CSCC Information Security

Session I: Identifying and Handling Sensitive Information

Topics Covered

- Why do I need to know about IT Security?
- Sensitive information defined
- Applicable laws and regulations
- CSCC training and policies
- University policies
- Practical tips
- Current and next steps
- Where to learn more

Why do I need to know about IT Security?

- Threats are increasing
- Granting agencies are requiring more comprehensive security plans
- The university has introduced new policies
- The CSCC has a number of existing and new policies
- We’re all responsible for protecting data and resources

Campus-wide statistics

- 30,000 attempted hacks per day
- Thousands of systems have malware on them in any one year
- ~1000 systems isolated a year
- >30-60 systems forensically analyzed by ITS, Information Security per year
- Hack motivations and perpetrators have changed

Sensitive data defined…sort of

Sensitive data is defined as information that is protected against unwarranted disclosure. Access to sensitive data should be safeguarded. Protection of sensitive data may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations.

Sensitive data also includes any information that is protected by University policy from unauthorized access. This information must be restricted to those with a legitimate business need for access. Examples of sensitive information may include, but are not limited to, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, financial donor information, information concerning select agents, system access passwords, information security records, and information file encryption keys.

Source: http://help.unc.edu/6446

Applicable Laws

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
- **NC Identity Theft Protection Act of 2005**
- **Federal Information Security Management Act of 2002 (FISMA)**
- **FDA 21 CFR Part 11**

Less applicable, but important statutes

- **Family Educational Rights and Privacy Act (FERPA):**
  - student records
- **Gramm Leach Bliley Act (GLBA):**
  - customer information
- **Payment Card Industry (PCI) Data Security Standard:**
  - credit card information
- **State Personnel Act:**
  - confidential personnel information
- **North Carolina Public Records Act:**
  - governs which records related to state business are public (email, salary information, etc).

Acronyms

- PHI: Protected Health Information
- PII: Personally Identifiable Information
- IIHI: Individually Identifiable Health Information
- IID: Individually Identifiable Data

What's included: obvious

- Contact info: names, addresses, phone/fax numbers, email, SSNs, driver's license numbers, personnel information, passwords
- Financial: credit card numbers, parent's surname, bank account numbers, PINs, etc
- Medical: medical record numbers, visit dates, biometric identifiers

What's included: less obvious

- All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

PHI: Deidentified vs. Limited Data Set

- Deidentified records:
  - data can't be used alone or in conjunction with other information to identify the patient
  - not subject to HIPAA
- Limited Data Sets:
  - can contain dates and geographic information, but no direct identifiers (names, contact info, SSNs, etc)
  - can be used without authorization or waivers of authorization, but data use agreements must be in place
    - Researchers will safeguard the data from unauthorized disclosure
    - Researchers will not attempt to identify individuals in the data set

Protecting Sensitive Information

- Physical vs. Electronic
- Requirements:
  - Access control
  - Audit trails
  - Disclosure tracking
  - Proper disposal
  - Authorization from individuals

CSCC Training and Policies

- CITI Training
- CSCC Rules of Behavior
  - Complex password requirements
  - Access control: least privilege
  - Appropriate storage/disposal of sensitive information
  - Encrypting sensitive information in transit
- SOPs for sensitive information
  - Confidential trash
  - Remote access
  - Network storage
  - Network/Server security (for Assist staff)

University Policies

- General User Password Policy:
  - complexity requirements, aging, not based on personal information (birthdates, names, ids, etc)
  - no sending of passwords in plain test
- Policy on the Transmission of Protected Health Information and Personal Identifying Information
  - encryption required when sending sensitive info
  - not required for on-campus transfers
  - UNC email encryption software
- Incident Management Policy
  - report incident to Information Security Liaison (Matt)
  - if ISL isn't available, report to Assist
- Protocol for Responding to Security Breaches of Certain Identifying Information
  - notifying affected individuals
  - compensation
  - legal ramifications of a breach

University Policies continued

- Standards for Electronic Media Disposal
  - destruction of hard drives, tapes, CDs, DVDs
- Security Liaison Policy
  - ISLs are in charge of security for departments and centers
  - regularly meet with ITS security and other ISLs
- Data Governance Policy
  - **Data Steward**: Dean, Director
  - **Data Owner**: PI, Faculty, or Staff collecting the data.
  - **Data Custodian**: IT Manager in charge of providing access to and securing data
- Information Security Policy and Standard
  - written in 2003, but still relevant
  - general summary policy; newer policies fill in more details

Practical Tips

http://help.unc.edu/6446

- Maintain inventory of sensitive data
- De-identify wherever possible
- Store electronic data on a securely administered server located in a physically secured area, and limit local workstation storage as much as possible
- Do not send passwords in plain text. Encrypt sensitive communications when transmitting or storing such communications electronically.

Practical Tips continued

- Use SSL or other secure connection to encrypt protected data in transit.
- Limit access to protected data to those who have a business reason to see it.
- Guard access to computers by using strong passwords.
- Change passwords periodically.
- Maintain password confidentially. Do not post passwords.

More information

- University policies:
  - http://its.unc.edu/ITS/about_its/its_policies/index.htm
- University HIPAA home:
  - http://www.unc.edu/hipaa/
- UNC sensitive information links:
  - http://help.unc.edu/6475
  - http://help.unc.edu/6446
- HIPAA
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf