Health Services
LOS ANGELES COUNTY

COUNTY OF LOS ANGELES DEPARTMENT OF HEALTH SERVICES
Christina R. Ghaly, M.D.
Director

Los Angeles County Department of Health Services

Policy & Procedure Title:	Safeguards for Protected Health Information (PHI)		
Category:	300-399 Operation Policy	**Policy No.:**	361.23
Effective Date:	1/1/2005	**Update (U)/Revision (R):**	09/01/2019 (U)
DHS Division/Unit of Origin:	Patient Safety, Risk Management, Privacy, and Compliance		
Policy Contact – Employee Name and Title and/or DHS Division: Jennifer Papp, R.D., CHPC, DHS Privacy Officer, Privacy Compliance			
Contact Phone Number (s):	(213) 288-7741		
Distribution: DHS-wide ☒	**If not DHS-wide, other distribution:**		

PURPOSE:

The purpose of this policy is to establish administrative, technical and physical safeguards to protect the security of Protected Health Information (PHI), Personally Identifiable Information (PII) and other confidential information from unauthorized viewing, acquisition, access, use or disclosure.

DEFINITIONS:

Desktop Workstation includes a stand-alone, generally stationary, personal computing device possibly connected to a network server or other computer.

Particularly Sensitive Health Information means protected health information that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

Personally Identifiable Information (PII) is 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 or linkable to a specific individual. PII includes, for example, name; home or business address; telephone, wireless, and/or fax number; short message service or text message address or other wireless device address; instant messaging address; credit card and other payment information; demographics information and/or other information that may identify an individual or allow online or offline contact with an individual.

Portable Computing Devices, includes, but is not limited to, the following:

- Portable computers, including, but not limited to, laptops, tablet computers and computers on wheels.
- Portable devices, including, but not limited to, personal digital assistants (PDAs), cameras, smartphones, cellular telephones, pagers, etc.
- Portable storage media, including, but not limited to, diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard disk drives
- Mobile computers that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to County Information Technology resources.

Protected Health Information (PHI) is identifiable information relating to the past, present, or future physical or mental health condition of an individual, provision of health care to an individual, or the past, present, or future payment for health care provided to an individual, and that identifies, or for which there is a reasonable basis to believe the information can be used to identify an individual. Identifiable information includes, but is not limited to, patient name; medical record number (MRN); financial identification number (FIN); date of birth, Social Security Number; and phone number. PHI does not include employment records maintained by DHS in its role as employer.

Workforce or Workforce Member means employees, contract staff, affiliates, volunteers, trainees, students, and other persons whose conduct, in the performance of work for DHS, under its direct control, whether or not they receive compensation from the County.

POLICY:

DHS will implement appropriate administrative, technical and physical safeguards that will reasonably protect PHI, PII and other confidential information from intentional or unintentional acquisition, viewing, access, use or disclosure that is in violation of DHS' Privacy Policies.

DHS' workforce members must reasonably safeguard PHI, PII and other confidential information to limit incidental acquisition, viewing, access, use or disclosure made pursuant to an otherwise permitted or required use or disclosure.

PROCEDURES:

The following procedures set forth minimum administrative, physical and technical safeguards regarding the protection of PHI, PII and other confidential information (hereafter known as PHI).

I. Administrative Safeguards

A. Oral Communications. DHS' workforce members must exercise due diligence to avoid unnecessary disclosure of PHI through oral communications. Enclosed offices, secure areas and/or interview rooms are preferred locations for verbal exchange of PHI. Conversations involving IPHI in public areas should be avoided, unless necessary to further treatment, payment, teaching, research or operational

purposes. A lowered voice should be used, and attention should be paid to unauthorized listeners in order to avoid unintentional disclosure of PHI. Dictation should not be conducted in public areas or places where unauthorized individuals could overhear.

B. Telephone Communications. Each DHS facility shall develop and implement protocols consistent with DHS guidelines to protect the confidentiality and privacy of patient information when communicating such information via telephone. Release of information over the phone may only be done if the person doing so has verified the identity of the person he or she is speaking with and that person is authorized to receive the information. DHS workforce members shall not discuss PHI with the caller until the following is verified:

1. Identity of the caller using at least two (2) patient identifiers:
    a. First and last name,
    b. Medical record number,
    c. Date of birth, and/or,
    d. Address

2. The caller's relationship to the patient and that the use and disclosure of the PHI is permissible.

If the caller's identity and relationship cannot be verified, DHS workforce members shall not release or disclose any PHI.

DHS workforce members will honor any agreements made with the patient or the patient's personal representative regarding alternate forms of communications or restrictions on the use or disclosure of the patient's PHI. Telephone communications involving PHI should be conducted in private areas whenever possible and in a low voice to ensure information is not overheard by unauthorized persons.

Speakerphones should only be used in private areas and attention must be paid to the sound level to avoid unnecessary disclosure.

C. Telephone Messages. When making calls, DHS workforce members shall not discuss PHI until the identity of the person on the telephone line has been confirmed. In the event an answering machine or voice mail system picks up the call, workforce members shall leave a message requesting a return phone call.

- The message shall include ONLY the patient's name and the DHS workforce member's name and telephone number (e.g., "This message is for Lisa Jones. Please contact Kitty Katz at (213) 555-1313").
- Messages left on an automatic answering machine or voice mail system shall not contain PHI (e.g., diagnosis, test results, etc.). Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested an alternate means of communication

as described in DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information (PHI)." The content of appointment reminders should not reveal particularly sensitive health information, directly or indirectly, such as the specific name of the unit/department of the hospital.

- Telephone messages regarding test results or containing information that links a patient's name to a particular medical condition should be avoided.

D. Electronic Communications. If a patient requests receipt of their PHI electronically, the DHS workforce members must ensure the information is encrypted. If the information cannot be encrypted, the information must be sent through an alternate secure means of communication.

E. Faxes. The following procedure must be followed when faxing PHI:

1. Only the PHI necessary to meet the requester's needs should be faxed. All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality statement. Use DHS' PHI Fax Form (Attachment A) or the form used by the facility.

2. Particularly sensitive health information should not be transmitted by fax, except in emergency situations or if required by a government agency. If particularly sensitive health information must be faxed, the recipient should be notified prior to the transmission, and the sender should immediately confirm the transmission was completed, if possible.

3. Workforce members should only fax PHI if they are authorized to do so in the performance of their job duties.

4. Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained prior to releasing PHI to third parties for purposes other than treatment, payment or health care operations as provided in DHS Policy 361.4, "Use and Disclosure of Protected Health Information Requiring Authorization". In certain instances an authorization may be needed to release information to a third party for payment, such as self-paid services or insurance purposes.

5. PHI may be faxed to an individual if the individual requests access to their own PHI in accordance with DHS Policy 361.15, "Access of Individual to Protected Health Information (PHI)/Designated Record Set."

6. Reasonable efforts should be made to ensure fax transmissions are sent to the correct destination. Frequently used numbers should be preprogrammed into fax machines or computers to avoid misdialing errors. Preprogrammed numbers should be verified on a routine basis. The numbers of new recipients should be verified prior to transmission.

7. Fax machines must be located in secure areas not readily accessible to visitors and patients. Incoming faxes containing PHI should not be left sitting on or near the machine.

8. Fax confirmation sheets should be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet should be attached to the document that was faxed. Verify receipt of the fax by contacting the intended recipient and noting such on the approved fax sheet. Confirmation sheets and documents shall be safeguarded and handled appropriately according to facility or medical records processes or shredded as necessary.

9. Misdirected faxes containing PHI should be investigated and reported to the supervisor and the facility Privacy Manager. The sender should make an attempt to call the recipient to retrieve the misdirected fax, if possible. Upon receipt of a misdirected fax from another entity, DHS workforce members should immediately contact the sender to inform them of the error, and properly destroy the information without reading or sharing it with others.

F. Mail.

1. Interoffice Mail: Use a sealed envelope (not one with holes in it) and properly address the envelope with the name of the recipient, the location and room number. Tape the opening and stamp or write "confidential" over the seal.

2. Outside Mail: Use a sealed envelope appropriate for U.S. Mail. Ensure the return address does not contain the name of the department or unit within the hospital to ensure added privacy.

G. Internet/Social Networking.

Internet/social networking sites must not be used to discuss patients or patient information. Workforce members must remember that although internet/social networking sites (e.g., Twitter, Facebook, YouTube, discussion forums, text messaging web mail, etc.) can be accessed on their own time from their own computing devices, they must not discuss patients or patient information on these sites. Even small amounts of information, when put together, can reveal identifying information about a patient and thus cause a violation of privacy laws.

1. Workforce members must not disclose any confidential or proprietary information of or about the County, DHS or any of our affiliates on social networking sites.

2. Workforce members must not portray themselves as representatives of the County or DHS or act on behalf of the County or DHS on social networking sites, unless specifically authorized to do so in writing.

3. Workforce members, including former workforce members, may be held liable for damages and potential criminal prosecution for breaching PHI used or disclosed while working for DHS.

4. Workforce members must not engage in internet/social networking activities on their personal computing device during County work hours.

H. Social Media

1. Workforce members must remember to not post information about patients or work-related issues on social networking sites such as Facebook, Twitter, Snapchat, Instagram, Google+, YouTube, Tumblr, WhatsApp, etc.

2. It does not matter if the workforce member is not using County equipment or if they are on their break or at home.

3. Due to the nature and type of work DHS workforce members do, just small bits of information put together, can reveal identifying information about patients and cause a violation of privacy laws.

I. Photographing and Recording Patients.

Photography, audio, or video recordings of patients may be taken for various purposes such as patient treatment, professional education, peer review, publication, research, law enforcement, public relations, marketing, news media, or for a patient's own personal memorialization. This may occur only after appropriate consent is obtained from all affected individuals

Photography, video, or audio recordings of patients obtained by workforce members is considered PHI and shall always be handled in a manner that protects the patient's privacy and is consistent with federal and State patient privacy laws. At no point shall workforce members use, share or post photos, video, or audio recordings of patients in any public social media forum or utilize them for personal use without explicit consent from the patient or their authorized representative.

Workforce members who photograph, video, or audio record a patient shall use facility-owned equipment and approved applications unless explicitly authorized, in writing, by the patient or the patient's personal representative.

1. Written patient authorization must be obtained prior to taking photographs, video, or recordings of patients.

2. Authorization must contain the specific reason and use. Any other or additional use or disclosure requires a new authorization.

3. Written procedures shall be developed and implemented for use of facility-owned cameras and memory cards. The procedures shall include the physical security of the equipment and safeguarding of the images and recordings, such as keeping the device in a locked cabinet/drawer, securely uploading the images and recordings and wiping the images from the device after use.

4. Approved applications (e.g., HIPAA Bridge) may be used that support image capture and secure communications between members of the healthcare team. However, messaging within the application does not take the place of appropriate documentation in the legal medical record.

5. A workforce member's use of personal photography or recording equipment (including cellular telephones and smartphones) is prohibited without the patient's explicit written consent to photograph, video and/or audio record.

6. Photography of medical records or any other document that contains PHI is strictly prohibited.

7. DHS Policy 304 provides guidelines for obtaining authorization to photograph and/or record patients.

J. Destruction Standards.

PHI must be discarded in a manner that protects the confidentiality of such information. Hardcopy documents should be shredded or placed them in a locked shredder bin instead of throwing them in the trash. The facility IT/Help Desk should be contacted to appropriately destroy electronic PHI stored on electronic media (e.g., CDs, USB thumb drives, hard drives, computer/laptops, etc.).

1. PHI awaiting disposal or destruction must be stored in secure containers, storage rooms, or centralized shredder bins that are appropriately labeled and properly disposed of on a regular basis. Reasonable steps must be taken to minimize access to those documents.

2. Storage rooms containing confidential information awaiting disposal must be locked after business hours or when authorized staff are not present.

3. Centralized bins or containers used for disposal of PHI must be sealed/locked and clearly labeled "confidential", 'PHI", or some other suitable term and placed in a secure location. Reasonable steps must be taken to minimize access to PHI.

4. Documents containing PHI must not be recycled or reused for scratch paper.

5. Portable media awaiting destruction/sanitization must be kept in a secure locked area.

II. Physical Safeguards

A. Paper Records. Paper records and medical charts must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier should be used to protect paper records from unauthorized access.

1. Paper records and medical charts on desks, counters or nurses stations must be placed face down or concealed to avoid viewing or access by unauthorized persons.

2. Paper records should be secured when the office is unattended by persons authorized to have access to those paper records.

3. Original paper records shall not be removed from the premises unless permitted by law, they are secured in a manner to safeguard the PHI, and they are not left unattended.

4. Do not store paper records in an area where they can be inadvertently thrown away or mistaken for trash.

III. Physical Access

A. Ensure all areas used to store PHI are properly secured and that only authorized personnel have access to those locations.

B. Persons authorized to enter areas where PHI is stored or viewed must wear an identifiable DHS badge or be escorted by an authorized DHS workforce member.

C. Persons attempting to enter an area where PHI is processed must have prior authorization from DHS management.

D. Workforce members must not allow others to use or share their badges or keycards and must verify access authorization for unknown people entering an area where PHI is stored or processed.

IV. Visitors, Vendors and Patients

Visitors, vendors, and patients must be appropriately monitored when on DHS premises where PHI is located to ensure the information remains secure. This means that persons who are not authorized DHS workforce members should not be in areas where patients are being seen or treated or where PHI is stored.

V. Computer Workstations

PHI on computer devices must be safeguarded from unauthorized viewing and unauthorized access through the following means:

A. Using polarized screens or other computer screen overlay devices that shield information on the screen;

B. Placing computers out of the visual range of persons other than the authorized users;

C. Clearing information from the screen when not actually being used;

D. Logging off the computer when leaving the workstation;

E. Using password protected screen savers when computer workstations are not in use; and

F. Positioning computers in areas that prohibit/restrict access by unauthorized individuals (e.g., not within reach of persons at counter, etc.).

VI. Remote Access or Working Offsite/Outside the Secure Work Environment

DHS employees are discouraged from removing PHI from DHS; however, it is recognized that there are some situations where work outside of the secured environment is necessary. When it is necessary for DHS staff to take patient information home or to another work environment, staff shall abide by the guidelines outlined in DHS Policy 935.11, "Workstation and Mobile Device Use & Security Policy".

VII. Technical Safeguards

Access to PHI is based on the role and job responsibilities of the workforce member. Workforce members will be assigned access to DHS' networks and systems based on their need to know and the minimum necessary information needed to fulfill their job responsibilities. A workforce member with access to a system for completion of certain assignments is not authorized to view, use or access other information in the system not related to their job responsibilities or particular assignment/case.

A. Technical safeguards regarding the security of PHI maintained in electronic form may include:

1. Logging off any electronic system containing PHI when leaving the computer even for a few minutes, or after obtaining necessary data.

2. Requiring computing devices to have a password-protected screen saver or other time-out feature.

3. Encrypting all portable computing devices such as laptops, USB/thumb drives, and other electronic devices containing PHI.

4. Ensuring that workforce members are familiar with the facility downtime procedures.

B. Passwords

1. Workforce members are responsible for safeguarding their passwords for access to the County information technology resources.

2. Workforce members are responsible for all transactions made using their passwords. Workforce members may not provide their password or use their password to provide access to another workforce member; or access County information technology resources with another workforce member's password or account. Some systems have a universal access password with a secondary password, neither of which shall be shared with workforce members who are not authorized to utilize the system.

3. Passwords must be changed on a regular basis to ensure security. Strong passwords include at least eight (8) characters, and uses a combination of uppercase and lowercase letters, numbers and/or special characters.

VIII. Use of Electronic Systems

DHS shall implement a combination of administrative, physical and technical safeguards to ensure the safety of PHI in electronic communications networks, including: (1) privacy and security awareness training of DHS Users concerning the transmission of PHI over electronic communication networks; (2) periodic reviews of this policy and procedure with DHS Users to confirm compliance; (3) constant security reminders; (4) use of password-protected screen savers and exercise of due diligence to ensure that electronic systems used for transmission and/or storage of PHI is shielded from viewing by unauthorized persons; and (5) other applicable safeguards outlined in this Policy.

A. Portable Computing Devices

1. All portable computing devices used to access and/or store PHI must comply with all applicable DHS and County IT resources policies, standards, and procedures.

2. Generally, DHS prohibits the download or storage of PHI on portable computing devices. However, DHS Users who, in the course of County business, must download or store PHI on portable computing devices are required to adhere to DHS policies and procedures for storage and use of PHI on portable computing devices.

3. If PHI is downloaded or stored on a portable computing device, that information must be safeguarded from unauthorized access and, without exception, the information must be encrypted.

4. A DHS User who intends to use their County-owned or personally-owned portable computing device to access and/or store PHI is required to obtain prior written authorization from DHS Information Technology.

B. E-mail

1. Non-County e-mail such as G-mail, Yahoo Mail, etc. must not be used for sending DHS-related PHI. Use of e-mail between a DHS User and a patient is permitted provided that the e-mail is encrypted and sent through the County's e-mail system.

2. Audits of outbound e-mail communications may be periodically performed to ensure that use of e-mail to transmit PHI is in accordance with Departmental policies. Refer to DHS Policy 935.20, "Acceptable Use Policy for County Information Technology Resources."

C. Online Web-based Document Sharing Services

Storing and/or sharing of PHI and other confidential information using non-County approved online web-based document sharing services (e.g., Google Docs, Microsoft Office Live, Open-Office, Dropbox, etc.) is strictly prohibited.

D. Meaningful Use

DHS will use a HIPAA compliant, secure portal to provide patients direct access to their medical information via the electronic medical record.

IX. Disciplinary Action

Unauthorized viewing, acquisition, access, use, or disclosure of confidential and/or PHI (including but not limited to medical records) will result in disciplinary action, up to and including discharge, as well as possible civil/criminal penalties, fines and disciplinary action against the individual's professional license, permit, registration, or certificate from using the issuing board or agency.

X. Document Retention

This policy will be retained for a period of at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later.

ATTACHMENTS/FORMS:

Attachment A – DHS Fax Form

REFERENCES/AUTHORITY:

45 Code of Federal Regulations, Part 164, Section 164.530(c)(1)

DHS Policy Numbers:

- 361.6 Right to Request Confidential Communications of Protected Health Information
- 361.15 Access of Individual to Protected Health Information (PHI)/Designated Record Set
- 361.26 Mitigation
- 935.043 Blackberry Handheld Devices for Remote GroupWise Access Policy
- 935.11 Workstation & Mobile Device Use and Security Policy
- 935.20 Acceptable Use Policy for County Information Technology Resources

DHS Discipline Manual and Guidelines