Purpose

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Understanding Sensitive Data and your role in protecting the confidentiality, integrity, and availability of data

Raise awareness about the requirements, policies, and standards of working with sensitive data

Help Sheps employees better understand the risks

Help Sheps employees better understand how to reduce the risks

Information Security

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Understanding Sensitive Data and your role in protecting the confidentiality, integrity, and availability of data

UNC Information Security Policy

All University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to campus who have access to University-owned or managed information through computing systems or devices ("Users") must maintain the security of that information and those systems and devices.

Policy on Sensitive Information

Sensitive Information in all its forms – written, spoken, electronically recorded, or printed – must be protected from accidental or intentional unauthorized modification, destruction, or disclosure.

http://its.unc.edu/ITS/about_its/its_policies/index.htm

What is Sensitive Data

UNC THE CECIL G. SHEPS CENTER FOR HEALTH SERVICES RESEARCH

UNC defines Sensitive Information as all data, in its original and duplicate form, which contains:

- "Personal Identifying Information" as defined by NC Identity Theft Protection Act of 2005.
- "Protected Health Information" as defined by HIPAA
- Student "education records" as defined by the Family Educational Rights and Privacy Act (FERPA)
- "Customer record information" as defined by the Gramm Leach Bliley Act
- "Card holder data" as defined by the Payment Card Industry (PCI) Data Security Standard
- Confidential "personnel information" as defined by the State Personnel Act
- Information deemed confidential by the NC Public Records Act

http://its.unc.edu/ITS/about_its/its_policies/index.htm

Relevant Sensitive Data

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

"Personal Identifying Information" (PII) as defined by NC Identity Theft Protection Act of 2005:

- Social Security numbers
- Employer taxpayer identification numbers
- Driver's license
- State identification card
- Passport numbers
- Banking account numbers
- Credit/Debit card numbers
- PIN codes
- Email addresses other Internet ids
- Digital signatures
- Any other financial resource numbers
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage

Relevant Sensitive Data

UNC THE CECIL G. SHEPS CENTER FOR HEALTH SERVICES RESEARCH

"Protected Health Information" (PHI) as defined by HIPAA:

- Names
- Geographic smaller than a State
- Dates related to individual
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health plan numbers
- Account numbers
- Certificate/license numbers
- Vehicle identification numbers
- Device identifiers
- Web URLS
- IP numbers
- Biometric identifiers
- Face photographic images
- Any other unique identifying number

UNC HIPAA home: http://www.unc.edu/hipaa/index.htm

The Need to Protect…

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Ensure Confidentiality, Integrity, and Availability of data

Protect against reasonably anticipated threats or hazards
Protect against reasonably anticipated uses or disclosures not permitted

Adhere to contracts and agreements
    Contracts and DUAs can be terminated

Loss of trust with business partner

Protect your ability to continue your work/research

Protect your reputation; Protect Sheps reputation

Disciplinary action, criminal and civil action

Things you can do

UNC THE CECIL G. SHEPS CENTER FOR HEALTH SERVICES RESEARCH

Use sensitive data ONLY WHEN NECESSARY

Become “Security Aware” – UNC ITS Security Policies; ICISS policies & procedures

Identify your risks and correct:

- Failure to use passwords or your unique user ID
- Use of weak or shared passwords
- Failure to use a protected screen saver or similar protective feature
- Failure to logoff after each use
- Use of unlicensed software
- Failure to run virus scans or install anti-viral software
- Failure to install personal firewalls
- Physical access by individuals who should not have access to your computer, laptop or confidential data on your workstation
- Mishandling of sensitive data according to DUAs and Contracts
- Mishandling of sensitive data on portable devices
- Misuse of email for sensitive information

Inventory and track your sensitive data

Talk with and work with Sheps IT staff

Passwords

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

- Never let other people use your userid and password to login to a system. You can be held responsible for any activity that happens under your userid
- Passwords should never be written down or stored where others can find it
- Don't reveal a password over the phone to ANYONE
  (neither Sheps nor ITS will ever ask you for your password over the phone)
- Don't reveal a password in an email message
  (neither Sheps nor ITS will ever ask you for your password in an email message)
- Don't share your password with a co-worker to do something for you
- Don’t reuse old passwords

Virus/Malware Protection

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

- Computers housing or accessing sensitive data MUST have Symantec Endpoint Protection (SEP ver.11) installed, active, and up-to-date. SEP-11 is required by UNC ITS Security Office. SEP version 11 for Sensitive Data includes pre-defined scanning schedules, automated notification on infection, and may include firewall options in the future.

- NEVER open any files attached to an email from an unknown, suspicious or untrustworthy source.

- Delete spam, chain email, and other junk email without forwarding to others

- Be cautious of the web sites you visit. Do not download and install software from web sites unless absolutely necessary for your work. **BE SAFE** by checking with the Sheps IT Support team before downloading and installing software.

- If your computer detects a virus or malware, stop using the computer and contact Sheps IT Support immediately at 966-5888.

Keep Your Computer Secure

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

- Shutdown your computer when not in use
- Keep Operating System patches up to date
- Lock your office, close the door when you leave – even if simply walking down the hall for a short time
- Implement automatic screen locks with password after inactivity time
- Regularly backup critical data

- **Include sensitive data ONLY WHEN ABSOLUTELY NECESSARY**

Laptop

- Never leave unattended in a public place
- Implement Whole Disk Encryption

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Office Environment

Sensitive Data = Restricted access

Access only via key to Sheps Center
- Sharing your Sheps Center key is prohibited
- If you lose your key, notify Sheps Business Office immediately

Guests
- Guests must be buzzed in by Sheps receptionist
- Ask who a guest is there to see – then verify with staff member
- Personally escort guest to destination staff or room

Report any unknown guests to Sheps management/Business Office
- Escort unknown visitor out – Get help, if necessary

Do Not prop doors open for others to enter!

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Portable Devices and Media

Portable Devices and Media include laptops, external hard drives, USB keys, flash memory, CDs/DVDs, tapes and other portable storage devices.

Sheps and UNC policies require management approval BEFORE any sensitive data can be placed on a portable device/media

Put sensitive data on portable devices and media ONLY when necessary and ONLY after getting management approval

After demonstrated need and approval, follow Sheps policy and procedures described in: "PLAN-0012 - Device and Removable Media Plan"

All Sheps laptops with sensitive data must be configured with PGP Whole Disk Encryption (WDE). If your laptop does not have WDE, contact the Sheps Computer Support group.

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Handling Hardcopy Documents

Printouts containing sensitive data – particularly direct identifiers – pose a significant security risk. Paper documents containing sensitive information may not be taken out of the Sheps offices without the approval of Sheps management.

When you print sensitive data, it is critical that you remove your printouts from the output tray of that printer as quickly as possible .

Paper documents containing sensitive information must be stored in locked file cabinets within the perimeter of the Sheps offices.

Disposal of printouts with sensitive data must be through shredding in the office or through the designated shredding vendor.

Workstation Security

Sheps Center users must follow the policies, procedures, and guidelines specified in UNC IT Security Policies, HIPAA training, and Sheps Rules of Behavior.

All laptops accessing sensitive data must be configured with Whole Disk Encryption

Workstations storing or having access to sensitive data must be configured with end-point protection (SEP-11) and Qualys vulnerability scans.

You should log off and shutdown your workstation at the end of the day or when away for a long period.

Disposal of workstations that have stored or accessed sensitive data must be conducted according to the UNC IT Security Policy

Notify Sheps Computer support immediately if you suspect malware or notice any other odd activity on your workstation.

See: “PLAN-0011 - Workstation Security Plan.docx”

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Sheps Secure Dataset Servers

If you work with sensitive data as defined by UNC ITS Security Policy, you must work with Sheps Computer Support to design a strategy for protecting that data.

The Center has designated Secure Dataset Servers for working with sensitive research data that fall under Data Use Agreements or Licenses that specify HIPAA or FISMA compliance.

See the Sheps Computer Support group for specific instructions on connecting to the Sheps Secure Dataset Servers

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Remote Connectivity

Remote connectivity to the Sheps Cecil server, the Sheps Secure Dataset Servers, and Sheps office computers is restricted to UNC Virtual Private Network (VPN) connections. To connect remotely, you must authenticate with the UNC VPN first, then connect to the destination computer.

Only UNC owned and Sheps maintained computers should be used to connect to the Sheps Secure Dataset Servers or other Sheps office computer. These computers will have the necessary malware protection software and vulnerability scanning configured to mitigate certain risks.

For specific questions about remote connectivity, contact the Sheps Computer Support group.

UNC
THE CECIL G. SHEPS CENTER
FOR HEALTH SERVICES RESEARCH

Required Training & Policies

- HIPAA Training – completed annually

- UNC Human Research Ethics training
  http://research.unc.edu/offices/human-research-ethics/researchers/training/index.htm
- UNC ITS Security Awareness
  https://itsapps.unc.edu/ITSSelfStudy/

- Sheps Security Training
  This document and other in-person training

- UNC IT Security Policies
  http://its.unc.edu/ITS/about_its/its_policies/index.htm