Suggested policy on secure storage and transport of protected health information

This is a draft policy you may use as the basis for developing your own policy on secure storage and transport of protected health information. You may wish to consult legal counsel.

Policy:

All protected health information (PHI) in paper or electronic form must be transported and stored in a secure manner to safeguard it against improper disclosure or loss. PHI will be stored or transported outside secure network servers only when necessary. Only the minimum amount of PHI necessary to accomplish the purpose of the use/disclosure should be transported.

Definitions:

"Transport" means to physically move PHI (whether on paper or mobile storage devices, such as a laptop, smartphone, USB/thumb drive or disk) from one location to another, by any means including foot, motor vehicle, courier, airplane or other. For example: moving a medical record from one clinic to another, from one department to another, or from the office to home.

"Protected health information" means information that relates to any of the following:

- Past, present or future physical or mental health or the condition of an individual
- The provision of healthcare to an individual
- The past, present or future payment for healthcare to an individual

Information qualifies as PHI if it identifies the individual, or if there is a reasonable basis to believe it could be used to identify the individual. PHI can be in paper or electronic form.

Procedures:

1. 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 or tampering.
2. Additional measures must be taken to secure PHI that is being transported outside of a facility. This assures confidentiality and integrity in the event of an accident, theft or other unforeseen event. PHI that is transported by motor vehicle:
    a. should be transported in a secure container, such as a locked box or briefcase whenever possible; and

b. should be transported without stops that involve leaving the vehicle unattended if possible. If stops must be made, do not leave PHI in the vehicle. Remove and secure it so that others cannot access it.

If an employee wishes to take PHI home, such employee must first obtain prior approval to do so. PHI in the home must be secured from access and view by family members and others. Workforce members shall log out of information systems immediately after use and shall secure their login and password so that others cannot use it.

3. Mobile devices must be password-protected and encrypted.
4. If PHI is lost, stolen or improperly accessed by others, immediately notify the privacy officer or information security officer. Immediately notify the privacy officer and file a police report if PHI is stolen.