Health Services
LOS ANGELES COUNTY

POLICIES AND PROCEDURES

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO: 361.23

PURPOSE:

To establish safeguards to protect the security of Protected Health Information and other confidential information from unauthorized viewing, acquisition, access, use or disclosure.

POLICY:

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

DHS' workforce must reasonably safeguard PHI to limit incidental access, use or disclosure made pursuant to an otherwise permitted or required 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.

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

- Portable computers, including, but not limited to, laptops and tablet computers
- Portable devices, including, but not limited to, personal digital assistants (PDAs), digital cameras, smartphones, cellular telephones, and pagers
- 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) means individually identifiable information relating to past, present or future physical or mental health or 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.

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

PROCEDURES:

The procedures below set forth minimum administrative, physical and technical safeguards regarding the protection of PHI.

I. Administrative Safeguards

A. Oral Communications. DHS' workforce must exercise due diligence to avoid unnecessary disclosures of PHI through oral communications. Enclosed offices and/or interview rooms are preferred locations for verbal exchange of PHI. Conversations involving PHI 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 and telephone conversations should be conducted away from public areas if possible. Speakerphones should only be used in private areas and attention must be paid to the sound level.

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 via telephone. Whenever it is necessary for DHS workforce members to discuss PHI via telephone with a patient or patient's family members or friends, other DHS workforce members, business associates, or other health care providers, workforce members must follow facility guidelines for protecting such information. Release of information over the phone may only be done if the person doing so is absolutely sure of the identity of the person he or she is speaking with and that person has a right to receive the information.

DHS workforce members will honor any agreements made with the patient or 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 a private area whenever

possible and in a low voice to ensure information is not overheard by unauthorized persons.

When receiving calls, DHS workforce members shall not discuss PHI with the caller until the following can be confirmed:

1. Identity of the caller (e.g., a "call back" to validate the number called, or definite voice recognition)

2. Verification that the caller has a need to know and the use and disclosure of PHI is permissible.

If confirmation cannot be made, DHS workforce members shall not confirm or deny that the patient has in the past or is currently receiving services from DHS.

C. Internet Communications. If a patient requests receipt of their PHI through the Internet, the 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.

D. Telephone Messages. When making calls, DHS workforce members shall not discuss PHI until the identity of the person on the phone line has been confirmed. In the event an answering machine or voice mail system picks up the call, staff should leave a message requesting that the person they need to speak to return the call.
   - The message shall include ONLY the name and telephone number of the person that should receive the return call (e.g., "This message is for Mary Jones. Please contact Mary Smith at 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 pursuant to DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information (PHI)." However, each provider and/or clinic should limit the amount of PHI that is disclosed in a telephone message.
   - 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.

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

1. Only the PHI necessary to meet the requester's needs should be faxed.

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 immediately notified prior to the transmission and the sender should immediately confirm the transmission was completed, if possible.

3. Workforce members should only fax PHI authorized as part of their work 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," unless otherwise permitted or required by law. 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 Individuals to Protected Health Information (PHI)/Designated Record Set."

6. All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality statement. Use DHS' PHI Fax Form or the form used by the facility.

7. 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.

8. 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.

9. 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.

10. Misdirected faxes containing PHI should be investigated and reported to the supervisor and the facility privacy coordinator. The sender should make an attempt to call the recipient to retrieve the misdirected fax, if possible. Do not read through faxes received in error: Contact the sender and advise that their fax was received in error and properly destroy the information.

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 as well as the location and room number. Tape the opening and stamp "confidential" over the seal.

2. Outside Mail: Use an appropriate sealed envelope 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 should remember that due to the nature of the work and the type of business they work in, just small bits of information, put together, can reveal identifying information about patients and cause them to violate 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 hold themselves out as representatives of the County or DHS or act on behalf of the County or DHS on social networking sites, unless specifically authorized in writing.

3. Workforce members, including former workforce members, may be held liable for damages and potential criminal prosecution for breaching PHI used or exposed to 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. Photographing and Recording Patients. Photographic or audio recordings of a patient may be taken for purposes of treatment, professional education, peer review, publication, research, law enforcement, public relations, marketing and news media only upon obtaining prior written patient consent and photographs must be filed in the patient's medical record. Disclosure of photographic or audio recordings constitutes the release of medical information and therefore requires prior authorization for use or disclosure of patient health information

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. Only facility-owned cameras, memory cards and other equipment may be used.

4. A workforce member's use of personal photography or recording equipment (including cellular telephones and smartphones) is prohibited.

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

6. DHS Policy 304 provides guidelines for photographing and recording patients.

I. Destruction Standards. PHI must be discarded in a manner that protects the confidentiality of such information. Shred hardcopy documents or place them in the locked shredder bin instead of throwing them in the trash. Contact your IT/Help

Desk to appropriately destroy ePHI located on electronic media (e.g. CD's, 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 confidential information must be sealed, 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 paper records.

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

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

III. Physical Access

A. 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.

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

C. 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 and Patients

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

V. Desktop Workstations

PHI on computer devices must be protected from unauthorized viewing and unauthorized access. Suggested means for ensuring this protection include:

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

E. Locating 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, the following guidelines in accordance with DHS Policy 935.11, "Workstation and Mobile Device Use & Security Policy" should be followed:

A. The remote work area must provide adequate privacy and security.

B. Confidential information should be secured in locked rooms or a locked storage container when not in use.

C. Home computers must comply with DHS standards including County approved anti-virus software and must adhere to County hardware/software protection standards and procedures.

D. While on train, bus, airplane or other form of mass transit ensure use of privacy screen as well as all other requirements under section V – Desktop Workstations. Paper documents must be kept out of sight or range of view by other passengers.

E. Confidential data may not be saved on removable devices (e.g. floppy drive, CD-ROM, external drive, USB/Thumb drive) unless it is approved and appropriate safeguards are in place (e.g., encryption).

F. Data/information must not be accessible by unauthorized persons/family members. All completed work, if not remotely accessed, must be saved to the original, encrypted external device AND removed completely from the home computer.

G External devices, portable computing devices, must be encrypted and maintained in a secure location/protected from theft or loss.

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 amount of information needed to fulfill their job responsibilities. Minimum necessary also applies to their access to the system. 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.

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

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

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

3. All portable computing devices such as laptops, USB/thumb drives, and other electronic devices containing PHI must be encrypted.

4. Workforce members should be familiar with their 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.

3. Workforce members may not provide their password or use their password to provide access to another workforce member; or access the County information technology resource 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.

4. Passwords must be changed on a regular basis to ensure security. Strong passwords include at least eight characters, such as a combination of letters, numbers and/or special characters.

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

VIII. Use of Electronic Systems

DHS shall implement a combination of administrative, physical and technical safeguards to protect PHI in electronic communications networks, including (1) privacy and security awareness training of DHS Users concerning the transmission of PHI over electronic communications networks; (2) periodic review of this policy and procedure with DHS Users to confirm compliance; (3) repeated 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 protected from viewing by unauthorized persons; and (5) other applicable safeguards outlined in this Policy.

A. Portable Computing Devices

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

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

3. If PHI and/or confidential information is downloaded or stored on a portable computing device, information must be protected 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 and/or confidential

information is required to obtain prior written authorization from the 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. Replying to e-mail with patient, confidential, and/or sensitive information: DHS users must follow the same procedures when replying to e-mail with patient, confidential, and/or sensitive information in the same manner as if it were originally created by the DHS User.

3. 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.

IX. Disciplinary Action

Unauthorized viewing, acquisition, access, use, or disclosure of confidential and/or protected health information (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 the issuing board or agency.

X. Document Retention

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

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO.: 361.23

REFERENCES:

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 Individuals 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