

Student Use Policy and Procedure

Portable Electronic Devices

POLICY

Since portable electronic devices, such as a laptop, mobile pc, or PDA, may contain sensitive information, students must take precautions to safeguard confidential patient information. All students should protect mobile devices with passwords. All clinical papers that may include patient information **MUST** be saved as password protected documents using Open Office. Students will use the passwords provided by the faculty for these documents. Students are responsible for maintaining HIPAA regulations with regard to private information. Since electronic devices are more enticing to thieves, mobile devices pose a special risk with regard to breaches of confidentiality. The following procedures are designed to provide security for sensitive information.

PROCEDURES

Saving Documents Using Passwords

- All documents containing ANY patient information will be stored in Open Office format using the approved password provided by faculty. Passwords for clinical information will be provided by faculty. Students will not keep passwords with the computers.
- Passwords should not be identified in any way that will associate them with the private documents (e.g. Passwords will not be labeled as “clinical paper passwords” or in any other identifiable manner.)
- Students may be asked to show faculty where confidential documents are filed at any time requested to ensure compliance with password use.

Security

- When students are working on documents containing any patient information, these documents will be treated as open electronic charts. Computers are not to be left unattended while sensitive documents are open. Students must close any document containing patient information and save the document using the provided password before leaving the computer.
- ASUS PCs are not to be left in any vehicle, even if the vehicle is locked.
- Students will not leave unattended computers in any public place, such as the library, Study Center, or classroom.
- In situations where the student shares living space with other students, computers will be stored out of sight when not in use.
- Students are responsible for securing the ASUS PCs.