CONFIDENTIALITY OF PATIENT/CLIENT INFORMATION

A GUIDE FOR AUTHORIZED SYSTEMS USERS

Health Services
LOS ANGELES COUNTY

PRIVACY OF PATIENT INFORMATION

It's the right thing to do…

Every patient/client has a right to privacy. To earn a patients/clients trust, you must protect their health information.

Federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and California laws require you to protect the privacy and security of all patient/client health information.

PRIVACY LAWS

HIPAA

- Requires you to protect the privacy and security of all **P**rotected **H**ealth **I**nformation **(PHI).**

HITECH Act

- The HITECH Act gave patients more rights and increased fines for violating the law.
- Requires covered entities to make a report when a patient's health information is kept on an unsecured computer/electronic device and is misused or wrongly given out.

CALIFORNIA

In addition to HIPAA and HITECH, there are important State laws and regulations that relate to the confidentiality of patient information.

- Confidentiality of Medical Information Act (CMIA)
- Patient Access to Health Records Act (PAHRA)

PHI AND PII

What is Protected Health Information (PHI)?

- Health information created, used, stored, or transmitted that could be used to describe the health and identity of a patient.
- Includes physical or health condition of the individual, the services or treatment provided, payment information, and information about past, current and future health problems.

What is Personally Identifiable Information (PII)?

- Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked to a specific individual.
- PII includes addresses, phone and fax numbers, payment information, demographic information and any information that may identify an individual.

PRIVACY AND PATIENT RIGHTS GRANTED UNDER PRIVACY LAWS

- Patient health information is protected in all forms, including paper, electronic, verbal, video, photos, etc.
- Patients may access, inspect, and request copies of their PHI.
- Patients may file a complaint.
- Patients may obtain a copy of the Notice of Privacy Practices.
- Patients may request a list of people/places where we provided their PHI.
- Patients are allowed to govern the use and disclosure of their information.
- Patients may restrict providing their PHI to a health plan or insurance company if they paid for the service out-of-pocket in full.

SECURITY OF PATIENT INFORMATION

- The HIPAA Security Rule covers all electronic Protected Health Information (ePHI) when stored and/or transmitted using any electronic device.
- ePHI is patient health information that is kept on computers and electronic media.
- Covered entities must take steps to make sure ePHI is complete, protected, and available. These steps include the development of policies and procedures, making sure computers are secured and ensuring staff members do not share their passwords.

MINIMUM NECESSARY

- Minimum necessary means you only access the information you need to do your job.
- Access to a system does not mean you have access to view confidential or patient information you do not need to do your job.
- Only give out just enough information for someone else to do their job.
- Before providing PHI/PII to an outside entity vendor make sure that the disclosure is covered by State or Federal HIPAA privacy laws.

THE FIVE WAYS PATIENT CONFIDENTIALITY IS MOST OFTEN VIOLATED

1. Lost or stolen unencrypted thumb drive/laptop or other portable device containing patient information.
2. Patient care staff talks to patient about his/her illness in front of a family member without giving the patient a chance to agree or object.
3. Staff members looking at medical information about a family member, friend, coworker, or high profile patient.
4. Providing a patient with another patient's PHI/PII.
5. Staff members not locking or logging off the computer when leaving the area.

YOUR RESPONSIBILITIES AS A AUTHORIZED SYSTEMS USER

- Take reasonable safeguards to protect PHI.
- Do not inappropriately access PHI.
- Practice the minimum necessary rule and only access the information needed to do your job.
- Use good judgment when discussing patient health information in front of spouses, family members and friends. If in doubt, Ask.
- Do not post information about patients or work-related issues on social media.
- Report possible and/or actual violations and breaches of DHS protected health information by notifying the DHS Help Desk at (323)409-8000.
- Do not share passwords.

YOUR RESPONSIBILITIES AS A AUTHORIZED SYSTEMS USER

- Properly dispose of PHI using confidential bins or shredders.
- Obtain permission to store electronic PHI on a laptop or other portable device, or USB thumb/flash drive and make sure the device is encrypted.
- Log off the computer when you are away from the work area or when the computer is not in use.
- Do not share passwords or your computer while logged on.

REPORTING VIOLATIONS AND BREACHES OF DHS PHI

Report security breaches to your supervisor or DHS Enterprise Help Desk at (323) 409-8000.

You will not be retaliated against for reporting a suspected or actual violation in good faith. False accusations will subject you to appropriate corrective action. Reporting a violation does not relieve you of liability if you were involved in the breach.

FINES AND PENALTIES

- Violations may result in fines against the organization that violated the law. You may be disciplined, as well as be personally fined and subject to imprisonment for violating patient privacy.
- If you need a professional credential to do your job, you may be reported to the issuing board or agency for additional action.

CONGRATULATIONS

You have completed the Confidentiality of Patient Information guide for a Authorized Systems User.

Complete the appropriate form for Non-County / Non-DHS once you close this window.