User Guidelines for HIPAA Compliance	Document No.	ITS-1028-G	Rev:	--
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	2-28-13	Revised:	--
				Page 1 of 14

Table of Contents

1 Purpose

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a broad federal law. Two components of HIPAA, the Privacy Rule and the Security Rule, govern the privacy of an individual's health information. The Privacy Rule regulates the use and disclosure of Protected Health Information (PHI). The Security Rule complements the Privacy Rule and identifies standards and implementation specifications that organizations must meet in order to be compliant. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (ePHI).

The California State University (CSU) has limited the scope of its compliance obligations by taking on "hybrid entity" status under HIPAA and formally designating CSU health care components [*Designation of Health Care Components for Purposes of the Health Care Portability and Accountability Act of 1996 (HIPAA)* - CSU Executive Order 877]. As a hybrid entity, only the designated CSU health care components, and not the entire institution, are required to comply fully with HIPAA. Although no department within CSULA has been designated by the CSU as a health care component, CSULA will implement these guidelines as minimum standards and as a best practice for ensuring the appropriate security of all health information received, maintained or transmitted (available currently or which may be created or used in the future).

2 Entities Affected by this Guideline

This guideline applies to all departments, services, clinics, programs and individuals who collect, maintain, access, transmit or receive protected health information on paper or electronically in connection with activities at CSULA.

3 Definitions

a) Administrative Safeguards: Administrative actions, policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect PHI and ePHI and to manage the conduct of the workforce in relation to the protection of that information.

b) Business Associates: Individuals or entities outside of the health care entity that receive, create or have access to individually identifiable health information and (1) perform a service on behalf of the health care entity, or (2) fit within the list of specific service providers including actuarial, claims processing, billing, benefit management, accounting, consulting, management, administrative, accreditation, data aggregation and financial services (See Third-party Service Provider).

c) Electronic Protected Health Information (ePHI): Any electronic information that is created or received by a health care provider that relates to the past, present or future physical or mental health of an individual and that identifies the individual. The definition of PHI in the Privacy and Security Rule excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) and employment records held by CSU in its role as employer.

d) Family Educational Rights and Privacy Act of 1974 (FERPA): A federal legislation in the United States that protects the privacy of students' personally identifiable information and applies to all educational institutions that receive federal funds.

e) HIPAA Privacy Rule: The standards for how protected patient health information should be controlled.

f) HIPAA Security Rule: The standards for certain health information specifically focusing on safeguarding electronic protected health information (ePHI).

g) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

h) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

i) Physical Safeguards: Physical measures, policies and procedures to protect a health care's documents, electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

j) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

k) Protected Health Information (PHI): Any information held by a health care entity which concerns health status, provision of health care or payment for health care that can be linked to an individual.

l) Technical Safeguards: Technology and the policy and procedures for its use that protect electronic health information and control access to it.

m) Third-party Service Provider: Refers to an entity that is undertaking an outsourced activity on behalf of the University or is performing system administrator duties on their offsite system that contains University protected data (e.g., vendors, vendor's subcontractors, business partners, consultants, etc.).

4 Guidelines

These guidelines address the five major sections outlined in the HIPAA Security Rule, which are:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies, Procedures and Documentation Requirements

4.1 Administrative Safeguards

Administrative safeguards address organizational controls – risk analysis and management, information system activity review, assigned security responsibility, workforce privacy and security, security awareness and training, password management, security incident procedures, contingency plans, third-party service providers (referred to as business associates in HIPAA materials) and evaluation.

4.1.1 Risk Analysis

The department manager should perform a yearly risk analysis, including a technical security assessment of systems managing ePHI, that will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of PHI and ePHI. Evaluation and risk assessment reports should be maintained for a minimum of 6 years.

4.1.2 Risk Management

Measures should be implemented to reduce risks and vulnerabilities including identifying and documenting potential risks and vulnerabilities that could impact the management of PHI and ePHI.

Policies and procedures that prevent, detect and correct security violations must be implemented.

4.1.3 Information System Activity Review

Information system activity records should be reviewed periodically – including audit logs, access reports and security incident tracking reports – to ensure that implemented security controls are effective and that ePHI has not been potentially compromised.

Measures should include:

- Enabling logging on computer systems managing ePHI.
- Developing a process for the review of exception reports and/or logs.
- Following System-wide Records/Information Retention and Disposition Schedules Implementation (System-wide Records/Information Retention and Disposition Schedules Implementation - CSU Executive Order 1031).
- Periodically reviewing and documenting compliance with the CSU and CSULA information security policies, procedures and guidelines.

4.1.4 Assigned Security Responsibility

The director of IT Security and Compliance is the individual responsible for overseeing development of the organization's information security policies and procedures.

A department that handles PHI, ePHI or systems managing ePHI should assign a department privacy and security official responsible for the adherence to security guidelines and the implementation of procedures required to protect the confidentiality, integrity and availability of PHI. This individual should coordinate information security activities with the director, IT Security and Compliance.

4.1.5 Workforce Security

The department manager should establish procedures to ensure that only authorized personnel have access to PHI and systems that manage ePHI.

Measures should include:

- Establishing a procedure that requires appropriate authorizing individual approval before any person is granted appropriate level of access to PHI, ePHI or to systems managing ePHI. The individual assigning the user name and implementing the authorized access should be different from the individual authorizing access.
- Performing appropriate background checks, where appropriate and approved by Human Resources Management, before any person is granted access to PHI, ePHI or to systems managing ePHI.
- Limiting authorized persons' access to PHI and ePHI to the extent that access to this information is appropriate for their job.
- Implementing procedures for terminating access to PHI and ePHI when the employment of a person ends or the job responsibilities of the person no longer warrants access.
- Periodically reviewing the accounts on systems managing ePHI to ensure that only currently authorized persons have access to these systems.
- Carefully managing system administrator accounts to ensure the accounts are used for only specific system administration functions. The number of these accounts should be kept to a minimum and provided only to personnel authorized to perform identified functions. Passwords or other authentication measures should be changed immediately upon the termination of systems personnel who accessed these accounts.

4.1.6 Security Awareness and Training

Department managers should ensure that timely privacy and security training, including HIPAA, FERPA and Information Security training, is provided to all employees handling health information.

Establish privacy and security training at the start of employment and at least every 2 years thereafter for all members of the workforce, including trainees, interns, students and volunteers, who have access to or are involved in the creation, transmission and storage of ePHI. Ensure that the training program includes the following: periodic security reminders (documented as to the type of reminder, its message and the date it was implemented), protection from malicious software (e.g., viruses, worms, etc.), log-in monitoring, and password management. The training program should be updated to take into account current vulnerabilities and threats.

4.1.7 Password Management

Department personnel will follow the University password standard (*ITS-2008-S Password Standards for Personal Systems*). A password stronger than designated in the University standard may be required if the department's risk analysis dictates.

4.1.8 Security Incident Procedures

Immediately upon detection of any actual or suspected breach in any type of media (e.g., electronic, paper, verbally, etc.), by any user, the incident must be reported to the ITS Help Desk or the director of IT Security and Compliance using *ITS-2812 Information Security Initial Incident Report*. Reporting should not be delayed until all information regarding an incident is gathered.

The forms *ITS-2817 Information Security Breach – Department Representative Checklist* and *ITS-2819 Information Security Incident Status Report* are to be used to document actual steps performed and strategies used to contain, eradicate and recover from a security incident and to report incident updates and prepare a final status report.

4.1.9 Contingency Plan

Procedures must be in place to respond to an emergency or system failure. Measures should include:

- Developing an emergency operation plan that minimizes the effects of a disaster and allows the organization to either maintain or quickly resume prioritized mission-critical functions.
- Procedures for responding to an emergency or occurrence that damages equipment or systems.
- Procedures to ensure exact data backup are created, maintained and retrievable to restore any loss of data (electronic and paper).
- Providing for adequate protection of the security of PHI while operating in emergency mode.
- Periodic testing of the emergency procedures with revisions made as necessary.
- Servers containing ePHI should be housed in securely managed locations that have provisions for prevention, detection, early warning of and recovery from emergency conditions created by earthquake, fire, water leakage or flooding, power disruption, air conditioning failures or other hazards.

4.1.10 Third-party Service Providers

Contracts with a third-party service provider (e.g., business associate or a CSULA employee, or office or department that performs activities that would make it a "business associate") require written confidentiality assurances that provides satisfactory assurance that appropriate safeguards will be applied to protect PHI and ePHI (see *ITS-1022-G User Guidelines for Information Security Contract Language*).

Contracts must require:

- Implementing safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the protected health information that it creates, receives, maintains or transmits.
- Ensuring that any agent, including a subcontractor, to whom it provides information, agrees to implement reasonable and appropriate safeguards.
- Reporting to the University any security incident of which it becomes aware.

- Making its policies and procedures and documentation available for purposes of determining compliance.
- Authorizing termination of the contract if the third-party provider has violated a material term of the contract.

4.1.11 Evaluation

HIPAA cites that it is a best practice to conduct an annual review to demonstrate compliance with these safeguards. CSULA, however, requires that all campus information security programs be reviewed on an annual basis. See section 4.6, Annual Review and Report, for specific department and administrator responsibilities.

4.2 Physical Safeguards

Physical safeguards are measures to protect documents, electronic information systems and related buildings and equipment from unauthorized intrusion.

4.2.1 Facility Access Controls

Access to secure locations should be limited to authorized users. Systems that manage ePHI or store PHI must be kept in areas with physical security controls that restrict access and should adhere to *ITS-1006-G User Guidelines for Securing Offices, Workspaces and Documents*.

4.2.2 Workstation Use

Inappropriate use of computer workstations can expose the University to risks, such as virus attacks, compromise of information systems and breaches of confidentiality. Only designated workstations possessing appropriate security controls will be used to access and manage ePHI. Measures should be in place to minimize inappropriate access to workstations by the public and to make workstations, systems and network inaccessible to the public. This security measure extends to the use of home machines and laptops. Laptop users should adhere to *ITS-1020-G User Guidelines for Mobile Computing*.

4.2.3 Device and Media Controls

Computers and other forms of electronic storage media that contain ePHI must have the data removed prior to reallocation within the department, within the University or before disposal. Procedures for the transfer or disposal of devices and media are included in *ITS-1017-G User Guidelines for the Safe Disposal, Transfer, or Reassignment of Electronic Storage Media*, *ITS-1021-G User Guidelines for Data Sanitization* and Administrative Procedure 507 - *Property Control*.

4.2.4 Maintenance Repairs and Modifications

Security repairs and modifications are made on a regular basis, including changing locks, routine maintenance and installing new security devices. Any maintenance repairs and modifications to physical components of the facility related to security should be documented.

4.3 Technical Safeguards

The technical safeguards section addresses topics such as access and audit controls, authentication of users, data integrity checks and transmission security (encryption).

4.3.1 Access Control

Security controls must be in place to protect the integrity and confidentiality of ePHI residing on computer systems, including applications, databases, workstations, servers and network equipment. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions.

Each user must be assigned a unique user identification. This allows the tracking of activity when that user is logged into the system and for the ability to hold a user accountable for functions performed when logged into a system.

4.3.2 Audit Controls

Reasonable and appropriate audit controls for systems that contain or use ePHI should be developed based on a risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities.

4.3.3 Integrity

Procedures should be in place to protect PHI and ePHI from improper alteration or destruction in any way.

4.3.4 Person or Entity Authentication

Controls must be in place that verify that a person seeking access to ePHI is the one claimed and to prevent unauthorized users from accessing ePHI.

4.3.5 Transmission Security

Controls must be in place that ensures that the integrity of ePHI is maintained when in transit. Secure transmission mechanisms that encrypt ePHI, as well as confirms that data integrity has been maintained should be used.

Unencrypted ePHI should not be e-mailed. Instead it should be kept in a separate shared department directory that only allows access to authorized individuals (see *ITS-1027-G User Guidelines for Encryption Security*).

4.3.6 Automatic Logoff

Users should log off the system or lock the terminal or console they are working on when their workstation is unattended. In addition, procedures should be implemented to terminate an electronic session after a predetermined time of inactivity. Automatic logoff is an effective way to prevent unauthorized users from accessing ePHI on a workstation when it is left unattended for a period of time.

4.4 Organizational Requirements

Organizational requirements require action and documentation that appropriate safeguards are implemented for PHI and ePHI.

4.4.1 Notification and Record Keeping

It is the responsibility of department personnel to report any security incidents immediately to the ITS Help Desk or the director of IT Security and Compliance. Security incidents resulting in harmful effects known to CSULA will be mitigated to the extent practical. Records of all security incidents and mitigation actions should be documented.

4.4.2 Information Security

Individuals who access, receive or otherwise handle or control protected health information on CSULA systems will do so securely and responsibly. These individuals are expected to exercise good judgment in maintaining the security of all protected health information and to continually educate themselves on information security issues.

4.4.3 Systems Administrators

Systems and network administrators will administer information systems and networks in a manner that protects the confidentiality, integrity and availability of the electronic protected health information (ePHI) that is stored in them or transmitted through them, including all systems that are connected to internet CSULA networks consistent with all applicable University policies (see *ITS-1001-G User Guidelines for Network Traffic Management*).

4.5 Policies, Procedures and Documentation Requirements

Reasonable and appropriate policies and procedures (in written or electronic form) must be implemented to comply with these guidelines. Changes to policies and procedures may be made at any time but must be documented.

4.6 Annual Review and Report

All departments, services, clinics, programs and individuals who collect, maintain, access, transmit or receive protected health information on paper or electronically are required to perform an annual review and attestation of their HIPAA compliance. These areas are responsible for the following:

- Appoint a HIPAA administrator or designee to oversee the area's HIPAA privacy and security program.
- Complete form *ITS-2810 Annual HIPAA Compliance Review* at the fiscal year-end.
- Attach completed form *ITS-2805 Information Security Risk Assessment Worksheet*.
- Submit the completed report to the director for IT Security and Compliance no later than July 15.
- The director for IT Security and Compliance will maintain a copy for CSU audit compliance file.
- The director for IT Security and Compliance will promptly submit the original to the HIPAA compliance coordinator in Human Resources Management.

- The HIPAA compliance coordinator is responsible for ensuring that all applicable reports have been submitted and verifying that the campus is fully compliant with all mandated requirements.
- The HIPAA compliance coordinator will work with the director for IT Security and Compliance to resolve any technical, physical or system non-compliant issues.

5 Contacts

a) Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

b) To report a security breach, contact the director, IT Security and Compliance at 323-343-2600 or e-mail itsecurity@calstatela.edu.

c) For questions regarding CSULA HIPAA compliance, contact the campus HIPAA compliance officer at 323-343-3676.

6 Applicable Federal and State Laws and Regulations

Federal	Title
Federal Privacy Act of 1974	**Federal Privacy Act of 1974** http://www.usdoj.gov/opcl/privacyact1974.htm This is a federal act that establishes a code of fair information practices governing the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	**Standards for Privacy of Individually Identifiable Health Information** http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf This is a federal law that protects the privacy of health records.

Federal	Title
HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment ACT (ARRA) of 2009	**HITECH Act** http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf This law modified the HIPAA rules to establish new limitations on the use and disclosure of protected health information and include provisions designed to strengthen and expand HIPAA's enforcement provisions

7 Related Documents and Resources

CSULA	Title
ITS-1001-G	**User Guidelines for Network Traffic Management** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1001-G_NetworkTrafficMgmt.pdf This guideline helps users meet established network bandwidth allocations and traffic standards to ensure that all University network and technology resources are managed securely.
ITS-1006-G	**User Guidelines for Securing Offices, Workspaces and Documents** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1006-G_SecureDocs-OfficesGuidelines.pdf This guideline helps the campus community protect offices, machines, devices and documents from unauthorized access to confidential, personal and proprietary information.
ITS-1017-G	**User Guidelines for Safe Disposal of Electronic Storage Media** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1017-G_SafeDisposalofElectronicStorageMedia.pdf This guideline outlines the steps departments and business units, students, faculty and staff should take to remove data and software and appropriately dispose of electronic equipment/devices.
ITS-1020-G	**User Guidelines for Mobile Computing** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1020-G_Mobile_Computing_I.pdf This guideline establishes an authorized method for controlling mobile computing devices that contain or access CSULA protected data.
ITS-1021-G	**User Guidelines for Data Sanitization** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1021-G_DataSanitization.pdf This guideline defines the appropriate data sanitization tools and procedures to meet security standards.

CSULA	Title
ITS-1022-G	**User Guidelines for Information Security Contract Language** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1022-G_Information_Security_Contract_Language.pdf This guideline defines the information security responsibilities and procedures that apply to all third-party service providers and provide templates with specific contract language to be included in third-party service provider agreements.
ITS-1027-G	**User Guidelines for Encryption Security** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-1027-G_EncryptionSecurity.pdf This guideline provides information on approved encryption algorithms, recommended encryption products and specific encryption tools and practices.
ITS-2006-S	**Information Classification, Handling and Disposal** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-2006-S_Information_Classification_Handling_and_Disposal.pdf This standard identifies the three levels of information classification and outlines the best practices for handling and disposing of protected data.
ITS-2008-S	**ITS Password Standards for Personal Systems** http://www.calstatela.edu/its/itsecurity/guidelines/ITS-2008-S_ITSPasswordStandards.pdf This standard provides guidance to all users regarding the security and management of passwords.
ITS-2804	**Lost/Stolen Computer/Electronic Storage Device Report** http://www.calstatela.edu/its/forms/ *Look under Information Security and Compliance* This form is used to report a lost or stolen computer or electronic storage device to University Police and IT Security and Compliance.
ITS-2810	**Annual HIPAA Compliance Review** http://www.calstatela.edu/its/forms/ *Look under Information Security and Compliance* This form is used by administrators of areas that collect, maintain, access, transmit or receive protected health information to conduct an annual review of HIPAA safeguards.
ITS-2812	**Information Security Initial Incident Report** http://www.calstatela.edu/its/forms/ *Look under Information Security and Compliance* Form used by departments to report an actual or suspected security incident to IT Security and Compliance.

CSULA	Title
ITS-2817	**Information Security Breach - Department Representative Checklist** http://www.calstatela.edu/its/forms/ *Look under Information Security and Compliance* Form used by the CSIRT department representative to document actual steps performed and strategies used to contain, eradicate and recover from a security incident.
ITS-2819	**Information Security Incident Status Report** http://www.calstatela.edu/its/forms/ *Look under Information Security and Compliance* Form used by the CSIRT department representative to record incident updates and prepare the final status report.
Administrative Procedure 507	**Property Control** http://www.calstatela.edu/univ/admfin/procedures/507.prf This procedure governs the accountability, control, inventory, movement and other responsibilities for University property.
Administrative Procedure 707	**Record Retention, Management and Disposition** http://www.calstatela.edu/univ/admfin/procedures/707.pdf This procedure establishes policy for the secure management of University records and the transfer of University records to the State Records Center, the retrieval of stored records and the destruction of obsolete records.
Chancellor's Office	**Title**
CSU Executive Order 877	**Designation of Health Care Components for Purposes of the Health Care Portability and Accountability Act of 1996 (HIPAA); Executive Order Number 877**. http://www.calstate.edu/EO/EO-877.html This Executive Order is established to govern the California State University's compliance obligations with respect to the administrative simplification rules promulgated under the Health Care Portability and Accountability Act of 1996 (HIPAA).
CSU Executive Order 1031	**System-wide Records/Information Retention and Disposition Schedules Implementation** http://www.calstate.edu/EO/EO-1031.html http://www.calstate.edu/recordsretention This Executive Order provides for the implementation of the California State University (CSU) System wide Records/Information Retention Schedules.

CSULA	Title
CSU Information Security Policy	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.
CSU HIPAA Portal	**The California State University HIPAA Portal** http://www.calstate.edu/hradm/hipaa/HIPAA_Portal1.shtml This portal is designed for HIPAA privacy and security representatives at CSU campuses to have access to HIPAA regulations and safeguards.