Training Objectives

• Provide a **basic overview** of how HIPAA serves to protect and secure patient privacy.

• Review **key updates** to HIPAA pursuant to the final Omnibus Rule (“Final Rule”) published by the U.S. Department of Health and Human Services (“HHS”) on January 25, 2013.

• Review **frequently asked questions** to demonstrate how HIPAA applies to common scenarios.

• Provide **practical tips** to protect and secure patient privacy.
HIPAA BASICS
What Is HIPAA?

Health Insurance Portability and Accountability Act of 1996

HIPAA is a federal law that requires a covered entity (“CE”), including a physician office, to:

• **protect the privacy** of patient health information;

• **ensure patient rights** relating to access, use and disclosure of health information; and

• **secure patient information** both physically and electronically.
What Is The Privacy Rule?

The HIPAA Privacy Rule protects the privacy of all “individually identifiable health information” held or transmitted by a CE or its business associates, in any form or media (including electronic, paper or oral).
What Is Individually Identifiable Health Information?

Individually identifiable health information or protected health information (“PHI”) is information, including demographic data, that relates to:

• the individual’s past, present, or future physical or mental health or 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;

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
What Are The 18 Identifiers Defined By HIPAA?

- Names
- Geographic subdivisions smaller than a State (i.e., addresses)
- All elements of dates except the year (i.e., birth date, admission date, service date, etc.)
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers (i.e., license plate)
- Device identifiers and serial numbers
- Internet Protocol (IP) addresses
- Web URLs
- Biometric identifiers (i.e., finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code or characteristic
What PHI Can Be Used or Disclosed Without Authorization?

HIPAA permits CEs to use or disclose PHI without patient authorization

- for treatment, payment and health care operations ("TPO"); or
- incident to an otherwise permitted use and disclosure.
What Use Or Disclosure Requires Patient Authorization?

Patient authorization is required:

• for use and disclosure of PHI not otherwise allowed by the Privacy Rule;

• for use and disclosure of psychotherapy notes, HIV/AIDS, substance abuse, genetic information;

• for most marketing communications;

• for the sale of PHI; and

• for research use or disclosure of PHI unless a regulatory permission or exemption applies.
What Is The Minimum Necessary Standard?

• CEs must make reasonable efforts to use, disclose, and request the *minimum amount* of PHI needed.

• This standard *does not* apply to disclosures:
  – to a health care provider for patient care or treatment purposes (*except* psychotherapy notes, HIV test results, substance abuse, and genetic information);
  – to the individual who is the subject of PHI; or
  – made pursuant to patient authorization.
What Is The Security Rule?

• The Security Rule protects all PHI a CE creates, receives, maintains or transmits in **electronic form** (“ePHI”).

• The Security Rule requires CEs to:
  – ensure confidentiality, integrity, and availability of ePHI;
  – identify and protect against threats to the security or integrity ePHI; and
  – protect against impermissible uses or disclosures.
HIPAA UPDATES
What Is The Final Rule?

Notice of Privacy Practices

The Final Rule required CEs to revise NPPs to include:

• Statement that the following to be made only with authorization:
  – uses and disclosures for marketing purposes;
  – uses and disclosures that constitute the sale of PHI;
  – most uses and disclosures of psychotherapy notes (if the CE maintains psychotherapy notes); and
  – other uses and disclosures not described in the NPP.

• Statement regarding individual’s right to notice of a breach.

• Notice of the right to opt out of fundraising communications (if conducted by CE).

• Statement regarding individual’s right to restrict disclosures of PHI to health plans if an individual has paid for services out of pocket in full.
Notice of Privacy Practices

NPP must be revised by September 23, 2013 and

• provided to all new patients;
• made available to existing patients upon request;
• posted to CE’s website; and
• posted in a prominent location on the premises.
Individual’s Right To Request Restrictions

• Under the Final Rule, CEs must permit individuals to request restrictions on the uses or disclosures of their PHI for TPO, and disclosures to family members and certain other permitted purposes. While CEs are not required to agree to such requests, if a CE does agree to the restriction, then the CE must abide by that restriction.

• However, CEs must comply with an individual’s request to restrict disclosure to a health plan if: (1) the disclosure is for payment or health care operations and not otherwise required by law, and (2) the PHI relates solely to a health care item or service for which the CE has been paid in full by someone other than the health plan.
Individual’s Right To Access

- The Final Rule requires CEs to provide an individual with a copy of e-PHI in the electronic form and format requested by the individual if such format is readily producible by the CE.

- If the requested format is not readily producible, the CE must offer to produce the electronic PHI in at least one readable electronic format.

- The Final Rule decreases the total time CEs have to respond to requests for access from 90 to **60 days**. CEs now have 30 days to respond, unless they provide the individual written notice of a one-time extension of up to 30 days, including the reason for the delay and the expected date of completion.
Business Associate Agreements

• The Privacy Rule requires CEs to obtain satisfactory assurances in writing from a business associate ("BA") that the BA will appropriately safeguard PHI.

• The Final Rule enlarges the definition of a BA to include:
  – a person or entity who creates, receives, maintains or transmits PHI on behalf of a CE;
  – a health information organization, e-prescribing gateway, or other entity that provides data transmission services to a CE and requires access on a routine basis to PHI;
  – an entity that offers a personal health record on behalf of a CE; and
  – subcontractors with access to PHI used by BAs.

• When a CE discloses information to a healthcare provider concerning treatment, the healthcare provider is not a BA.

• The Final Rule modifies the required provisions for BA agreements.
Marketing

• The Final Rule expands the definition of “marketing,” which requires patient authorization, to include communications about health-related products or services (whether as part of treatment or health care operations) if the CE receives “financial remuneration” in exchange for making the communication from or on behalf of the third party whose product or service is being described.

• Financial remuneration includes payments in exchange for making marketing communications, but not in-kind benefits.
Marketing

Marketing does not include:

• Refill reminders or communications about a drug/biologic currently prescribed to an individual, but only if any financial remuneration is reasonably related to the CE’s cost of making the communication.

• Face-to-face communications even if remuneration is received from a third party or a promotional gift of nominal value is provided by the CE.

• Communications promoting health in general that do not promote a product or service from a particular provider.

• Communications about government programs.
Sale Of PHI

• The Final Rule defines the term “sale of PHI” for the first time as “a disclosure of protected health information by a CE or BA . . . where the CE or BA directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.”

• The Final Rule expressly prohibits CEs or BAs from receiving direct or indirect remuneration in exchange for the disclosure of PHI, unless the CE first obtains patient authorization or an exception applies.
Definition Of Breach

• A breach is the acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA, which compromises the security or privacy of PHI.

• The Final Rule *lowers the bar* for determining a breach, and states that an impermissible use or disclosure of PHI is “*presumed* to be a breach unless the CE demonstrates that there is a *low probability* that the PHI has been compromised.”

• CE must conduct a risk analysis to determine whether a breach has occurred.
Breach Risk Analysis

CEs must consider four “objective factors” in performing a risk analysis:

• the nature and extent of PHI involved, including the type of identifiers and the likelihood of re-identification;
• the unauthorized person who used the PHI or to whom the disclosure was made;
• whether the PHI was actually acquired or viewed; and
• the extent to which the risk to the PHI has been mitigated.
Breach Exceptions

Breach exceptions include:

• unintentional acquisition, access, or use of PHI by an employee or agent of a CE or BA if such acquisition, access, or use was made in good faith and within the scope of the employment or professional relationship of such person, and such information is not further acquired, accessed, used, or disclosed by any other person;

• inadvertent disclosure of PHI from one person authorized to access PHI at a CE or BA to another person similarly situated at the same CE or BA, and the information is not further acquired, accessed, used or disclosed without authorization; and

• when an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.
Breach Notifications

• CEs must promptly notify individuals when a reportable breach is discovered. A breach is “discovered” the first day the breach is known or should reasonably have been known to the CE.

• Notification must occur within 60 days from discovery of the breach, unless law enforcement requests a delay.

• Notices must include a brief description of what happened and the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
Breach Notifications

• A covered entity must notify major local media outlets of a breach affecting more than 500 individuals at the same time notice is given to the individuals and HHS.

• The Final Rule requires CEs to notify HHS of all breaches affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were “discovered.”
FREQUENTLY ASKED HIPAA QUESTIONS
Q1. Can health care providers and staff share PHI for treatment, payment or health care operations without patient authorization?
A1. YES

The Privacy Rule allows doctors, nurses, hospitals, lab technicians, other health care providers and staff to use or disclose PHI (such as X-rays, lab and pathology reports, diagnoses, and other medical information) for TPO without patient authorization. This includes sharing the information to consult with other providers, to treat a different patient, or to refer the patient.
Q2. Can patient information be maintained outside of exam rooms even though the potential exists for patient information to be incidentally disclosed to others?
A2. YES

The Privacy Rule allows CEs to engage in common and important health care practices as long as they implement reasonable safeguards to protect patient privacy and disclose or use the minimum amount of PHI necessary.

For example, WHERE REASONABLE PRECAUTIONS have been taken, the Privacy Rule does not prohibit CEs from maintaining sign in sheets (without medical information), patient charts outside of exam rooms, displaying patient names on the outside of patient charts, or calling out patient names in waiting rooms.

SAFEGUARDS: reasonably limit access to these areas, try to place patient charts with identifying information covered, limit the amount of information to the minimum necessary (e.g., do not call out the patient’s full name unless necessary, test results or reason for the visit).
Q3. Can health care providers and staff engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?
A3. YES

• The Privacy Rule does not prohibit providers from talking to each other and to patients. The Privacy Rule recognizes that oral communications must occur freely and quickly in treatment settings, and may be overhead.

• For example, the following practices are permissible where REASONABLE PRECAUTIONS to minimize incidental disclosures are taken:
  – A provider may instruct an administrative staff member to bill a patient for a particular procedure, and even if there is a possibility to be overheard by one or more persons in the waiting room.
  – Nurses or other health care professionals may discuss a patient’s condition over the phone with the patient, a provider, or a family member.

• SAFEGUARDS: speak quietly, inform the patient that you are going to discuss PHI and give them a chance to object, be aware of your surroundings and try to take reasonable steps to avoid being overheard.
Q4. Can health care providers and staff leave messages for patients at their homes, either on an answering machine or with family members?
The Privacy Rule allows health care providers to leave messages for patients on their answering machines when REASONABLE SAFEGUARDS are used to protect the patient’s privacy and limit the amount of information disclosed. For example, you may leave your name and number and ask the patient to call you back.

The Privacy Rule allows health care providers to leave a message with a family member or other person who answers the phone when a patient is not home. However, you must take REASONABLE SAFEGUARDS to limit the amount of information disclosed and use your professional judgment to assure that such disclosures are in the best interest of the individual.

BE AWARE that where a patient has requested that a CE communicate in a confidential manner, such as by alternative means or at an alternative location, CE MUST honor that request.
Q5. Can a health care provider use facsimile to send PHI to other health care providers or to an insurer?
A5. YES

• The Privacy Rule allows health care providers to fax PHI to other health care providers and insurers as long as REASONABLE SAFEGUARDS are employed.

• SAFEGUARDS: double check the fax address for accuracy before sending, use a cover sheet that does not include PHI, confirm that the fax was received, and limit the amount of information disclosed through fax to the minimum necessary.
Q6. Can health care providers and staff use e-mail to discuss PHI with their other providers or patients?
The Privacy Rule allows health care providers and staff to communicate electronically, such as through e-mail, with other providers and patients, provided they apply REASONABLE SAFEGUARDS when doing so.

SAFEGUARDS: double check the e-mail address for accuracy before sending, encrypt all e-mail sent externally, limit the amount of information disclosed through e-mail.

Prior to sending any unsecured (i.e., unencrypted) e-mail containing PHI to a patient, you should alert the patient to the risks of using unencrypted e-mail and let the patient decide whether to continue with this form of communication.
Q7. Can health care providers and staff discuss PHI with a patient’s family, friends or others involved in care or payment?
A7. YES

• HIPAA allows health care providers to share relevant PHI with family, friends or others involved in a patient’s health care or payment if: (1) the individual gives the provider permission, (2) the individual is present and does not object to sharing the information or (3) if the individual is not present, the provider determines based on professional judgment that it's in the patient’s best interest.

• For example: a doctor may discuss treatment in front of a friend if the patient asked the person to come into the exam room; and staff may discuss a bill with a family member if the individual does not object.

• If the provider discloses PHI based on oral permission from the individual, the provider should try to document it in the record.
TIPS TO PROTECT AND SECURE PATIENT PRIVACY
Privacy Tips

• Make sure you have appropriate privacy policies in place, and when applicable, comply with VHS Privacy Policies (including 13.10 – 13.17, 13.19-13.20);
• Lock file cabinets, office doors;
• Protect patient records from prying eyes;
• Speak softly when discussing health care matters in semi-private rooms;
• Avoid discussions about patients in public if possible (i.e., cafeteria lines, lobbies or elevators);
• Double check fax numbers or addresses before transmitting information;
• Do not leave PHI on copy machines, fax machines or printers;
• If allowed, be careful when taking PHI off-site (never leave PHI unattended in your bag or car); and
• Properly dispose of PHI (i.e., shred or place in secured bins).
Security Tips

• Make sure you have appropriate security policies, and when applicable, comply with VHS Security Policies (including 35.01-35.13);
• Use safe computer skills (i.e., log out, ensure information on your computer screen is not visible to passersby, etc.);
• Properly manage your passwords (i.e., update passwords, password protect your work and personal devices, do not share passwords);
• Double check e-mail addresses before sending ePHI;
• Encrypt e-mails before sending ePHI;
• Do not share PHI on social media (i.e., Facebook, Twitter, etc.);
• Ensure all devices used to access and store ePHI are encrypted (including your personal computer, laptop, smart phone, etc.); and
• Make sure your computer has anti-virus and security updates.
Online Resources

• U.S. Department of Health & Human Services:  
  http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

• Office for Civil Rights:  http://www.hhs.gov/ocr/office/index.html


• Centers for Medicare & Medicaid Services:  