Health Information Portability and Accountability Act (HIPAA) Privacy Regulations, effective April 14, 2003

Primary Goals of the HIPAA Legislation:

• Assure health insurance portability
• Reduce healthcare fraud and abuse
• Simplify electronic administrative processes
• Guarantee security and privacy of health information

HIPAA is the most sweeping legislation to affect healthcare since Medicare in 1965. Nearly everyone will be affected: payors, employers, providers, clearinghouses, practice management system vendors, billing agents, and service organizations. In regard to protecting patient information, security is defined as the protection of information, data and systems from accidental or intentional access by unauthorized users. Common threats to patient information security include talking about patients, using identifiable information such as names, diagnosis, etc., in public areas.

Examples of Protected Health Information:

• Clinical information
• Name/social security numbers
• Name of relatives/family name/employer
• Health plan numbers/account numbers
• Telephone numbers/fax numbers/e-mails
• All dates related to the individual—birth, service
• Geographic subdivision smaller than state
• Any information that can reasonably identify a patient

Penalties for Non-compliance With HIPAA Regulations:

<table>
<thead>
<tr>
<th>Monetary Penalty</th>
<th>Term of Imprisonment</th>
<th>Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>$100</td>
<td>N/A</td>
<td>Single violation of a provision</td>
</tr>
<tr>
<td>Up to $25,000</td>
<td>N/A</td>
<td>Multiple violations of an identical requirement for prohibition made during a calendar year</td>
</tr>
<tr>
<td>Up to $50,000</td>
<td>Up to one-year</td>
<td>Wrongful disclosure of individually identifiable health information</td>
</tr>
<tr>
<td>Up to $100,000</td>
<td>Up to five years</td>
<td>Wrongful disclosure of individually identifiable health information committed under false pretenses</td>
</tr>
<tr>
<td>Up to $250,000</td>
<td>Up to 10 years</td>
<td>Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.</td>
</tr>
</tbody>
</table>

Failure to implement transaction sets can result in fines of $225,000 per year or more ($25,000 per requirement, times nine transactions). 

Failure to implement privacy and security measures can result in imprisonment.
Patient Rights:
• Patients have the right to:
  – Look at and obtain a copy of their health information.
  – Know how their health information has been used and to whom it has been disclosed.
  – File a formal compliant if their privacy has been violated.
  – Patient or parental consent must be obtained before a patient’s health information can be released to family members.
  – Protecting patient information includes all forms of communication – electronic, written and verbal.

Notice of Privacy Practices:
• Covered Entities must provide a simple explanation of their privacy practices. Direct treatment providers must make a good faith effort to obtain written acknowledgment of receipt of the notice of privacy practices.

Authorization:
• All Covered Entities must obtain individual authorization for each use or disclosure of treatment, payment or health care operations (PHI) for non-TPO activities.

Minimum Necessary:
• Employees should use only the information minimally necessary to do their job.

Business Associates:
• Covered Entities may disclose PHI to business associates. They are required to have contracts that require their Business Associates to observe certain privacy standards listed in the Regulations.

Personal Representatives (Parents):
• HIPAA gives control of a minor’s PHI to the parent, guardian, or person acting in loco parentis with certain exceptions.
• HIPAA does not overturn state laws that give providers discretion to disclose PHI to parents or prohibit the disclosure of PHI to a parent.
• Verification of the personal representative’s identity is a critical overlap with physical security.

Health-related Communications and Marketing:
• Marketing activities using PHI require authorization from each person for each use of their PHI.

Research:
• PHI may not be used or disclosed for research without the standard written HIPAA authorization or a waiver of authorization approved by the Committee on Clinical Investigations.

PRIVACY DO’S
■ Immediately remove all patient health information from printers, fax machines and photocopiers.
■ Dispose of protected health information in the appropriate confidential bin.
■ When conducting a conversation regarding a patient, do so in a private place or speak quietly so you can’t be overheard.
■ Keep medical records and other documents containing personal health information out of public view.
■ When possible, close patient/examining room doors or draw curtains and speak softly when discussing patients’ health information.
■ Treat other people’s confidential information as if it were your own.
■ Password protect your laptop computer and your personal digital assistant (pda).
■ Report privacy violations in the Hospital to the Privacy Officer, at Extension 2302, so we can improve our organization’s privacy practices.

PRIVACY DON’TS
■ Don’t share confidential patient information with anyone who doesn’t need to know it to do his or her job.
■ Don’t share passwords on your computer.
■ Never access information about a patient unless you need it to do your job.
■ Don’t walk away from open medical records, lab results, or computers etc. Close records first and use a bookmark, if necessary.
CHILDREN'S HOSPITAL LOS ANGELES
HIPAA COMPETENCY TEST

1. Which of the following statements about confidentiality and protecting patient information are true?
   ■ Only authorized people are allowed to look at or use patient information
   ■ Any health information that can identify a person must be treated as confidential
   ■ Confidential information should be shared only with those who have the “need to know”
   ■ All of the above

2. In regards to protecting patient information, security is defined as:
   ■ The requirement that all patient information either be under lock and key or protected by security officers
   ■ The protection of information, data and systems from accidental or intentional access by unauthorized users
   ■ None of the above
   ■ All of the above

3. Which of the following standards require health care organizations to protect patient information?
   ■ Chain of Trust (COT)
   ■ Prospective Payment System (PPS)
   ■ Health Insurance Portability and Accountability Act (HIPAA)
   ■ Outcomes Assessment Information Set (OASIS)

4. Organizations that violate patient privacy and security standards can suffer penalties such as:
   ■ Fines, possibly in the thousands of dollars
   ■ Imprisonment
   ■ Bad public relations
   ■ All of the above

5. Common threats to patient information security include:
   ■ Talking about patients, using identifiable information such as names, diagnosis, etc., in public areas
   ■ Logging off the computer when finished
   ■ Maintaining patient listings and other information out of the view of unauthorized people
   ■ All of the above

6. Patients have the right to:
   ■ Look at and obtain a copy of their health information
   ■ Know how their health information has been used and to whom it has been disclosed
   ■ File a formal complaint if their privacy has been violated
   ■ All of the above

7. Protected health information (PHI) is any information that can identify a patient.
   ■ True
   ■ False

8. Talking about a patient’s condition or diagnosis, while in a public area, would be a violation of patient privacy even if the patient’s name were not mentioned.
   ■ True
   ■ False

9. Patient or parental consent must be obtained before a patient’s health information can be released to family members.
   ■ True
   ■ False

10. Protecting patient information includes all forms of communication – electronic, written and verbal.
    ■ True
    ■ False

Student Name (print) ___________________________ Nursing School ___________________________
Student Signature ___________________________ Date ___________________________
Nursing Instructor Name ___________________________ CHLA Preceptor Name (if applicable) ___________________________

Submit to:
Leslie Neuman, Coordinator
Clinical Services, Staff Development, Mail Stop 74
Children’s Hospital Los Angeles

Revised April 27, 2016

Score: _____% _____