UW Department of Orthopaedics

Information Security

Overview of User Responsibilities

At the University of Washington we have a responsibility to maintain a secure and safe work environment, including our electronic environment. With information technology tools and devices that now serve us both in our work environment and in our personal computing environment, it's important that we manage all of our electronic computing devices appropriately. Practicing secure computing is everyone's responsibility because one infected computer or system can quickly infect others. This is a brief summary of your responsibilities surrounding information security in the Department of Orthopaedics.

Overview: All faculty, staff, students and volunteers in the Department of Orthopaedics, using computing devices connected to UW and UW Medicine networks (wired or wireless) or using UW and UW Medicine electronic data have a responsibility to comply with UW and UW Medicine policies. These policies are designed to meet the federal and state laws applicable to our business objectives and can be found on the web:

UW Information Security Policies: http://www.washington.edu/admin/rules/policies/APS/TOC00.html
UW Medicine Information Security Policies: http://security.uwmedicine.org/guidance/policy/default.asp

User Accounts: You are provided user accounts to conduct your work at the UW and you are responsible for managing these accounts in a secure way. You will be held accountable for what is done with your user accounts.

- Protect your computer access accounts, privileges, and all associated passwords. Don't login for others; each employee is to be granted individual access based on his/her duties and responsibilities.
- Never share or tell anyone your password. UW staff, including UW Information Technology consultants, will NEVER ask for your password. Email messages that ask you to send your UW NetID and password (such as to "verify your account") are fakes and should not be responded to.
- Use passwords that are difficult to guess. EX: Password, abc123, 123456 are not good passwords.

At Your Computer: Your desktop, laptop and other portable device(s) should be protected from both physical theft and electronic tampering. If you have questions, email orthohlp@uw.edu or call (206) 221-5380.

- Protect, and maintain, any personally owned devices that are used for work in the same way you would protect your work devices (these include smart phones, laptop and tablet computers).
- When you use a mobile device like a laptop or tablet to access UW Medicine confidential information then you must encrypt the data in storage.
- Designated system administrators are permitted to install software and licensed software on UW devices.
- Maintain an up to date operating system on all of your personal devices that interact with PHI.
- Up to date firewalls and anti-virus software are required at the UW. Also use anti-virus software to scan all thumb drives, CDs, and downloaded files provided to you by others.
- Always secure your computer and/or your office door when you leave your work area.
- Be wary and cautious if you receive strange email even if the name of the sender is familiar. Many scams use known contacts and/or mimic common vendors (e.g. PayPal, Microsoft, banks) and will ask you to click on an embedded link in the email to take some action.
- If you have access to protected health information (PHI) and work in an area where patients or the public have access, you must be especially careful about protecting patient information. Where possible, orient your monitor away from public view and/or attach a privacy screen.
- When purchasing new equipment, check with the CSG for computer standards such as operating systems and security applications to be included in the purchase.

In Your Workspace: Use appropriate measures to physically protect information on and around your work area.

- Lock away paper and computer media containing confidential or critical business information in suitable locked cabinets, desks or offices when not in use or when unattended.
- Do not leave fax machines or copiers in unattended places where they can be accessed by unauthorized individuals. Clear critical business and confidential documents from shared printers and fax machines immediately.

***Incident Reporting*:** It is the responsibility of all UW workforce members to report information security incidents when they occur. As soon as you recognize, or suspect, an information security incident may have occurred, report it to the CSG as soon as possible, email: orthohlp@uw.edu or call (206) 221-5380.

Resources: Below are several web links that provide additional security information. If you have any questions or suggestions contact the CSG directly, orthohlp@uw.edu.

UW Information Technology (IT Connect) – Safe and Secure Computing:
http://www.washington.edu/itconnect/security/

UW Medicine Information Technology Services Security:
https://security.uwmedicine.org/default.asp