PRESENTER'S GUIDE

"HIPAA RULES AND COMPLIANCE"

Training for
HIPAA REGULATIONS

Quality Safety and Health Products, for Today... and Tomorrow

OUTLINE OF MAJOR PROGRAM POINTS

OUTLINE OF MAJOR PROGRAM POINTS

The following outline summarizes the major points of information presented in the program. The outline can be used to review the program before conducting a classroom session, as well as in preparing to lead a class discussion about the program.

- **With the advent of electronic processing, communication and storage of medical data it's much easier to share patient information among the healthcare professionals who treat them.**
  - But how can people's private health information be kept confidential and secure at the same time?

- **In the U.S. this concern has been addressed by a group of federal laws known as "HIPAA", the Health Insurance Portability and Accountability Act of 1996.**
  - And everyone who works in healthcare-related fields should have a practical understanding of the HIPAA regulations and how HIPAA affects them.

- **HIPAA established three rules for safeguarding the privacy and security of patients' medical information.**

- **The HIPAA "Privacy Rule" gives patients specific rights regarding their health information.**
  - It also regulates who else can have access to this information.

- **The HIPAA "Security Rule" established standards for safeguarding this information when it is transmitted or stored in electronic form.**

- **The HIPAA "Enforcement Rule" set up procedures for investigating potential violations of HIPAA regulations, and established penalties to help enforce compliance.**

- **HIPAA was followed by two other acts that related to the privacy and security of health information:**
  - The Genetic Information Nondiscrimination Act (GINA) focused on protecting people's genetic information.
  - The Health Information Technology for Economic and Clinical Health Act (HITECH) extended the reach of HIPAA requirements and updated the penalties for violating them.

- **In 2013 a final "omnibus rule" officially integrated GINA and HITECH with HIPAA, and created the final health information regulations that are in force today.**

- **HIPAA defines "protected health information" (PHI) as any data about a person's health, their healthcare, or payment for their healthcare that:**
  - Is created or collected by a healthcare provider, health plan or "healthcare clearing house", their business associates and subcontractors.
  - Is transmitted or maintained in electronic form or any other medium.
  - And identifies the person, or could be used to identify the person, that it relates to.

- **PHI can include things such as:**
  - Physicians' notes.
  - Healthcare billing information.
  - Blood test results.
  - Doctors' telephone records.
  - MRI scans.
  - Appointment scheduling notes.

- **PHI can be in any form… oral, recorded, written down on paper, stored on a computer or on the internet.**

- **PHI that is stored or transmitted in electronic form is sometimes referred to as "EPHI".**
  - Just keep in mind that whatever term is used, the "P" stands for "protected"!

- **HIPAA groups the organizations and people that are responsible for protecting health information into three categories:**
  - "Covered entities".
  - "Business associates".
  - "Subcontractors".

- **A covered entity is a healthcare provider that transmits health information in connection with certain types of administrative and financial transactions electronically.**
  - Doctors, clinics, psychologists, dentists, nursing homes and pharmacies can all be covered entities.

- **A covered entity can also be a health plan, such as a health insurance company, HMO or government program that pays for healthcare (such as Medicare and Medicaid) as well as military and veterans' programs.**

- **A healthcare clearinghouse can also be a covered entity.**
  - This includes entities that process nonstandard health information received from another entity into a standard form.

- **A business associate is a person or business that has access to PHI as a result of working with or providing services to a covered entity.**

- **Business associates can include:**
  - A physician's medical transcriptionist.
  - A consultant who performs utilization reviews for a hospital.
  - Or an accounting firm that audits a company's health plan.

- **A subcontractor is a person or business who has access to PHI while they are working with or providing services to a business associate. For example:**
  - When the CPA firm that is a business associate of a covered entity buys data storage services from a third party, that third party is a subcontractor.
  - If a medical transcriptionist has a local computer services company inspect the contents of her hard drive, that company is a subcontractor.

- **Knowing what types of companies fit into these various categories is important, because chances are you or your employer fall into one of them, so you will need to comply with HIPAA regulations.**

- **Under HIPAA, patients have specific rights regarding their protected health information.**
  - First, covered entities are required to provide patients with a "Notice of Privacy Practices" (NPP).
  - This document outlines the entity's policies regarding the use and disclosure of a patient's PHI.

- **The NPP must be given to patients:**
  - The first day they are provided with a service.
  - Or as soon as possible following an emergency.

- **Under HIPAA, patients have the right to inspect, correct and request that changes be made to their PHI.**

- **Patients may also request that their PHI be communicated to them by other than the normal means and at alternate locations to protect confidentiality. For example, a patient could:**
  - Ask a fertility clinic not to call them at work, but to send them an email at home.
  - Ask a specialist not to send an appointment reminder by postcard, but enclosed in an envelope.

- **In some cases, a patient's request for access to their own PHI may be denied by the covered entity. This can occur when the information:**
  - Is in the form of psychotherapy notes.
  - Has been compiled for use in a civil, criminal or administrative proceeding.
  - Is held by a correctional institution and access could jeopardize the health and safety of inmates, employees or others.
  - And in certain other limited circumstances.

- **In these cases, HIPAA requires the covered entity to:**
  - Provide the patient with a written explanation of why their request is being denied.
  - Inform them of how they can complain to the covered entity's Privacy Officer or to the Department of Health and Human Services.

- **A patient also has a right to:**
  - Designate a third party to receive their EPHI.
  - Request an accounting of PHI disclosures made by a covered entity for up to 6 years prior to the request.

- **If for any reason the patient is incapable of exercising their rights, for example if they are small children or mentally handicapped, a representative can be chosen to exercise these rights on their behalf.**

- **HIPAA uses the terms "use" and "disclose" to describe the two ways that protected health information can be "handled".**
  - "Use" occurs when a covered entity examines, applies or analyzes the information.
  - "Disclosure" takes place when the information is released, transferred to, or accessed by a business associate or subcontractor.

- **The "use" and "disclosure" of PHI is <u>permitted</u>:**
  - For disclosure to the patient.
  - With patient authorization or agreement.
  - For purposes of treatment, payment and day-to-day healthcare.
  - For incidental uses, such as doctors talking to patients in a semi-private room where other patients or personnel may be present.

- **The "use" or "disclosure" of PHI is <u>required</u>:**
  - When it's requested or authorized by the patient.
  - When it's requested by the Department of Health and Human Services.

- **And since healthcare providers need access to PHI to provide quality care to a patient, patients cannot restrict disclosure of their PHI for purposes of medical treatment.**
    - But patients can restrict disclosure to a health plan or the plan's business associates, if the person has already paid for the treatment themselves.

- **HIPAA restricts how much patient PHI can be used or disclosed by enforcing the "minimum necessary" standard.**
    - This standard requires that any PHI that is not strictly necessary to "get the job done" will not be used by a covered entity or disclosed to a business associate or subcontractor.

- **There are several situations where this minimum PHI may be used or disclosed without patient authorization. The most common of these is:**
    - In day-to-day healthcare operations, such as patient treatment.
    - When a health plan is making payment for services that a patient has received.

- **The minimum necessary PHI may also be shared without patient permission or authorization when it's:**
    - In the interest of public health.
    - To control or prevent disease.
    - For health oversight activities.
    - To monitor FDA-regulated products.
    - To comply with a HIPAA investigation.
    - And for certain law enforcement purposes.

- **At a minimum, a patient's signed authorization is <u>not</u> required, but their verbal permission <u>is</u> required, to use or disclose minimum PHI for the purpose of:**
    - Maintaining a covered entity's patient directory.
    - Informing family or other people who are involved in a patient's care.

- **However, a signed patient authorization is required for the use or disclosure of psychotherapy notes, unless that use or disclosure is:**
  - Required by the healthcare provider.
  - Permitted or required by law.

- **Another thing that the HIPAA final omnibus rule did was to set stricter limits for how PHI may be used or disclosed for marketing purposes.**
  - But it is less stringent about using PHI for fundraising.

- **The Privacy Rule defines "marketing" as:**
  - "A communication about a product or service that encourages recipients of the communication to purchase or use that product or service".
  - Initially this applied only to covered entities.

- **But "marketing" is also defined as:**
  - "An arrangement in which a covered entity discloses (patients') PHI to another entity that will use it for a communication that encourages the recipients to purchase or use a product or service."

- **For an individual's PHI to be used or disclosed for the purpose of these two types of "marketing", the covered entity must first obtain the patient's signed authorization.**
- **However, a marketing communication does not require a patient's authorization when it is made in the form of:**
  - A face-to-face communication.
  - Or a gift of nominal value that is given to the patient by the covered entity.

- **There are three other types of communication that are not considered to be "marketing" where PHI can be used or disclosed without the patient's authorization.**
    - If they describe health-related products or services that are provided by or included in a plan of benefits from the covered entity making the communication.
    - If they are made for the treatment of the patient, such as a pharmacy sending prescription refill reminders, or a physician providing free samples of a prescription drug to the patient.
    - Or if they are made to coordinate care, or to recommend alternative treatments, providers or service locations to the patient.

- **As for "fundraising", HIPAA does not require patient authorization or permission for their PHI to be used for fundraising purposes.**
    - The only requirement is that all fundraising-type communications must include a simple method (such as an email address or toll-free telephone number) that can be used to opt out of receiving any additional fundraising communications.

- **HIPAA's Security Rule deals with protecting the confidentiality and integrity of PHI when it is in electronic form (known as EPHI).**
    - The rule is intended to prevent EPHI from being accessed by unauthorized persons or otherwise tampered with.
    - To accomplish this, the Security Rule requires the use of administrative, technical and physical safeguards on the part of entities that have custody of this information.

- **"Administrative safeguards" are policies and procedures that limit access to EPHI. They include:**
  - Systems that detect, correct and prevent security breaches.
  - "Incident policies" that describe how to respond to a breach, if one occurs.
  - Ongoing audits and evaluations that will ensure compliance with HIPAA regulations.
  - Contingency plans for protecting EPHI during emergencies and natural disasters.

- **"Technical safeguards" protect the data storage and transmission systems that handle EPHI from <u>inside</u> computer systems and networks, such as:**
  - Monitoring and anti-virus software.
  - Encryption and digital signatures.
  - "Alarms" regarding suspicious activity.

- **Physical safeguards work from the <u>outside</u>. They restrict access to computers and other high-tech equipment that stores and transmits EPHI, as well as the rooms and buildings that house the equipment. They include:**
  - Parking restrictions, security guards and ID badges.
  - Unique personal IDs as well as regularly updated passwords (remember, never share your password with anyone else!).
  - And controls that keep EPHI secure when computer hardware or software is being moved or disposed of.

- **The HIPAA-mandated policies, procedures and safeguards we have discussed are all designed to ensure the privacy and security of protected health information.**
  - But when impermissible access, acquisition, use or disclosure of PHI occurs in spite of these measures, that violation is called a "breach".

- **If a breach is suspected, HIPAA presumes that one has actually occurred unless the covered entity which is involved can demonstrate that there is a low probability that PHI was actually compromised.**

- **If it is determined that a breach has in fact occurred, the covered entity must inform patients of that fact.**
  - This "breach notification" must be accomplished within 60 days of the date of the breach.

- **If the breach affects the PHI of 500 people or more, the news media must be informed of the breach as well.**

- **HIPAA also requires that the Department of Health and Human Services be notified of <u>all</u> breaches.**

- **The penalties for having a data breach occur can be significant, up to $1.5 million per violation.**

- **Anyone who creates, receives, maintains or transmits PHI on behalf of a covered entity can be subject to these penalties, including individuals and business entities.**
  - So there are strong incentives for you and your employer to follow HIPAA guidelines carefully.

*** * * SUMMARY * * ***

- **HIPAA is a set of federal laws that protects the privacy and security of patients' health information.**

- **Protected health information, (PHI), can be any data about a person's health, their healthcare or payment for their healthcare that identifies the person, or that could be used to identify the person that it relates to.**

- **PHI can be in any form… oral, written or electronic.**

- **HIPAA groups businesses and individuals that have access to PHI into three categories:**
  - Covered entities.
  - Business associates.
  - Subcontractors.

- **All of these groups are bound by the HIPAA privacy, security and enforcement rules.**

- **Penalties for HIPAA violations can be significant, in excess of a million dollars.**

- **The use of digital information technology has made it possible to make better healthcare available to more people, but that benefit should not have to come at the cost of anyone's privacy.**

- **When you understand the objectives of the HIPAA regulations and the procedures that make them work, you can help to guarantee the confidentiality of every patient's private health information, every day!**