DEPARTMENT OF HEALTH SERVICES
COUNTY OF LOS ANGELES

SUBJECT: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI)

POLICY NO: 361.23

PURPOSE:

To establish safeguards that must be implemented by DHS to protect the confidentiality of protected health information.

POLICY:

Set forth below are policies establishing minimum administrative and physical standards regarding the protection of protected health information that DHS must enforce. DHS may develop additional policies and procedures that are stricter than the parameters set forth below in order to maximize the protection of protected health information in support of their specific circumstances and requirements. The development and implementation of policies and procedures in addition to those stated herein must be approved by the Chief Information Privacy Officer.

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

DHS' Workforce must reasonably safeguard PHI to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

DEFINITIONS:

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.

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.

Workforce or Workforce Member means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for DHS, is under its direct control, whether or not they are paid by the County.

PROCEDURES:

A. Administrative Safeguards.

1) Oral Communications. DHS' Workforce must exercise due care to avoid unnecessary disclosures of protected health information through oral communications. Conversations in public areas should be avoided, unless necessary to further patient care, research or teaching purposes. Voices should be modulated and attention should be paid to unauthorized listeners in order to avoid unnecessary disclosures of protected health information. Patient identifying information only should be disclosed during oral conversations when necessary to further treatment, payment, teaching, research or operational purposes. Dictation and telephone conversations should be conducted away from public areas if possible. Speakerphones only should be used in private areas.

2) Cellular Telephones. The use of cellular phones is not prohibited as a means of disclosing or using PHI. However, their use poses a higher risk of interception as compared to legacy landline telephones. Landline telephones should be used if the conversation will involve the disclosure of PHI.

3) Telephone Messages. Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested an alternative means of communication pursuant to **DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information."** However, each provider and/or clinic should limit the amount of protected health information that is disclosed in a telephone message. The content of appointment reminders should not reveal Particularly Sensitive Health Information, directly or indirectly. Telephone messages regarding test results or that contain information that links a patient's name to a particular medical condition should be avoided.

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

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

b) 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 immediately prior to the transmission and the sender should immediately confirm that the transmission was completed, if possible.

c) DHS should designate employees who can fax, or approve the faxing of, protected health information. Unauthorized employees, students and volunteers should never fax protected health information.

d) Unless otherwise permitted or required by law, a properly completed and signed authorization must be obtained before releasing protected health information to third parties for purposes other than treatment, payment or health care operations as provided in **DHS Policy No. 361.4, "Use and Disclosure of Protected Health Information Requiring Authorization."** Protected health information may be faxed to an individual if the individual requests access to their own protected health information in accordance with **DHS Policy No. 361.15, "Access of Individuals to Protected Health Information (PHI)/Designated Record Set."**

e) All faxes containing protected health information must be accompanied by a cover sheet that includes a confidentiality notice. Use DHS' ***PHI FAX Form***.

f) Reasonable efforts should be made to ensure that 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.

g) Fax machines must be located in secure areas not readily accessible to visitors and patients. Incoming faxes containing protected health information should not be left sitting on or near the machine.

h) 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.

i) All instances of misdirected faxes containing protected health information should be investigated and mitigated pursuant to **DHS Policy No. 361.26, "Mitigation."**

5) Mail. Protected health information should be mailed within the County's departments in sealed envelopes. Protected health information mailed outside the County's departments should go via first class mail and should be concealed. Appointment reminders may be mailed to patients, unless the patient has requested an alternative means of communication pursuant to **DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information."**

6) Destruction Standards. Protected health information must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing protected health information should be destroyed or shredded. Magnetic media and diskettes containing protected health information should be overwritten or reformatted.

   a) PHI awaiting disposal must be stored in containers that are appropriately labeled and are properly disposed of on a regular basis.

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

   c) Centralized bins or containers used for disposed confidential information must be sealed, clearly labeled "confidential", "PHI" or some other suitable term and placed in a locked storage room.

   d) Facilities or sites that do not have protected storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to PHI.

B. Physical Safeguards.

1) 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.

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

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

   c) Original paper records and medical charts should not be removed from the premises unless necessary to provide care or treatment to a patient or required by law.

      i. DHS employees should not remove paper records or medical charts for their own convenience.

      ii. Any paper records and medical charts removed from DHS' premises should be checked out according to DHS' policies and procedures and should be returned as quickly as possible.

iii. The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out or removed them.

iv. Paper records and medical charts that are removed from DHS' premises must not be left unattended in places in which unauthorized persons can gain access.

v. Paper records and medical charts must not be left in unlocked automobiles or in view of passers-by.

vi. The theft or loss of any paper record or medical chart should be reported to the DHS' Privacy Officer so that mitigation options can be considered.

C. Physical Access

1) Persons authorized to enter areas where PHI is stored or viewed must wear identifiable, DHS employee badges or be escorted by an authorized County employee.

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

3) Employees must not allow others to use or share their badges and must verify access authorization for unknown people entering an area where PHI is stored or processed.

4) Terminated or transferred personnel must be escorted in areas where PHI is stored or processed.

D. Escorting Visitors and Patients.

Visitors and patients must be appropriately monitored when on DHS' premises where protected health information is located to ensure they do not access protected health information about other patients without permission. This means that persons who are not part of DHS' Workforce should not be in areas in which patients are being seen or treated or where PHI is stored without appropriate supervision.

E. Computer/Work Stations.

Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. Suggested means for ensuring this protection include:

1) Use of polarized screens or other computer screen overlay devices that shield information on the screen;

2) Placement of computers out of the visual range of persons other than the authorized user;

3) Clearing information from the screen when not actually being used;

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

F. Technical Safeguards.

1) Technical safeguards regarding the protection of Protected Health Information maintained in electronic form may include:
   - Log off any electronic system containing PHI when leaving the computer or after obtaining necessary data
   - Do not share computer passwords or leave them out where they can be seen.
   - Change passwords every three (3) months.
   - Ensure all computers and laptops used to access PHI are properly secured.
   - Become familiar with departmental contingency plan.
   - Ensure that all areas used to store PHI are properly secured and that only authorized personnel have access to these locations.

2) Use of Electronic Systems. Until appropriate security mechanisms are implemented and supporting policies are published, DHS' Workforce will not be permitted to use the following electronic systems for the distribution, processing or storage of PHI:

   a) Electronic mail or email;

   b) Personal Digital Assistance (PDA), such as Palm Pilot, iPAQ, Window's CE or other similar devices.

c) Wireless networks

G. 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.

REFERENCES

Code of Federal Regulations 45 § 164.530 (c) (1)
DHS Policy Nos. 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"