The University of Iowa
HIPAA Privacy Rule
Policies and Procedures

PROTECTED HEALTH INFORMATION TRANSFERRED TO OTHER SYSTEMS

Purpose: To outline security safeguards that must be in place when PHI is transferred to other systems and devices.

Policy: Protected Health Information (PHI) transferred from university computers, systems or devices to other systems or devices are subject to the requirements of the Privacy Rule. The need for rigorous security provisions applies to all devices that contain PHI, regardless of device type, ownership, or the method of transfer.

Any individual or entity electing to download report data or transferring to a personal or hand-held computer is responsible for ensuring the security and privacy of PHI on the target system. Protection controls can include (but are not limited to) the use of strong passwords changed at regular intervals; the use and enforcement of system locks or session time-out controls; secure equipment storage; procedures for purging PHI from magnetic media prior to device release or reuse. This applies to PHI used in any device regardless of location or ownership.

Use of downloaded or transferred data is limited to the acceptable uses delineated in the Privacy Rule (treatment, payment, and operations, which include research and education); subject to the "minimum necessary" standard. The use of downloaded or transferred data for the purposes above does not grant the right to share the data with other individuals and/or entities or to subsequent transfers. Violations of these regulations can result in severe legal and financial penalties.