MERCER

Human Resource Consulting

May 21, 2003

HIPAA Privacy Overview

Presented to the California State University

MMC Marsh & McLennan Companies

Agenda

- Introduction
- HIPAA privacy regulations
- HIPAA privacy impact on CSU
- Next steps/action items

HIPAA Privacy Regulations

What is HIPAA Privacy?

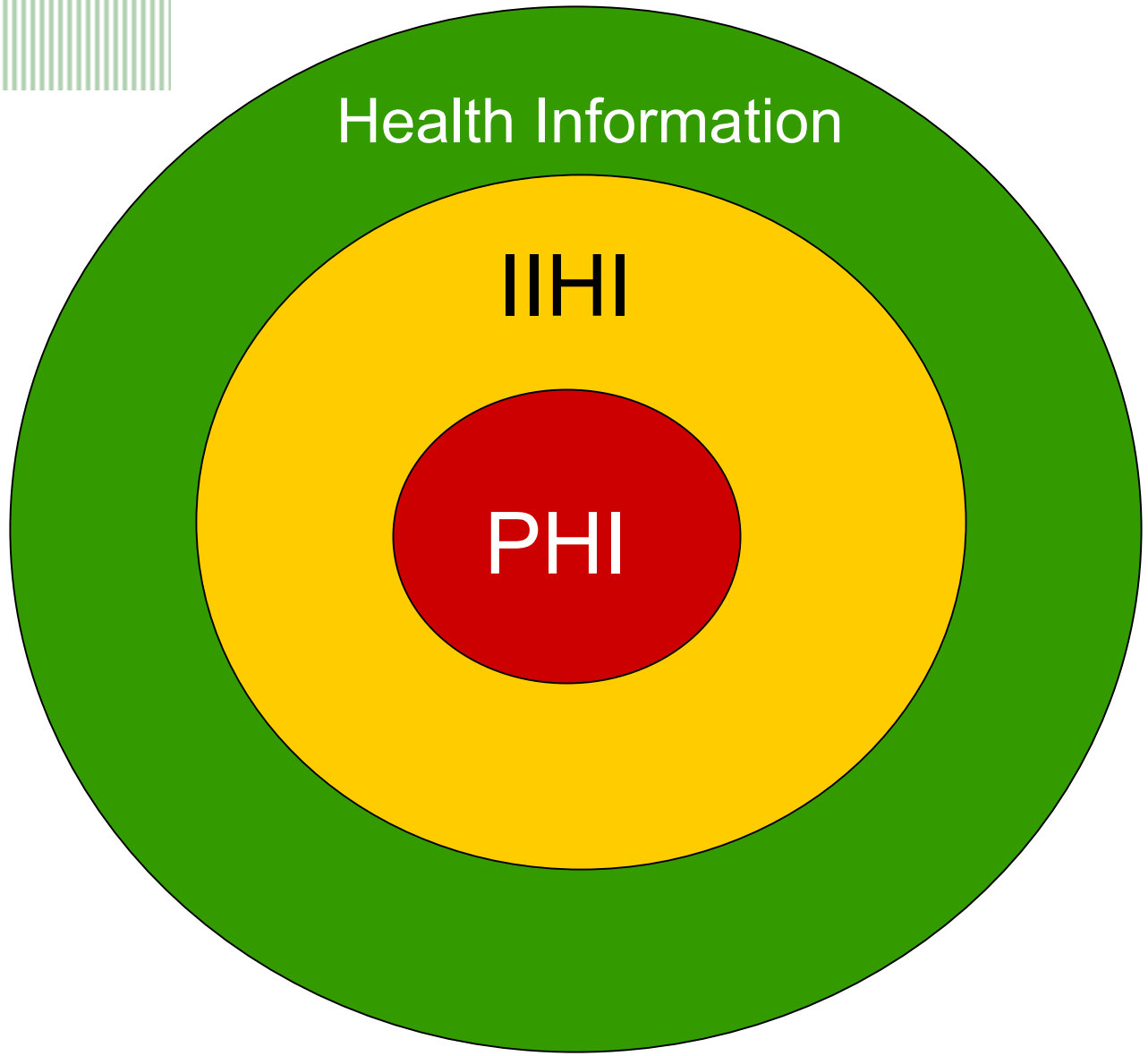
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – Title 2 Administrative Simplification
  - Privacy (our focus today)
  - Electronic Data Interchange
  - Security
- The HIPAA privacy regulations are effective April 14, 2003 and cover the privacy and security of individual medical information used, transmitted or retained by employer sponsored health plans and other covered entities
- The HIPAA privacy regulations will be enforced by the HHS Office of Civil Rights through complaints and selected audits
  - Civil Penalties – Up to $25K per standard
  - Criminal Penalties – Fines up to $250K per standard and 10 years in prison
  - Other Penalties – Private lawsuits under state law or ERISA

HIPAA Privacy Regulations

What information is protected under the HIPAA privacy regulations?

- Protected Health Information (PHI) is any health information that is:
  - Individually identifiable (reasonable basis to believe information could identify individual) and related to the individual's physical, mental or other condition, the provision of health care to the individual, or the payment of health care for the individual
  - Created, maintained, transmitted or received by a health provider, health plan, clearinghouse, or employer in its health care capacity
  - In any medium – written, electronic or verbal
- Does not include personal medical information that is obtained by employer for employment purposes
  - Compliance with FMLA, ADA, worker's compensation, administration of sick leave, etc.

What is PHI?



HIPAA Privacy Regulations

The HIPAA privacy regulations apply to covered entities.

- What is a covered entity?
  - Health plans (e.g., health insurers, HMOs, employer-sponsored health plans)
    - CSU sponsored health plans, including the Health Care Reimbursement Account (HCRA) Plan and possibly campus employee assistance programs (EAP)
  - Health care providers that transmit health data electronically
  - Health care clearinghouses
- What is a health plan?
  - "Health plan" is broadly defined – an arrangement that provides (or pays the cost of) health care. CSU is a plan sponsor of a number of health plans as follows:
    - Medical and prescription drug plans (PERS Health Care Providers)
    - Dental plans (Delta Dental and PMI)
    - Vision Plans (CPIC Life)
    - Health care flexible spending arrangements (HCRA)
    - Employee assistance plans that provide counseling (maybe some campus EAPs)

HIPAA Privacy Regulations

- What is not a covered entity?
  - Employers*
  - Third party administrators*
  - Disability, Workers' Compensation and Life Insurance Plans

* *But the HIPAA regulations make it clear that employers and their TPAs may be affected based on their roles as plan sponsors and business associates*

Employers will be responsible for their employees who handle individual health information when they help with the administration of the employer sponsored health plans (e.g., customer service) compliance with the HIPAA privacy regulations

HIPAA Privacy Regulations

What is a business associate?

- Entity that performs functions for or provides services to a health plan or other covered entity
- Includes: FSA administrators, claims administrators, utilization management vendors, pharmacy benefit managers, consultants, attorneys, auditors, etc.
- May include COBRA administrators
- Does not include insurers and HMOs, because they are covered entities under HIPAA

HIPAA Privacy Regulations

What are key requirements of the HIPAA privacy regulations?

- Covered entities must establish a privacy policy and structure, including restrictions on use or disclosure of PHI without participant authorization
  - Applies to both fully-insured health plans and self-funded health plans (i.e., flexible spending accounts).
- Business associates must abide by the HIPAA privacy regulations in storing, maintaining, or transmitting PHI in any form
  - Employers/plan sponsors will generally be responsible for ensuring that business associates comply with HIPAA's privacy regulations through contractual agreements
- Individuals have certain rights concerning their PHI

HIPAA Privacy Impact on CSU

Who is considered the covered entity?

- CSU sponsored health plans (including the fully-insured plans, HCRA and possibly, the EAPs) and CSU's health care insurance carriers are covered entities under the HIPAA privacy regulations

When do CSU's health plans and health care insurance carriers have to comply with the HIPAA privacy regulations?

- Both HCRA and campus EAPs fall under the HIPAA "small plan rule" and are not required to comply with HIPAA privacy regulations until April 14, 2004
- Not all campus EAPs may be subject to HIPAA regulations. Further review is required.
- The remainder of CSU's health plans and CSU's health care insurance carriers must comply with the HIPAA privacy regulations by April 14, 2003

HIPAA Privacy Impact on CSU

What are the general HIPAA privacy protocols?

- CSU staff members handling PHI must safeguard it against intentional or accidental misuse
- CSU staff members handling PHI may access or disclose only the "minimum necessary" amount of information to accomplish the task at hand
- CSU staff members handling PHI will be trained regarding CSU HIPAA policies and procedures
- PHI will be subject to CSU HIPAA policies and procedures, as well as to applicable participant notices
- Plan participants will have certain rights regarding their own PHI
- CSU staff members who violate CSU HIPAA policies and procedures that protect PHI will be sanctioned
- CSU staff members are prohibited from retaliating against participants who file a compliant or otherwise exercise their privacy rights under HIPAA
- Only certain CSU staff members will be permitted to handle PHI
- Under certain circumstances, CSU staff members handling PHI must obtain a participant's authorization before using or disclosing the participant's PHI (e.g., claim advocacy)

HIPAA Privacy Impact on CSU

Important campus human resources activities impacted by the HIPAA privacy regulations

- Claims advocacy
- Participant requests for assistance with specific medical conditions
- Certain questions regarding a participant's medical coverage

In most cases, CSU staff members will need to obtain a participant's authorization to obtain PHI from CSU's health plans, business associates or health care insurance carriers.

HIPAA Privacy Impact on CSU

How can CSU staff members ensure PHI remains confidential?

- Funnel incoming mail and faxes through distinct channels to limit access to PHI
- Limit the number of photo copies made of documents containing PHI
- Implementing “clean desk” policy
- Lock all files when not in use
- Do not keep fax machines, computer equipment, printers, copiers, manual files where PHI may be received in public areas
- Limit the use of PHI in e-mails and add confidentiality statements to e-mails
- Encrypt information as necessary
- Require password entry for files containing PHI on public servers
- Discuss PHI in areas where you will not be overheard (i.e., behind closed doors)

HIPAA Privacy Impact on CSU

What are CSU health plan participants' rights regarding their PHI?

- Right to receive privacy notices
- Right to inspect and copy their PHI*
- Right to amend their PHI*
- Right to request restricted use of their PHI (though covered entities need not accept those restrictions)
- Right to receive accounting of non-routine disclosures of their PHI
- Right to file complaints about privacy violations

These rights apply to PHI held by CSU staff members involved in plan administration, business associates, or CSU's health care insurance carriers. Most participant inquiries will be directed to the CSU's health care insurance carriers (i.e., PERS medical, Delta, PMI, CPIC Life).

*Health Plans can deny these requests only under certain circumstances

HIPAA Privacy Impact on CSU

HIPAA items implemented to date

- CSU health care insurance carriers, subject to HIPAA privacy regulations effective April 14, 2003, have or are in the process of notifying their CSU plan participants of HIPAA privacy regulations
  - This includes all CSU active employees and retirees with CSU sponsored benefits (medical, dental, and vision)
  - PERS, PMI, and CPIC/MES have completed notification to its CSU plan participants
  - Delta Dental is currently in the process of notifying its CSU plan participants
- Chancellor's Office is issuing an Executive Order to govern the California State University's HIPAA compliance obligations

Next Steps/Action Items

What's Next?

- Systemwide Human Resources Administration to provide electronic copies of the employee PHI authorization form and privacy notices (from each health care insurance carrier) to campuses by early June
- Campus Human Resources staff or CSU's health care insurance carriers to provide newly benefits eligible employees with HIPAA privacy notice upon enrollment
- Systemwide Human Resources Administration to issue a technical letter informing presidents of HIPAA privacy regulations to be issued subsequent to the Executive Order
- Systemwide Human Resources Administration to send an EAP questionnaire in June to campuses in order to determine which campus plans are subject to HIPAA privacy regulations

Next Steps/Action Items

What's Next?

- Systemwide Human Resources Administration to provide campuses with a CSU HIPAA policy manual
- Systemwide Human Resources Administration to develop a HIPAA Compliance web site on the Systemwide Human Resources Administration Web Site
- Systemwide Human Resources Administration and Mercer Human Resource Consulting to conduct HIPAA privacy regulations training at the Benefits Officer's Workshop in August 2003
- CSU to be HIPAA compliant for HCRA and EAPs by April 14, 2004