PHI SECURITY AND DATA SANITATION

POLICY:

Clinical Engineering Department will protect and handle patient health information in accordance to HIPAA policy and practice.

PURPOSE:

To protect Patient Health Information when removing equipment from service in accordance with 45 CFR 164.310 (Physical safeguards)

DEFINITION:

Patient Health Information (PHI): Clinical data captured during diagnosis and treatment: demographic, research, epidemiological and reference data.

HIPAA: The Health Insurance Portability and Accountability Act

PROCEDURE:

1. If equipment which contains PHI is to be stored for a period of time, it shall be labeled that it contains PHI and shall be safe-guarded and secured from unauthorized access. 45 CFR 164.312 (Technical safeguards)
2. If equipment which contains PHI is to be disposed of, the following PHI Security/data sanitation method shall be followed:
   a. Choose one of the following methods to remove EPHI from Media according to media type.
      i. Completely erase the hard drive as per DOD 5220.22M (5570)
         - The DOD 5220.22M data sanitization method used in various data destruction programs to overwrite existing information on a hard drive or other storage device.

      ii. Destroy hard drive utilizing one of these methods:
         - Hard drives may be destroyed utilizing a NSA approved degausser to disrupt the magnetic domains.
         - Hard drives may be destroyed by removing the platter and drilling or sanding it.

      iii. If the hard drive is destroyed by a vendor, the vendor shall provide certification/proof of destruction.

      iv. SSD or hybrid drives should be sanitized IAW NIST 800 88
3. If a device is to be transferred to another entity through sale or donation and the

destruction of the hard drive would affect the functionality and/or value of the device, the hard drive may not be destroyed. However, LHH Clinical Engineering Services or service designee must ~~make reasonable efforts to~~ remove or otherwise make PHI unattainable.

4. In the event that a hard drive is not removed upon transfer as described above, the hospital HIPAA Compliance Officer will be notified and any guidance from said officer will be followed.

ATTACHMENT:
None

REFERENCE:
None