RANCHO LOS AMIGOS
NATIONAL REHABILITATION CENTER

ADMINISTRATIVE POLICY AND PROCEDURE

Subject: SAFEGUARDS FOR PROTECTED HEALTH INFORMATION (PHI) **Policy No.:** A154

Supersedes:	March 9, 2011	Review Date:	March 21, 2023
Origin Date:	March 9, 2011	Revision Date:	March 21, 2023

PURPOSE:
To establish safeguards that DHS must implement to protect the confidentiality of Protected Health Information (PHI).

POLICY:
Set forth below are the policies establishing minimum administrative and physical standards regarding protecting Protected Health Information (PHI) that DHS must enforce. DHS may develop additional policies and procedures that are stricter than the parameters set forth below to maximize the security 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 to reasonably safeguard protected health information from any intentional or unintentional use or disclosure that violates DHS Privacy Policies.

DHS workforce members must reasonably safeguard PHI to limit incidental uses or disclosures made according to an otherwise permitted or required use or disclosure.

DEFINITIONS:
Internal E-Mail means e-mail sent between or among DHS users using a DHS-provided E-mail account. Internal E-Mail is encrypted and secure.

External E-Mail means e-mail sent using a third-party e-mail account from outside of DHS. External E-mail includes e-mail sent using a web-based e-mail system furnished through a foreign Internet service, regardless of whether the e-mail is sent from within a DHS facility. Protected health information means individually identifiable information relating to an individual's past, present, or future physical or mental health or condition, the provision of health care to an individual, or the past, present, or next payment for the health care provided to an individual.

Particularly Sensitive Health Information means protected health information generally considered highly confidential, including, but not limited to, mental health, drug and alcohol abuse, and infectious 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 the entity pays them.

PROCEDURE:

A. **Administrative Safeguards**

1. **Oral Communications.** DHS workforce members 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 to prevent unnecessary disclosures of protected health information. Patient identifying information only should be disclosed during 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. Speaker phones only should be used in private spaces.

2. **Cellular Telephones.** The use of Cellular phones is not prohibited as a means of disclosing PHI. However, their use poses a higher risk of interception than legacy landline telephones. Landline telephones should be used if the conversation involves 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 under **DHS Policy No. 361.6, "Right to Request Confidential Communications of Protected Health Information."** However, each provider or clinic should limit the amount of protected health information disclosed in a telephone message. The content of appointment reminders should not directly or indirectly reveal Particularly Sensitive Health Information. Telephone messages regarding test results or data 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 emergencies or if required by a government agency. If Particularly Sensitive Health Information must be faxed, the recipient should be notified immediately before the transmission, and the sender should directly confirm that the transfer 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."** PHI may be faxed to an individual if they request access to their protected health information under **DHS Police 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 the 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 phone numbers of new recipients should be confirmed before 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 misdirected faxes containing protected health information should be investigated and mitigated under **DHS Policy No. 361.26, "Mitigation."**

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

6. **Destruction Standards.** Protected health information must be discarded to preserve 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 appropriately labeled containers and adequately disposed of regularly.

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

c. Centralized bins or containers used for disposing of 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 types of physical barriers 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 access 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 from DHS management.

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

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

D. **Escorting Visitors and Patients**

1. 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 not part of DHS' Workforce should not be in areas where patients are being seen or treated or where PHI is stored without appropriate supervision.

E. **Computer/Workstations**

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

   a. Use of polarized screen filters or other computer screen overlay devices that shield information on the screen.

   b. Placement of computers out of the visual range of persons other than the authorized user.

   c. Clearing information from the screen when not being used.

   d. Using password-protected screensavers when the computer workstation is 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 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 adequately secured.

   - Become familiar with a departmental contingency plan.

   - Ensure that areas used to store PHI are adequately secured and that only authorized personnel can access these locations.

G. **Use of Electronic Systems**

1. DHS shall implement a combination of administrative, physical, and technical safeguards to protect PHI in electronic communications networks, including
   a. security awareness training of DHS Users concerning the transmission of PHI over the electronic communications network;

   b. Implementation of E-Mail Guidelines (see section G.2.c below);

   c. periodic review of this policy and procedure and E-Mail Guidelines with DHS Users to confirm compliance;

   d. repeated security reminders;

   e. Use of password-protected screen savers and exercise of due diligence to ensure that electronic systems used for transmission or storage of PHI are protected from viewing by unauthorized persons; and

   f. Other applicable safeguards are outlined in this policy.

2. **E-mail:**
   a. Internal E-Mail. Internal E-mail (i.e., within the secure DHS networks) is permitted to transmit PHI. Users shall be provided unique usernames and passwords for access to their E-mail accounts and must comply with the DHS Acceptable Use Policy.

   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 users, which are necessary to ensure appropriate patient care and to be carried out payment and health care operations activities. De-identified information is to be used in place of PHI whenever feasible.

   c. All DHS users who use E-mail to transmit PHI shall sign the form acknowledging they have read and received a copy and agree to abide by the "Guidelines Governing the Use of E-mail Involving PHI.

   d. Replying to External E-Mail with PHI. DHS users typically receive many External E-mails 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-main with PHI in the same manner as if the DHS user initially created it.

   e. Audits of outbound E-mail communications will be periodically performed to ensure that the use of E-mail to transmit PHI is as per 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 defined by the DHS Network Security Architecture and County guidelines for Wireless Network Security is not permitted and must be removed from service.

4. **Electronic Transmission of Clinical Laboratory Tests**
   a. The Healthcare professional must obtain California-compliant authorization from the patient for the patient to receive their laboratory results by Internet posting or other electronic means. (Cal. Health & Safety Code §123148(b)(1)). A patient (or their 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. the 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. If a healthcare professional arranges for the electronic transmission of test results. In that case, the results must be delivered to the patient reasonably, 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 another electronic manner, access must be restricted by using a secure personal identification number.

   d. If the patient asks to receive their 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**
   1. This policy will be retained for at least six (6) years from its creation or when it was last in effect, whichever is later.

REFERENCES:
Code of Federal Regulations 45 § 164.530 ©) (1)
DHS Policy No. 361.6, Right to Request Confidential Communications of Protected Health Information
DHS Policy No. 361.26, Mitigation
RLANRC Admin Policy A149, Access of Individuals to Protected Health Information (PHI)/Designated Record Set