IT Orientation - Privacy

February 7, 2018

Scott Schafer
University Privacy Officer
Overview

- What does Penn’s Privacy Office do?
- What is data privacy?
- Protecting Penn data
- Key takeaways
- Resources
What does Penn’s Privacy Office do?

- Core functions (often in conjunction with ISC)
  - Awareness-raising
  - Risk assessment program (SPIA)
  - Third party reviews
  - Incident response
  - Advisory services
  - Reporting to Trustees and Executive Oversight Committee
What Is Data Privacy?

Individuals’ ability to be aware of, and (often) control, the data collected about them, and the use and sharing of the data.

Security is a major component of privacy because of the focus on protecting confidential data from unauthorized access and disclosure.
Major Privacy Laws, Standards & Policies

- FERPA (student records)
- HIPAA (health records)
- GLB (financial data)
- PCI Standards (payment card data)
- State breach notification laws
- Privacy in Electronic Environment (Penn policy)
- Social Security Numbers Policy (Penn policy)
FERPA

- Protects students’ education records
- Imposes an obligation to use reasonable data security measures to prevent unauthorized access
- Ensures that school officials obtain access only to those education records in which they have legitimate educational interests (Example: role-based access)
Social Security Numbers Policy

- **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 data that must be kept
Basic Rule

- Personal Data may be shared:
  - upon notice or consent from the individual
  - for legitimate purposes
  - with authorized individuals
  - using appropriate security measures
Questions to Ask Yourself

- **What?**
  What Information is involved?
  Is it personal or sensitive information?

- **Why?**
  Why is the data being collected?
  Is the purpose allowed?

- **Who?**
  Who is it being shared with?
  Is this person authorized?

- **How?**
  How is it being shared?
  Is it sufficiently secure?
SPIA – What Is It?

- Security and Privacy Impact Assessment
- School/Center-based risk assessment performed on an annual basis
- Program and tools to address privacy and security risks in databases and applications
  - Inventory
  - Evaluate risks and prioritize
  - Identify and adopt remediation steps
Some general observations:

- Currently reaches 36 Schools and Centers
- Hundreds of applications and databases reviewed
- Significant clean-up of obsolete systems
- Deep impact in broadening awareness of security and privacy
- Identified systems that require stronger security controls and establish timeframes/budgets to achieve goals
- Improvements in safeguards and controls
Third Parties

- Increased use of vendors

- Where personally-identifiable data is being created, stored or used, need strong confidentiality provisions, and sometimes legally-required language (for example: FERPA, HIPAA)

- Tools to Assess Vendors
  - Cloud Computing Guidance
  - Data Sensitivity and Review Framework
  - SPIA for Vendors
Disposition of Data of Faculty and Staff Who Leave 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, intellectual property, personal data
Takeaways as IT Professionals

- Look for opportunities to:
  - Eliminate, convert, truncate, secure SSNs
  - Utilize the SPIA program
  - Apply the Cloud Computing Guidance and tools
  - Double check on appropriate use
  - Requests to access e-mails/docs of others—Policy on Privacy in Electronic Environment
  - Use available tools (Secure Share, Identity Finder)
Resources

- [www.upenn.edu/privacy](http://www.upenn.edu/privacy)
  - Protect Penn Data
  - Protect Yourself
  - Policies and Guidance
  - Tips and Training
  - Privacy Topics A to Z

- [privacy@upenn.edu](mailto:privacy@upenn.edu)

- Online training in KnowledgeLink – select “Information Privacy and Security at Penn”