Technical Information Regarding OHSU’s Electronic Health Record System

Security
• Unique user IDs and passwords are required to access the system.
• Passwords kept confidential and not shared.
• The system automatically logs off (time-out) the user if the user hasn't used the system for a period of time.
• The location of the data is physically secure
• The system has a virus detection/protection program.

Monitor Access
• Clinical trial monitors may have access to the electronic health records.
• Clinical trial monitors are issued a password for read-only access to the electronic data for subjects participating in the clinical trial.
• Completion of a site-specific access request form is required before accessing the system.

Data Collection
• The system can produce accurate and complete electronic and printed readable copies of electronic records, suitable for review and copying.
• The system is backed-up nightly to prevent loss of data.
• Data backups are made and kept according to OHSU policy, which also addresses disaster recovery.

Audit Trail
• OHSU’s system includes a secure, tamperproof, and printable audit trail for capturing changes to information in the electronic system, which contain the following items in the audit trail:
  – user name/ID of who authored the change
  – Date stamp
  – Time stamp
  – Reason for change
  – Original data is accessible within the history of the change
• OHSU’s system employs tamperproof electronic signatures which incorporate the following features:
  – User ID
  – Password
– Date Stamp
– Time Stamp
– The meaning associated with the signature (for example: review, approval, responsibility, and/or authorship, etc.)

**Procedures, Policies and Training**

- OHSU policy governs use of the system. These policies include information regarding:
  - System Administration access vs. user access
  - Maintenance of user ID’s and passwords
  - Electronic record retention
  - Data backup and retention
  - Disaster recovery
  - Operations during system downtime
- Documented training is required of all users prior to accessing OHSU’s system.
- Change control detailing who has system access and what level of access is documented.
- OHSU electronic records are archived in accordance to local regulations for clinical studies or patient records, whichever is longer.
- There any no changes planned to the system which may affect access of the method in which source data is recorded.