The Privacy & Security of Protected Health Information

By the end of this course, you should:
• Be familiar with the patient’s rights to privacy under HIPAA Privacy Act
• Be able to identify Protected Health Information is and the PHI identifiers
• Be familiar with how to protect the patient’s privacy and how to properly dispose of PHI
• Be able to determine what **not** to post on social media
• Be able to identify what a breach is and how it is reported to the Compliance Officer
What is HIPAA?

**Health Insurance Portability and Accountability Act of 1996**

A federal law enacted to:

- Protect the privacy of a patient’s personal health information
- Provide for the physical and electronic security of personal health information
- Simplify billing and other transactions with Standardized Codes Sets and Transactions
- Specify new rights of patients to approve access/use of their medical information
The Essential Element of HIPAA: Protected Health Information (PHI)

PHI includes:

- A patient’s personal health, billing, or demographic information
- Any information, including photographic images, that makes patient identification possible
- In any format (Oral, Paper, Picture or Electronic)
- Created or housed by a covered entity (hospital, physician, health insurance payer) or a business associate of a covered entity

Privacy and security are not just about protecting data; they are about protecting people.

NavicentHealth
Everything about us is all about you.
PHI Identifiers

- PHI includes any number, character, or code that may be used to identify an individual.
- The description (even minus explicit identifiers) of any situation or event that is very unique will also constitute PHI. The uniqueness of a situation or event can serve to identify individual patient(s).
- The Minimum Necessary concept should always be taken into strong consideration (next slide).
Minimum Necessary or “Need to Know”

- You are permitted to view and disclose PHI to others that you obtain from your job only when your job requires it to be viewed or disclosed.

- All members of the workforce contribute to the care of the patient, but that does NOT mean everyone needs to see health information about patients.
Notice of Privacy Practices (NPP)

- This is a document that describes how Medical Information about the patient may be used and disclosed and how the patient can get access to this information.
- Must be prominently displayed:
  - Made available through the Website
  - Provide a copy of the NPP to anyone who asks
- Details the patients’ rights under HIPAA Privacy Rule
  - Obtain Acknowledgement of Receipt of NPP
  - Document good faith effort to obtain Acknowledgement
  - Document reason for refusal if patient or responsible individual will not sign
Uses & Disclosures of PHI that do not require patient authorization

TPO situations include:

- **Treatment:** Navicent Health may use and disclose PHI to deliver care. This may take place between any of the people assigned to care for an individual who is the subject of the PHI.

- **Payment:** Navicent Health may use and disclose PHI for billing and collection of payment purposes for the delivery of care.

- **Operations:** Navicent Health may use and disclose PHI as part of its daily business practices. This helps us improve our health care services and make sure we are following all related laws.
Social Media

- Per the Navicent Health confidentiality agreement: Do not discuss patient, financial, employee, or business information on social media
- Navicent Health employees posting photos of patients on social media is **not** allowed (even if the patient says it is OK)
- Posting descriptions of situations regarding a patient’s treatment or Navicent Health business issues (even devoid of explicit identifiers) is **not** allowed
- Navicent Health employees have been disciplined for Facebook related infractions
Taking Photos or Videos of Patients

- Staff members are **not** allowed to take photos or videos of patients. Taking a video or photo of a patient is a HIPAA violation.

- The only exception to this is when authorized employees take photos or videos for medical research, marketing, or education. A written informed consent signed by the patient is required before these types of photos or videos are taken.
Steps to Protect Patient Privacy

• Respect the patient’s information the same way you would expect others to respect your personal health information.
• Close treatment room doors or use privacy curtains.
• Ensure that medical records are not left where others can see or gain access to them.
• Make sure computer screens containing PHI are not visible to others not involved with the patient.
• Do not place anything with a patient’s name or identifier in the regular trash. It must be shredded. “Shred It” bins are placed throughout the hospital and offices for safe and convenient disposal of patient information.
What is a Breach?

A breach is an event that compromises the security, privacy, or integrity of *unsecured* PHI*. Including:

- Unauthorized acquisition
- Unauthorized access
- Unauthorized use
- Unauthorized disclosure

*Unsecured PHI* = not protected by approved encryption methods or destruction (ex: paper charts).
A Breach of PHI after HITECH: 
*Notification to Patients*

Federal law requires us to provide written notification to patients any time their PHI is used or disclosed in a manner not permitted by the HIPAA Privacy Rule.

We are required to report all PHI breaches to the U.S. Department of Health & Human Services (HHS):

- Annually if <500 individuals are affected by a single breach event
- Immediately if >500 individuals are affected by a single breach event:
  - Breach details get posted to the “Wall of Shame” – HHS Website
  - We must notify prominent, local media and do a press release
You should immediately report all suspected PHI breaches to the Privacy Officer or the Compliance Officer.

The Privacy Officer will conduct a full investigation.

Determination will be made if a Breach occurred and if notification is required.

We only have 60-days to complete the process.
HIPAA Enforcement Actions May Directly Affect Employees

- If you are found to be responsible for any type of a HIPAA violation that a State Attorney General believes has threatened or in some way harmed an individual who is a resident of the Attorney General’s State, you can be held responsible for your actions in a civil action.

- Recent criminal HIPAA cases should also serve as a wake-up call for healthcare workers involved in nefarious activity.
  - "Employees should know that they are being monitored, and that they will get caught, that they likely will be fired ... and could be prosecuted", says privacy attorney Kirk Nahra.
Secure Your Records!

HIPAA requires you to secure all electronic and paper documents and files containing PHI. You have a responsibility to your patients to protect their PHI.

In 2014, an $800,000 fine was charged against Parkview Health Systems, Inc. They left 71 boxes with 5,000 to 8,000 patient records on a physician’s porch. This was within 20 feet of the road, and right around the corner from a heavily trafficked public shopping mall.

This is an extreme example, but the moral of the story is - secure those records!
HIPAA Prosecution for Malicious Harm and Personal Gain

Andrea Smith and her husband were indicted for violations of the HIPAA administrative simplification act, as well as conspiracy to wrongfully use and disclose protected health information. According to the indictment, at the time of offense, Smith was a licensed practical nurse working in a medical clinic located in Jonesboro, Arkansas. She accessed the protected health information of a patient of the clinic, and then shared that information with her husband. Her husband then informed the patient that he was planning to use the information in an upcoming legal proceeding against the patient.

Smith pled guilty to the charge of wrongfully disclosing protected health information for malicious harm or personal gain. In exchange, the government dismissed the conspiracy count against both of them, and also dismissed a remaining count against her husband. Smith faced a maximum penalty of ten years of imprisonment, a fine of no more than $250,000, or both, and a term of supervised release of no more than three years.
Another HIPAA Prosecution

The U.S. Department of Justice announced the criminal indictment of Joshua Hippler, a 30-year-old former employee of an unnamed hospital in East Texas.

The indictment, filed on March 26th in the U.S. District Court in Tyler, Texas, charges Hippler with wrongful disclosure of individual identifiable health information, with the intent to sell, transfer, and use for personal gain.
Help Us Protect Each Other

- **Do not** share your system passwords.
- **Do not** copy PHI or remove PHI from the facility without approval to do so for permitted use or disclosure.
- Secure your laptop and other mobile devices
  - Lock in your office if you do not take with you at the end of the day
  - **Do not** leave unattended in your vehicle
  - Password protect your mobile device
- **Do not** “snoop” in the records or other PHI of co-workers, family or friends.
- Shred all paper PHI after you have finished using the information.
- **Do not** post photos or comments about patients on social media for any reason.
Visitor Monitoring & Identification

All employees should question unescorted visitors or other persons who are in restricted areas without ID.

All workforce members **must** wear their ID badge.

- Employees
- Students
- Contractors
- Volunteers
Portable Devices, Email, and Texting

Guidelines:

• All Navicent Health laptops containing PHI must be encrypted.
  • If you are unsure if your laptop is encrypted, contact IT
• Only encrypted devices should be used when accessing or storing PHI.
• Personal email accounts should not be used when dealing with PHI (ex: Hotmail, Gmail, Yahoo).
• PHI should not be transmitted via SMS (text messaging).
Reporting HIPAA Violations

Report known or suspected HIPAA violations to the Privacy Officer or to the Compliance Officer.

- It is part of your job to report instances where you suspect policies are being broken.

You may report anonymously, if you wish.

- You will not be retaliated against if you make a good faith report of a privacy violation, even if you were mistaken.
- 24/7 Compliance Helpline
Contact Info

Compliance Helpline: 633-7736 or 1-888-380-9008
Anonymous and Confidential

Roy Griffis, Jr., Interim Chief Compliance Officer/Privacy Officer
Phone: 478-633-6990
Email: griffisjr.roy@navicenthealth.org

Richard Jones, Senior IT Auditor
Phone: 478-633-2164
Email: jones.Richard@navicenthealth.org

Wesley Hardy, Compliance Business Analyst
Phone: 478-633-1650
Email: hardy.wesley2@navicenthealth.org
Testing

- Please click link below for module testing.

http://w3.mcccg.org/iota/test-HIPAA.asp