Health Insurance Portability and Accountability Act (HIPAA) Education

Developed Fall 2013 by:
Emily Anderson
MSN Clinical Nurse Specialist Student
CSU, Dominguez Hills – School of Nursing
Learning Objectives

- Discuss patient rights in regard to privacy of protected health information (PHI)
- Identify methods of upholding patient’s rights to privacy and confidentiality
- List the potential academic, professional, and legal consequences of violating HIPAA guidelines
- Apply HIPAA guidelines to clinical situations
What is HIPAA?

Created in 1996 to protect the privacy of personal health information & ensure the security of electronic protected health information (PHI) and personally identifiable information (PII).

(National Conference of State Legislators, 2013)
What does HIPAA do?

- Establishes national standards that govern use & disclosure of protected health information (PHI) for healthcare providers & organizations.

- Establishes significant penalties for violators (e.g., monetary fines, imprisonment, employment termination, and possible license revocation).

(National Conference of State Legislators, 2013)
HIPAA Definitions

❖ Protected Health Information (PHI):

Information created or received by a healthcare provider, health plan, public health authority, employer, life insurer, or school/university that relates to an individual’s past, present, or future physical or mental health.

(National Institute of Standards and Technology [NIST], 2010)
HIPAA Definitions

- **Personally Identifiably Information (PII):**
  Any uniquely identifying individual information

*Examples:* name, social security number, driver’s license or ID card number, date of birth, e-mail address, financial account information, photograph, medical record number, etc.

(National Institute of Standards and Technology [NIST], 2010)
HIPAA Definitions

**Confidential Information**: Any information (e.g., personally identifiable information (PII), protected health information (PHI), electronic-PHI, or financial) involving patients, employees, students or residents that requires specific authorization to access.

(National Institute of Standards and Technology [NIST], 2010)
Patient Rights to Privacy

All organizations must provide patients with the following:

- Notice of agency’s privacy policy
- Control over the use and disclosure of their protected health information (PHI)
- Confirmation that PHI will be used only for treatment, payment, operations & other lawful uses
- Access to their PHI
- Ability to request amendment or addendum to PHI
- Access to records of PHI disclosures
- Means to file privacy complaints to an agency compliance officer

Permitted Uses of PHI

Healthcare treatment, payment, or healthcare operations (TPO): Protected health information (PHI) & personally identifiably information (PII) can be disclosed for:

• Coordination of health care services
• Payment, billing, or claims
• Quality assessment, legal cases, training in areas of healthcare, compliance audits, medical review, accreditation and business management.

(HHS, 2003; National Nurse, 2011)
Other Permitted Uses of PHI (Without Consent)

- Victims of neglect/abuse/violence
- Organ/tissue donations
- Research
- Worker’s compensation
- Threat to self/others
- Public health activities

(HHS, 2003)
Patient Privacy & Authorization Policy

Patient authorization/consent

- Required for all non-permitted disclosures of protected health information

Opportunity to object

- Patients can object to certain disclosures of protected health information

(HHS, 2003)
5 U.S.C. 552a: The Privacy Act (PA)

- Prohibits disclosure of patient information unless patient consent is obtained or it falls under a permitted use.


- Prohibits disclosure of Healthcare Agency patients’ (and their dependents) names and home addresses unless specifically authorized by statute.

38. U.S.C. 7332

- Prohibits disclosure of patient information related to drug & alcohol abuse, HIV infection, and sickle cell anemia unless specifically authorized by the statute.

(Office of the Law Revision Counsel, 2013)
Unauthorized Access & Disclosure

- **Unnecessary browsing or medical record entry**: employees are prohibited from accessing family, friends, celebrity, VIP, or own medical records.

- **Unnecessary sharing**: confidential information may not be communicated to anyone without a need to know.

- **Inappropriate use of social or electronic media**: sharing PHI, PII, or confidential information, including photographs & videos on personal or social media sites is prohibited.

(National Nurse, 2011)
## Security & Privacy Principles

<table>
<thead>
<tr>
<th>Discuss PHI only as it applies to education &amp; patient care</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclose only the PHI/PII allowed/required by law</td>
</tr>
<tr>
<td>Follow minimum necessary rule</td>
</tr>
<tr>
<td>Do not assume</td>
</tr>
<tr>
<td>Do the right thing</td>
</tr>
</tbody>
</table>

(Kaiser Permanente, 2012; National Nurse, 2011)
Student Requirements

- Do not discuss PHI/PII in public places or via social networks
- Utilize initials only when identifying patients
- Remove all individually identifiable elements from PHI
- Only dispose of PHI in appropriate shredder bins
- Secure computer passwords & log-off when finished
- Do not photocopy/fax/un-securely e-mail PHI
- Only access information needed to complete educational assignments or fulfill the student role

(Kaiser Permanente, 2012)
Breach of Privacy/Security

❖ **Breach:**
  ❖ Compromise in security or privacy of confidential info via unauthorized acquisition, access, use, or disclosure of use

❖ **HITECH Act (2009):**
Requires organizations to report breaches that affect >500 individuals to gov’t & patients

(U.S. Department of Health & Human Services, 2013)
Breach of Privacy/Security

- Reported HIPAA violations (2012):
  - 571 breaches involving
    - 39.1% theft
    - 36.3% loss
    - 9.4% unknown
    - 8.6% hacking/IT incident
    - 0.8% improper disposal

(U.S. Department of Health & Human Services, 2013)
Social Networking

- Comply with American Nurses Association & National Council of State Boards of Nursing recommendations:
  - Do not take pictures or videos of patients
  - Do not post information or photos that can lead to patient identification
  - Do not establish personal or social media relationships with patients or former patients
  - Avoid making offensive comments about coworkers or employers
  - Immediately report privacy violations to appropriate authorities

(ANA, 2011; NCSBN, 2011)
Social Networking Resources

**ANA social networking tip sheet:**

**ANA tip card for nurses using social media:**

**NCSBN social media guidelines:**

**NSCBN social media video:**
https://www.ncsbn.org/2930.htm

(ANA, 2011; NCSBN, 2011)
Fraud, Abuse, & Retaliation

- All individuals (patients, family, staff, etc.) have the right to report suspected illegal, unethical, or otherwise inappropriate acts and verbalize concerns without fear of retaliation.

- **Non-retaliation policies**: those who retaliate against anyone reporting or refusing to participate in violations will be subject to strict disciplinary action.

(HHS, 2003)
Violation Consequences

**Civil Penalties:**
- Minimum $100-$10,000 per violation
- Maximum $50,000 per violation with annual maximum of $1.5 million

**Criminal Penalties:**
- $50,000-$250,000 per offense
- Imprisonment for one to ten years

**Academic Penalties:**
- Academic suspension, course failure, dismissal from school of nursing, disciplinary action by Board of Nursing

(American Medical Association [AMA], 2013)
Case Examples

(U.S. Department of Health & Human Services, 2013; NCSBN, 2011)

Scenario: nursing student posted a photo of a patient to social media without identifying his name.

Consequence: Photo was reported to hospital officials by another nurse & the nursing student was expelled.
**Scenario:** Nursing students created a blog where a clinical error that occurred at a hospital was discussed.

**Consequence:** The blog was discovered & reported by a community member; the students face discipline for violating employee/university policies.
**Scenario:** A nurse practitioner accessed the medical records of her ex-husband at work

**Consequence:** An internal audit discovered her electronic fingerprint on the chart; her access to the electronic record system was terminated & it was reported to Board of Nursing
References


Return to the Webpage to take the HIPAA Quiz and Print Your Certificate