About this Tool
"Information Security for Residents"...

Purpose: Provide materials to inform and educate Residents in order to reach compliance regarding information security.

Audience: New Residents

Information Security for Residents

Outlining Your Responsibilities for Information Security

Information Security Overview

Information Security is not just about computers, it is how we go about our business here at UW Medicine.

- ☆ Information Security is a responsibility of each members of the UW Medicine Workforce*

  * Faculty, employees, trainees, volunteers, and other persons who perform work for UW Medicine

The Standard Responsibilities (1)

- Comply with the state & federal law
  - **Federal Copyright Law**

    Unauthorized use of software, images, music, or files is regarded as a serious matter and any such use is without the consent of UW Medicine, those responsible for such abuse may be held legally accountable as well as be held accountable for violation of UW Medicine Policy.
  - **Use of Departmental Computers (RCW 42.52.360, WAC 292-110-010)**

    Aside from *occasional* and *de minimus* (e.g., of minimal cost to the State) use, the policy prohibits the personal use of computers, email and the Internet. This limitation is similar to permitted personal use of non-computer resources, such as telephone calls.

The Standard Responsibilities

- Follow University of Washington and UW Medicine policies

University of Washington:

http://www.washington.edu/admin/

Go to: Reference/Resources:
Policies/Procedures:

UW Medicine:

Privacy:

http://depts.washington.edu/comply/privacy.shtml

Information Security:

http://depts.washington.edu/comply/security.shtml

Responsibilities Directly Related to UW Medicine Information Security

- Maintain confidentiality;
- Protect access accounts, privileges, and associated passwords;
- Accept accountability for your individual user accounts;
- Do not share userID and/or password (this includes logging in for others…)

Information Security Responsibilities (2)

- Report all suspected security and/or policy breaches to the IT Services help Desk by phone: 206.543.7012 or email: mcsos@u.washington.edu;
- Do Not Download, Install or Run Unknown Files or Software – Use only licensed and authorized software;
- Do Not Disable workstations firewalls and/or anti-virus.

Apply Reasonable Safeguards

- Log off or secure your workstations when not in use or unattended
- Store CONFIDENTIAL information in suitable locked cabinets or desks when not in use
- Clear CONFIDENTIAL information from printers immediately
- Dispose of CONFIDENTIAL information in a secure manner (e.g., locked recycle bins)

Classification of Information

UW Medicine classifies its information to include an assessment for confidentiality level, which can be set as PUBLIC, RESTRICTED or CONFIDENTIAL.

Protected Health Information (PHI) is very sensitive in nature and requires careful controls and protection.

PHI is an example of a CONFIDENTIAL classification.

Protected Health Information (PHI)

- Relates to the past, present, or future physical or mental health or condition of an individual; or
- Relates to the provision of health care to an individual; or
- Relates to the past, present, or future payment for the provision of health care to an individual; and
- Identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

UW Medicine has exclusive rights over the information within its systems.

WARNING:
Your Email is NOT Private

Before you freely email personal thoughts or information, please consider unlike telephone conversations, email and its archives are subject to legal and public inspection and that many computers retain old emails in archives for years.

Lawyers subpoena email as a part of evidence gathering.

Private watchdog groups, outside University of Washington and Washington State, monitor email for abuse, and.

If you would not want to see your most sensitive and/or private email printed in newspapers, do not send it.

Minimum Information Security Requirements PDAs & Smart Phones using Wireless or PHI

1. Updated and patched operating system
2. No automatic login. Configure the OS to not automatically log you in.
3. Password protected using a complex password.
4. Use active network filtering or firewall.
5. Use active protection against malicious software & scan for viruses prior to connecting to the UW Medicine network. Any workstation used to synchronize PDA should have current antivirus software installed on it.
6. If others use your PDA or smart phone - Each user needs own log-on & password.
7. If you use wireless transmissions, install a VPN client on your PDA.
8. If you do not use wireless transmissions, disable the wireless port to reduce the risk of sensitive data being transmitted to unauthorized individuals.

Minimum Information Security Requirements Workstations (Including Laptops)

- Approved operating system that is patched in a timely manner
- Protection against malicious software (i.e. anti-virus protection)
- Filtering or firewall protection
- Approved network media & protocols
- Enabled logging and auditing
- Disable all unused system services
- Unique accounts & complex passwords

Sanctions

- The regulation requires that we apply appropriate sanctions against individuals if you fail to comply with the security policies and procedures.
- UW Medicine has sanctions for the failure to follow policy and/or for a breach of patient confidentiality or information security.

UW Medicine Resource for HIPAA Compliance Questions

Richard Meeks
HIPAA Compliance Officer
UW Medicine Compliance
206-543-0300
meeksr@u.washington.edu

UW Medicine Resources for Complaints & Investigations

Privacy Official's Contact numbers for UW Medicine entities:

University of Washington Medical Center & Clinics	(206) 598-4342
Harborview Medical Center & Clinics	(206) 744-9003
UW Medicine Neighborhood Clinics (UWPN)	(206) 520-5505
University of Washington Sports Medicine Clinic	(206) 543-1552
University of Washington East Specialties Clinic	(206) 520-2222
University of Washington Hall Health Primary Care Center	(206) 685-1081
University of Washington Physicians	(206) 543-6420
University of Washington School of Medicine	(206) 543-0300

Use of Departmental Computers (RCW 42.52.360, WAC 292-110-010)

In 1997, the State of Washington Executive Ethics Board defined permitted personal activities on State owned computers. This policy was amended in 2002 to permit limited Internet use. Aside from *occasional* and *de minimus* (e.g., of minimal cost to the State) use, the policy prohibits the personal use of computers, email and the Internet. This limitation is similar to permitted personal use of non-computer resources, such as telephone calls. The State allows limited personal use of computer resources provided the use:

- Results in little or no cost to the State;
- Does not interfere with the employee's official duties;
- Is brief in duration, occurs infrequently, and is the effective use of time and resources;
- Does not disrupt or distract from the conduct of State business due to volume or frequency;
- Does not compromise the security or integrity of State property, information or software;
- Does not disrupt other State employees and does not obligate them to make personal use of State resources.

More:
Using Washington State Equipment

Washington State law also prohibits the use of UW Medicine computers for personal business-related, commercial, campaign or political purposes, or to promote an outside business or group or to conduct illegal activities. Additionally, employees are prohibited from allowing any member of the public to make personal use of state computers and computing resources.

Washington State specifically prohibits use of the computer for all political and commercial activities. The following items have been additionally called out in detail.

- Notices for selling of personal items on any State owned computer system.
- Notices for charity/fund raising events whether selling an item or raising money unless the activity is University sponsored.

Many Internet Activities Expressly Prohibited

Although de minimus personal Internet use is now allowable, many Internet activities are still prohibited. Downloading copyrighted files, such as MP3 music files, may violate copyright law, and subject UW and you to penalties and fines. Other examples of improper or excessive use are included in the Executive Ethics Board web site: http://www.wa.gov/ethics

and the UW Administrative Policy web site http://www.washington.edu/admin/adminpro/APS/47.02.html

Some examples of permitted activities may be prohibited in Lab Medicine because of their potential impacts. For example, extensive use of streaming video or streaming audio can overload the capacity of the network and interfere with the laboratory information system.

Secure Disposal of Media

- Paper Documentation - Paper records shall be shredded, pulped or otherwise obliterated in a manner that prevents reconstruction.
- Microfilm/Microfiche - Microfilm and microfiche must be pulverized.
- Laser Disks - The laser disks used in write once-read many (WORM) document imaging applications shall be pulverized.
- Floppy Disks - Floppy disks shall be pulverized.
- Compact Discs (CDs) and Digital Versatile Disc (DVDs) - CDs/DVDs shall be pulverized.
- Magnetic Tape & Video Tape - The preferred method for destroying computerized data is magnetic degaussing. If destruction is not achieved by degaussing, destruction must be executed in a manner that assures the information cannot be reconstructed.
- Hard Drives - To assure that computerized data is destroyed when equipment is decommissioned, use a three-pass binary overwrite of the entire disk. If overwriting is not possible, permission to remove and pulverize the hard drive must be obtained from surplus2@u.washington.edu. System Operator or designee shall log disposal of hard drives in order to maintain an audit trail.
- Carbon Rolls (from printers or fax machines) - Send carbon rollers that have been removed from printers or fax machines to Environmental Services for destruction by autoclaving.

Protect Against Malicious Software

- Use anti-virus software to scan all diskettes and files provided to you by others or after using them on another computer
- Do not open email attachments from unknown senders.
- Verify attachments from known senders and scan them before opening. If the user expects an attachment, make sure that the attachment's file type and sender are consistent with what was expected
- Follow this same process for Internet downloads.

Questions?

Please let Rich Masse know if you have any questions.

rmasse@uw.edu

or

206-685-4356

UW Medicine
Resource for Questions

The School of Medicine
Compliance Officer

somcompl@uw.edu

206-543-0300