The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

COURSE OVERVIEW

Confidentiality is one of the most basic rights that our clients have. All healthcare workers are legally and morally bound to protect the confidentiality of others.

This course is designed to:

1. Give you an overview of The Health Insurance Portability and Accountability Act of 1996 (HIPAA).
2. Familiarize you with any major changes that have been implemented with the new 2013 Omnibus Rule Changes.
3. Help you recognize the serious consequences if you fail to comply with HIPAA.

HIPAA INTRODUCTION

HIPAA was established in 1996 by the US Congress. The major purpose of HIPAA is to define and limit the circumstances in which an individual's protected health information (PHI) may be used or disclosed; to combat waste, fraud and abuse in health care; to promote medical savings accounts; to improve long-term care services and coverage; and to simplify the health insurance process. The Federal Government, through HIPAA, created national privacy and security standards for the protection of patients and their medical information. HIPAA Consists of Three Parts

- **Privacy:** Protects the privacy of a client's health care data (including genetic information).
- **Security:** Controls the confidentiality of electronically protected health information or ePHI (including how it is stored and accessed).
- **EDI:** Electronic Data Exchange or EDI defines the format of electronic transfers of information between providers and payers to carry out financial or administrative activities related to health care (includes coding, billing and insurance verification).

PROTECTED HEALTH INFORMATION

The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."

"Individually identifiable health information" is information that relates to:

- The individual's past, present or future physical or mental health condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual.

Examples of PHI include:

- Name
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code…….
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death……..
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images…..
- Any other unique identifying number, characteristic…..

THE PRIVACY RULE

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities. PHI may not be used or disclosed unless (a) the Privacy Rule permits or requires it; or (b) the individual (or the individual's representative) authorizes in writing the use or disclosure of the information.

A covered entity is **required to disclose** PHI in two situations (1) when an individual (or their personal representative) requests access to, or an accounting of disclosures of their PHI, and (2) to HSS for compliance purposes or enforcement action.

Consent

The Privacy Rule permits, but does not require, a covered entity to obtain patient consent voluntarily for uses and disclosures of PHI in relation to treatment, payment, and health care operations.

Authorizations

A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for TPO or otherwise permitted by the Privacy. An authorization must be in writing and be written in specific terms. The authorization must contain specific information regarding the information to be disclosed or used, the person(s) disclosing the information, the person(s) receiving the information the expiration and the right to revoke in writing.

Required elements of a written authorization include:

- Specific description of PHI to be used/disclosed
- Who can use/disclose PHI
- To whom the PHI can be used/disclosed
- Purpose of the use/disclosure
- Expiration date or event
- Signature of patient, with date
- Right to revoke in writing; and the exceptions and instructions regarding the procedure, or a reference to the Notice if this information is there
- A statement about the covered entity's ability/inability to condition the authorization on treatment, payment, eligibility, or enrollment
- A statement that once disclosed, the PHI may no longer be protected by the HIPAA Privacy Rule, or an alternative statement if the disclosure is to another covered entity
- If use or disclosure is for marketing purposes, and the covered entity will receive remuneration, a statement must be included to that effect

The Rule permits uses and disclosures without individual authorization including those:

- To the individual
- For treatment, payment, and health care operations (TPO)
- Incidental uses/disclosures
- To business associates with a business associate agreement

- *To the individual:* The Rule permits an individual to:

    - Get a copy of their medical records
    - Ask for changes to their medical records
    - Find out and limit how their PHI may be used
    - Know who has received their PHI
    - Have communications sent to an alternate location or by an alternate means
    - File complaints and participate in investigations

- The Rule allows A Covered Entity to use *or disclose* PHI as long as it relates to TPO

    - *Treatment* – providing care to clients
    - *Payment* – the provision of benefits and premium payments
    - *Operations* – normal business activities such as reporting, quality improvement, training, auditing, customer service and resolution of grievances, data collections and eligibility checks.

- *Incidental uses and disclosures*: Incidental uses and disclosures are

    - "Incident to" another use or disclosure that is permitted or required by the Rule
    - Those that occur even though the minimum necessary and safeguard standards are met

- ***Other uses/disclosures that do not require an authorization include**:*

    - Required by law
    - Public health activities
    - About victims of abuse, neglect, or domestic violence
    - Health oversight activities
    - Judicial and administrative proceedings
    - Law enforcement purposes
    - Cadaveric organ, eye, or tissue donation
    - To avert a threat to health or safety

- ***Permitted uses/disclosures where written authorization is required include:***

    - Marketing
    - Psychotherapy notes (except when the covered entity is using the notes for treatment, to defend itself in legal proceedings brought against it, for compliance investigation or required by law.
    - All uses or disclosures not otherwise permitted (examples: disclosure to life insurance, drug test results to employer, and disclosure of child's physical results to school)

Limiting Uses and Disclosures to the Minimum Necessary

The principle of "minimum necessary" is an important aspect of the Privacy Rule for all employees to be aware of. According to this principle a covered entity must make every effort to use, disclose or request THE MINIMUM amount of PHI needed to accomplish the intended purpose of the use, disclosure or request.

When you are using, disclosing or requesting PHI it is your responsibility to make every effort to limit uses, disclosures and requests for PHI to the minimum necessary to accomplish and the intended purpose of the use disclosure or request. The entire health record should not be used, disclosed or requested unless the entire health record is required for the intended purpose and/or for the treatment of the client. *Always consult with your supervisor or compliance officer if you need clarification on using, disclosing or requesting PHI.*

If anyone asks you to release protected information outside of routine TPO, you are required to get written authorization. A copy of the completed authorization must be given to the client. A client may revoke an authorization at any time. Written authorizations should be in plain language. A description of the disclosed or released information is required.

The minimum necessary requirement is not imposed in any of the following circumstances:

- Disclosure to, or requests by, a health care provider for treatment
- Uses or disclosures made to the individual or the individual's personal representative
- Disclosure to HHS for compliance purposes
- Use or disclosure required by law

Individual Rights

All individuals have the right to:

- Receive a Notice of Privacy Practices for PHI. This notice includes
  - Required header and content, in plain language
  - How their PHI will be used and/or disclosed by a covered entity
  - Their individual rights
  - The covered entity's duties
- Inspect and Copy
- Request an Accounting of Disclosures
- Request an Amendment
- Request a Restriction
- Request Confidential Communication
- File a Complaint

THE SECURITY RULE

The Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

All covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

Confidentiality, according to The Security Rule, means that e-PHI is not available to or disclosed to any unauthorized persons. In addition to supporting the confidentiality requirements of The Privacy Rule, The Security Rule also promotes maintaining the integrity and availability of e-PHI. "Integrity" refers to the fact that e-PHI is not to be altered or destroyed in an unauthorized manner. "Availability" refers to the fat that e-PHI is to be accessible and usable on demand by an authorized person.
The Security Rule is flexible and scalable and allows covered entities to assess their own needs and develop solutions appropriate for their specific environments. A covered entity is required to establish administrative, physical and technical safeguards to protect e-PHI.

- Administrative: A covered entity must (a) identify and analyze potential risks to e-PHI and implement measures to reduce risks, (b) designate a security official who is responsible for developing and implementing its security policies and procedures, (c) implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access), and (c) provide for appropriate authorization and supervision of workforce members who work with e-PHI, and (d) perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

- Physical: A covered entity must limit physical access to its facilities and ensure that only authorized access is allowed. A covered entity must implement policies and procedures for the proper use and access to electronic media and workstations. In addition, the covered entity must have policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media.

- Technical: A covered entity must (a) implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI) (b) implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.(c) implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed, and (d) implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

OMNIBUS RULE – SEPTEMBER 20, 2013

Final modifications to the HIPAA Privacy, Security, and Enforcement Rules require:

- Modifications to individual authorization (allows "opt in" check boxes to be used in Consent and Authorization forms)
- Modifications to the Notice of Privacy Practices and redistribution
- Business associates of covered entities are now responsible for HIPAA Privacy/Security breaches and reporting. (New business associate agreements)
- Individual rights to request e-copies of their health record and to restrict disclosures to a health plan concerning treatment for which one has paid out of pocket.
- New breach reporting requirements
- Privacy rule copies Genetic Information Nondiscrimination Act (GINA) to prohibit health plans from using or disclosing genetic information for underwriting purposes.
- Individuals deceased longer than 50 years are no longer covered

THE HITECH ACT

HITECH is designed to encourage healthcare providers to adopt health information technology in a standardized manner and to protect private health information.

- The ***Health Information Technology for Economic and Clinical Health Act*** (HITECH) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g. creation of a national health care infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

- Because this legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act also widens the scope of privacy and security protections available under HIPAA; it increases the potential legal liability for noncompliance; and it provides for more enforcement.

The HITECH Act - stipulates that, beginning in 2011, healthcare providers will be offered financial incentives for demonstrating meaningful use of electronic health records (EHR). Incentives will be offered until 2015, after which time penalties may be levied for failing to demonstrate such use.

Modifications mandated by the Health Information Technology for Economic and Clinical Health or (HITECH) Act.

- Expanded an individual's right to receive electronic copies of health information at the patient's request.
- Restricted disclosures to health plans concerning treatment for which the individual has paid the out-of-pocket amount in full.
- Required modifications to and redistribution of a covered entity's notice of privacy practice.
- Modified the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools.
- Enable access to decedent information by family members or others (PHI protections cease 50 years from date of death)
- There are new use and disclosure regulations on using a patient's PHI for sales and marketing as well as fundraising.

Business Associates and Subcontractors

Before the HITECH Act, the Security and Privacy Rules did not apply directly to business associates of covered entities. Business Associates and their subcontractors are now directly liable for the HIPAA Privacy and Security Requirements.

Enforcement of non-compliance

There are increased penalties for those entities that do not comply with the new Breach of Notification regulations.

THE OFFICE OF CIVIL RIGHTS (OCR) within the Department of Health and Human Services (HHS) enforces the civil penalties. THE DEPARTMENT OF JUSTICE is responsible for enforcing the criminal penalties.

- When you break confidentiality, everybody loses and nobody wins! You could be subject to civil monetary fines and criminal penalties.

- Unknown Violation - Individual did not know about the violation, and could not have known about it even with the exercise of reasonable prudence or care.
- Reasonable Cause - An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.
- Willful Neglect - The conscious, intentional failure or reckless indifference to the obligation to comply with the regulations.

HIPAA Violation Penalties

Violation Type	Minimum Penalty	Maximum Penalty
Individual didn't know (and by exercising reasonable diligence would not have known) that he or she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation is due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation is due to willful neglect, but individual corrected violation within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
Violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

WebPT

Breach Notification for Unsecured Protected Health Information under the HITECH Act -

The OCR (Office of Civil Rights), require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach. The Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of Health and Human Services (HHS) of breaches of unsecured protected health information reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

PRIVACY POLICES AND PROCEDURES

Covered entities and business associates must institute and maintain privacy policies and procedures to protect PHI. Covered entities must:

- Put in place administrative, technical, and physical safeguards to protect against intentional or unintentional use or disclosure of PHI that violates the Rule
- Reasonably safeguard PHI to limit incidental uses or disclosures
- Have an established complaint process
- Have an established process for documentation of the complaints and their resolution
- Have an employee designated to receive and document the complaints
- Provide training to their workforce and document that the training occurred
- Have and apply appropriate sanctions when a member of the workforce does not comply with privacy policies and procedures or with the Privacy Rule
- Mitigate to the extent practicable harmful effects caused by their improper use or disclosure of a patient's PHI that is known to the covered entity

Covered entities may not retaliate in any form against anyone who:

- Files a complaint of a privacy violation
- Exercises a right under the Rule
- Participates in a process established by the Rule

Covered entities must:

- Maintain policies and procedures in paper or electronic form
- If a communication is required to be in writing, maintain such writing, or an electronic copy, as documentation
- If an action, activity, or designation is required to be documented, maintain a paper or electronic record of such action, activity, or designation

A covered entity must retain required documents for six years from the date of their creation or the date when they were last in effect, whichever is later.

MANAGING COMPUTERIZED HEALTH CARE INFORMATION

One key element of protecting our client's PHI lies in maintaining the security of our internal systems which house and transmit ePHI (electronically protected health information).

- Only access this Protected Health Information on a **"need to know"** basis to do your job.
- Never access any Protected Health Information even a close relative's for personal interest without prior written consent.
- Don't ask a physician or co-worker to access Protected Health Information for you.
- To safeguard our client's ePHI when using a computer, always "log off" or use the option to lock your computer screen that prevents other users from gaining access to your applications.

Federal and State requirements mandate that we take certain steps when sending sensitive information. To safely send client information you have four options:

1. Calling the person on the phone.
2. Hand delivering information to the person, in an envelope marked "confidential".
3. Emailing to non-facility employees, by password protecting a Microsoft Word document, or
4. Emailing facility employees, by encrypting the email.

Helpful Note:

- Do not follow unsolicited links and do not open or respond to unsolicited email messages.
- Use caution when visiting websites
- Use caution when entering personal information online

Think before you click! Delete all suspicious emails.

How to Manage Texting

Text messaging has become a major part of how individuals communicate today and is considered a quick and easy way to send information. The unfortunate aspect about text messaging is that it not secure and can violate HIPAA safety and privacy regulations. HIPAA does not specifically prohibit text messaging PHI within an organization or to another healthcare provider. However, healthcare providers do need to consider the safeguards of their organization when it comes to transmitting ePHI. Text messages are generally not secure because the information can be exposed to third parties due to such things as lost or stolen mobile devices as well as improper disposal of a device. Considering the security risks involved with text messaging PHI, organizations should explore having encrypted text messaging to protect against privacy breaches or prohibit text messaging ePHI completely. It is recommended that your organization conduct a risk analysis to identify possible exposures related to texting ePHI, and then create policies and procedures in relation to texting ePHI and conduct staff training to ensure implantation of these policies and procedures. Each healthcare organization must decide what is the best solution and controls in regards to ePHI.

HELPFUL TIPS TO SECURE PHI

- Never discuss PHI where others can hear you such as hallways, lunch rooms, or elevators.
- When you have an enquiry by phone verify that there is an authorization on the clients file
- Be on our guard:
    - Your responsibility doesn't end on your shift.
    - Don't divulge patient/customer or employee information at your church, school, college, home, the shopping mall, or in other social settings.
    - If you're asked just say - *"I'm sorry, that information is confidential."*
    - Don't copy or reproduce any confidential information unless you need it to do your job.
    - Don't let anyone else copy confidential information either.

- Lock PHI in your drawer when you leave your desk or cubicle
- Lock your door when you leave your office
- Turn over or cover PHI when a coworker approaches you
- Don't leave PHI in fax machines or copiers
- Shred all paper when disposing of PHI

- Keep Protected Health Information in a safe location
    - Store away from public view.
    - Don't leave Protected Health Information on countertops in view of customers.
    - Be aware of computer screen locations – the information should not be viewable to others.
    - Log off your computer when you leave your station.
- You are obligated to protect patient/customer privacy and any other confidential information when you see or hear a breach occurring by reporting this to someone who can advocate for the patient/customer. This includes unauthorized use, duplication, disclosure, or dissemination of PHI.

Another key element to the protection of our client's PHI is to keep the physical building or facility where you work secure. Here are a few tips that will help protect our facilities:

- Wear your ID badge at all times
- When entering the building, be sure others who are entering with you are authorized employees with ID badges
- Keep hallway doors that lead to client care areas closed and
- Request vendors and contracted individuals to sign-in and obtain vendor ID badges when visiting a restricted area.

SECURITY MANAGEMENT

Various security measures exist in order to increase overall safety and security within the buildings as well as the surrounding outdoor environment. Some of these include: exterior lighting, identification of 'high-risk' areas requiring additional security (medical record areas, medication rooms, business office), security rounds, visitor sign-in and identification, surveillance cameras, employee identification (picture ID badges), management of access to keys and/or door code locks, etc. Some helpful tips:

- Do not prop open doors that should be locked.
- Correct any physical security problems you can at the time you discover them (for example, closing doors that are propped open) and then report these physical breaches to your Security officer, and
- To reduce the risk of loss and/or prevent identity theft, you should secure valuables, such as purses and briefcases, in locked drawers or cabinets when you are not in your office.

Resources:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
http://www.hhshipaasagtraining.com/module2.php
www.lexology.com/library/detail.aspx?g=33c5a01c-150c-4ad8-9b7e...
*www.slideshare.net/.../**hipaa**-compliance-**training**-internal-presentation*
www.youtube.com/watch?v=dv0FYBhpdX0