Privacy Laws Affecting College Data

George Bailey

Information Security

Ivy Tech Community College

Tech Day 2006 – Columbus, IN

93,023,845

- Records **revealed** due to security breaches between 2/15/2005 – 10/18/2006!
- **Result**
  - Implementation of restrictive organizational policies
  - State and Federal legislation
  - Industry regulations
- Late breaking news…http://www.cnn.com/2006/POLITICS/10/24/chicago.elections.ap/index.html

Why?

- Estimated to cost **$90.00** per breached record – *Gartner Research*
- Undesirable publicity
- Increased compliancy requirements
- Industry fines
- Push from constituents - Fear of Identity Theft
- Potential litigation
- Potential loss of student enrollment

Movie

Laws & Regulations Affecting Higher Education

- Family Educational Rights and Privacy Act
- Health Insurance Portability and Accountability Act
- Gramm-Leach Bliley Act
- Payment Card Industry Data Security Standard
- State Privacy Laws (e.g. Indiana *P.L.91-2005*)
- Forth coming Federal laws

FERPA

Family Educational Rights and Privacy Act

- Must have **written** permission from the student in order to release any information from their educational record
- Student has the right to inspect and review educational records
- Student has the right to request correction of records which they believe to be inaccurate or misleading
- Allows schools to disclose records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest
  - Other schools to which a student is transferring
  - Specified officials for audit or evaluation purposes
  - Appropriate parties in connection with financial aid to a student
  - Accrediting organizations
  - To comply with a judicial order or lawfully issued subpoena
  - Appropriate officials in cases of health and safety emergencies
  - State and local authorities, within a juvenile justice system, or pursuant to specific State law
- Directory information can be disclosed. Students must be able to OPT out.

FERPA
What can Ivy Tech Do?

- Identify sources of sensitive data
  - Internal forms
    - How is data collected
  - Regional databases
    - Where is data stored
  - Internal processes
    - Where is data collected?
- Know who needs access to sensitive data
  - Practice “Need-to-know”
  - Use existing Data Classification Standard
  - **DON’T** disclose data without consent of student

HIPAA

Health Insurance Portability and Accountability Act

- What's protected
  - Any information in student's medical records
  - Conversations doctor has about student's care
  - Health information stored in computing systems (insurer, care provider, school)
  - Most other health information held by others

HIPAA
What can Ivy Tech Do?

- Be cautious how nursing programs interface with hospital programs
- Have Confidentiality Policy for “live” data used in nursing curriculum
- Inform Information Technology Security Office when interfacing with external sources of medial data

GLBA

The Financial Modernization Act

- Higher Education is directly affected
  - Financial Aid collects GLBA protected information
  - Acceptance of credit cards
  - Should develop precautions to ensure the security and confidentiality of student records and financial information
  - Protect unauthorized access or disclosure to personal information
- Get GLBA “like” agreements between school and outside service providers
- Inform ITSO of any outside agreements
  - We can help negotiate requirements

PCI-DSS

Payment Card Industry's Data Security Standard

- Requirements
  - Build and maintain secure network
  - Protect card holder data
  - Maintain vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy
- Why should we be compliant?
  - Large fines if data is compromised
  - Ability to accept/process credit cards

PCI-DSS
What can Ivy Tech Do?

- **DON'T** store credit card information
- Isolate your point-of-sale systems
- Know your CC processor, get confirmation that they are PCI-DSS compliant
- Inform ITSO about your systems
  - Quarterly scans
  - Confirm isolation

P.L. 91-2005

Indiana's SSN Disclosure Law

- Prohibits disclosure of SSN of an individual
- Institutions must notify individuals in the event of SSN disclosure
- May disclose the Social Security number of an individual to a **state, local or federal agency** unless prohibited by state law, federal law or court order
- Disclosure by an agency of the last 4 digits of an individual's Social Security number is **not** a prohibited disclosure, but may violate other laws (FERPA)

P.L. 91-2005
What can Ivy Tech Do?

- Ivy Tech can ensure compliance by:
  - Eliminate the use of Social Security numbers as the primary identifier
  - Develop Social Security number policies
  - Institute a policy for document disposal and educate employees and students regarding the policy.
  - Follow existing data retention policies
  - Educate regarding sanctions for prohibited disclosure
  - Refrain from using and purchasing software requiring Social Security number as main identifier
  - Ensure that forms used by the region indicate whether disclosure is voluntary or mandatory **!! GET SIGNATURE !!**
  - Regions need to work with ITSO to assist monitoring the use of Social Security numbers and ensure compliance with the policies

Resources

- FERPA
  - http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- HIPAA
  - http://www.hhs.gov/ocr/hipaa/
- GLBA
  - http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
- PCI-DSS
  - http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html
- SB-0503
  - http://www.in.gov/legislative/ic/code/title4/ar1/

Questions