HIPAA AND HITECH
ADM – 067.4 Attachment D
Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule
Health Information Technology for Economic and Clinical Health (HITECH) Act

Primary Goals of the HIPAA/HITECH Legislation

- Ensure health insurance portability
- Prevent fraud, waste, and abuse
- Simplify electronic administrative processes
- Establish standards to protect the privacy of health information

All Covered Entities (CEs) and their workforce members are required to abide by HIPAA/HITECH. "Covered Entities" include health plans, health care clearinghouses, and health care providers. The Act defines a "health care provider" as "a provider of medical or health services…and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." The provider definition is very broad and includes non-traditional services, such as acupuncture and case management.

HITECH expanded the reach of HIPAA by applying the standards and requirements of the Act to Business Associates. In general, a Business Associate (BA) is any individual or entity that creates, receives, maintains, or transmits PHI on behalf of a Covered Entity for a regulated function or activity, such as claims processing, data analysis, quality assurance, etc.

HIPAA Privacy Rule

The HIPAA Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information" (PHI).

"Individually identifiable health information" is information, including demographic data, that relates to (1) the individual's past, present, or future physical or mental health or condition; (2) the provision of health care to the individual; or (3) the past, present, or future payment for the provision of health care to the individual, and identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers, including but not limited to:

- Name
- Mailing address, email address, telephone number, and fax number
- All dates related to the individual (date of birth, date of death, etc.)
- Social Security Number
- Medical Record Number

- Biometric identifiers (finger and voice prints)
- Full face photographs and other comparable images

Penalties for Non-compliance with HIPAA/HITECH Regulations

Individuals who fail to comply with this policy will be subject to sanctions under *ADM 096.0 Sanctioning of Workforce and Mitigation* and *ADM 049.0 Disciplinary Counseling Procedures*, up to and including termination, in addition to monetary fines and possible imprisonment under federal law.

Patient Rights

- Access
  - Right to access and receive a copy of one's own PHI (in paper or electronic format)
- Amendment
  - Request an amendment to information believed to be incomplete or incorrect
- Accounting of Disclosures
  - Information about how the patient's health information has been used and to whom it has been disclosed.
- Restriction
  - Right to request a restriction on the use and disclosure of the individual's PHI (including a restriction on disclosure to a health plan for services paid-in-full by the individual)
- Confidential Communications
  - Right to request alternative forms of communications (e.g. mail sent to PO Box instead of street address, no messages on home answering machine, etc.)
- Complaints
  - Patients have the right to file a formal complaint, to the hospital and/or the Office for Civil Rights in the Department of Health & Human Services (OCR), the entity that oversees and enforces HIPAA/HITECH, if they believe their rights have been violated.
- Notice of Privacy Practices (NPP)
  - A covered entity must provide patients with a Notice of Privacy Practices (NPP), notifying individuals of the entity's legal duties and privacy practices with respect to PHI.

Authorization

Unless otherwise authorized by law or CHLA policy, a patient/personal representative's written consent must be obtained before his/her PHI may be used or disclosed for purposes other than treatment, payment, or operations.

Except in certain situations, uses and disclosures of PHI must comply with the principle of Minimum Necessary, which requires a covered entity or business associate to make reasonable efforts to use, disclose, and request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure, or request.

Prior to disclosing any PHI, the individual must verify the recipient's identity and authority to receive the PHI. For example, the parent or legal guardian of a minor child is the patient's "personal representative" and therefore able to receive information about his/her treatment, diagnosis, etc.

Any inappropriate viewing of a patient's medical or financial information without a direct need for diagnosis, treatment, payment, or other lawful use is considered "unauthorized" and subject to the sanctions outlined

above. Under HIPAA, a breach is generally defined as any impermissible use or disclosure of health information under the Privacy Rule that compromises the privacy or security of the PHI.

PRIVACY DO'S

- ❑ Immediately remove all patient health information from printers, fax machines, and photocopiers.
- ❑ Dispose of protected health information in the appropriate confidential shredding 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 when discussing patients' health information.
- ❑ Ensure that all devices used to access or store CHLA data and protected health information (PHI) are encrypted in compliance with applicable CHLA policies. This includes laptops, desktops, tablets, smartphones, etc.
- ❑ Report potential privacy violations to the Chief Compliance & Privacy Officer, at Extension 12302, or by email to privacy@chla.usc.edu.

PRIVACY DON'TS

- ❑ Don't share confidential patient information with anyone who doesn't need to know the information to perform his or her job function.
- ❑ Don't share passwords or allow anyone else to use your login credentials.
- ❑ Do not leave devices used to store or access CHLA data unattended, including in a vehicle or unlocked office.

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. What kind of individually identifiable health information is protected by the HIPAA Privacy Rule?
   - ❒ Paper
   - ❒ Electronic
   - ❒ Verbal
   - ❒ All of the above

4. Organizations that violate patient privacy and security standards can suffer penalties such as:
   - ❒ Fines, possibly in the millions of dollars
   - ❒ Imprisonment
   - ❒ Negative publicity and reputational harm
   - ❒ 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
   - ❒ Failing to log off the computer when finished
   - ❒ Maintaining patient listings and other information in public view
   - ❒ 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. What makes a strong password?
   - ❒ Using at least 8 characters
   - ❒ Using mixed upper and lower case characters
   - ❒ Using special characters or symbols
   - ❒ All of the above

8. You accidentally fax paperwork containing PHI to the wrong number. The recipient calls to let you know, and agrees to destroy the documents immediately. Should you report this to the Compliance Office?
   - ❒ Yes
   - ❒ No

9. Unless authorized by law or CHLA policy, a patient/personal representative's written consent must be obtained before his/her PHI may be used or disclosed for purposes other than treatment, payment, or operations.

- ❒ True
- ❒ False

10. Any device used to access or store CHLA data must be encrypted.
    - ❒ True
    - ❒ False

I have read and understand all materials presented about HIPAA and HITECH.

_____ _____

Signature Date

_____

Print Name