PRIVACY AND SECURITY PROTECTIONS
FOR THE REMOVAL AND TRANSPORT OF PROTECTED HEALTH INFORMATION

PURPOSE

The purpose of this policy is to set forth controls related to removal of Protected Health Information (PHI) or Personal Information (PI) from the medical center and transport of medical information within the medical center. This policy does not replace IT Security policies for protection of electronic patient information including requirements related to emailing patient information.

POLICY STATEMENT

Stanford Hospital and Clinics (including all SHC-affiliated locations), Lucile Packard Children's Hospital (including all LPCH-affiliated locations), and the Stanford University School of Medicine (collectively, "Stanford Medicine") are committed to complying with state and federal requirements related to the privacy and security of patient information. Workforce Members at Stanford Medicine, as well as those with whom Stanford Medicine conducts its business, have a legal and ethical responsibility to maintain the confidentiality, privacy and security of all PHI/PI, to protect PHI/PI at all times and to guard against the loss of, or unauthorized access to, use or disclosure of, PHI/PI when removing it from the medical center up through its return, and when transporting it within the medical center. Such removal and transport of PHI/PI shall not occur in a manner inconsistent with this policy. Principles and procedures in this policy apply to PHI/PI in all media, including paper and electronic format. Consistent with other policies, PHI/PI that is removed from the premises should never be verbally discussed with any unauthorized person.

DEFINITIONS

Protected Health Information ("PHI") is defined as information that (i) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (iii) that identifies the individual, or provides a reasonable basis to identify the individual. PHI does not include employment records held by Stanford Medicine in its capacity as an employer, or information that has been de-identified in accordance with the HIPAA Privacy Standards.

Personal Information ("PI") is a person's first name and last name, or first initial and last name, in combination with any one of the following data elements that relate to such person:

- Social Security Number (SSN);
- Driver's license or state-issued identification card number; or
- Financial account number, credit or debit card number (e.g., health insurance policy number).

Personal information shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

De-identification is defined as the process by which PHI is stripped of specific data elements, as defined by HIPAA, in order to assure that personal identities cannot readily be identified from data sets.

Workforce Members are defined as faculty, employees (including temporary employees), researchers, volunteers, trainees, and other persons whose conduct, in the performance of work, is under the direct control of Stanford Medicine, whether or not they are paid by Stanford Medicine.

Supervisor: For the purposes of this policy, *Supervisor* is used in the context of approval for a Workforce Member to remove PHI/PI from the medical center or transport PHI/PI within the medical center. It is understood that from time-to-time the duties of senior operational leadership (Directors and above) and faculty will require them to conduct Stanford Medicine business for which this policy requires Supervisor approval. Such approval for senior operational leadership and faculty is self-granted, provided that they have ensured that all safeguards and other privacy and security controls are in place. For research activities, *Supervisor* means the Principal Investigator or Protocol Director.

Medical Center is any location owned, leased or operated by Stanford Medicine, wherever located.

PRINCIPLES

1. PHI/PI shall be treated as confidential and shall be safeguarded according to Stanford Medicine policies at all times.

2. Treatment, payment, healthcare operations, education, IRB-approved research and other Stanford Medicine business involving the permissible use or disclosure of PHI/PI should be conducted within the medical center whenever feasible. Removal of PHI/PI from the medical center by Workforce Members shall occur solely for job-related purposes and with the approval of the Workforce Member's Supervisor. Removal of PHI/PI from the medical center should not be approved for reasons related to the convenience of the Workforce Member, but rather for instances where the work requiring the PHI cannot practically be conducted on-site in a timely manner, and only after due consideration of alternative ways to remotely perform the work, such as VPN access to PHI/PI or secure scanning of PHI/PI for access from the remote site.

3. The Workforce Member taking the PHI/PI off-site and the approving Supervisor are responsible for ensuring that only the minimum amount of PHI/PI necessary to perform the off-site work is approved and removed from the medical center. De-identified patient information or limited data sets shall be used whenever possible. The approving Supervisor and the Workforce Member removing the PHI/PI, or the Workforce Member transporting the information within the medical center, should be able to account for every element of PHI/PI removed from or transported within the medical center, whether electronic or paper, and should be able to reconstruct the exact PHI/PI that was removed from or transported within the medical center.

4. Appropriate safeguards shall be diligently followed regarding secure transport of PHI/PI off-site and within the medical center. PHI/PI must be in the immediate personal possession of the workforce member at all times during transport, for example, from the time the PHI/PI is taken from the medical center to the time of arrival at the off-site location, or from location-to-location within the medical center.

5. Appropriate safeguards shall be diligently followed regarding securing PHI/PI at the off-site location. PHI must be secured in a manner so that it cannot be accessed by unauthorized individuals.

6. PHI that is lost, stolen, accessed viewed or reviewed by unauthorized individuals, or the confidentiality of which has been otherwise compromised, shall be reported immediately by the Workforce Member to the Privacy Office for their institution for appropriate investigation, including the filing of police reports when appropriate. Reports must be made immediately, including nights and weekends, to:

SHC/LPCH Privacy Office:
From off-campus phone: 650-723-8222; Pager 25584
From any Stanford Medicine phone: 38222; Pager 25584
privacyofficer@stanfordmed.org,
Privacy Officer (during regular business hours) at 650-724-2572

School of Medicine Privacy Office:
medprivacy@stanford.edu
650-725-1828

PROCEDURES

1. PHI should be saved or stored on secure medical center network servers whenever feasible. Saving or storing PHI/PI on computer or laptop hard drives, personal laptops or other personal devices, flash drives or USB drives, external drives, and other removable media is prohibited unless the device is encrypted to Stanford Medicine standards, password protected and meets other applicable Stanford Medicine security requirements.

2. Before the decision is made by the Workforce Member and the Workforce Member's supervisor to remove electronic PHI from the premises, IT Security must be contacted to determine whether a viable alternative is available to remotely access the PHI/PI needed to perform the job-related work.

3. PHI/PI should not be printed at off-site locations, for example, home or public printers, unless a Stanford Medicine business need exists to do so.

4. Safeguards must be in place to prevent unauthorized individuals, such as family members, conference attendees or the general public, from viewing or accessing PHI/PI at off-site locations.

5. PHI/PI must be safeguarded during transport and in the personal possession of the Workforce Member at all times. PHI shall not be left unattended in publicly-accessible locations.

6. PHI/PI transported for purposes such as off-site storage, office relocation and new location openings shall be safeguarded to prevent the loss of or unauthorized access to PHI/PI. Only medical center approved off-site storage locations may be used for storing records, documents and electronic media containing PHI/PI. Records and documents containing PHI must be inventoried before off-site storage. See Appendix B for securing documents and records containing PHI/PI for off-site storage or office/department relocation

COMPLIANCE

1. All Workforce Members are responsible for ensuring that individuals comply with those policy provisions that are applicable to their respective duties and responsibilities.

2. Workforce Member failure to protect the privacy, confidentiality, and security of patient information is detrimental to the mission, goals, and operations of Stanford Medicine. Serious consequences can result from failing to protect patient information, up to and including termination.

3. Violations of this policy will be reported to the Privacy Office and any other department as appropriate or in accordance with applicable Stanford Medicine policy. Violations will be investigated to determine the nature, extent, and potential risk to Stanford Medicine**.**

APPENDIX A

GUIDELINES FOR SUPERVISORS WHEN AUTHORIZING REMOVAL/TRANSPORT OF PHI/PI

- Ensure that there is no other secure way to access the requested PHI/PI, e.g., via VPN to a secured network.
- Ensure that the request is reasonable and meets the minimum necessary standard.
- Ensure that the individual requesting the PHI/PI has a reasonable plan in place to adequately safeguard/protect the information, e.g. storage on an encrypted flash drive or other mobile device.
- Removal of paper PHI/PI should be a "last resort" only, when no other secure alternatives exist. If paper PHI/PI is to be removed, the requestor must have a plan in place to safeguard the information, which should include a detailed inventory of the information (i.e. names and specific data elements).
- Instruct the requestor to immediately report the loss or theft of PHI/PI (whether on an encrypted device or not) to the Privacy Office.

GUIDELINES FOR WORKFORCE MEMBERS REQUESTING TO TRANSPORT/REMOVE PHI/PI

- Secure network options for accessing the requested PHI/PI must first be explored before PHI/PI can be removed from the Stanford Medicine campus.
- If secure network access is not available, then consider only Stanford Medicine-approved, secure electronic methods for removing the PHI/PI, e.g. webmail, encrypted mobile devices, Stanford Medicine-approved cloud storage providers, etc.
- When accessing webmail via a non-Stanford Medicine computer, **do not** open any attachments that might contain PHI/PI, as a copy of that PHI/PI will remain on that computer.
- Removal of paper PHI/PI should be a "last resort" only, when no other secure alternatives exist. If paper PHI/PI is to be removed, the requestor must have a plan in place to safeguard the information, which should include a detailed inventory of the information (i.e. names and specific data elements).
- Paper PHI must be kept with the requestor at all times during transit to and from the Stanford Medicine campus.
- Paper PHI/PI must be stored in locked filing cabinets, storage lockers, or bags when not in transit.
- Immediately report the loss or theft of PHI/PI (whether on an encrypted device or not) to the Privacy Office.

APPENDIX B

Safeguards for Removing PHI for Off-Site Storage and Relocation

Paper documents and files

1. Inventory files and document types in each box to account for all documents.
2. Complete a packing or inventory slip for each box with the inventoried items. Give a copy of the slip to the off-site storage contact or mover and keep a copy for your records. Note: Appropriate business associate agreements must be in place for contractors who will be assisting in moving and storing patient information if such services require access to PHI.
3. Do not place any patient names or other PHI on the packing slip.
4. Place a clearly marked label on the outside of your box marked "Confidential: Special Handling".
5. Seal boxes with tape or use totes with locking clips. Note: Documents shipped via courier or USPS, Fedex, UPS or other carrier must be safeguarded as follows:
    a. Place documents in sealed envelopes marked "Confidential".
    b. Place the sealed envelope(s) in a larger envelope or box for affixing the shipping label.
    c. Place a face sheet with the disclaimer in Appendix B in each envelope or box.
6. Do not place boxes with PHI unattended in hallways or other unsecured areas.
7. If records and documents with PHI are no longer needed, dispose of the documents in secure shred bins. Be careful not to dispose of PHI in bins intended for disposal of newspapers and magazines. When cleaning out desks in preparation for a move, be careful not to inadvertently throw documents with PHI into the trash.

Packing Slip Cover Sheet

Use this cover sheet when shipping documents containing patient information in accordance with this policy:

A. Recipient's Information	**B. Sender's Information**
Name:	Name:
Facility:	Facility:
Telephone Number:	Telephone Number:
Address:	Address:
**** CONFIDENTIALITY NOTICE **** Documents contained in this package may contain confidential information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this package in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this package in error, please notify the sender immediately by calling the phone number above to arrange for destruction of these documents. Thank you.	