The average cost of a PDA? $300
The average cost of encryption software for the PDA? $30
The cost of a lost or stolen PDA with sensitive data that has NOT been encrypted? PRICELESS

Ever felt that panic when you can’t find your PDA? The biggest security threat to a PDA is loss or theft. What type of information could be exposed if your PDA were lost or stolen today?

- Passwords?
- E-mail?
- Sensitive work information such as Protected Health Information (PHI), financial or personnel information?
- Personal information such as bank account information, credit card numbers, social security numbers?

Although we can never completely eliminate the possibility of loss or theft, we can ensure that the information on our handheld device is protected.

Tips to Secure PDA’s and other Handheld Devices:

1. Enable a power-on password - Use a strong password with a minimum password length of 8 characters or keys and require a password in order to sync or backup the device to the desktop.
2. Encrypt sensitive data – By encrypting files, you ensure that unauthorized people can’t view data even if they have physical access to the device. When using encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data. Encryption software is built into some PDAs. (You have to activate it before it will work!) It is also available from several reputable vendors such as: PDA Defense, Bluefire Security, Credant, Certicom, Trust Digital…
3. Configure the device to log-off or power down no longer than (15) minutes after the last user activity.
4. Enable device reset (data erasure) if an incorrect password is entered more than (5) consecutive times.
5. Use anti-virus and firewall software – AV/Firewall software for handheld devices is available from F-Secure, Trendmicro, Symantec…
6. Disable Bluetooth and other network device connections (Infrared, 802.11, CDMA, GPRS) when not in use to prevent handheld device viruses and other malicious activity.
7. Never leave your handheld device unattended.
8. Use Virtual Private Network (VPN) when the handheld device connects to the organization over the Internet in order to access and transmit data securely.
9. Keep patches up to date for the software operating on your device. This will prevent attackers from taking advantage of known vulnerabilities.
10. Immediately report the loss, theft or any unauthorized use of your handheld device that has been used to store or access protected health information or other sensitive information to the School of Medicine HIPAA Security Officer.

Please review The School of Medicine Policy for Handheld Computing Devices and ensure that you are in compliance.