1.6.2 PRIVACY AND SECURITY OF HEALTH INFORMATION (HIPAA)

Last updated on: 03/15/2013

Formerly Known As Policy Number: 16.2

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 on the University HIPAA website and the Group Health Plan HIPAA policies. The Group Health Plan maintains HIPAA policies and procedures in the Resource Library section of the Benefits website. 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.

Authority:
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 Health Care ("SHC"), including Menlo Health Alliance and Lucile Packard Children's Hospital ("LPCH"), and their respective ERISA health benefit plans have separate HIPAA policies.

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/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 designated as part of the Stanford University HIPAA Components can be found on the Stanford University HIPAA website [3] or requested from the University Privacy Officer. Anyone who believes that his/her department or program uses or discloses PHI and ought to 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 Health Care ("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 [3] or requested from the University Privacy Officer.

5. Privacy and Security Information
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 comply 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 [3] for more details.

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 login 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, 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.

See Appendix A: Guidelines for the Implementation of Corrective Action in Matters Involving Violations of Patient, Research Participant and other Medical Information Privacy or Security.

If the workforce member requires anonymity, he or she may also report such matters to the Institutional Compliance Hotline [4]. If the workforce member does not have internet access, he or she may contact Institutional Compliance at (650) 721-COMP or 721-2667.

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 Attacks

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.

See Appendix A: Guidelines for the Implementation of Corrective Action in Matters Involving Violations of Patient, Research Participant and other Medical Information Privacy or Security.

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 Office**, privacy@stanford.edu [5] or call [6](650) 725-1828.
- **Information Security Office**, securityofficer@stanford.edu [7]

14. Appendix A: Guidelines for the Implementation of Corrective Action in Matters Involving Violations of Patient, Research Participant and other Medical Information Privacy or Security

OVERVIEW

Stanford University is committed to conducting business in compliance with all applicable laws, regulations and University policies. The University endeavors to provide a strong infrastructure that promotes a culture committed to safeguarding the privacy and security of patient, medical and research participant information. These guidelines serve a dual purpose. They provide faculty, staff, trainees, students, contractors, vendors, volunteers, and other members of the Stanford community (“workforce members”) notice of the consequences they will face for violating the Health Insurance Portability and Accountability Act (“HIPAA”), the Health Information Technology Economic and Clinical Health (HITECH) Act, the Confidentiality of Medical Information Act (“COMIA”), or other federal and state laws and regulations governing the confidentiality and security of patient information (“applicable laws”), or University policies relating to privacy and security of patient, medical and research participant information.

Separately, the guidelines provide University offices (e.g., privacy offices, human resources, academic and student affairs offices) and individual managers direction in determining appropriate consequences for workforce members who violate applicable laws or University policies that safeguard protected health information (“PHI”) and other patient medical information. These guidelines should be used in conjunction with the corrective action or discipline policy applicable to the relevant workforce member including:

- **Guide Memo 1.1.1 [8]:** Code of Conduct
- **Guide Memo 2.1.16 [9]:** Addressing Conduct and Performance Issues
- **Collective Bargaining Agreement between SEIU Local 2007 and Stanford [10]** Section 12.7
For definitions pertaining to HIPAA and frequently asked questions relating to HIPAA and other applicable laws relating to the protection of patient health information, see the University’s HIPAA [1] website.

PRINCIPLES

A. Imposition of Appropriate Sanctions

Workforce members will be sanctioned appropriately in the event that they:

1. access, use or disclose more than the minimum PHI necessary to complete their job-related functions;
2. fail to adequately protect PHI in accordance with Stanford University’s information security policies;
3. fail to promptly report a known or suspected HIPAA violation; or
4. violate any of Stanford University’s other HIPAA policies, procedures or guidelines.

Sanctions may also be imposed for failure to report a known or suspected HIPAA violation or for violating any of Stanford University’s other HIPAA policies, procedures or guidelines. Sanctions for violations of HIPAA may include, without limitation, counseling, written warning, suspension, and termination. A workforce member’s compensation and eligibility to continue in an academic or training program may also be impacted in the event of a violation. These guidelines are not intended to dictate a particular consequence in any particular situation. Rather, in consultation with the appropriate Human Resources and/or Privacy Office, managers, academic affairs and student affairs administrators have the discretion to decide:

1. at which level to start the corrective action process based on the severity of the offense, the potential or actual harm to the patient and/or the Hospital(s) or University, and any mitigating factors; and
2. whether immediate termination is justified based on the seriousness of the offense.

B. Levels of Violations

The level of a violation is determined by the severity of the privacy or security breach, whether the breach was intentional or unintentional or motivated by malice or personal gain, and the impact on the patient and/or institution. The following outlines some, but not all, types of violations and categorizes them broadly according to likely severity.

Level 1: A workforce member carelessly or inadvertently accesses PHI without a job-related need to know, or carelessly or unintentionally reveals PHI to which he/she has authorized access. Examples of Level 1 violations include, but are not limited to:

1. Leaving PHI in a public area in the workplace or disposing of it in the trash instead of shredding receptacles;
2. Misdirecting faxes, emails or other documents that contain PHI;
3. Discussing PHI in public areas where the discussion could be overheard;
4. Other behaviors reflecting carelessness or lack of judgment in handling PHI.

Level 2: A workforce member intentionally accesses PHI without authorization or seriously fails to protect PHI. Examples of Level 2 violations include, but are not limited to:

1. Intentionally accessing or asking another to access PHI without a job-related need to know, the PHI or a friend, relative, co-worker, public personality or any other individual (including searching for the
existence of a record or an address or phone number);
(2) Leaving paper files and records, computers, laptops, notebooks, smart phones or other devices containing PHI accessible and unattended;
(3) Sharing log-in IDs and passwords with others;
(4) Using personal email accounts (e.g., Hotmail, Gmail, Yahoo), cloud computing, or other media or storage devices not approved by Stanford University for transmission or storage of PHI or not meeting required security standards (such as encryption, secure email, password protection);
(5) Removing PHI from the Stanford University workplace without supervisor approval or failing to appropriately safeguard PHI if removed with supervisor approval or while in transit;
(6) Other behaviors reflecting intentional conduct or serious failure to safeguard PHI.

Level 3: A workforce member intentionally accesses, uses or discloses PHI without authorization, often motivated by willful disregard, malice or personal gain. A Level 3 violation is considered serious misconduct. Examples of Level 3 violations include, but are not limited to:

(1) Intentionally using or disclosing without a job-related need to know the PHI of a friend, relative, co-worker, public personality, or any other individual’s PHI;
(2) Accessing, using or disclosing PHI for personal purposes or gain, or with an intent to harm the patient or any third party;
(3) Discussing or disclosing PHI with any third party either directly or via social networking or blogging sites, such as Twitter and Facebook.
(4) Intentionally assisting an individual in gaining unauthorized access to PHI.
(5) Jeopardizing the integrity of Stanford University’s systems.
(6) Failing to cooperate during the investigation of a privacy or security incident.
(7) Falsifying information during a privacy investigation or reporting in bad faith or for malicious purposes.
(8) Other behaviors reflecting personal purpose or gain, malice or misconduct.

C. Considerations in Evaluating Violation for Appropriate Sanctions
Factors in determining appropriate disciplinary action may include, but are not limited to:

(1) Whether the breach was intentional or inadvertent;
(2) The nature of the breach, including whether the breach involved specially protected information such as HIV, psychiatric, substance abuse, or genetic data;
(3) The magnitude of the breach, including the number of patients and the volume of protected health information accessed, used or disclosed;
(4) The workforce member’s motive in accessing, using or disclosing PHI, and whether there was an element of malice or desire for personal gain;
(5) Whether the workforce member has committed prior HIPAA violations;
(6) The workforce member’s response or conduct during investigation;
(7) Risk of harm to the victim(s) of the breach or to the University;
(8) The existence of any compelling, aggravating or mitigating factors.

PROCEDURES
A. Prompt Reporting and Investigation

Each workforce member must report any alleged, apparent, or potential violations of HIPAA or applicable privacy and security laws promptly (within no more than twenty-four hours) to his/her supervisor/designee or to the supervisor’s supervisor. Suspected violations shall be investigated appropriately and in coordination with the relevant supervisor, Human Resources officer, and the Privacy Officer. Matters involving faculty, students or trainees should also be brought to the attention of the appropriate senior associate dean(s) which may include:

- Senior Associate Deans for Clinical Affairs—for events related to clinical faculty
- Senior Associate Dean for Medical Student Education—for events related to medical students
- Senior Associate Dean for Finance and Administration—for events related to any other individuals to whom this policy applies
- Dean, Vice Dean and Senior Associate Dean for Academic Affairs, as applicable—for events related to faculty
- Senior Associate Dean for Graduate Education and Postdoctoral Affairs—for events related to graduate students or postdoctoral scholars

Results of the investigation and any decision regarding discipline will be documented in writing and disciplinary actions will be made part of the workforce member’s personnel, training or student file. Discipline will be issued in accordance with existing discipline or corrective action policies applicable to the particular workforce member. When faculty members are involved, the Senior Associate Dean shall be consulted, and the faculty member shall have the rights outlined in relevant faculty policies and grievance procedures. The cognizant vice president or dean, or his or her designee, retains final authority concerning sanctions and will review any sanction involving suspension, dismissal, or termination before it is implemented.

In the event of a possible violation of HIPAA or applicable law involving both University and SHC or LPCH personnel, the investigation must be coordinated and any correction actions or sanctions must be consistent between the organizations. Reports to state/federal oversight agencies may be required. In addition to any internal corrective action, employees may be subject to criminal and civil penalties, and referral to applicable licensing boards.

B. Guidelines for Sanctions

The following will serve as guidelines for appropriate sanctions for violations of HIPAA or other applicable laws or policies.

**Faculty:**
Appropriate sanctions will be imposed in accordance with the Statement on Faculty Discipline, Faculty Handbook section 4.3.

**Employees, post-doctoral fellows, volunteers:**
Students enrolled in undergraduate or graduate degree programs:

- **Level 1:** Violations shall, in most cases, result in oral or written counseling and/or retraining. Repeat Level 1 violations shall be subject to further disciplinary action up to and including termination.
- **Level 2:** Violations shall, in most cases, result in a written disciplinary warning with or without an unpaid suspension, and retraining shall be required. Disciplinary action up to and including termination may be taken for repeat Level 2 violations.
- **Level 3:** Violations, in most cases, shall result in immediate termination of employment, academic appointment or ending of a volunteer assignment.

**Students enrolled in undergraduate or graduate degree programs:**

- **Level 1:** Violations shall, in most cases, result in oral counseling and/or retraining. Repeat Level 1
violations shall be subject to progressive disciplinary action up to and including termination from the program of study.

**Level 2:** Violations shall, in most cases, result in a written reprimand in the student's file and retraining. The student may also be suspended from the program of study.

**Level 3:** Violations, in most cases, shall result in immediate termination from the program of study.

**Contractors/Vendors:**
Violations of any level shall, in most cases, result in termination of the contract/business relationship and disqualification from future contractual/business relationships.