reported to your Executive team, Risk Manager/Compliance Officer/Legal Counsel.

Be sure to document your investigations of any breach allegations and your follow up and actions. Staff must be trained to report any suspicions to you immediately. This was already required under HIPAA, and has been strengthened by these new provisions in HITECH.

**AUTHORIZATIONS AND RELEASES § 164.508 and § 164.512 :** HIPAA adds some required elements for CE's to be sure are included in any release of information forms (in addition to those required by Maine State Law). Specifically, HIPAA privacy standards require that a specific expiration date or event be listed, and that the authority of someone other than the patient who signs be documented. An authorization that complies with both Maine Law and the Privacy Requirements will include:

- ❑ Specific and meaningful description of information to be disclosed
- ❑ Name or SPECIFIC identification of hospital, entity, or class of persons authorized to disclose
- ❑ Name or specific identification of hospital, entity, or class of persons to whom the PHI is to be disclosed
- ❑ A description of the purpose of the disclosure (at the request of the patient IS sufficient)
- ❑ Specific expiration date or event which signals expiration of the release

- ❑ A statement that the patient may revoke the authorization in writing (Maine licensing and best practice also requires that a verbal revocation be accepted), and, if this is done, the revocation may be the basis for denial of health benefits or other insurance coverage or benefits
- ❑ A statement regarding the exceptions to the right to revoke or a reference to the NPP that includes this information
- ❑ The form must state that the person is entitled to a copy
- ❑ A statement that the CE may not condition treatment, payment or enrollment or eligibility for benefits on the patient's willingness to sign, or, if there are consequences to refusing to sign, what these are
- ❑ Whether there may be re-disclosure of the information and, if so, what the consequences of this may be
- ❑ A statement that the patient may refuse to sign but that this might result in improper diagnosis or treatment, denial of coverage or other insurance or other adverse consequences
- ❑ The authorization must be signed by the patient and/or legal representative, and dated. If signed electronically, it must be authenticated. If signed by someone other than the patient, this person's authority to sign (relationship) must be documented.

***To conform to Maine HIV law, CFR 42 regarding substance abuse records, and the Rights of Recipients of Mental Health Services the following elements must be present in addition to those listed above when releasing information pertaining to Mental Health, HIV and/or substance abuse:***

- ❑ The patient's authorization to release any information relating to the diagnosis or treatment of an HIV infection.
- ❑ The patient's authorization to release any information relating to the diagnosis or treatment of alcohol or drug abuse, the fact that this information may not be re-released and/or used in a criminal proceeding against the patient.
- ❑ The patient's authorization to release any information relating to the diagnosis or treatment of mental health and whether they want to review the information before it is released.

**ELEMENTS REQUIRED FOR AUTHORIZATION § 164.508 (c)** All of the above mentioned elements must be addressed before information may be released, unless there is a medical emergency or other exception. In the case of a medical emergency, the patient should be treated and the authorization obtained as soon as possible after the patient is treated. Maine state law allows 30 months for authorizations to be considered valid. Under mental health regulations this authorization is valid for one year. It is important to remember that these timeframes are for the specific information cited on the authorization form only; if other information is needed another authorization must be obtained. Each organization should have facility-specific written policies outlining release of information and timelines for how long an authorization is valid (remember, these timeframes cannot be longer than the state or federal guidelines, but they can be

more stringent). If there are any questions about whether information should be released, contact your organization's legal representative.

**VERIFICATION OF THE IDENTITY OF THE REQUESTOR §164.514(h)(1):**

A covered entity must verify the identity and authority of any individual requesting access to protected health information.

- ❑ **Individuals:** Covered entity will verify the identity of any person requesting PHI who is not already known to the organization at the time of the request. Verification of identity will include:
  - ❑ Status as a member of the workforce
  - ❑ Provision of a photo identification such as a driver's license, passport, or other government-issued photo identification
  - ❑ Comparing signatures on file to the signature on the release
  
- ❑ **Telephone requests:** Callers requesting PHI will be asked to identify themselves and their relationship to the patient. Extreme care should be taken in responding to requests by telephone.
  - ❑ Authentication information will include the patient's name, date of birth and at least one other identifying number, such as medical record number, social security number, etc.
  - ❑ If the caller is unable to provide additional authentication information, or the staff taking the call has concerns regarding the caller's identity, callback verification should be used.
  
- ❑ **Public Officials:** Verification of identity and authority of public officials will include:
  - ❑ The provision of official credentials, an ID badge, or other proof of governmental status
  - ❑ A written request on the appropriate government letterhead, accompanied by a properly executed patient authorization or court order (subpoena is insufficient unless DHHS investigative)
  - ❑ If the request is made by an individual on behalf of a public official, the requestor provides a written statement of governmental authority on appropriate letterhead, a contract for services, memorandum of agreement, or purchase order. (note: Maine Medical Examiners may obtain PHI with a faxed request on their letterhead. Out of state Medical Examiners should go through the Maine Medical Examiner or have written authorization from the patient's LAR).
  
- ❑ **Authority:** Verification of authority will include:
  - ❑ Status of a member of the workforce who has authority to request information; or
  - ❑ The person making the request is the subject of the PHI; or
  - ❑ The person making the request is an authorized personal representative of the patient with appropriate documentation (parent, guardian, or Power of Attorney, etc.); and/or

- ❑ The request is in writing, has been signed by the subject of the PHI or his/her legal representative and meets the requirements of an authorization
- ❑ **Exceptions:**
  - ❑ If the requestor is known to the covered entity, identity verification is not required.
  - ❑ If the covered entity knows the requestor has the authority to request PHI they are not required to verify authority. This should be documented in the medical record.
  - ❑ Verification of identity is not required of persons requesting information from the facility directory.
  - ❑ Verification of identity is not required of family members and others involved in the care of the patient.

## **MEDICAL IDENTITY THEFT**

Various regulations require organizations to take steps to minimize instances of identity theft, including medical identity theft. This can cause financial and personal problems for the victim, and in the case of medical identity theft could even lead to a serious adverse event (for instance, the patient whose identity has been stolen doesn't have an allergy the "fraud" patient has, so a serious med error occurs.)

Organizations are encouraged to have policies and procedures for identifying identity theft (red flags may include repeatedly returned mail, different dates of birth or insurance information) and to train the workforce on how spot potential instances of identity theft.

## **TRAINING**

**WORK FORCE TRAINING § Section 164.530:** The final Privacy rule states "a covered entity must train all members of its work force on the policies and procedures with respect to PHI as necessary and appropriate for the members of the work force to carry out their function within the covered entity." All members of a CE's work force are required to be trained in all Privacy rule-related policies and procedures. The term "work force" is defined as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." Thus, even if an organization contracts with, for instance, a cleaning service, those workers must receive HIPAA training since they are in essence extensions of the work force.

All new members of the work force must be trained within a reasonable period of time after their start date. Also, when there is a "material change" in the policies and procedures each member of the work force who is affected by the change must be trained within a reasonable time of the effective date of the change.

Documentation to support the training of the covered entities work force must be generated and must be retained in either written or electronic form for six years from the date it was generated.

The Privacy rule does not regulate how covered entities should go about the training, but AHIMA has published a Practice Brief titled “HIPAA Privacy and Security Training” which is a good source of information and provides a sample training program.

Healthcare providers should view training as the single most important part of successful compliance with the Privacy rule. The better the training, the better the compliance.

## **IMPLEMENTATION STRATEGIES/RESOURCES**

- ✓ Have a HIPAA Committee or Privacy Committee. You can't do this alone!
- ✓ Conduct a self-assessment and document the gaps you have and how you plan to fill them. Repeat as necessary.
- ✓ AHIMA has Practice Briefs, Journal Articles and information in the FORE Body of Knowledge. Also, there is a Community of Practice on HIPAA that you should join. You can post questions there and find out what your peers across the country are doing and thinking. There are some sample policies, forms and even training programs posted for your use.
- ✓ Maine Hospital Association commissioned a preemption analysis and sample forms and policies that are an excellent resource for HIPAA. This document takes Maine Law, HIPAA and other relevant law, lays them out side by side, and makes recommendations about which applies in many circumstances. Consult the MHA to purchase.
- ✓ Read the regulations and especially the frequently asked questions (<http://aspe.os.dhhs.gov/adminsimp/>)
- ✓ Develop a list of Business Associates and make sure contracts include required BA language (these all require updating since the HITECH provisions).
- ✓ There are many HIPAA Publications out there. The Legislative Committee recommends *HIPAA Briefing* (HCPRO) and, of course, *Medical Records Briefing*.
- ✓ There are many seminars available for you to attend.
- ✓ NETWORK! Call your MeHIMA Colleagues!