IT Orientation - Privacy

May 8, 2013

Maura Johnston, University Privacy Officer
Overview

- What is privacy?
- Protecting Penn data
- Protecting yourself
- Resources
What Is Privacy, And How Does It Relate to Security?

Privacy refers to the ability of a person to know about and often control information collected about them, and the use and sharing of that information. In addition, security is a major component of privacy because of the focus on protecting confidential data from unauthorized access and disclosure.
Some Major Privacy Laws, Standards & Policies

- FERPA (student records)
- HIPAA (health records)
- GLBA (financial data)
- PCI Standards (credit card data)
- CAN SPAM (e-mail)
- State breach notification laws
- Electronic privacy (Penn policy)
- CCTV policy (Penn policy)
Fair Information Principles

- Notice
- Appropriate Use
  - Choice – opt in and opt out
- Access to records
- Minimization
- Third party agreements
- Security – administrative, technical, physical
What is Appropriate Use?

- Sharing student data with U. Officials generally appropriate
  - U. Officials need to have a legitimate educational interest
- Other data sharing requires a specific choice:
  - Opt-in: student records, staff and faculty records, alumni data, etc.
  - Opt-out: directory information for all of the above
- Electronic Privacy
  - Penn more protective than law – but also flexible
  - Must meet standard and get approvals
- List requests
- Bulk e-mail
- Social media considerations
SSN Policy – Basic Requirements

- Scope – all faculty, staff, contractors and agents in connection with Penn-oriented functions

- Best efforts to identify and reduce availability of SSNs
  - Inventory SSNs
    - Identity Finder tool recommended
  - Remediate –
    - eliminate, convert or truncate
    - secure the data
    - restrictions on transmission
SPIA – What Is It?

- Program and tools to address privacy and security risks in databases and applications
  - Inventory
  - Evaluate risks and prioritize
  - Identify and adopt remediation steps

- Cohort-based program
  - 5 Cohorts
  - U-wide implementation
Some general observations:
- Significant clean up of obsolete systems
- Much deeper impact for raising awareness than previous programs
- Winnowing down to systems that require stronger security controls and identifying timeframes and budgets to achieve goals
- Common areas of concern

Monthly meetings for discussion of issues/questions
SPIA “Next Generation” in planning stage
FERPA – Some Highlights for IT

- FERPA requires reasonable methods to ensure that school officials obtain access only to those education records in which they have legitimate educational interests.
  - If not through technological and physical controls, then administrative policy must meet requirement
- Also requires reasonable methods to identify and authenticate identity of parents, students, school officials and others to whom personally identifiable information from education records is disclosed.
Third Parties

- Increased use of outsourcing
- Allowable, legal, and often quite efficient and recommended
- But, where personally-identifiable data is being created, stored or used, need strong confidentiality provisions, and sometimes legally-required language (for example, FERPA, HIPAA)
- Be aware of potential cloud computing issues – see Cloud Computing Guidance, Data Sensitivity and Review Framework, SPIA for Vendors tool
Website Privacy Template

- Guidance
- Importance of posting such statements, particularly where personally-identifiable data is collected
- Importance of writing statements properly and accurately
- Template
- Required on e-commerce sites
Requirements from Credit Card Issuers

- Payment Card Industry (PCI) Data Security Standard imposes specific security requirements
  - Significant financial penalties for failure to meet standard
- Major compliance efforts at Penn and UPHS
Disposition of Data of Faculty and Staff Who Have Left Penn

- Goals:
  - Raise awareness of the need to consider documents/data of such individuals
  - Provide ownership of and framework for making decisions
  - Identify potential interests: required retention, business continuity, research grant issues, academic collaborators, potential litigation, intellectual property, institutional history, personal data
Eliminate Unnecessary Data

- The best way to protect data is not to have it
- Securely shred and delete when appropriate
- Resources to help determine when and how to do this

www.archives.upenn.edu/urc/recrdret/guide2.html
www.upenn.edu/oacp/privacy/penndata/shredding-paper-records.html
www.upenn.edu/oacp/privacy/penndata/secure-file-deletion.html
Take Aways as IT Professionals

- Look for opportunities to:
  - Eliminate, convert, truncate, secure SSNs
  - Utilize the SPIA program
  - Securely delete sensitive data
  - Apply the Cloud Computing Guidance and tools
  - Double check on appropriate use
  - Focus areas: large list requests, bulk e-mail, requests to access e-mails/docs of others
  - Use available tools (such as Secure Share, Identity Finder, PGP encryption service)
What are you doing about privacy today?

Visit www.upenn.edu/privacy for the facts:

**Facebook.** Get to know and use important privacy settings.

**Smartphones and tablets.** Follow Penn ISC’s Top 10 security tips for mobile devices.

**Cloud Services.** Avoid putting sensitive data on cloud services if you don’t know or like their privacy terms. Backup data you care about.

**Identity Theft.** Stop receiving pre-approved credit offers that “dumpster divers” abuse. Order your free credit report and check for fraudulent activity.

**Penn Privacy Choices.** Check out Penn’s own online privacy choices.

**Ask questions.** Consult a Privacy Liaison or Penn’s Privacy Office.

Visit Penn Privacy at www.upenn.edu/privacy for more specifics and resources.
Resources

- www.upenn.edu/privacy
- privacy@upenn.edu
- 215-PCOMPLY
- Privacy Liaisons
  - Local point of contact for privacy matters
- Online training in KnowledgeLink – select “Information Privacy and Security at Penn”
  - Takes 20-25 minutes; learning games
- SANS “Securing the Human” modules