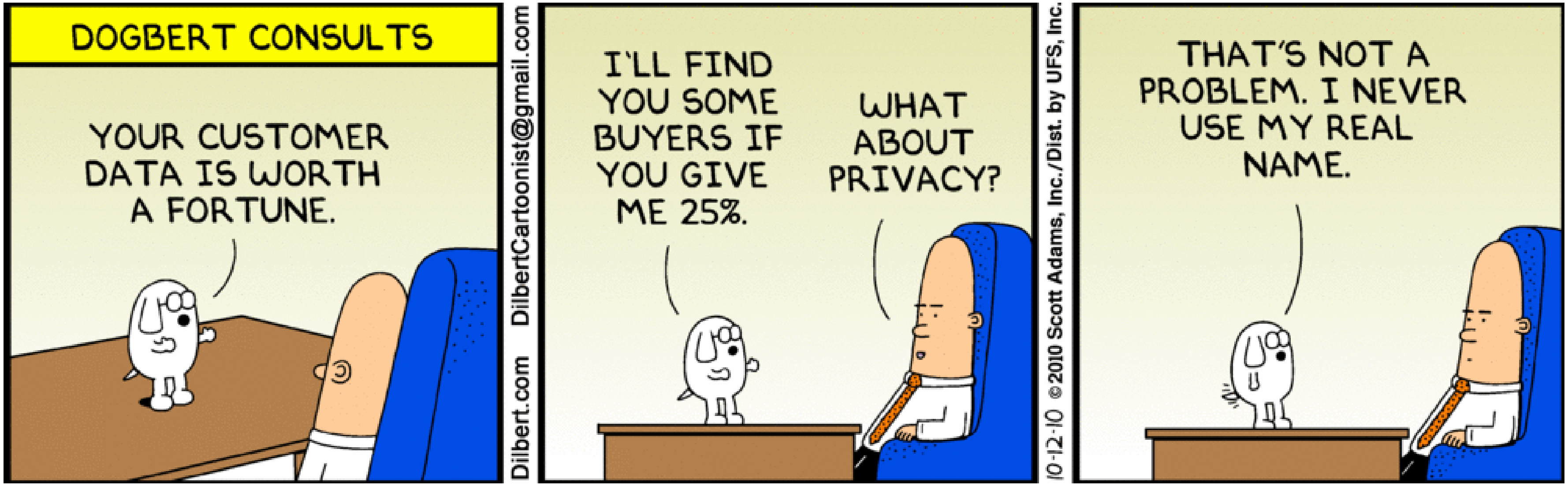
Dealing with Sensitive Data: Helping You Protect You


DOGBERT CONSULTS
YOUR CUSTOMER DATA IS WORTH A FORTUNE.
I'LL FIND YOU SOME BUYERS IF YOU GIVE ME 25%.
WHAT ABOUT PRIVACY?
THAT'S NOT A PROBLEM. I NEVER USE MY REAL NAME.
Dilbert.com DilbertCartoonist@gmail.com
10-12-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.

Why the Focus on Data Security?

- Because some data collection and use is federally regulated, and data security is a core regulatory component. Ignoring it can:
  - Get you:
    - Fined
    - Fired
    - Criminally Prosecuted

- Impact your ability to get future funding, and dramatically delay your work

- Leave you fighting for your very identity

What We’ll Cover

- Data, Sensitive Vs. Not
- Data Regulations – what you can and can’t do (PHI)
- Safe Harbor and Other Protections
- Acceptable Use of Sensitive Data
- Common Areas of Risk
- Common Threats
- Protecting Yourself
- Know Your Environment
- Educate Yourself
- Who Can Help?
- Questions?

Key Takeaways

- To inform you about the data that must be protected
- To provide some information about tools and behaviors to help you do so
- To give you a better understanding of why data security has become so important to the University, to the School, and hopefully, to YOU

The Basics

- What is Data?
  - Dictionary.com says it is “Facts and statistics collected together for reference or analysis.”

- Data can be gathered/created for any number of purposes – business, research, education, etc.

- What you can do with the data you create/collect depends on what data you’re gathering and why.

All Data is Not Equal

- The Government bases its data protection regulations on three classes of data:
  - Highly Sensitive Data
  - Confidential Data
  - Public Data

- The regulations apply to the “Highly Sensitive” class, which is comprised of:
  - PHI: Protected Health Information
  - PII: Personally Identifiable Data

PHI In-depth

- “Individually identifiable health information” is information, including demographic data, that relates to:
  - the individual’s past, present or future physical or mental health or condition,
  - the provision of health care to the individual, or
  - the past, present, or future payment for the provision of health care to the individual,
  - and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.[13] Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

(HHS.gov)

What are the Regulations?

- Data use regulations are in place at both the State and Federal levels via the following:
  - Health Insurance Portability and Accountability Act (HIPAA, 1996), Privacy (2003) and Security (2006)
  - NY State SSN Breach Act (2004)
  - The Health Information Technology for Economic and Clinical Health (HITECH, 2009)

- Under the health-related acts, healthcare providers, health plans, and healthcare clearing houses (aka "Covered Entities") must act to protect the privacy and security of health information. The SSN breach act does the same for personal non-health-related data.

Why Do We Care?

- As part of the CUMC campus, Mailman is automatically considered part of the "Covered Entity" to which the regulations apply. Even though we are not technically a healthcare provider, plan, or clearing house.

- The HITECH act provides for *significant* financial penalties in the event of a leak of PHI. In the case of negligence or intent, even **criminal prosecution** is on the table.

- Leaks of sensitive PII can carry similar monetary and criminal penalties, depending on what state your institution is headquartered.

HITECH in Action

- ***Hospital To Pay Millions After Embarrassing Data Breach Put Patient Info On Google!***
  (Business Insider, May ’14)

- ***New York-Presbyterian, Columbia to pay largest HIPAA settlement: $4.8 million!***
  (Modern Healthcare, May ‘14)

- ***Server mishap results in largest HIPAA fine to date!***
  (FierceHealthIT, May ‘14)

We Are Under Attack

- **Data breach at Home Depot leads to fraud**
  - **Credit card numbers hacked from the home improvement retailer are being used in fraudulent transactions.** (Fortune Magazine, Sept. ‘14)

- **Target Now Says 70 Million People Hit in Data Breach**
  Neiman Marcus Also Says Its Customer Data Was Hacked (WSJ, Jan ‘14)

- **Data Breach Bulletin: Dairy Queen, JP Morgan Chase, AT&T** (Forbes, Oct ‘14)

So How do You Stay Out of Trouble?

- Know and follow the data regulations – what you can and can’t do
- Avoid using sensitive data
- Understand that YOUR behavior can be either your biggest protection or your biggest risk
- Be paranoid

The Regulations

- “The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights. At the same time**, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes.”** A guiding principle of the Privacy Rule is the “Minimum Necessary” standard, which says that Covered Entities and their Business Associates **must make all reasonable efforts to limit disclosures of PHI to the minimum amount necessary to accomplish the intended purpose**.

The Regulations (cont'd)

- "The Security Rule specifies a series of **administrative, physical, and technical safeguards** for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information. "

- HITECH **promotes the adoption and meaningful use of health information technology.** Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several **provisions that strengthen the civil and criminal enforcement of the HIPAA rules.**

(HHS.gov)

Practical Application: PHI Use in Research

- **You can use PHI for Research under these circumstances:**
  - **Written Authorization:** A covered entity may disclose protected health information provided that the individual who is the subject of the information (or the individual's personal representative) authorizes it in writing; and
  - **W/Out Written Authorization:**
    - **Documented Institutional Review Board (IRB) or Privacy Board Approval.** (See Your IRB)

PHI Use (cont'd)

- **Preparatory to Research**: Representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose. This provision might be used, for example, **to design a research study or to assess the feasibility of conducting a study.**

PHI Use (cont'd)

- **Research on PHI of Decedents**. Representations from the researcher, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the PHI being sought is necessary for the research, and, at the **request of the covered entity, documentation of the death** of the individuals about whom information is being sought.

PHI Use (cont’d)

- **Limited Data Sets with a Data Use Agreement.** A data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher for research, public health, or health care operations. A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual.

PHI Use (cont'd)

- **Transition Provisions.** Under the Privacy Rule, a covered entity may use and disclose protected health information that was created or received for research, either before or after the applicable compliance date, if the covered entity obtained any one of the following prior to April 14, 2003.

- **An authorization or other express legal permission** from an individual to use or disclose protected health information for the research;

- The **informed consent** of the individual to participate in the research;

PHI Use (cont'd)

- A waiver of authorization approved by either an IRB or a privacy board (in accordance with 45 CFR 164.512(i)(1)(i)); or
- A waiver of informed consent by an IRB in accordance with the Common Rule or an exception under FDA's human subject protection regulations at 21 CFR 50.24.

(HHS.gov)

Caution

- **Written Authorization:** Make sure you use an approved subject authorization form. Consult with your Sponsored Project Office (SPA) or Institutional Review Board (IRB) on the protocols for receiving subject consent.

- **Limited Data Set with Data Use Agreement**: Regulatory requirements for Data Use Agreements are very specific. Need to work with SPA representatives to get the Data Use Agreement reviewed and approved ***before*** the data is received.

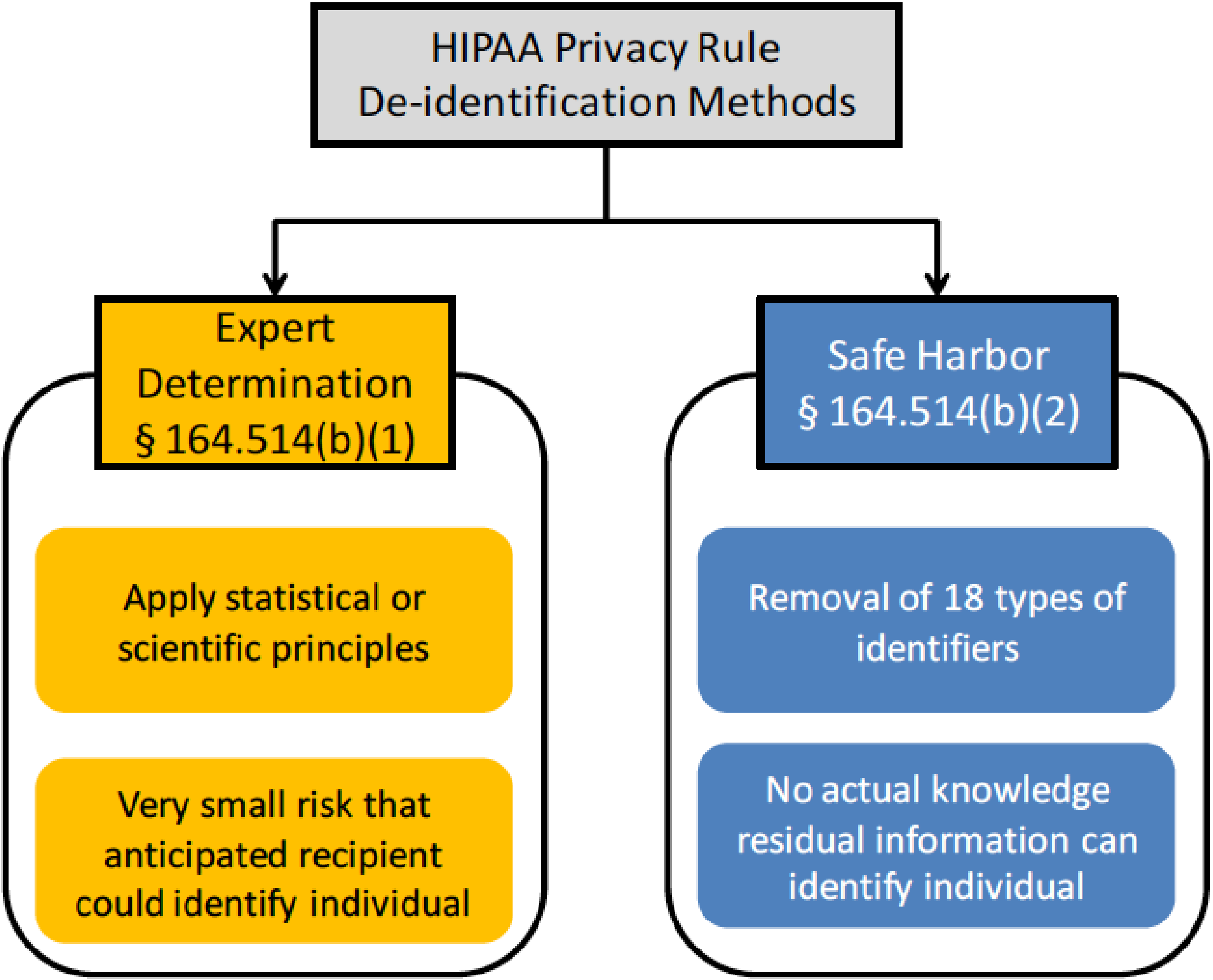
So How do You Stay Out of Trouble?

- Know and follow the data regulations – what you can and can’t do
- Avoid using sensitive data
- Shift the liability to someone else
- Understand that YOUR behavior can be either your biggest protection or your biggest risk
- Be paranoid

Avoid Sensitive Data

- Ask yourself, can you accomplish your goal without using regulated data?

- De-Identify *regulated* data to make it *unregulated*. Take the sensitive information out.



HIPAA Privacy Rule
De-identification Methods

Expert Determination
§ 164.514(b)(1)

Apply statistical or scientific principles

Very small risk that anticipated recipient could identify individual

Safe Harbor
§ 164.514(b)(2)

Removal of 18 types of identifiers

No actual knowledge residual information can identify individual

Identifiable Elements

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
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 plates
13. Device identifiers and serial numbers
14. Web URLs
15. IP addresses
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for *re-identification*

So How do You Stay Out of Trouble?

- Know and follow the data regulations – what you can and can’t do
- Avoid using sensitive data
- Shift the liability to someone else
- Understand that YOUR behavior can be either your biggest protection or your biggest risk
- Be paranoid

The Business Associate

- The HIPAA Privacy Rule says that business associates – subcontractors, vendors, etc. that create, use, or disclose PHI to perform or assist in the functions of a Covered Entity have to meet HIPAA Requirements or be liable

- The Business Associate Agreement (signed between a covered entity and a service provider) says that the service provider is operating to HIPAA standards and **accepts liability in the event it discloses PHI illegally**

- Shift as much of the work related to the collection, analysis, storage of PHI to the business associate to decrease your own liability

HHS.gov

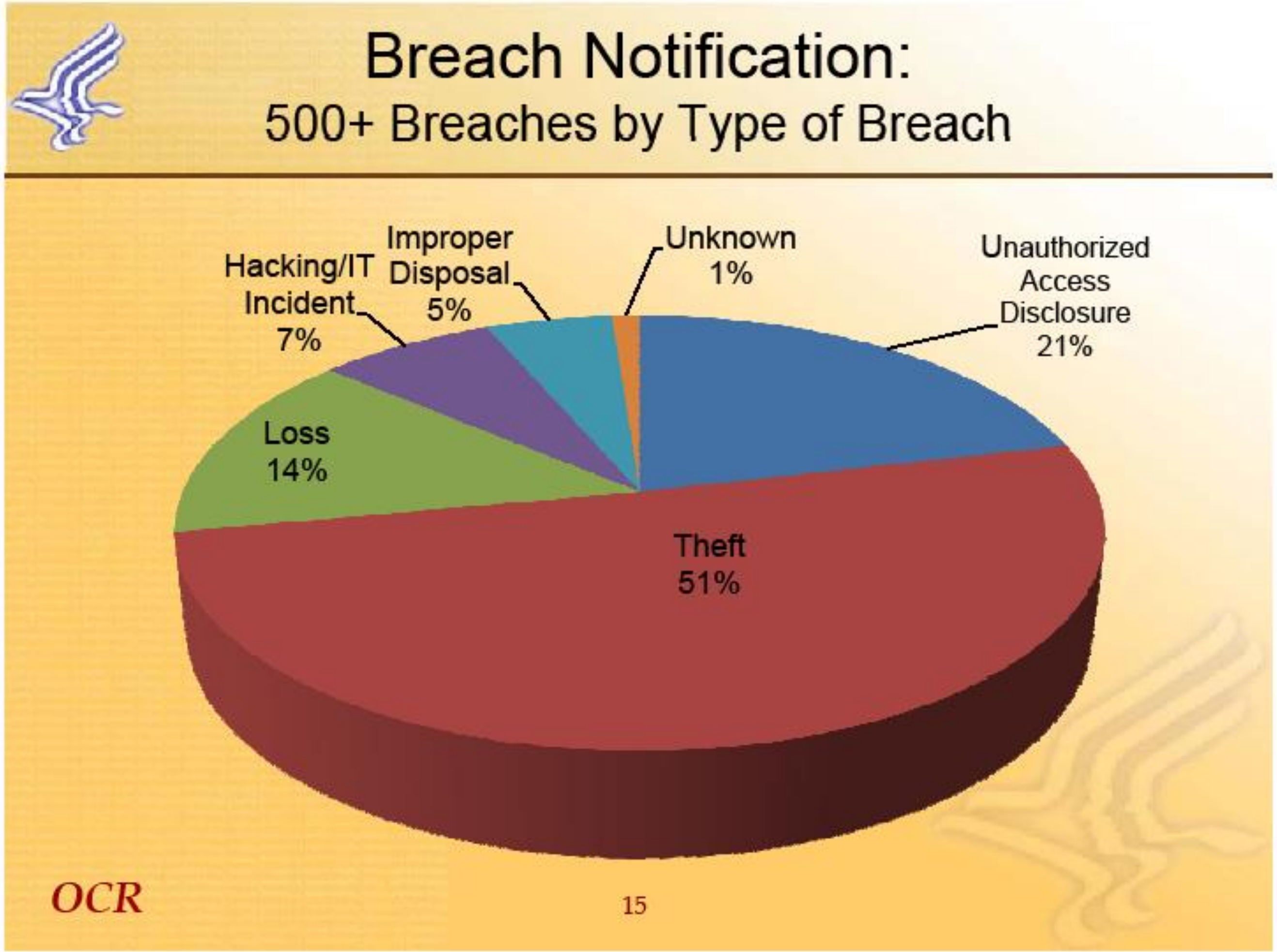
So How do You Stay Out of Trouble?

- Know and follow the data regulations – what you can and can’t do
- Avoid using sensitive data
- Shift the liability to someone else
- Understand that YOUR behavior is your biggest risk
- Be paranoid

Know Your Weak Spots

- You have four main areas of vulnerability:
  - YOU: Weak passwords or password sharing, falling for scams, going “cheap or free”, etc.
  - Hardware: Phones, laptops, desktops, servers, tablets, etc. and issues related to set-up and maintenance
  - Software: Who are you trusting with your data? Downloaded app, enterprise package, custom application, open source (or not) database
  - Environment: Physical security of your equipment

Know the Threats



Breach Notification:

500+ Breaches by Type of Breach

OCR

15

Protect Your Devices

- Password Protect *all* your devices with *strong* passwords
  - Change every 90 days – use password safe software ★
- Set your devices to auto-lock after a period of inactivity (5 minutes or less) ★
- Physically secure your devices and/or environment ★
- Protect your devices with anti-virus ★
- Enable firewalls ★
- Purchase apps only from reputable vendors; disable settings option to download apps from "unknown sources"
- Run as a standard user not administrator ★
- Avoid file sharing software ★

Encrypt, Encrypt, Encrypt

© Can Stock Photo - csp7291832

- Encryption gives CUMC “Safe Harbor” so it 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 (Windows) and Filevault 2 (Mac)
  - 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★
  - 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 O 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

Beware Phishers

- Never click on a link in an unsolicited e-mail if they are asking you to provide information.

- Never provide credentials over the phone, no matter who they say they are

- Do not EVER share your credentials with a colleague or friend ★

Make Use of Existing Secure Resources

- The School provides free secure data storage:
  - 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 ★

- If you need your own servers, outsource to a CUMC IT-certified secure server or host; If you must have your own, get them CUMC Certified via the System Certification ★ Program: http://cumc.columbia.edu/it

…and Avoid Insecure Ones

- Do not use third party e-mail providers, like Google, Hotmail, Yahoo, etc., for *work* ★

- Replace DropBox with Box or SpiderOak for file sharing or better yet, get an SFTP account with CUMC IT

- Do not used any data storage resources for sensitive data that are not certified “compliant” by CUMC IT Security (You may also need a BAA.) ★

…and

- Use only Secure Databases:
  - MS Access is user-friendly and cheap, but it should *never* be used for sensitive data. (Microsoft itself does not recommend it for sensitive data.) It's a file-based database engine, which means your data is stored in a file that theoretically all users can access. Experts have demonstrated that a determined user can simply copy the database file on portable media, take it off site, and with a little skill access the data.

  - My SQL or SQL Server are more secure, because you actually have to access native files on the server to break in. Standard users don't have access to those files; it requires a much more sophisticated hack

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.”

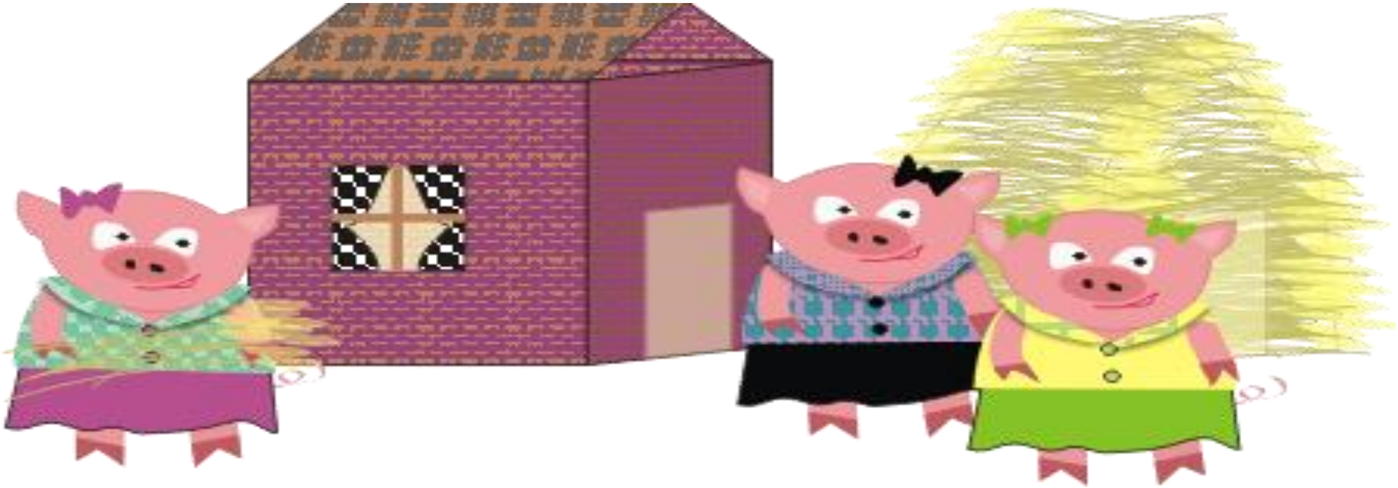
Budget for Data Security

- 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 NIST 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 and found wanting. It is MUCH cheaper and faster to build it correctly than to repair it!



Educate Yourself

- Administrators/owners of applications and servers must take technical data security training, but you can take it, too. Visit the *Data Security & Me* section of the Mailman IT Website for details.

- Attend CUMC’s annual HIPAA/HITECH presentation. It is announced by e-mail. You can also watch the latest one online at the Mailman IT site.

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

- Links to all can be found in *Policy Central* on the Mailman IT Website.

Who Can Help?

- CUMC Help Desk (5 Help)

- CUMC IT Security (5 Help)

- CUMC Privacy: http://www.cumc.columbia.edu/hipaa
- IRB: http://www.cumc.columbia.edu/dept/irb
- SPA: http://spa.columbia.edu

- es2222@cumc.columbia.edu

So How do You Stay Out of Trouble?

- Know and follow the data regulations – what you can and can’t do
- Avoid using sensitive data
- Shift the liability to someone else
- Understand that YOUR behavior can be either your biggest protection or your biggest risk
- Be paranoid