Transporting Protected Health Information

All protected health information in paper and electronic form must be **transported** and **stored** in a secure manner to safeguard it against improper disclosure and/or loss.

- **PHI that is being transported within a facility,** such as from one department to another, must be attended or supervised at all times, or otherwise secured to avoid unauthorized access, loss and/or tampering.

PHI that is transported by motor vehicle:

- Should be transported in a secure container such as a locked box or briefcase whenever possible; and
- Should be transported without stops that involve leaving the vehicle unattended if possible.
- If stops must be made do not leave the PHI in the vehicle. Remove it and secure it so that others who do not have a need to know it cannot access it if the vehicle is broken in to or stolen.

Securing PHI that is taken home, to another location, or accessed remotely:

Remote access into the computer network via VPN is preferable to taking PHI home. To obtain remote access, complete the form at:

https://net.unmc.edu/netid/accountrequestremote.php

If PHI is accessed from home or is taken home to work during off-hours:

- Employees' supervisor should be notified & approve such work at home off-hours
- PHI in the home must be secured from access or view by family members & others
- Workforce members shall log out of information immediately after use and shall secure their login and password so that others cannot use it

Mobile devices must be password protected and encrypted. For additional information, refer to the End User Device procedure.

If PHI is lost, stolen or improperly accessed by others, immediately notify the ITS Help Desk, Privacy Officer or Information Security Officer. Immediately notify UNMC Security and file a police report if PHI is stolen.

January 2012