Your laptop is for conducting Providence business. Protect it and your data from theft or loss.
Your laptop is encrypted
Encryption is a process that disguises data so it cannot be read by unauthorized individuals. For encryption to be effective, your laptop must be shut down or logged off and not left in “stand by” or “hibernate.”

Keep data secure
- When working off-site, use your secure VPN login to access files on the network drives. Do not transfer files to a non-Providence computer using a thumb drive or e-mail.
- When sending confidential information to a recipient outside of Providence, type ‘provsecure’ in the subject line of your Outlook message to secure its contents.
- Maintain the security of your computer by not tampering with firewalls or anti-virus programs.
- Adding software to your laptop can cause other components of the computer to malfunction. Contact your local Help Desk if you need to add a new software application.
- Providence laptops need to be connected to our network at least once each month for a minimum of two hours to receive automatic updates for functionality.
- Family members and friends are not authorized to use your laptop.

Traveling with your laptop
- A vehicle is not considered a secure location and a laptop should never be left unattended in a vehicle.
- Keep your laptop with your carry-on luggage; do not check it in.
- When working outside a Providence facility, take additional measures to secure your laptop when leaving it unattended, such as using a cable lock.

Reporting a loss or theft
Act immediately if your laptop is lost or stolen by notifying your manager and reporting the incident to the Providence Security Operations Center.

You will need to report:
- Circumstances of loss or theft
- Type of information on the laptop (i.e., patient data, financial data)
- Encryption status -- Was the laptop powered on and in “stand by” or “hibernate?” Was the laptop logged off or powered off?