# 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:**

*Internal E-Mail* means e-mail sent between or among DHS users using DHS-provided Novell Groupwise e-mail services. Internal E-Mail is considered encrypted and secure.

*External E-Mail* means e-mail sent by a DHS user to an e-mail account outside the DHS-provided Novell Groupwise e-mail services. External e-mail includes e-mail sent using a web-based e-mail system furnished through an external Internet service, regardless of whether the e-mail is sent from within a DHS facility or not.

*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.

**APPROVED BY:** Thomas Garthwaite

**EFFECTIVE DATE:** January 1, 2005

**SUPERSEDES:** April 14, 2003

*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 the Department, its offices, programs or facilities, is under the direct control of the Department, office, program or facility, regardless of whether they are paid by the entity.

**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.

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.

G. Use of Electronic Systems.

DHS shall implement a combination of administrative, physical and technical safeguards to protect PHI in electronic communications networks, including (1) security awareness training of DHS Users concerning the transmission of PHI over electronic communications networks; (2) implementation of E-Mail Guidelines (see section G.2.c below); (3) periodic review of this policy and procedure and E-Mail Guidelines with DHS Users to confirm compliance; (4) repeated security reminders; (5) 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 (6) other applicable safeguards outlined in this Policy.

1) Personal Digital Assistants (PDAs)

   a) All PDA users will be provided specific training on the risks of using PDAs for PHI and will be required to recertify their understanding and compliance with HIPAA privacy policies and procedures.

   b) PDAs, whether procured by DHS or personally owned, will be permitted for PHI use but must be registered with the DHS CISO or designee (cluster Information Security Coordinator) and must conform to departmental standards for password protection.

2) E-mail

a) Internal E-Mail. Use of Internal E-Mail (i.e., within the secure DHS networks) is permitted to transmit PHI. Users shall be provided with unique user ID and passwords for access to their individual e-mail accounts and must comply with DHS/local facility Acceptable Use Policies.

b) External E-Mail. Use of External E-mail (i.e., outside the secure DHS networks) to transmit PHI is permitted in limited circumstances, when no other more secure method of communication is feasible. Use of External E-mail to transmit or store PHI is limited to uses which are necessary to ensure appropriate patient care and/or to carry out payment and health care operations activities. De-identified information is to be used in lieu of PHI whenever feasible.

c) All DHS users who use E-Mail to transmit PHI shall sign the form acknowledging they have read, received a copy, and agree to abide by the "Guidelines Governing the Use of E-Mail Involving PHI (the "E-Mail Guidelines," which is Attachment 1 to this Policy). The copy of the E-Mail Guidelines signed by the DHS User shall be held by the DHS CISO or designee (cluster Information Security Coordinator). Use of External E-mail between a DHS User and a patient is permitted in accordance with the E-Mail Guidelines.

d) Replying to External E-Mail with PHI. DHS users typically receive a large amount of External E-mail that may contain PHI. DHS does not regulate External E-mail beyond anti-virus and spam control technologies. DHS users must follow the same procedures when replying to External E-mail with PHI in the same manner as if it were originally created by the DHS user.

e) Audits of outbound e-mail communications will be periodically performed to ensure that use of e-mail to transmit PHI is in accordance with this policy and procedure and the E-mail Guidelines.

3) Wireless Local Area Networks (WLANs)

a) WLANs that currently implement or have plans to implement WLAN security as defined by the DHS Network Security Architecture and County guidelines for Wireless Network Security are permitted for PHI use, but must have a WLAN topology and security plan submitted and approved by the DHS CISO or designee.

b) WLANs that do not meet or plan to meet WLAN security guidelines as defined by the DHS Network Security Architecture and County guidelines for Wireless Network Security are not permitted and must be removed from service.

4) Electronic Transmission of Clinical Laboratory Tests

a. The health care professional must obtain a California-compliant authorization from the patient for the patient to receive his or her laboratory results by Internet posting or other electronic means. (Cal. Health & Safety Code § 123148(b)(1)). A patient (or his or her physician) may revoke this authorization at any time and without penalty, except to the extent that action has been taken in reliance on the authorization.

b. The transmission of the following clinical laboratory test results (and any other related results) to a patient by Internet posting or other electronic means is prohibited by law: (i) HIV antibody test; (ii) presence of hepatitis antigens; (iii) drug abuse; and (iv) test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy.

c. In the event that a health care professional arranges for the electronic transmission of test results, the results must be delivered to the patient in a reasonable time period, but only after the results have been reviewed by the health care professional. When clinical laboratory test results are delivered to a patient via Internet posting or other electronic manner, access must be restricted by the use of a secure personal identification number.

d. If the patient asks to receive his or her laboratory test results by Internet posting, the health care professional is required to inform the patient of any charges that may be incurred directly to the patient or insurer for the service and that the patient may call the health care professional for a more detailed explanation of the laboratory test results when delivered.

H. 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"

**ATTACHMENT 1**

## DHS Guidelines Governing the Use of E-Mail Involving Protected Health Information ("PHI")

1. Impermissible Content of External E-Mail Messages. External e-mail messages should not be used for transmitting or discussing PHI that is particularly sensitive. E-mail messages shall not communicate or refer to the following: (a) AIDS or HIV diagnosis; (b) results of HIV antibody testing; (c) results of hepatitis antigens testing; (d) a diagnosis of substance abuse; (e) results of drug testing; (f) test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy; (g) a diagnosis of substance abuse; (h) elder or child abuse/neglect; or (i) a diagnosis of a mental disorder.

2. Security of E-Mail Communications. Password protected screen-savers shall be in use on all desktop workstations where e-mail communications containing PHI might be viewed, and e-mail containing PHI must not be left open on the computer screen when the DHS User leaves the workstation. E-mail containing PHI may be forwarded to third parties **only** when either (1) those parties are affiliated with DHS and are responsible for the care of the patient, or (2) the patient's written consent is obtained, or (3) all information which could be used to identify the patient has been removed from the e-mail. Prior to sending messages, the "TO:" field should be double-checked for the name of the appropriate recipient, in order to avoid the inappropriate transmission of PHI.

3. E-Mail Regarding Urgent Matters Prohibited. E-mail containing PHI shall not be relied upon for communications regarding matters requiring urgent communication with a patient or a health care professional. However, e-mail may be used as a supplement to telephone calls and other appropriate methods for urgent communication, provided that these additional methods for attempting to communicate with the patient or health care professional are documented in the medical record.

4. Acknowledgement of Messages and Confirmation of Health Care Professional's Actions. Where available, DHS health care professionals should use the "return receipt notification" function with each e-mail message containing PHI sent to another health care professional or patient. If notification of receipt is not received within a reasonable time, considering the subject matter of the message, the health care professional (or his or her designee) should follow up with the patient or health care professional by telephone or other appropriate form of communication. When an action requested by the patient or health care professional via e-mail has been completed, such as submission of a prescription refill, scheduling of an appointment or completion of a consultation request, the patient or health care professional shall be notified by reply e-mail.

5. Special Rules for the Use of E-Mail Between Health Care Professionals and Patients.

5.1 Initiation of E-Mail Communication with a Patient. The use of e-mail between any User and a patient shall occur only when the patient has requested that e-mail be used for communications, and only after the patient has signed an E-Mail Consent Form entitled "Informed Consent to the Use of E-Mail." The health care professional responsible for the patient's treatment is responsible for verifying the patient's written signature on the E-Mail Consent Form, and co-signing that Form, prior to the first e-mail communication from DHS to the patient. The E-Mail Consent Form shall be made a part of the patient's medical record.

5.2 Periodic Confirmation of Patient's Desire to Receive E-Mail Communication. Every six (6) months, or at each clinical encounter between a health care professional and a patient who has signed an E-Mail Consent Form, whichever is less frequent, the health care professional or his or her designee shall verify and document on the medical record whether the patient wishes to continue receiving e-mail communications at the e-mail address listed on the E-Mail Consent Form.

5.3 Turn-Around Time for E-Mail Messages from Patient (Review And Response). Each e-mail message from a patient shall be reviewed by the health care professional or his or her designee in a timely fashion comparable to the return of telephone messages or written communications from the patient.

5.4 Escalation of Communication. Each e-mail communication from a health care professional to a patient is to include a statement substantially similar to the following:

*If at any time you believe that our e-mail communications are not meeting your needs, please contact me by telephone at ____/___-_____; by letter mail at [give address]; or make an appointment for a clinic visit by calling ___/___-_____.*

5.5 Use of Group E-mails. Special precautions must be taken with "group e-mails," or e-mail addressed to more than one patient simultaneously. E-mail messages containing PHI should not be sent to more than one patient at a time. E-mail messages to multiple patients should not contain patient names or other identifying information in the message body of the e-mail. The recipient list of patients receiving a single group e-mail should be placed in the "blind cc:" or "bcc:" address field only so that the e-mail recipients are not visible to one another.

5.6 Use of E-Mail to Transmit Clinical Laboratory Results.

5.6.1 The health care professional must obtain a California-regulation compliant authorization from the patient for the patient to receive his or her laboratory results by Internet posting or other electronic means. A patient (or his or her physician) may revoke this authorization at any time and without penalty, except to the extent that action has been taken in reliance on the authorization.

5.6.2 Under California law, e-mail may not be used to transmit the following clinical laboratory test results (and any other related results) to a patient: (i) HIV antibody test; (ii) presence of hepatitis antigens; (iii) drug abuse; and (iv) test results related to routinely

processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy.

5.7 Archiving of E-Mail Communications with Patients. A copy of each e-mail message received from or sent to a patient by a health care professional shall be made a part of the patient's medical record. The health care professional (or his or her designee) is responsible for either transmitting the message into the patient's electronic medical record or for printing a copy of the message for insertion into the patient's paper medical record.

By my signature below, I acknowledge that I have read and received a copy of the DHS Guidelines Governing the Use of E-Mail Involving Protected Health Information and agree to abide by these guidelines.

_____ _____

Signature Date

**DEPARTMENT OF HEALTH SERVICES**
**COUNTY OF LOS ANGELES**

**{Insert facility name, address, phone number, fax number}**
**FAX COVER SHEET**

Date Transmitted: _____ Time Transmitted: _____

Number of Pages (including cover sheet): _____

**TO:** _____ Fax #: _____

Facility: _____ Telephone #: _____

Address: _____

**FROM:** _____ Fax #: _____

Telephone #: _____

Comments:

_____

_____

_____

_____

**The information contained in this facsimile is privileged and confidential and is intended only for the use of the recipient listed above. If you are neither the intended recipient or the employee or agent of the intended recipient responsible for the delivery of this information, you are hereby notified that the disclosure, copying, use or distribution of this information is strictly prohibited. If you have received this transmission in error, please notify us immediately by telephone to arrange for the return of the transmitted documents to us or to verify their destruction.**

**VERIFICATION OF TRANSMISSION OF PHI**

Please contact _____ at _____ to verify receipt of this Fax or to report problems with the transmission.

I verify the receiver of this Fax has confirmed its transmission:

Name: _____ Date: _____ Time: _____
**DHS Representative**

**DEPARTMENT OF HEALTH SERVICES**
**COUNTY OF LOS ANGELES**

**{Insert facility name, address, phone number, fax number}**
**FAX COVER SHEET**

Date Transmitted: _____ Time Transmitted: _____

Number of Pages (including cover sheet): _____

**TO:** _____ Fax #: _____

Facility: _____ Telephone #: _____

Address: _____

**FROM:** _____ Fax #: _____

Telephone #: _____

Comments:

_____
_____
_____
_____

**The information contained in this facsimile is privileged and confidential and is intended only for the use of the recipient listed above. If you are neither the intended recipient or the employee or agent of the intended recipient responsible for the delivery of this information, you are hereby notified that the disclosure, copying, use or distribution of this information is strictly prohibited. If you have received this transmission in error, please notify us immediately by telephone to arrange for the return of the transmitted documents to us or to verify their destruction.**

**VERIFICATION OF TRANSMISSION OF PHI**

Please contact _____ at _____ to verify receipt of this Fax or to report problems with the transmission.

I verify the receiver of this Fax has confirmed its transmission:

Name: _____ Date: _____ Time: _____
**DHS Representative**