Cyber Security Awareness Training: LDI Health Services Research Data Center (HSRDC)
Introduction

This HSRDC Cyber Security Awareness course is required of all individuals accessing the HSRDC server. Careful review of these slides and return of your signed certification document to Mollie Epstein (Blockley 1131) will fulfill your requirement for annual information security awareness training established under HSRDC and University of Pennsylvania policy. Remember that while the information you review in this course is specific to the HSRDC, many of the principles discussed are also relevant to you as a personal computer user in other environments.
"Cyber Security Awareness" is the knowledge that individuals authorized to utilize the HSRDC share the responsibility to protect the computer system and the data stored there. Cyber Security Awareness refers to the personal responsibility each of us assumes for ensuring:

- the confidentiality and integrity of private data.
- timely and uninterrupted availability of HSRDC resources for all authorized users.
- University and HSRDC information systems are protected from the potential of fraud, waste and abuse.
Why the HSRDC exists

• The HSRDC exists to provide a highly secure data analysis center for LDI investigators and their authorized research staff members.

• As such, the HSRDC is specifically limited to the storage and analysis of highly sensitive health care data, including individually identifiable electronic records, provided by health care systems, insurers, and/or the federal government.
The Importance of Securing Federal Data on the HSRDC

• Use of federal data (Medicare, Medicaid, etc.) is a privilege granted by the federal government under strict Data Use Agreements (DUAs) with University faculty.

• The government is extremely sensitive to misuse or loss of its data. A recent loss of a portable disk drive by a research staff member in a VA hospital in Alabama nearly resulted in the permanent cancellation of all research activities that use VA data nationwide. The same could easily happen were Medicare, Medicaid, or other sensitive federal data to be lost or misused.
Penalties for Violations of Data Use Agreements

• Breaches of these agreements, including but not limited to loss of portable storage devices with government data, computer log evidence of unapproved downloads, or access or use of data by unauthorized persons, could lead to:
  – Criminal prosecution, including substantial fines and prison time, for research staff and their principal investigators.
  – Cancellation of ALL research data use agreements at the University of Pennsylvania by the federal government, adversely affecting the careers of over 100 faculty and staff.
Key Contacts

• Please be aware of any activity that might violate and/or compromise the security of UPENN and the HSRDC information systems.

• Report all incidents to:
  – Nate DiGiorgio, Systems Architect
    nathansd@mail.med.upenn.edu
  – Mollie Epstein, Data Center Coordinator
    mollie@mail.med.upenn.edu
Outline of Cybersecurity Best Practices

• Passwords
• Computer security habits
• Knowledge of what constitutes misuse/inappropriate use of the server
Passwords

- Passwords are important tools protecting the HSRDC information systems.
- Your HSRDC password should not be the same as a password used on any other computing environment.
- Keep your password secret to protect yourself and your work. If you must record your password in order to remember it, keep it in a secure place, to which only you have access.
Passwords

Passwords must:

• Be constructed of at least eight characters (i.e., Gabc123&). Use at least three of the following four kinds of characters:
  - Upper case letters (ABC...)
  - Lower-case letters (...xyz)
  - Numbers (0123456789)
  - "Special characters," such as: #, &, *, or @

• Be changed at least every 120 days. You will receive a reminder 15 days prior to your password expiration when you log onto the server.

• If you forget your password, our system staff are able to reset it for you.

• Using these rules will provide you with a "strong" password, which is required by the HSRDC.
Passwords

The following is an example on how to create a strong password:

- Think of a sentence that is meaningful to you and that you can easily remember.
  "I like a good cup of coffee in the morning."
- Now take the first letter of each word: Ilagcocitm
- Capitalize one or two letters: iLagcocitm
- Replace a couple letters with numbers that are similar to that letter: E becomes 3, L or I becomes 1 or !, a becomes @, o ("oh") becomes 0 (zero).
- "ILagcocitm" now becomes "1L@gc0c!tM."
- This is a very strong password because it does not contain any dictionary words and it contains all 4 types of characters that are recommended (uppercase, lowercase, numbers and symbols).
Passwords

- Many factors can contribute to poor passwords, which are easily “hacked.” Some of the most notable are:
  - Passwords that are not "strong“—see previous slides.
  - Use of common words easily obtained from a dictionary.
  - Passwords referring to your personal life (for example, names of family members or pets).
- Easily identifiable passwords are an open invitation to hackers.
Passwords

• Rules of Thumb:
  – Follow the rules for strong passwords.
  – Do not use personal references (names, birthdays, addresses, etc.).
  – Change your passwords at least every 120 days. If you suspect that someone is trying or may have obtained your password, change it immediately (UNIX command: `passwd`), and inform the HSRDC systems staff.
  – Be sure nobody can observe you while you type your password. If you are in a shared office, position your keyboard so that it is not easy to see what you type.
  – If you record your passwords, you should store them in a manner where they cannot be accessed by others.
System Security: 6 Habits of Secure IT Users

There are some simple habits you can adopt that, if performed consistently, may dramatically reduce the chances that the security of the HSRDC is compromised.

1. **Lock your computer when you are away from it**
   - Keyboard shortcut: Windows logo key + L
   - Enable your screen saver to start after 15 minutes of inactivity and require a password to sign back in.

2. **Log off the server if you are not actively using it**
   - run long jobs using UNIX batch mode with prefix ‘nohup’ (i.e. nohup sas mycode.sas &).

3. **Do not allow others except University information technology local support providers to access your PC**
   - You are strongly recommended to limit access any other personal computer you use to make a remote connection to the HSRDC.

4. Do not use public PCs (e.g. library PCs with an internet connection) or other shared devices to make remote connections to the HSRDC
   • for example, if you are in a cafe in a new city and your computer reports that 4 wireless networks are in range ("Starbucks1", "Sbux", "Star-bucks", "Tmobile"), there is a chance you might accidentally select a malicious network that is named in such a way to fool you into trusting it. It may be designed to intercept your traffic or redirect your network packets somewhere else.

5. Lock your office door when you leave your office

6. Enable host security software
   • Install an AntiVirus client and enable automatic updates (Penn provides Norton for Mac OS X and Symantec for Windows at http://www.upenn.edu/computing/virus/).
   • Make sure the host firewall is on ("Windows Firewall" for Windows users and "Sharing" tab for Mac OS X users).
   • Make sure Automatic Updates are enabled for Windows users.
System Security: Social Engineering

• Social engineering is an unauthorized person's manipulation of your trust to get you to share information or resources that you should not share.
• Make sure when you are asked by someone to provide information or allow the use of your computer or server accounts that you are certain of who they are and of their authorization to have/use that information or access as part of their job. Dishonest "social engineers" look for almost any kind of information to misuse.
• In general, no one should ever use someone else’s login account to access the HSRDC server.
• HSRDC staff will never send you an email or call you asking for your password.
System Security: Downloads

• Downloading of any data on the HSRDC server to your own PC, laptop, or portable storage devices is **prohibited**, unless you have specific permission to do so in a Data Use Agreement executed between the Principal Investigator of your project and the Federal Government, State Government, or other owner of the data.
System Security: Backups

- HSRDC systems administrators are able to ensure your work is saved in several places (backed up) so it will not be lost in the event of a hardware or software failure.

- In order for your work to be backed up, you must notify the system administrators of the specific directory and path name of the work you want backed up.

- If you have any questions about the backup procedures or procedure to follow for data restoration, contact Nate DiGiorgio or John Quigley.
Misuse or Inappropriate Use/1

- Any use of the server for activities that are not related to IRB and HSRDC approved research projects or formal educational activities under the direct supervision of a faculty member at the University of Pennsylvania is expressly prohibited.

- Use of the server for commercial purposes, or in support of "for profit" activities, or in support of other outside employment or business activity (e.g. consulting for pay) is also prohibited.
Misuse or Inappropriate Use/2

- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software; copyrighted, trademarked, or material with other intellectual property rights beyond fair use; proprietary data; or export-controlled software or data is also prohibited.
Misuse or Inappropriate Use/3

• The creation, uploading, storage, or transmission of sexually explicit or sexually oriented materials.
• The creation, uploading, storage, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.
• Uploading unapproved software, unapproved data, or any peer-to-peer file sharing (e.g., Kazaa) is also prohibited on the HSRDC servers.
Questions?

• Questions from students regarding these policies should be directed to supervising faculty in your degree programs.

• Questions from University staff should be directed to your supervising principal investigator.

• Questions from Principal Investigators and other faculty members can be directed to the HSRDC Director, Pete Groeneveld, MD, MS at petergro@mail.med.upenn.edu
Summary

• This brief presentation has outlined the policies for secure use of the LDI HSRDC that must be followed to ensure this valuable resource is protected and will continue to be available for health services research at Penn.

• Please print and sign the accompanying certification sheet indicating that you have reviewed and agree to abide by the policies presented here.

• This form should be returned to Mollie Epstein (1131 Blockley Hall), mollie@mail.med.upenn.edu.