Bridging the Gap

Protecting Paper Records

Ann Geyer
Chief Privacy and Security Officer
Topics

- Understanding information privacy
- What information should be protected
- Recommended practices for paper
- What to do if data is breached
Paper Breaches

Business 27%
Education 17%
Finance 10%
Government 33%
Health 13%

Paper = 25% of all breaches

Identity Theft Resource Center 2010
General Causes

- Carelessness: 22%
- Insider data theft: 25%
- Stolen laptops: 32%
- 3P data theft: 21%

Employees involved in ½ the breaches
What Paper Needs Protection?

› Data that we have responsibility for
  › PII—an individual’s data
    › Students, patients, employees, visitors . . .

› Official record systems
  › Financial, HR, Enrollment, Grades . . .

› Other data on paper
  › Copies, temporary work papers, . . .
Information Privacy

- Information Privacy is about the terms and conditions under which we collect an individual’s data

- Objective is to create a fair deal

- Individuals exchange their private data for our guarantees of privacy protections

- Law & ethics require us to provide reasonable safeguards even if we offer no guarantees
Privacy Principles

- 1973 Fair Information Privacy Principles
  - Transparency & notice
  - Choice & consent
  - Use limitations
  - Inspection & correction
  - Accountability
Question 1

My department wants to know what information has the most value for our clients. We decide to record what pages are visited and what information is viewed.

Does this activity require privacy protections?

A — YES
B — NO
Question 2

Information is collected to enroll students in a summer session course. The information is subsequently used to solicit these individuals for campus donations.

Has a privacy violation occurred?

A — YES
B — NO
Protection Objectives

Privacy
- Give notice
- Get consent
- Minimize data
- Use within scope
- Inspect & correct
- Eliminate ASAP

Security
- Track location
- Restrict access
- Maintain accurately
- Prevent loss or theft
- Monitor and audit
Basic Considerations

- What information do you have
- Where do you keep it
- Who is authorized to use it (need to know)
- Where can they use it
- To whom can it be disclosed (need to know)
- How will you deliver it
- How long will you keep it
- How do you know when to destroy it
- How will it be destroyed
Question 3

Mary telecommutes 2 days a week. She routinely takes her files and papers home. What should Mary do to protect this information?

A — Do not leave papers in car
B — Scan and email material to self
C — Keep copies of material in office
D — Have a lockable file cabinet at home
E — Limit the amount of data she works on at one time
Rule #1  Handle PII like Cash

- Know what you have
- Know where it is
- Know who has access to it
- Know if it changes
- Know where it's gone
- Account for it when asked
Don’t Leave It Lying Around

- Lock it away at the end of work
- Don’t take it home
- Clean & tidy
Paper Storage

- Label the boxes
  - Confidential
  - Destruction Date
  - Contact Info
- Seal Boxes
- Document storage location
- Keep clean and tidy

Lost or misplaced records are a data breach
Destruction

- Confidential data
  - Cross cut shred
  - Burn for highly sensitive info

- Campus Mailing Services
  - Shredders
  - Confidential bins
  - Managed secure destruction

Be sensitive to
Selling for recycling
Using for scrap paper
The library routinely sells books, copies, and other services to its patrons most of whom pay by credit card. The credit card number is noted on the sales receipt. The receipt is used to record the sale in the general ledger, settle the payment with the bank, process a return, and then stored for a 5 year retention period.

What could the library do to improve its level of data protection?

A – Limit the period for returns
B – Automate its settlement process
C – Black out the CC# before storing
D – Move the CC# before storing
Checklist

- Document protection procedures
  - Know what data you have
  - Categorize it for privacy purposes
  - Keep in locked locations
  - Keep locations clean and tidy
  - Limit removal
  - Set short retention periods
  - Design forms for removal
  - Destroy correctly
  - Remind self and others often
How to Report a Breach

- **When?**
  - As soon as a reasonable suspicion occurs that confidential data is lost, misplaced, or stolen

- **Who?**
  - If PII to CPSO at security.berkeley.edu
  - Other confidential data to data proprietor

- **What happens next?**
  - Contain loss
  - Determine scope
  - Notify if necessary
  - Root cause
  - Remediate
Prevention Is the Key

The time taken to prevent damage and loss of records is cheaper than the cost of disaster recovery.
Addendum to Presentation

Privacy statement (From UC Berkeley Online Activities Policy)

Technology service providers (any campus department) who collect data via website interfaces must adhere to the provisions of the Privacy Statement for UC Berkeley Websites (http://technology.berkeley.edu/privacy/privacy-statement.html) and must post a privacy statement to notify users regarding the types and uses of data that is gathered.