

Privacy and Security of Health Information (HIPAA)

- Authority** This Guide Memo was approved by the Vice President for Business Affairs and Chief Financial Officer.
- Applicability** This policy applies to all staff, faculty, physicians, volunteers, students, consultants, contractors and subcontractors who are performing as part of the workforce of the Stanford University HIPAA Components, except University-sponsored ERISA health benefit plans and Stanford Hospital and Clinics (“SHC”), including Menlo Health Alliance, and Lucille Packard Children’s Hospital at Stanford, which have separate HIPAA policies.
- Summary** This Guide Memo describes Stanford University’s implementation of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its regulations (the “Privacy Rule” and the “Security Rule”) governing the protection of identifiable health information by health care providers and health plans. It references the Stanford University HIPAA Manual which contains more complete HIPAA policies. The policies maintained in the manual outline more specific rights of individuals regarding their protected health information (“PHI”) as well as the operational and system requirements to comply with the Privacy and Security Rules. Section headings of this Guide Memo are:
1. THE PRIVACY RULE
 2. THE SECURITY RULE
 3. STANFORD UNIVERSITY HIPAA COMPONENTS DESIGNATION
 4. PRIVACY AND SECURITY ADMINISTRATION
 5. POLICIES AND PROCEDURES
 6. SAFEGUARDS
 7. REQUESTS FOR ADDITIONAL RESTRICTIONS
 8. WAIVER OF RIGHTS
 9. TRAINING
 10. VIOLATIONS
 11. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS
 12. SANCTIONS
 13. EVALUATION AND REPORTING
 14. FOR MORE INFORMATION

1. THE PRIVACY RULE

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) Privacy Rule limits Stanford University’s use and disclosure of information that could potentially associate an individual’s identity with his or her health information. Stanford University may not use or disclose PHI except as authorized by the individual, or as permitted or required by law. Use or disclosure of health information that does not have the potential to reveal an individual’s identity is not limited.

2. THE SECURITY RULE

The Security Rule requires Stanford University to implement administrative, technical, and physical safeguards to ensure the confidentiality, integrity and availability of PHI that is maintained in an electronic form (“ePHI”) and to protect ePHI against any reasonably anticipated threats or hazards, unauthorized uses or disclosures. The Security Rule protects ePHI stored in University systems, during processing, and during transmission.

3. STANFORD UNIVERSITY HIPAA COMPONENTS DESIGNATION

The portions of Stanford University that provide health care, or share PHI with those portions, are “health care components” and are known collectively as the “Stanford University HIPAA Components”. Stanford University has authorized its Privacy Officer to designate the health care components to be included in the Stanford University HIPAA Components. A list of the schools, departments and functions that have been designated as part of the Stanford University HIPAA Components can be found in the Stanford University HIPAA Manual at <http://hipaa.stanford.edu/manual/> or requested from the University Privacy Officer. Anyone who believes that his or her department or program uses or discloses PHI and should be designated as part of the Stanford University HIPAA Components should contact the University Privacy Officer.

In addition, the Stanford University HIPAA Components have joined with Stanford Hospital and Clinics (“SHC”), including Menlo Health Alliance, and Lucille Packard Children’s Hospital at Stanford (“LPCH”), which are together referred to as the “Hospitals”, to form a single affiliated entity under the Privacy and Security Rules, known as the Stanford Affiliated Covered Entity. By combining as a single affiliated entity, the Stanford University HIPAA Components and the Hospitals have the greatest flexibility to share information with one another to accomplish their missions.

4. PRIVACY AND SECURITY ADMINISTRATION

a. Privacy Officials

Stanford University has designated a HIPAA privacy officer (the “University Privacy Officer”) for the Stanford University HIPAA Components and the Stanford Affiliated Covered Entity. The University Privacy Officer is responsible for the development and implementation of the policies and procedures necessary to comply with the Privacy Rule. Contact information for the University Privacy Officer is located in Section 14, below.

The University Privacy Officer may request that local privacy officials are designated by a school, department or program included in the Stanford University HIPAA Components (collectively and individually referred to as “program”) as necessary in order to implement the policies within their program effectively. Programs will promptly comply with any such request.

b. Security Officials

Stanford University has designated a HIPAA security officer (the “Stanford Information Security Officer”) for the Stanford University HIPAA Components. The Stanford Information Security Officer is responsible for the security of Stanford University HIPAA Components ePHI, including development of the policies and procedures necessary to comply with the Security Rule and the implementation of security measures to protect ePHI. Contact information for the Stanford Information Security Officer is located in Section 14, below.

The Stanford Information Security Officer may designate local security officials (“delegates”) as necessary to facilitate the implementation of policies, local procedures, and security measures.

5. POLICIES AND PROCEDURES

The University Privacy Officer has developed policies and guidelines designed to keep Stanford University in compliance with the Privacy Rule. The University Privacy Officer may add or modify policies and guidelines as necessary and appropriate to incorporate changes in the law or to improve the effectiveness of compliance with the Privacy Rule. The Stanford Information Security Officer has developed policies and guidelines to comply with the Security Rule and may add or modify those policies and guidelines as necessary and appropriate to improve Security Rule compliance.

These policies are designated as Stanford University HIPAA Privacy and Security Policies and can be obtained through the Stanford University HIPAA Manual available at <http://hipaa.stanford.edu/manual/> or by contacting the University Privacy Officer or Stanford Information Security Officer, as applicable. Each program included in the Stanford University HIPAA Components must develop, implement, document, and train its workforce on the procedures necessary to be in compliance with the Stanford University HIPAA Manual and this Administrative Guide Memo 23.10. For information concerning specific program procedures, workforce members should contact the local privacy or security official, as appropriate, or his or her supervisor.

Programs will comply with requests by the University Privacy Officer, the Stanford Information Security Officer, the Office of the General Counsel and/or the Internal Audit Department to make written procedures and training materials available for review.

6. SAFEGUARDS

The Stanford University HIPAA Components will institute reasonable and appropriate administrative, technical, and physical safeguards to protect PHI from any intentional, incidental or unintentional use or disclosure that is in violation of the requirements of HIPAA, the Privacy Rule, the Security Rule or the Stanford University HIPAA Manual.

Please see the Stanford University HIPAA Manual for more details at <http://hipaa.stanford.edu/manual/>.

7. REQUESTS FOR ADDITIONAL RESTRICTIONS

Under the HIPAA Privacy Rule, an individual has the right to request that the Stanford University HIPAA Components use and/or disclose their PHI only to carry out treatment, effect payment, or further health care operations. The Stanford University HIPAA Components are not required to grant such requests; however, they will consider and respond to such requests in a timely manner.

Requests for additional restrictions must be forwarded to and approved by the University Privacy Officer. If the University Privacy Officer agrees to an individual's request for restrictions on the use or disclosure of PHI, the program must inform the individual that the restriction granted only applies to the PHI within that program's control.

To ensure compliance with additional privacy protections granted by the Stanford University HIPAA Components, its workforce is expected to review an individual's records for possible restrictions before using or disclosing PHI.

8. WAIVER OF RIGHTS

The Stanford University HIPAA Components will not require individuals to waive their rights under HIPAA as a condition of the provision of treatment or payment, except where treatment may be legally conditioned upon the signing of an authorization (e.g., research involving treatment).

9. TRAINING

The Stanford University HIPAA Components will train members of its workforce, including management, on the privacy and security policies contained in the Stanford University HIPAA Manual at <http://hipaa.stanford.edu/manual/> and program procedures to the extent necessary or appropriate for the members of the workforce to carry out their functions. New members of the workforce for whom HIPAA training is necessary or appropriate will be trained prior to initial contact with PHI and in no event later than 30 days from the first date of employment. Each member of the workforce whose functions are affected by a material change in the policies or procedures will be trained on those changes in a timely manner, but normally not later than 30 working days from the effective date of the change. Programs will document that workforce training has been completed and will retain these records in the format requested by the University Privacy Officer and Stanford Information Security Officer. Training documentation will be provided upon request to the University Privacy Officer or the Secretary of the United States Department of Health and Human Services.

The Stanford Information Security Officer or delegate will implement a security awareness program to instruct all workforce members on good security practices. The content of the security awareness program will include, but not be limited to information about (i) guarding against, detecting and reporting malicious software, (ii) monitoring log-in attempts and reporting discrepancies, and (iii) creating, changing and safeguarding passwords. The program will include periodic updates and reminders on pertinent security measures and issues, including environmental and operational changes affecting the security of ePHI.

10. VIOLATIONS

Anyone who knows or has reason to believe that the Privacy Rule and/or Security Rule, the policies contained in the Stanford HIPAA Manual, the policies contained in this Administrative Guide Memo 23.10, or any program procedure developed to implement these regulations and policies have been violated should report the matter promptly to his or her supervisor, a local HIPAA official, the University Privacy Officer or Stanford Information Security Officer, as appropriate. All reported matters will be investigated in a timely manner and, when possible, should be handled confidentially.

If the workforce member requires anonymity, he or she may also report such matters to the Institutional Compliance Hotline (<http://institutionalcompliance.stanford.edu/report/>). If the workforce member does not have internet access, he or she may contact Institutional Compliance at 650-725-0076.

To the extent practical, any known harmful effect from a violation of the Privacy Rule or the Security Rule or a security incident will be mitigated. Where appropriate, sanctions will be considered and imposed by the program and/or the University. Programs should document all investigations, resolutions, remedies and sanctions, and forward a copy of such documentation to the University Privacy Officer or Stanford Information Security Officer, as appropriate.

11. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

The Stanford University HIPAA Components will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient, physician, employee, or any other person for exercising his or her rights, or for participating in any process, established under the Privacy Rule or Security Rule, including submitting a complaint or reporting a violation. Any attempt to retaliate against a person for reporting a violation in accordance with paragraph 10, above, may itself be considered a violation of this policy and may result in sanctions. An individual who raises concerns about any act or practice allegedly made unlawful by the Privacy Rule or the Security Rule, however, must have a good faith belief that the act or practice is unlawful, and the manner of raising such concerns must be reasonable and not violate the Privacy Rule or Security Rule.

12. SANCTIONS

Violations of the Privacy Rule or Security Rule may, under certain circumstances, result in civil or criminal penalties. Members of the workforce who violate the Privacy Rule, the Security Rule, policies contained in this Guide Memo 23.10 or the Stanford University HIPAA Manual at <http://hipaa.stanford.edu/manual/>, or any program's procedures implementing these policies, may be subject to disciplinary action up to and including termination of employment, contract, or other relationship with the University.

13. EVALUATION AND REPORTING

Each program will provide to the University Privacy Officer or Stanford Information Security Officer all requested information in order that the University Privacy Officer or Stanford Information Security Officer may (i) adequately address complaints, (ii) respond to requests from the Secretary of the United States Department of Health and Human Services (HHS) or other HHS official and (iii) inform Stanford University or Hospital leadership about compliance with the Privacy and Security Rules.

Stanford University HIPAA Components will periodically, and when deemed necessary in response to environmental or operational changes affecting the security of ePHI (e.g., newly identified security risks, newly adopted technologies), conduct a technical and non-technical evaluation of its security safeguards to establish the extent to which its security policies and procedures meet the requirements of the Security Rule; and (ii) document its compliance with the Security Rule.

14. FOR MORE INFORMATION

- a. **Questions** – If you have questions about these policies, please contact your supervisor. Department management should contact the appropriate program official and/or the University Privacy Officer (with respect to the Privacy Rule) or Stanford Information Security Officer (with respect to the Security Rule) with any questions related to the interpretation of these policies and/or the development of departmental procedures. It is important that all questions be resolved as soon as possible to ensure compliance with the Privacy Rule and Security Rule.

University Privacy Officer – Contact the University Privacy Officer at privacyofficer@stanford.edu or call 650-723-3331.

Stanford Information Security Officer – Contact the Stanford Information Security Officer at securityofficer@stanford.edu.

- b. **HIPAA Website** – The Stanford University HIPPA Manual and definitions of terms are available to the workforce at <http://hipaa.stanford.edu>.