Subject: HIPAA Regulations as Amended by the HITECH Act – Update of Privacy and Security Compliance for CSU Human Resources Operations

Overview

Audience: Human Resources Officers, Benefits Officers, and/or campus designee(s) responsible for human resources operations, including benefits administration.

Action Items: Campuses are required to adhere to HIPAA, as amended by HITECH, regarding privacy and security compliance obligations.

Affected Employee Groups/Units: All employees

Summary

The California State University is mandated by federal law to comply with the federal Standards for Privacy of Individually Identifiable Health Information (PHI) under Title II of the Health Insurance Portability and Accountability Act of 1996 (known as HIPAA), as amended by the HITECH Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act of 2009). The HITECH Act augments HIPAA’s privacy and security related components; establishes breach reporting requirements; applies HIPAA privacy and security requirements and penalties to business associates; and is an expansion of HIPAA rules and obligations. Therefore, this document should be read in its entirety.

This letter updates privacy and security compliance obligations related to the California State University’s (CSU) human resources operations, established under the Health Insurance Portability and Accountability Act (HIPAA), as amended by The Health Information Technology for Economic and Clinical Health (HITECH) Act (Title XIII, Subtitle D of the American Recovery and Reinvestment Act (ARRA) of 2009). The HITECH Act augments HIPAA’s privacy and security related components, and is an expansion of HIPAA rules and obligations.

The HITECH Act:

1) Applies the same HIPAA privacy and security requirements (and penalties) for covered entities to business associates, and mandates that security requirements be incorporated into all business associate contracts;

2) Requires HHS to conduct compliance audits in conjunction with stringent enforcement of HIPAA compliance by the HHS Office of Civil Rights;
3) Establishes mandatory federal privacy and security breach reporting requirements for entities subject to HIPAA compliance, including business associates;

4) Requires security breaches be reported to the media, if the number of impacted individuals is 500 or more;

5) Dramatically increases HIPAA-related penalties that were previously limited to $100 - $25,000. They now range from a minimum of $100 to $50,000 per day of violation, with an annual cap of $1.5 million for the same violation in any one year.

6) Establishes criminal penalties that are applicable to individuals, not just the entity in violation. In cases of “knowing misuse,” criminal penalties include monetary fines of $50,000 up to $250,000, and imprisonment of one (1) to ten (10) years. See the fine structure below:

<table>
<thead>
<tr>
<th>Type of Violation</th>
<th>Each Violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due to Unknowing Violation</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to reasonable cause but not willful neglect</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to willful neglect that is timely corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to willful neglect if not timely corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

**HIPAA Privacy Regulations – Impact on CSU**

The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of personal health information (PHI), including individual medical records and sets limits and conditions on the uses and disclosures that may be made of such information. The Privacy Rule also gives individuals rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. At the CSU, the HIPAA Privacy Rule is enforced by the CSU HIPAA Privacy Official within Human Resources Management (HRM), in the Chancellor's Office. Additional information regarding HIPAA Privacy regulations and safeguarding PHI can be located in the CSU HIPAA Policy (Attachment A), and the HIPAA Privacy Manual (Attachment B).

**HIPAA Security Regulations – Impact on the CSU**

The HIPAA Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting (electronic) e-PHI.

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by employees.

At the CSU, the HIPAA Security Rule is enforced by the Chief Information Security Officer at the Chancellor’s Office, who also serves a dual role as the CSU HIPAA Security Official. For additional information regarding the CSU’s Information Security Policy, please refer to the following website: [http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml](http://www.calstate.edu/icsuam/sections/8000/8050.0.shtml), and the CSU HIPAA Policy.
CSU Privacy Notice

In accordance with HIPAA guidelines, the CSU revised its Privacy Notice (see Attachment C) and released an electronic copy to campuses on February 26, 2010, with instructions to provide a copy to all new hires. Human Resources Management (HRM) coordinated a mass mailing of the revised Notice to all current employees that was completed in early March 2010.

Business Associate Agreement

In a previous HR Letter (HR 2004-22), it was established that HIPAA privacy compliance extended to the Health Care Reimbursement Account (HCRA) plan and external campus-sponsored Employee Assistance Programs (EAP), in addition to business associates. As a result of the HITECH Act, these entities are now subject to the same HIPAA privacy and security requirements (and penalties) that were previously limited to covered entities, and it mandates that security obligations be incorporated into all business associate contracts.

Consequently, CSU released two electronic versions of the revised CSU Business Associate Agreement (see Attachment D) to campuses on February 26, 2010, which included required HITECH language. Campuses were instructed to obtain a signed copy of either the Business Associate Agreement or the Business Associate Agreement Amendment (as deemed appropriate) and forward a copy to Human Resources Management in the Chancellor’s Office. In the future, if the campus replaces its current EAP provider, or establishes an EAP program and secures an external EAP provider, a signed copy of the business associate agreement must be forwarded to the CSU HIPAA Privacy Official.

The following campuses utilize an external EAP: CSU Bakersfield; CSU Channel Islands; CSU Dominguez Hills; CSU East Bay; CSU Humboldt; CSU Los Angeles; CSU Maritime Academy; San Diego State University; San Jose State University; San Luis Obispo; CSU San Marcos; Sonoma State University; and CSU Stanislaus.

The CSU HIPAA Privacy Official also maintains a signed copy of the Business associate Agreement for the third party administrator of the HCRA plan.

Breach Notification Requirements

The HITECH Act definition of a PHI breach is as follows:

(A) IN GENERAL. The term ‘breach’ means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

If a breach of physical PHI or ePHI occurs, it must be reported immediately upon discovery to the CSU HIPAA Privacy and CSU HIPAA Security Officials at the Chancellor’s Office, and the campus Information Security Officer (ISO). The campus HIPAA Privacy Contact must also forward a completed Breach Incident Report Form to the CSU HIPAA Privacy and CSU HIPAA Security Officials at the Chancellor’s Office (see sections 7.05 and 11.07 of the HIPAA Privacy Manual), and record the incident in the Breach log, also located in the HIPAA Manual.

Typically, breaches that impact fewer than 500 individuals are reported on an annual basis to HHS, and must be reported to the impacted individuals within 60 days of discovery. Breaches that impact 500 or more individuals must be reported to HHS, the media and the impacted individuals within 60 days of discovery.

The CSU HIPAA Privacy and CSU HIPAA Security Officials will evaluate the breach to determine if breach notice rules are applicable, and will provide campus guidance accordingly, with regard to reporting to appropriate agencies, and the development of required breach notice(s) for impacted individuals.
HIPAA Privacy and Security Training Webcast

To prepare campuses for the changes made by HITECH to HIPAA Privacy and Security rules, HRM, in collaboration with its benefits consultant Mercer, held a HIPAA Privacy and Security Training Webcast on March 9, 2010. The training provided an overview of the privacy and security rules, best practices for safeguarding PHI, in addition to information regarding the breach notification rules. This webcast was recorded and access is available (with User ID and Password) at: http://centralstationu.calstate.edu. Campus individuals that need access to this training module should contact the CSU HIPAA Privacy Official to obtain a User ID and password.

CSU HIPAA Privacy and Security Policy Components

The CSU HIPAA and Security Policy are comprised of several pertinent documents provided as Attachments listed below:

Attachment A: Revised CSU HIPAA Privacy Policy

The revised CSU HIPAA Privacy Policy has been updated with pertinent information regarding the HITECH Act, safeguards for protecting physical and electronic PHI, identifies the CSU HIPAA Privacy Official and CSU HIPAA Security Official, and provides breach notification instructions.

Attachment B: HIPAA Privacy Manual

The revised CSU HIPAA Privacy Manual has been updated with HITECH Act information and references; and contact information of the CSU HIPAA Privacy Official. This version also contains additional HIPAA forms, including breach notification and breach log. Though it is comprehensive, it should be read in its entirety.

Attachment C: Revised HIPAA Privacy Notice

The revised HIPAA Privacy Notice, as previously stated, has been updated with appropriate HITECH language. Campuses should continue distributing this version to new hires, or to any employee that requests a copy.

Attachment D: Revised Business Associate Agreements

The revised HIPAA Privacy and Business Associate Agreement and the HIPAA Business Associate Agreement Amendment contain updated HITECH language regarding HIPAA privacy and security.

Attachment E: Revised “Authorization to Use and/or Disclose Personal Health Plan Information” Form

The revised “Authorization to Use and/or Disclose Personal Health Plan Information” form has been updated with the appropriate CSU logo. A signed authorization must be obtained from an employee if the Benefits office is assisting an employee with a health care related claim, or if PHI must be used for purposes deemed necessary by HIPAA Privacy rules.

Attachment F: HIPAA Privacy and Security Training Presentation

The PDF version of the HIPAA Privacy and Security Training Webcast PowerPoint presentation provides an overview of HIPAA Privacy and Security, and a copy should be provided to new human resources and/or benefits staff.

Attachment G: Campus HIPAA Privacy Contacts

Each campus, including the Chancellor's Office has a HIPAA Privacy Contact. The campus HIPAA Privacy Contact for human resources and benefits is the campus Benefits Officer (see attached list).
Attachment H: Data Security Practices

The Chancellor’s Office Information Security Management developed a list of “Top Ten Good Security Practices,” with pertinent information on security practices when handling and/or accessing sensitive information.

CSU HIPAA Privacy Official and CSU HIPAA Security Official

The designated CSU HIPAA Privacy Official and CSU HIPAA Security Official are as follows:

<table>
<thead>
<tr>
<th>CSU HIPAA Privacy Official:</th>
<th>Michelle Hamilton</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title:</td>
<td>Manager, Benefits and HR Programs</td>
</tr>
<tr>
<td>Address:</td>
<td>CSU Office of the Chancellor Human Resources Management 401 Golden Shore Long Beach, CA 90802</td>
</tr>
<tr>
<td>Phone:</td>
<td>562/951-4413 or 562/951-4411</td>
</tr>
<tr>
<td>Facsimile:</td>
<td>562/951-4954</td>
</tr>
<tr>
<td>E-mail:</td>
<td><a href="mailto:mhamilton@calstate.edu">mhamilton@calstate.edu</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CSU HIPAA Security Official:</th>
<th>Cheryl Washington</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title:</td>
<td>CSU Chief Information Security Officer</td>
</tr>
<tr>
<td>Address:</td>
<td>CSU Office of the Chancellor 401 Golden Shore Long Beach, CA 90802</td>
</tr>
<tr>
<td>Phone:</td>
<td>562-951-4190</td>
</tr>
<tr>
<td>Facsimile:</td>
<td>562-477-5951</td>
</tr>
<tr>
<td>E-mail:</td>
<td><a href="mailto:cwashington@calstate.edu">cwashington@calstate.edu</a></td>
</tr>
</tbody>
</table>

The contact information for each campus’ Information Security Officer can be obtained by either contacting the Information Security Office at the respective campus, or the CSU Chief Information Security Officer located at the Chancellor’s Office.

Additional Resources

- The HIPAA Privacy Rule is located at 45 CFR Part 160 and Part 164, and can be downloaded at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt.

Full Text of HITECH Act:


Additional Information

DCRA/HCRA Administrative Guide has been updated to reflect the HIPAA and HITECH regulations, and will be issued to campuses in a separate communication.

As mentioned, campus human resources departments are encouraged to review the HIPAA Privacy manual, HIPAA Privacy and Security Policy and other HIPAA-related materials outlined in this HR Letter to ensure compliance with the regulations. If you have questions, please call the CSU HIPAA Privacy Official at (562) 951-4413.
Please note: HIPAA Privacy and Security information with impact to additional departments within CSU is forthcoming.

This memorandum and attachments are also available on the Human Resources Management’s Web site at: http://www.calstate.edu/HRadm/memos.shtml.

GEB/mh

Attachments