

HIPAA DID YOU KNOW???



Directions: Once CE module is open, the eight page educational module is printer friendly. The post test is on pages 7 & 8 with detailed instructions located in the post test section. Thank you for your participation.

HIPAA training/Continuing Education MCDS, SCSC, NSC, TW
For All Clinical and Office Staff

What is HIPAA?

“HIPAA”, is an acronym for the Health Insurance Portability & Accountability Act.

HIPAA is a Federal law enacted to:

- Protect the privacy of a patient’s personal and health information.
- Provide for the physical and electronic security of personal health information.
- Simplify billing and other transactions with standardized code sets and transactions.
- Specify new rights of patients to approve access/use of their medical information.

What are the HIPAA requirements?

- To protect the privacy and security of an individual’s Protected Health Information (PHI)
- To require the use of “minimum necessary”
- To extend the rights of individuals over the use of their PHI

What Patient Information Must We Protect?

We must protect an individual's personal and health information that...

- Is created, received, or maintained by a health care provider
- Is written, spoken, or electronic
- And includes at least one of the 18 personal identifiers in association with health information.

PHI

18 Identifiers defined by HIPAA

Name

Postal address

All elements of dates except year

Telephone number

Fax number

Email address

URL address

IP address

Social security number

Account numbers

License numbers

Medical record number

Health plan beneficiary number

Device identifiers and serial numbers

Vehicle identifiers and serial numbers

Biometric identifiers (finger and voice prints)

Full face photos and other comparable images

Any other unique identifying number, code, or characteristic

To Use or Disclose PHI

The surgery centers must give each patient a **Notice of Privacy Practices** that:

- Describes how the centers may use and disclose the patient's PHI and
- Advises the patient of his/her privacy rights
- Each center must attempt to obtain the patient's signature acknowledging receipt of the Notice, EXCEPT in emergency situations. If a signature is not obtained, the center must document the reason it was not.

For Purposes other than treatment, payment, operations...

Unless required or permitted by law, the centers must obtain written authorization from the patient to use, disclose or access patient information:

- **Patient authorization:** allows for centers to disclose information for other purposes.
- **Minimum necessary** applies to all uses and disclosures for payment and all healthcare operations.

State and Federal Laws Mandate all PHI be protected in the following formats:

All personal and health information that exists for **EVERY** individual in **ANY** form:

- Written
- Spoken
- Electronic

Who Uses PHI at our Surgery Centers?

- Anyone who works with or may see health, financial, or confidential information with HIPAA PHI identifiers
- Everyone who uses a computer or electronic device which stores and/or transmits information

Such as: Surgery Center employees
 Administrative staff with access to PHI
 Almost *Everyone* at one time or another!

Why is protecting **privacy and security** important?

- We all want our privacy protected.
- It's the right thing to do.
- HIPAA and Illinois laws require us to protect a person's privacy.
- The surgery center's policy requires everyone to follow privacy and security policies.

Do not look at, read, use or tell others about an individual's information (PHI) unless it is a part of your job.

Remember...

- **Use** only if necessary to perform job responsibilities
- **Use** the minimum necessary to perform your job
- **Follow** the surgery centers policies and procedures for information, confidentiality and security.

What does this mean for me as an employee?

All nurses, doctors, and staff must comply with these laws and regulations to ensure the privacy of our patients' protected health information (PHI). Any employee who violates HIPAA will be subject to the corrective action process, up to and including termination.

Incidental Use and Disclosure

Covers communication needed to provide effective patient care, such as:

- Healthcare providers discussing patient care
- Doctors conferring with patients' families

Health care providers are to make reasonable efforts to protect the privacy and dignity of all patients'.

- Avoid public areas, when discussing patient care.
- When talking to patients, draw curtains, and speak softly not to be overheard.
- You are permitted to discuss a patient in a public area if necessary, but you can not use the patient's name.
- Healthcare employees are not permitted to access a friend's PHI.
- Healthcare staff are allowed to keep patients' charts at bedsides, or outside exam rooms as long as the PHI is protected, the patient's name may be on the chart.
- If you leave a message, leave your name and number to confirm an appointment, or ask for a call back.
- Sign-in sheets are permitted, but limit the sign-in data to protect privacy.

You Can Protect PHI/Electronic PHI

- Verbal Awareness
- Written Paper/Hard Copy Protections
- Safe Computing Skills
- Reporting Suspected Security Incident

HIPAA Security Reminders

- Password protect your computer
- Backup your electronic information
- Send email securely
- Keep office secured
- Keep disks locked up
- Run Anti-virus, anti-spam, anti-spyware

Be Aware that Electronic PHI is everywhere

- Email (incoming and outgoing)
- Faxes (incoming and outgoing)
- PDA's, cell phones
- Laptops
- Zip disks, CDs, floppies, flash drives, memory sticks

We need to protect the entire lifecycle of PHI

- ✓ From Intake/creation of PHI
- ✓ Storage of PHI
- ✓ Destruction of PHI
- ✓ For any format of PHI

References

www.hhs.gov/ocr/hipaa

HIPAA training/Continuing Education Post Test **MCDS, SCSC, NSC, TW**
Page 7.

Name: _____ Date: _____

Post-Test

The post test found on pages 7 and 8 will evaluate your understanding of HIPAA.

Please write your name and date on pages 7 & 8, and circle your home base/surgery center. Return your completed post test to your manager or to the clinical educator. It will be graded and placed in your educational file.

Thank you in advance for your time and cooperation.

1. HIPAA is a federal law enacted to protect the privacy of a patient's personal and health information and provide for its physical and electronic security.

True

False

2. Who has to follow the HIPAA Laws?

- A. Physicians
- B. Physicians and all health care providers
- C. Only supervisors and other administrators

3. PHI stands for Personal and Health Information.

True

False

4. Examples of PHI include:

- A. name, address, birthdate, SS #, email address
- B. test results, medical records, diagnosis
- C. billing records, referral authorizations
- D. all of the above.

5. Under HIPAA, patients have certain rights contained in the following document:

- A. Confidentiality Statement
- B. Notice of Privacy Practices
- C. Information Release Form

HIPAA training/Continuing Education Post Test **MCDS, SCSC, NSC, TW**
Page 8.

Name: _____ Date: _____

6. Your sister's best friend had surgery done at the surgery center where you work. Your sister asks you to find out what kind of surgery she had done. What should you do?

- A. Pull the chart, note the surgical diagnosis and report back to your sister.
- B. Log into the billing system and check on the CPT codes.
- C. Explain to your sister, that it is a violation of the patient's privacy and health information to ask or look around for such information.
- D. None of the above.

7. State and Federal laws, as well as our organizations policy, requires what form of PHI to remain confidential?

- A. written
- B. spoken
- C. electronic
- d. All of the above.

8. Because I have access to confidential patient information as part of my job, I can look up anyone's record, even if they are not my patient, as long as I keep the information to myself.

True

False

9. You can protect patient information by:

- A. Protecting verbal or written information
- B. Utilizing safe computing skills
- C. Reporting suspected security incidents
- D. All of the above.

10. After a patient receives the Notice of Privacy practices, when can our organization access, use or disclose PHI?

- A. For treatment of a patient
- B. For payment of bills
- C. For healthcare operations
- d. All of the above.