HIPAA Understanding & Complying

Cortland G. Kalanavich, RHIA
HIPAA Privacy Officer
Diamond Pharmacy Services

What is HIPAA?

- **Health Insurance Portability and Accountability Act**
  - HIPAA Privacy:
    - Developed to provide a means for protecting the privacy of individually identifiable Health Information (IIHI).
  - HIPAA Security:
    - Developed to protect patient’s Protected Health Information (PHI), focusing on computer operating systems and technical components of protecting information.

Who Must Comply?

- Any organization handling health care data who submits billing claims in electronic form is considered a Covered Entity (CE) under HIPAA Laws:
  - Healthcare Providers:
    - Doctors
    - Clinics
    - Psychologists
    - Dentists
    - Chiropractors
    - Nursing Homes
    - Pharmacies
**Who Must Comply?**

- **Health Plans:**
  - Health insurance companies
  - HMO’s
  - Company health plans
  - Government programs that pay for health care, such as Medicare, Medicaid and military and veterans health care programs

- **Health Care Clearinghouses:**
  - Public or private entities, including billing services & repricing companies, that process non-standard health information they receive from another entity into standard information (i.e., standard electronic format or data content), or vice versa

---

**Protected Health Information (PHI)**

- **Individually Identifiable Health Information (IIHI) in any form:**
  - Electronic
  - Written
  - Oral

- **IIHI includes demographic data that relates to:**
  - The patient’s past, present or future physical or mental health or condition,
  - The provision of health care to the patient, or
  - The past, present or future payment for the provision of health care to the patient

---

**Protected Health Information (PHI)**

- **Demographic data:**
  - Name
  - Address
  - Telephone Number
  - Date of Birth
  - Social Security Number
  - Medical Records Number
  - Account Numbers
  - Email Addresses

** Anything that identifies the patient as a person **
**Protected Health Information (PHI)**

- **Limiting Uses and Disclosures**
  - **Minimum Necessary:**
    - Use, disclose, request and release only the minimum amount of information necessary to accomplish the intended use.
  - **Access and Uses:**
    - For internal uses, restrict access and uses of PHI based on specific staff roles.

- **Treatment, Payment & Health Care Operations (TPO)**
  - Covered Entities can use and disclose PHI for its own TPO and disclose information with other covered entities for purposes of TPO.
  - **Definitions:**
    - **Treatment** – the provision, coordination or management of health care and related services for an individual by one or more health care providers
    - **Payment** – encompasses activities of a health plan to obtain payment or reimbursement for health care delivered to an individual
    - **Health Care Operations** – include any of the following: (a) quality assessment & improvement activities, (b) competency & assurance activities, (c) conducting or arranging for medical review, audits or development, management & administration and (f) business management & general administrative activities of the entity

- **Tips to protect PHI:**
  - Passwords
  - Audit Logs
  - Lock computer screens when not in use
  - Turn over documents containing PHI when work areas are unattended
  - Shred bins
  - Physical layout
  - Staff training
  - Confidentiality & Non-Disclosure Agreements
## Protected Health Information (PHI)

- **Tips to protect PHI (continued):**
  - Fax cover sheets
  - Email encryption
  - Policies & Procedures
  - Business Associate Agreements
  - Notice of Privacy Practices
  - Acknowledgement and Consent forms

## Updated Regulations

- The expanded Omnibus Rule outlined in the Health Information Technology for Economic and Clinical Health (HITECH) Act mandated changes to HIPAA regulations.
- September 23, 2013 compliance deadline (with 1 year to update existing Business Associate Agreements).

## Updated Regulations

- **Enhanced security & privacy of PHI**
- **Expanded responsibilities:**
  - Greater restrictions on uses and disclosures of PHI
  - Breach assessment and notification
  - Updated documents and policies:
    - Notice of Privacy Practices
    - Business Associate Agreements
    - Privacy policies
    - Breach response plans
- **Greater Enforcement:**
  - “HIPAA Police”
  - Increased fines
  - Lawsuits
  - Individuals can now be held responsible for breaches of PHI
Updated Regulations

- Department of Health and Human Services (HHS) wants to see a “culture of compliance”
  - Update (as necessary) & follow your policies and procedures
  - Update your Business Associate Agreements (BAA) & Notice of Privacy Practices
  - Make a “good faith effort” to protect PHI in any form
  - Train staff & ensure they have a good understanding of these laws

Information Breaches

- What is a breach?
  - An impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI.

- Examples:
  - A relative is provided PHI about a patient in a clinic
  - A nurse provides PHI to an inquisitive police officer
  - An employee accesses PHI of a family member for personal reasons

- What to do when a breach occurs:
  - Within 60 days:
    - Notify the individuals
      - Those that received the information in error and those whose information was improperly disclosed
    - Place a notice on your website (if applicable)
    - Notify the media if more than 500 individuals are involved
    - Provide remedy (phone number, email address, etc.)
    - Notify the Secretary of Health and Human Services (HHS)
    - Breach Notification Log
    - Risk Assessment
Information Breaches

- **Breach Notification Log**
  - Include the following:
    - Date of breach
    - Date of discovery of breach
    - Approximate number of individuals affected
    - Type of breach (ex: theft, unauthorized access/disclosure, loss, improper disposal, hacking/IT incident, etc.)
    - Location of breached info (ex: paper, server, laptop, etc.)
    - Type of unsecured PHI involved (ex: full name, SSN, DOB, address, account number, etc.)

- **Risk Assessment:**
  - The nature & extent of PHI involved
  - Types of identifiers
  - Likelihood of re-identification
  - Amount of data
  - Sensitivity of data
  - Type of unauthorized individual who used the PHI
  - Whether PHI was truly acquired or viewed

- **Exceptions to the definition of a “breach” – Notification NOT necessary:**
  - The unintentional acquisition, access or use of PHI by an employee, if such acquisition, access or use was made in good faith and within the scope of authority.
  - The inadvertent disclosure of PHI by a person authorized to access PHI to another person authorized to access PHI.
  - Further disclosure is not permitted.
  - The CE or BA has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.
### Information Breaches

- **Damage Control:**
  - Document, Document, Document
  - Risk Assessments
  - Breach Logs
  - Employee Training Logs
  - Policies & procedures...follow them!
  - Confidentiality & Non-Disclosure Agreements
  - Business Associate Agreements
  - Audit Logs
- Encrypt stored data & data on the move
- Perform background checks on employees
- Remind staff and business partners of their legal duty to protect patient/customer data

### Staff Training

- **Objectives:**
  - Understand what HIPAA is and the requirements of federal (HIPAA) and state privacy & security laws; and your facilities policies and procedures regarding patient privacy & security
  - Understand how these laws affect each employee in their particular position and how they can protect confidential and sensitive information (PHI)
  - Understand consequences of not abiding by these laws
  - Provide instructions on reporting information breaches and security incidents

- **Customize trainings to suit your facility and employees needs**
- **Keep training material and training logs on file to show employees have completed training**
- **Sign Confidentiality and Non-Disclosure Agreements**
- **Train at the time of hire (orientation), review the information annually and train anytime there is a need (errors, changes & updates to the laws)**
- **Make sure employees know who they can go to when they have questions or concerns relating to HIPAA laws**
Enforcement Rule

- **Who enforces HIPAA?**
  - Office of Civil Rights (OCR)
  - Department of Justice (DOJ)
  - Federal Bureau of Investigation (FBI)
  - State & Local Authorities (if requested)

- **Your Patients!**

- **Violations & Enforcement**
  - Failure to comply with HIPAA can result in civil & criminal penalties

<table>
<thead>
<tr>
<th>HIPAA Violation</th>
<th>Minimum Civil Penalty</th>
<th>Maximum Civil Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willful neglect in reasonable care (repeat)</td>
<td>$100,000/repeat violation</td>
<td>Unlimited (annual maximum of $1.5 million)</td>
</tr>
<tr>
<td>HIPAA violations due to reasonable care is not due to willful neglect</td>
<td>$100,000/violation with an annual maximum of $1.5 million</td>
<td>$10,000/violation with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violations due to willful neglect but violations occurred after rule receival</td>
<td>$10,000/down with an annual maximum of $1.5 million</td>
<td>$100,000/violation with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>HIPAA violations result in disregard &amp; noncompliance</td>
<td>$10,000/violation with an annual maximum of $1.5 million</td>
<td>$50,000/violation with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>

Enforcement Rule

- **Concept of Knowledge**
  - In order to properly enforce a violation, the level of knowledge must be established
  - Knowledge that the violation took place
  - "Lack of knowledge" is not an acceptable excuse if due to a failure to self-inform about compliance obligations or to investigate complaints or other indications of non-compliance

  ****Ignorance of the law is no excuse!**

Enforcement Rule

- **Willful Neglect**
  - Consciously, intentional failure or reckless indifference to the obligations to comply with HIPAA
  - Example:
    - An employee working at a hospital medical record department forgets to use the encrypted software when preparing a file to be sent to Medicare. The file is transmitted but Medicare did not receive it and a breach was made. The employee fearing termination creates the file again in the correct software and resends, but fails to follow the rules when breach is made.

- **Reasonable Cause**
  - Shown not to be willful neglect
  - Example:
    - A company went into a HIPAA audit & provided a gap analysis that was incomplete because a particular item had not yet been addressed. The violation is due to reasonable cause and not willful neglect.
  - Minimum fine: $1,000/incident with annual maximum of $100,000 for repeat violations
  - Maximum fine: $50,000/incident with annual maximum of $1.5 million for repeat violations
Summary

- Understand the laws
- Yearly staff training/re-training
- Yearly risk assessments
- Policy & procedure manual (develop, monitor & update)
- Update forms:
  - NPP
  - BAA
- Breach management
- Penalties for non-compliance

Questions?

Knock knock. Who’s there? HIPAA. HIPAA who?
Sorry, I can't tell you THAT...