

Privacy and Security of Health Information (HIPAA)

- Authority** This Guide Memo was approved by the Vice President for Business Affairs and Chief Financial Officer and the Vice President of Human Resources.
- Applicability** This policy applies to all staff, faculty, physicians, volunteers, students, consultants, contractors and subcontractors who are part of the Stanford University HIPAA Components and the Stanford University Group Health Plan (“Group Health Plan”) workforce. Stanford Hospital and Clinics (“SHC”), including Menlo Health Alliance and Lucile Packard Children’s Hospital (“LPCH”), and their respective ERISA health benefit plans 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 (“Privacy Rule” and “Security Rule”) governing the protection of identifiable health information by health care providers and health plans. The portions of Stanford University that are impacted by HIPAA include the Stanford University HIPAA Components and the Group Health Plan, defined in Sections 3 and 4, respectively.

This Guide Memo references Stanford University HIPAA Components policies that can be found on the University HIPAA website at <http://hipaa.stanford.edu> and the Group Health Plan HIPAA policies. The Group Health Plan maintains HIPAA policies and procedures in its Resource Library on the HR network server shared drive (“Benefits”) accessible to Benefits staff. These policies 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 are:

1. THE PRIVACY RULE
2. THE SECURITY RULE
3. STANFORD UNIVERSITY HIPAA COMPONENTS DESIGNATION
4. GROUP HEALTH PLAN
5. PRIVACY AND SECURITY ADMINISTRATION
6. POLICIES AND PROCEDURES
7. SAFEGUARDS
8. TRAINING
9. VIOLATIONS
10. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS
11. SANCTIONS
12. EVALUATION AND REPORTING
13. 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 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 on the Stanford University HIPAA website at <http://hipaa.stanford.edu/> 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 Stanford Hospital and Clinics (“SHC”), including Menlo Health Alliance and Lucile 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. GROUP HEALTH PLAN

As an employer, Stanford University sponsors and maintains various ERISA health benefits plans that comprise the Group Health Plan. The Group Health Plan is a separate covered entity from the Stanford University HIPAA Components and, as such, has separate HIPAA privacy and security policies. The list of the plans included in the Group Health Plan can be found on the Stanford University HIPAA website at <http://hipaa.stanford.edu/> or requested from the University Privacy Officer.

5. 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, the Stanford Affiliated Covered Entity and the Group Health Plan. 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 13.

The University Privacy Officer may request that local privacy officials be designated by a school, department or program included in the Stanford University HIPAA Components or by the Group Health Plan (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 “Chief Information Security Officer”) for the Stanford University HIPAA Components and the Group Health Plan. The Chief Information Security Officer is responsible for the security of Stanford University HIPAA Components and Group Health Plan 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 Chief Information Security Officer is located in Section 13.

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

6. POLICIES AND PROCEDURES

The University Privacy Officer has developed policies and guidelines designed to keep the Stanford University HIPAA Components and the Group Health Plan 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 Chief 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.

Each of the Stanford University HIPAA Components programs and the Group Health Plan must develop, implement, document, and train its workforce on the procedures necessary to be in compliance with the appropriate HIPAA policies and this Administrative Guide Memo. 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 Chief 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.

7. SAFEGUARDS

The Stanford University HIPAA Components and the Group Health Plan 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 policies.

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

8. TRAINING

The Stanford University HIPAA Components and Group Health Plan will train members of their respective workforces, including management, on the Stanford University privacy and security policies 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 Chief Information Security Officer. Training documentation will be provided on request to the University Privacy Officer or the Secretary of the United States Department of Health and Human Services.

The Chief Information Security Officer 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 (a) guarding against, detecting and reporting malicious software, (b) monitoring log-in attempts and reporting discrepancies, and (c) 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.

9. VIOLATIONS

Anyone who knows or has reason to believe that the Privacy Rule and/or Security Rule, the Stanford University HIPAA policies, 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 Chief Information Security Officer, as appropriate. All reported matters will be investigated in a timely manner and, when possible, will 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) 721-1667.

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 Chief Information Security Officer, as appropriate.

10. REFRAINING FROM INTIMIDATING OR RETALIATORY ACTS

The Stanford University HIPAA Components and Group Health Plan 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 Section 9 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.

11. 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 or the Stanford University HIPAA policies, 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.

12. EVALUATION AND REPORTING

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

Stanford University HIPAA Components and the Group Health Plan 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 document its compliance with the Security Rule.

13. FOR MORE INFORMATION

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 the Chief 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.
- **Chief Information Security Officer** – Contact the Chief Information Security Officer at securityofficer@stanford.edu.