

Data Security Basics: Helping You Protect You



Why the Focus on Data Security?

- Because ignoring it can get you:
 - Fined
 - Fired
 - Criminally Prosecuted
- It can also impact your ability to get future funding, and dramatically delay your work

Course Goals

- To better understand why data security is so important to the University, to the School, and to you
- To inform you of the data security policies that regulate our work at Columbia
- To share which data must be protected, and to provide some information about tools to help you do so
- **Help you protect yourself and your life's work**

What is Data?

- Dictionary.com says it is “Facts and statistics collected together for reference or analysis.”
- The data can be gathered for any number of purposes – business, research, education, etc.
 - When it comes to data security, the “why” is irrelevant. We care about the what:
 - Business and intellectual data, processes, resources, clinical and genetic data, demographic data, financial data, etc.

What Data Are We Worried About Protecting?

- All data is not equal. We're worried about what is generally termed "sensitive data."
- Sensitive data typically falls into two categories -- PHI and PII.
 - PHI: Personally Identifiable Health Information
 - PII: Personally Identifiable Data

Why Are We So Concerned?

- Use of PHI and PII is regulated by both the State and Federal Government via the following:
 - NY State SSN Breach Act (2004)
 - HIPAA Privacy (2003) and Security (2006)
 - HITECH (2009)
- As of the adoption of HITECH, institutions that leak “sensitive data” are subject to significant penalties. Medical institutions, such as CUMC, are subject to ENORMOUS penalties: Monetary fines, costly investigations, and potentially **criminal prosecution**

But I don't Have Any "Sensitive Data!"

- The most common comment from faculty and staff about data security is “it doesn't apply to me. I don't deal with sensitive data.” But it does apply.
- As part of the CUMC Community, the Mailman School uses the same network as the hospital. Our data travels on the same pipe, and our colleagues do have sensitive data. A hole in security at Mailman is a hole in security at the hospital



Why Should *You* Worry?

- At CUMC, the penalties flow down hill.
 - According to CUMC’s “Guidelines for Sanctioning Violations of Policy on Unauthorized Access, Use or Disclosure of PHI/PII” (Dec ’12) can result in:
 - Fines as high as \$75,000 or more *per incident* for the department responsible
 - Termination/Non-Renewal of the noncompliant faculty/staff member
 - Criminal prosecution of faculty/staff
- The government (OCR), and therefore CUMC, is serious about going after offenders

CUMC/NYP Breach

- HITECH Google Breach (2010)
 - 6800 ICU patients, 10 SSN, rest clinical data
 - Letters, engagement with external call center
 - Report to Attorney General's office of NY, NJ, MA, etc.
 - Report to OCR
 - Reaching **7 figure** expenditure
 - 4 rounds of OCR request of documentation
 - OCR visit and interview
 - Likely to be fined with severe requirements in change of processes



Other Institutions, Large & Small

- April 2012 – Phoenix Cardiac Surgery
 - \$100K fine
 - Failed to secure an appointment calendaring application
 - Failed to have risk analysis and management processes, policies, and procedures as required
 - 5-6 physician practice

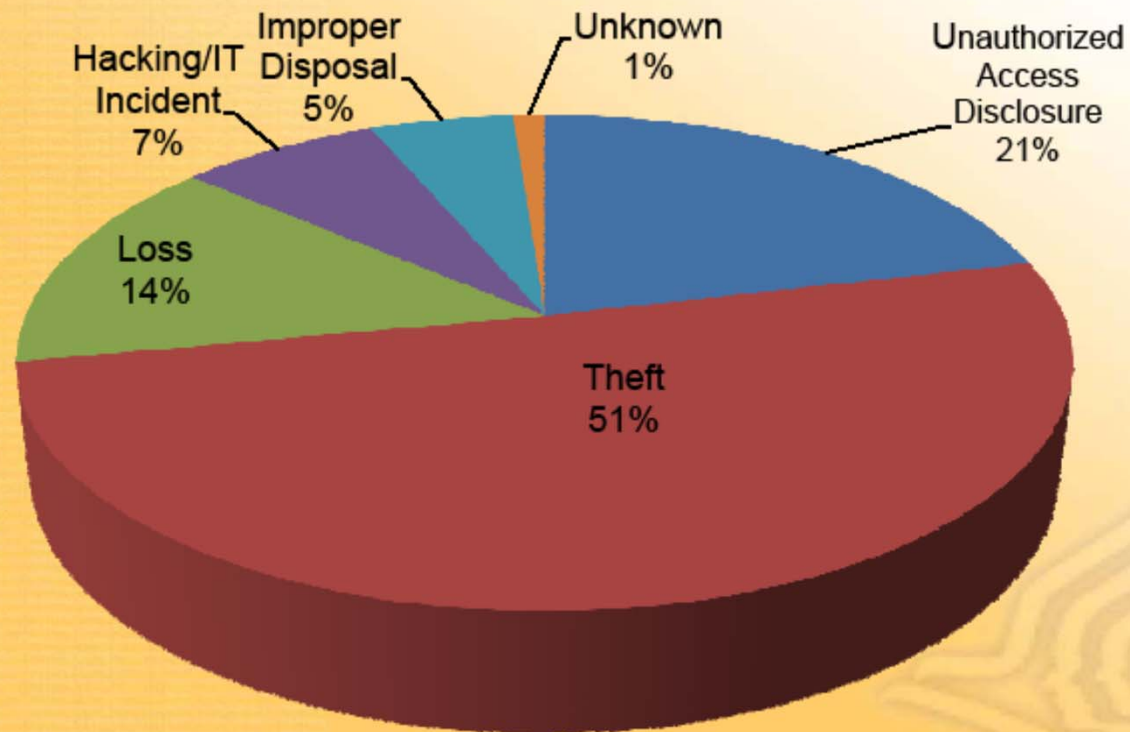
- March 2012 – BlueCross/BlueShield of TN
 - \$1.5 Million fine
 - Theft of servers containing PHI
 - Failure to assess and remediate changes in risk to PHI resulting from relocation of data

How Big is the Problem?

- Between September '09 to March '12
 - 409 breach reports involving more than 500 individuals
 - **65% of the breaches resulted from theft and loss;**
70% involved sensitive data
 - Laptops and portable storage devices (USBs, hard drives, etc.) account for 37% of large breaches
 - Breaches involving paper records account for 24%
- 50,000 reports of breaches impacting under 500 individuals

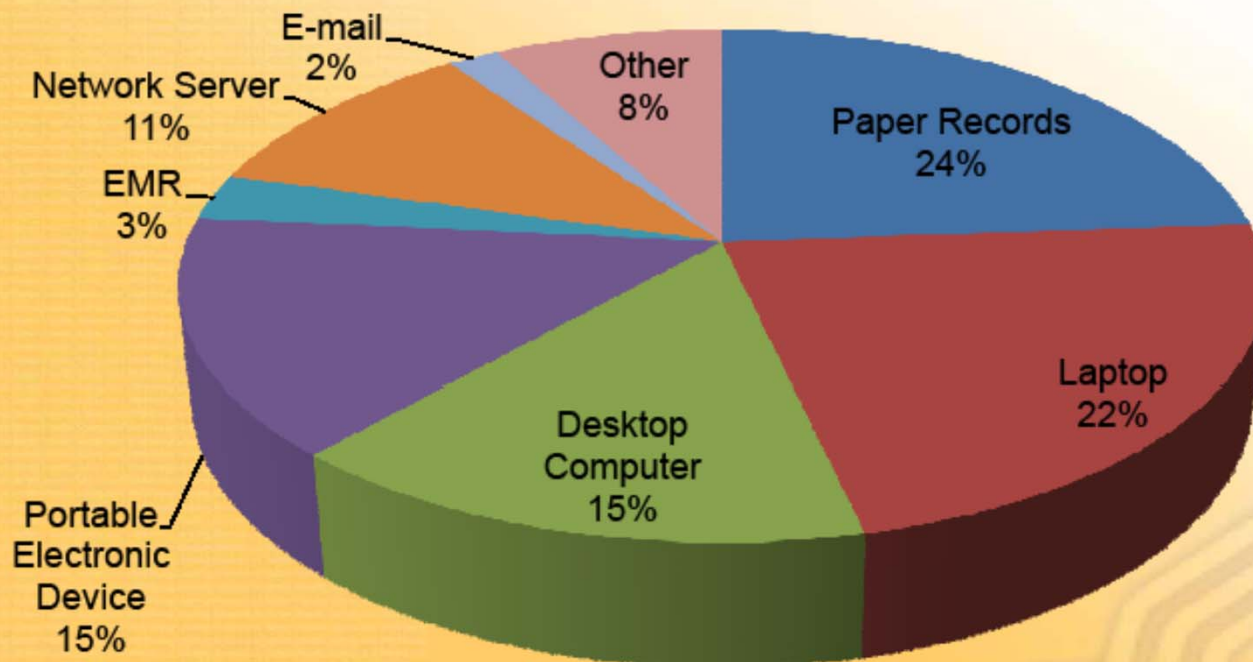


Breach Notification: 500+ Breaches by Type of Breach





Breach Notification: 500+ Breaches by Location of Breach



How Do You Protect Yourself?



© Charles Schultz



Know Your Weak Spots

- There are four main areas of vulnerability:
 - Software: Whether it's a custom application or off the shelf
 - Hardware: Configuration and maintenance issues
 - Environmental: Physical security of equipment
 - You and Your Colleagues: Weak passwords, password sharing, poorly maintained desktops/laptops, downloading "iffy/bad" software, falling for scams



Know and Abide by Our Policies

- There are three policy tiers that govern our work for the School:
 - The University Administrative Policy Library section “Computing & Technology”
 - CUMC’s “IT Policies, Procedures and Guidelines”
 - Mailman School’s Key Guidelines & Policies
 - CUMC’s System Certification Requirement: All servers and custom software applications need to be registered with CUMC IT Security to be certified “secure” prior to being allowed on the network
- Links to all can be found in *Policy Central* on the Mailman IT Website.

Use the *Principle of Least Privilege* in All Things


“That an individual, program or system process is not granted any more access privileges than are necessary to perform the task.”



Make Use of Existing Secure Resources

- The Mailman School provides secure data storage via CUMC IT's file server at no charge:
 - O drives hold personal work data (1 GB to start, more available on request)
 - P drives hold project data accessible by one or many
- CUMC IT provides Exchange e-mail accounts for all work-related e-mail as well as a Sharepoint server for secure project collaboration
- Use CU's secure *Connected* Back-up service
- If you need your own servers, outsource to a CUMC IT-certified secure server or host

...and Avoid Insecure Ones

- Do not use third party e-mail providers, like Google, Hotmail, Yahoo, etc., for work 
- Replace DropBox with SpiderOak for file sharing or better yet, get an SFTP account with CUMC IT
- Do not use any data storage resources that are not covered by a CUMC Business Associates Agreement (BAA) and certified “compliant” by CUMC IT Security

De-Identify Your Sensitive Data

- HIPAA Privacy Rule:
 - “allows a covered entity to de-identify data by removing all 18 elements that could be used to identify the individual or the individual's relatives, employers, or household members...”
 1. Names
 2. All geographic subdivisions smaller than a state
 3. All elements of dates (except year) for dates directly related to an individual
 4. Telephone numbers
 5. Facsimile numbers
 6. Electronic mail addresses

De-Identify Your Sensitive Data (2)

7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

Encrypt, Encrypt, Encrypt



- Encryption is REQUIRED for all laptops and portable devices; desktop machines must be encrypted if they hold sensitive data
- CUMC-approved encryption software includes:
Bitlocker with PBA and Filevault 2
 - You can use Bitlocker and Filevault to encrypt USB drives, external hard drives, SD cards, etc.
 - Encryption keys should ALWAYS be stored in your O drive – that way it is secure, but you can access it from anywhere, anytime

Keep a Clean “House”

- Don't keep data around that you don't need
 - Wipe old data from computer hard drives you want to dispose of or repurpose -- ask your Mailman Tech for aid
 - Destroy old media before discarding it (Cds, Dvds, back-up tapes, USBs). The School has media shredders at ARB and 600 buildings for this purpose
 - Delete old e-mail; back-up critical e-mail to the P drive
 - Keep all the data you DO need on the P or O drives, not locally on your machine or portable devices
 - Consider ALL your data, not just the data you've collected while at Mailman

Use Sound Computing Practices

- Highlights
 - Use strong passwords for all of your logins and change them at least every 90 days
 - A strong password is at least 8 characters long and a combination of upper and lowercase letters, numbers and symbols
 - Make sure you have virus/malware protection on your computer with auto update enabled
 - Activate your OS' native firewall
 - Enable a locking screensaver (w/strong password requirement) that runs after 15 minutes of inactivity
 - Never share your passwords or leave them lying near your computer

Educate Yourself

- Take the Mailman School's Information Security Awareness Online course – required for all
- Administrators/owners of applications and servers that access or contain sensitive data must take technical data security training. Visit the *Data Security & Me* section of the Mailman IT Website for details.
- Attend CUMC's annual HIPAA/HITECH. It is announced by e-mail. You can also watch the latest one online at the Mailman IT site.

Budget for Data Security

- If your project requires a server or custom software application, provide the appropriate resources to support it:
 - **Hardware:** Use trained system administrators and computer technicians to support your equipment; Insist on device “hardening” and patching/maintenance
 - **Environmental:** House your equipment in compliant data centers
 - **Data Collection and Management:** Hire data experts who know how to gather, store, analyze, and archive your sensitive data

Budget for Data Security (2)

- Software: Hire knowledgeable programmers who code to official data security standards
- You are ultimately going to pay anyway, either to build and maintain the system properly at the beginning, or to fix the system after it is assessed by CUMC IT Security. It is MUCH cheaper and faster to build it correctly than to repair it!



Who can help?

- Your Mailman IT Tech
- The central Mailman IT Office
 - Data security audit support
 - Certified vendor list
 - Encryption, etc.
- Department of Biostatistics
- CUMC IT Security

Questions?

HITECH Act (ARRA)

- **HITECH Breach Notification Law – Effective Sept 2009**
 - *Applies to all electronic “unsecured PHI”*
 - *Requires immediate notification to the Federal Government if more than 500 individuals effected*
 - *Annual notification if less that 500 individuals effected*
 - *Requires notification to a major media outlet*
 - *Breach will be listed on a public website*
 - *Requires individual notification to patients*
- **Criminal penalties** - apply to **individual** or employee of a covered entity