Data Storage and Security Policies

Department of Medicine IT Services

Modified 01.08.2015

UW Medicine policy regarding data access, storage, and security can be found on the UW Medicine website at https://security.uwmedicine.org/guidance/policy/default.asp.

Data Storage

All restricted and/or confidential data must be encrypted or otherwise physically secured in a manner sufficient to prevent its theft or inappropriate use. This includes data in transit (that is, data that is being removed from its origin computing system by electronic or physical means).

All electronic data must be backed up to meet the business need for that data. All data must be available in the event of an emergency.

Policies DS-1, DT-1, DB-1, DB-2 - https://security.uwmedicine.org/guidance/policy/electronic_data/default.asp
Policies PS-1, PS-2 - https://security.uwmedicine.org/guidance/policy/computingdevice_system/default.asp
https://security.uwmedicine.org/guidance/technical/encryption/default.asp
Physical Data Security Controls - https://security.uwmedicine.org/guidance/standards/system_security/default.asp

Personally-Owned Computing Devices

Devices owned by personnel that are used for UW Medicine business operations must comply with the same security requirements as those owned by the University.

Policy POCD-1 - https://security.uwmedicine.org/guidance/policy/computingdevice_system/default.asp
https://security.uwmedicine.org/guidance/technical/mobile_devices/default.asp

Use of Cloud Storage

Consumer cloud services are not acceptable for storing restricted and/or confidential data. Compliant cloud services require a business associate agreement (BAA) between the provider and the University (or any department thereof).

Unacceptable cloud storage services include:

- Dropbox
- Google Drive
- Box
- SpiderOak

UW OneDrive for Business is acceptable to use for all data types.

https://security.uwmedicine.org/guidance/technical/cloud_computing/default.asp

Passwords

UW Medicine workforce members must use strong passwords for their accounts. Strong passwords are at least 8 characters in length and include a mix of uppercase and lowercase letters, numbers, and symbols.

All passwords used for University business must be changed at least once every 120 days.

Policies UAM-1, UAM-2 - https://security.uwmedicine.org/guidance/policy/workforce_member/default.asp

Compliant Email Resources

All UW business must be conducted using an approved email service. Approved University email resources include UW Deskmail, UW Exchange Online/Office 365, UW Medicine Exchange, and Department of Medicine (Outpost) Exchange.

Unacceptable email systems include:

- UW Google Apps
- Gmail
- Hotmail/Outlook.com
- Yahoo

https://security.uwmedicine.org/guidance/technical/electronic_comm/email/default.asp