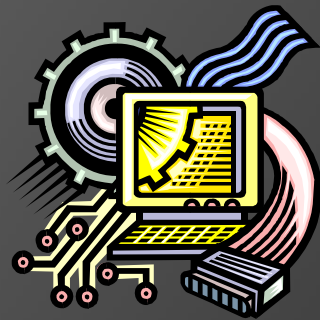


Privacy and Security in a Digital World

# REGULATORY ISSUES IN CAMPUS COMPUTING



# Regulatory Topics

Family Educational Rights and Privacy Act of 1974

Health Insurance Portability and Accountability Act of 1996

Gramm-Leach-Bliley Act of 1999

Sampling of Other, Applicable Federal Laws

Potential Legislation and Liability

# Family Educational Rights and Privacy Act (FERPA)

- Cornerstone of federal privacy requirements in higher education
- Prohibits disclosure of “personally identifiable education information” without student’s permission
- Applies to educational records in any format
- No individual right of action, but enforced by DoEd. Family Policy Compliance Office.
  - Penalty is loss of federal funding. Avoid penalty with substantial compliance
  - No loss yet by any institution.

# Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Provides for individual medical records rights, privacy obligations of PHI holders, security obligations, e-transactions standardization
- Privacy Rule included mini-security requirements
- Security obligations went into effect April 2005
- Security Rule includes Administrative, Physical and Technical Safeguards
- May provide a standard for privacy requirements under Maryland's health records confidentiality law

# Gramm-Leach-Bliley Act of 1999 (GLB)

- In 2002 the Federal Trade Commission interpreted its regulations to include educational institutions as covered financial institutions
- Covers the security of all non-public personally-identifiable financial information of customer of the organization, in any format whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the organization or its affiliates
- Compliance with FERPA is deemed to be compliance with GLB
- Educational institutions remain responsible for following GLB security requirements



# Privacy Coverage Compared

## FERPA

Protects “educational records” (maintained by Inst.), in any format, containing personally identifiable information such as:

- Individual Grades
- GPA
- SSN
- Date of Birth
- Gender
- Class Schedule
- Hours earned
- Work Study records

## HIPAA

Protected Health Information\* (PHI) means:

- Medical Records
- Lab Reports
- Radiology Reports
- Provider Notes
- Billing and Payment records for health care
- Immunization Records
- Mental Health Notes – Special care provided under MD law

*\*Privacy covers all PHI, Security covers E-PHI*

## GLB

Personally Identifiable Financial Information in any format includes:

- Financial aid application
- Credit data
- Tax returns of parents
- Reports for direct lending/student loans and request for federal draw reports
- Student financial information included on various athletic compliance forms
- University-administered loans to employees
- Loan collections

# Security Requirements Compared

## FERPA

- No set, specific requirements
- No clear consensus in higher ed on what is needed
- No court decisions on third party breach

## HIPAA

- Administrative Safeguards
  - 8 subsections on processes, procedures, and training
  - Risk Analysis is foundation
- Physical Safeguards
  - 4 sections on facility access, workstation security, and device and media controls
- Technical Safeguards
  - 5 sections covering mechanisms for Access control, Audit control, Data integrity, Authentication, Transmission security

## GLB

- Develop comprehensive security program
  - Risk Assessment
  - Risk Mitigation
- Assess employee training needs
- Flow down confidentiality obligations to business partners with access to covered information

# FERPA Issues

- ⦿ Communication of digital records across the campus network and the internet
- ⦿ Security of protected educational records (3rd party breach/access liability not yet tested in court)
- ⦿ FPCO interpretation of FERPA to disallow use of “last 4” of SSN for grading
- ⦿ Impact of E-SIGN and UETA on FERPA Release viability- allows e-mail of disclosure authorizations
- ⦿ No individual right of action, but state laws may allow for action.

# HIPAA Security Issues

- ⦿ Requirements within each Safeguard category are either “Required” or “Addressable”
- ⦿ Required safeguards must be implemented
- ⦿ Addressable safeguards provide a choice:
  - Implement action
  - Develop an equivalent measure that provides adequate security (equivalency documentation required)
  - Do not implement any action, but document why implementation is not reasonable and appropriate for the organization

# A Sampling of Additional Federal Laws

- ⦿ **Electronic Communications Privacy Act (ECPA)** - prohibits unauthorized use or interception of any wire, oral, or electronic communication (likely substance only)
  - Also protects against unauthorized access to/disclosure of electronically stored communications (private network may have some added flexibility)
- ⦿ **USA PATRIOT Act** - allows release of stored e-communications to law enforcement if reasonable belief that info must be provided to avoid injury to any person
- ⦿ **Computer Fraud and Abuse Act** - criminalizes unauthorized access to computers used in interstate or foreign commerce or communication
- ⦿ **TEACH Act (Technology Education And Copyright Harmonization)** - relaxes copyright restrictions for certain types of content used in distance ed, provided privacy and security (“technologically feasible”) restrictions are in place to limit transmission to enrolled students

# Coming Legislation and Liability

- The expanding multitude of privacy laws has sensitized people and legislators to privacy rights
- Although no private right of action in HIPAA, various state medical records laws do allow for private action. These laws previously gave no security standards upon which plaintiffs could rely. HIPAA safeguards may bootstrap state claims.
- Many states are considering information collection laws involving children, health records, consumer information, library patron records, and ANY records involving SSN (e.g. CA law bars schools and healthcare providers from printing the SSN on any materials mailed to individuals-may impact out of state providers of distance ed).

