HIPAA 101: Student Self-Learning Module & Test

Information:
This self-learning module meets the HIPAA 101 competency for Students. This requirement must be met once (it is not an annual requirement).

Instructions:
Step 1: Read the self-learning module.
Step 2: Print and complete the test.
Step 3: Return completed tests to:
  Skip Panter
  Professional Development
  Samaritan Health Services
  3600 NW Samaritan Drive
  Corvallis, Oregon 97330

Learning Objectives
At the end of this self-learning module, you should:
  • Know what HIPAA is and where it came from
  • Know why we should care about it
  • Have a basic understanding of the HIPAA standards and their impact on the culture of the organization
  • Know your role in HIPAA compliance

Synopsis review of HIPAA 101
What is HIPAA?
  • HIPAA is the Health Insurance Portability and Accountability Act
  • It was originally intended to provide for the continuation of health insurance coverage for individuals when they have changed jobs
  • The Administrative Simplification provisions were added to lower administrative health care costs by conducting more business electronically
HIPAA 101: Self Learning Module

An Introduction to the HIPAA Regulations

**Background: Where Did HIPAA Come From?**

**Cost Concerns**
- A New England Journal article stated that the U.S. spends about $400 billion each year on administrative services related to health care
- That’s around 20% of the total cost of health care each year in the U.S.
- The Congress estimated that approximately $87 billion could be saved annually if administrative efficiencies could be improved by:
  - Requiring more health care transactions to be conducted electronically, which would reduce paperwork, and
  - By standardizing health care transactions

**Privacy Concerns**
- As more business is conducted electronically, however, it becomes more difficult to protect the privacy of the data.
  - A national survey revealed that the greatest concern of Americans in this century is that personal health or financial information will be accessible to those who may use it inappropriately
  - The increasing availability of information on the Internet adds to people’s fears
  - Those fears are increasing as breaches of information security become more publicized, such as hackers accessing and misusing someone’s credit card number

**Breaches of Patient Privacy**
- Arthur Ashe, the well-known tennis player, contracted AIDS from a blood transfusion and was diagnosed and treated in a Richmond, Virginia hospital.
  - The family asked that this diagnosis be kept confidential, but the information was leaked from the hospital, creating a lot of public concern about the ability of hospitals to treat patient information confidentially.
- DNA information was used by Burlington Northern Railroad to deny employment to a job applicant
- Some other examples of privacy breaches listed below are only a fraction of all cases.
  - A bank accesses records and calls in loans of cancer patients
  - A medical student sells “promising” cases to a malpractice lawyer
  - A hospital Emergency Department employee shares patient information with an attorney for financial gain

**Why should you care about HIPAA?**
- The first reason is that HIPAA is the law. We don’t have the option to simply ignore it
The second reason is that many of the HIPAA standards are likely to be incorporated into existing accreditation standards (such as the JCAHO) and annual financial audit procedures.

A third reason is that many of the HIPAA regulations make good common sense.

Finally, we should care because every employee will be impacted by HIPAA, and could be penalized for violating HIPAA regulations.

HIPAA Privacy and Security Standards

Privacy vs. Security

First: some definitions—

**Security**: involves mechanisms for protecting access to systems and data

**Privacy**: involves rules governing the use and disclosure of data

HIPAA Privacy Standards

Protected Health Information

- The privacy standards were developed to limit the ways in which information that can be used to identify an individual may be used or disclosed.
- Protected Health Information is individually identifiable health information that is maintained or transmitted electronically, or in any other form or medium.
- That means that information transmitted orally is protected, as well as information that is maintained or transmitted electronically or on paper.

Consumer Rights Regarding Their Health Information

- The hospital is required to give patients a clear written explanation of how they can use, keep, and disclose their health information. This is called a notice of Privacy Practices, and the regulations identify specific information that it must contain.
• While patients cannot alter the existing content of their medical records, they do have the right to request that the hospital amend their records, by adding information to those records.
• The hospital may refuse that request if, among other things, it determines that the information in dispute is accurate and complete.

Limitations on the use of Medical Information
• Protected Health Information can be used without patient consent only for purposes of treating the patient, getting paid for health care services, and normal day-to-day health care operations.
• Disclosures for any other reason require a written authorization from the patient.
• Patients will be able to revoke an authorization (but not retroactively)
• Disclosures of protected health information must be limited to the minimum necessary for the purpose of the disclosure.
• Staff members that do not have a need for protected health information to do their jobs should not have access to it.

Other Allowable Disclosures
• The organization may, however, disclose some protected information without the patient’s authorization, for such things as:
  ‧ Oversight of the health care organization, such as quality assurance activities
  ‧ Public health needs
  ‧ Emergency circumstances
  ‧ Current patient directories
  ‧ Activities related to national defense and security

HIPAA Security Standard

Security Standards
• The security standards are written to keep protected health information from being accessed by unauthorized individuals.
• It requires the hospital to “maintain reasonable and appropriate administrative, technical, and physical safeguards” to protect that information.
• The HIPAA security standards are organized into four categories
  ‧ Administrative procedures to ensure that threats or violations can be prevented, detected and resolved (security training, hiring practices, system audits)
  ‧ Physical safeguards to protect Protected Health Information from fire, disaster and unauthorized access (locks, keys, storage protection)
  ‧ Technical security services to control and monitor access (passwords, audit trails, automatic logoff)
  ‧ Network security to protect unauthorized access to data transmitted over a network (encryption, detection systems)

Challenges Include:
• Developing policies and procedures to comply with the privacy standards
- Documenting compliance with those policies and procedures
- Modifying the culture of the organization to comply with HIPAA

**Your Greatest Risk Exposure Will Be:**
- Disgruntled patients who feel that the privacy of their personal health information has been compromised

**Your Role in HIPAA Compliance:**
- Make every reasonable effort to protect the privacy of our patient’s health information
- Report any concern about suspected violations of patient privacy to the hospital Privacy Officer
HIPAA 101: The Test

Completion of this test meets the competency requirement for HIPAA 101. Please write in your name and school. Complete the test and return it to:

Skip Panter
Professional Development
Samaritan Health Services
3600 NW Samaritan Drive
Corvallis, Oregon 97330

Please circle all answers that apply:

1. The hospital may use the patient’s health information for whatever purposes that it deems necessary.
   a. True____
   b. False____

2. Patients have the right to amend their medical records under HIPPA.
   a. True____
   b. False____

3. All clinical staff may have access to any patient records under HIPAA.
   a. True____
   b. False____

4. All employees within the hospital system will be impacted by HIPAA.
   a. True____
   b. False____