Data Stewardship: The most important things to know

The ability to access information electronically provides convenience and enables productivity for all of us. Unfortunately, this convenience is also a risk. Don't be a victim of a data breach. Protect your equipment.

You are responsible for Data Stewardship.

It is your responsibility to protect **Confidential** and **Restricted** information from being inappropriately revealed or damaged by anyone either maliciously or unintentionally.

- **Confidential Data** --protection of confidential data is required by law.
  - PHI (protected health information)--protected by HIPAA - All PHI breaches must be reported to the federal government Office for Civil Rights and to the State Attorney General, e.g. patient Information
  - Individual Student Records--protected by FERPA
  - Individual financial information (e.g., payment card, bank information)
  - Other personal information (e.g., Social Security number, home address, personal contact information, performance reviews)
  - Proprietary--intellectual property or trade secrets
- **Restricted Data** -- data that is not regulated, but for business purposes, is considered protected either by contract or best practice, e.g. contract pricing, study data

Protect yourself from a breach of confidential or restricted data:

- **Assume your devices contain confidential or restricted data, even without intentional action on your part.**
  - Email can and often does contain some confidential or restricted information in attachments and in the body of long email threads
  - Files that are synced from a file sharing system like *OneDrive for Business* may contain confidential or restricted information
- **Encrypt your devices – Never assume they are already encrypted.**

  Encryption is not the same as Password protection. You need both!

  Encryption protects the data storage units inside devices from being removed from the original device and read on another device. All of the following types of devices can be encrypted:
  - Smart phones
  - Laptops/Tablets
  - Mobile devices of all types: thumb drives, jump drives, external hard drives, etc.
  - Desktops (Encrypt desktops even if they are in a locked environment.)
- **Password protect your devices**
  - Passwords help protect devices from access by anyone who is not authorized to do so.
  - "Proper" passwords must be complex:
    - At least 8 characters long
    - Contain at least 1 numeric character
    - Contain at least 1 symbol
    - Be a mix of upper and lower case characters
  - Passwords should be changed often; at least every 120 days

  <u>Password protect and encrypt and you greatly reduced the likelihood of a data breach in the event of a loss or theft!</u>

Free help with Password Protection, Encryption and Compute in Place:

If you are in the Department of Medicine visit a data Stewardship Kiosk

- To view the kiosk schedule: https://depts.washington.edu/domis/kioskschedule or call IS Help 206-616-8805 and arrange an appointment

Email ishelp@medicine.washington.edu

Visit the DoM IT Services Web Site for more information:

- https://depts.washington.edu/domis

Visit the UW Medicine Security site for more information:

- https://security.uwmedicine.org

- **To find, lock and/or remove data from your lost or Stolen Cell Phone / Table:**
  - On Apple devices Enable "find my iPhone/Mac" – Allows you to find and/or remotely remove data from you're device.
  - On Android devices use the 'Android Manager Website' – Allows you to Find, Lock and/or remotely remove data from you're device.

- **Compute in Place: DO NOT copy information to your mobile or remote devices – if it's not on your device, a breach due to loss or theft can't occur.**
  - Whenever possible use a web-based email tool to access your email – this keeps your email on the server, not on your mobile/remote device!
    - If you use an email program e.g. Outlook, on your mobile device) the email is likely stored locally
    - If you use a program (e.g. Outlook) to access your email, configure it to not store (cache) email locally
  - Use a VPN (virtual private network) to access UW Medicine resources from off the network
  - Whenever possible use Remote Desktop or Terminal Server to work from off-site locations – this keeps the information off your mobile/remote device!
  - If the UW system has an encrypted web interface (denoted by "https://"), use it instead of a desktop application – this keeps most information off your mobile/remote device!

- **Do not use unauthorized cloud or other offsite services**

  DO NOT send or store confidential or restricted information using unapproved cloud services or applications. The approved vendor products listed below are the only ones that may be used with confidential or restricted information, as the University of Washington has executed the appropriate legal agreements with the vendors for this purpose:

Cloud Applications **Approved** for use with Restricted or Confidential Information	Cloud Applications **NOT** Approved for use with Restricted or Confidential Information
OneDrive for Business	OneDrive
Lync	Google Apps
Azure	iCloud
Office 365	DropBox
	Amazon Web Services

For the most current information on cloud services visit:
http://security.uwmedicine.org/guidance/technical/cloud_computing/default.asp