

Safe Password Management

For safe password management, a “Password Manager” can be used as long as the following guidelines, which are recommended by UMass Medical School Information Security, are followed:

- Encrypted
- Wipes the database clean after 5 failed logon attempts
- The database is password protected – and this password cannot be written down or stored elsewhere
- 2 Factor Authentication
- Recommended that the Password Manager is stored on a desktop or mobile device, and not in the cloud

