Vanderbilt University Medical Center statement on approaches to maintaining the accuracy, reliability, integrity, availability, and authenticity of clinical records and electronic signatures.

Current Version – 20 May 2014
Original - 1 July 2008

Reliable and timely access to clinical information is at the heart of safe and effective team-based healthcare. Vanderbilt University Medical Center (VUMC) depends upon a rich fabric of inter-related information systems acquired from vendors and integrated with locally developed systems built and maintained by professional staff of the VUMC Informatics Center. This document outlines the organization's approach to maintaining the accuracy, reliability, integrity, and authenticity of clinical records and associated electronic signatures. It is divided into the following sections:

- Limiting system access to authorized individuals
- Operational system checks
- Authority checks
- Device checks
- Ensuring that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- Controls over systems documentation including change controls
- Electronic signatures
- Audit Trails
- Copies of Records
- Records Retention

Policies and Standard Operating Procedures are in place that provides additional detail on each of the topics addressed in this summary document. Such policies include, but are not limited to:

Access to Confidential Information, IM 10-30.03
Access to Protected Patient Information by Job Role IM 10-30.10
Confidentiality of Protected Patient Information IM 10-30.01
Authorization and Access to Electronic Systems and Applications, IM 10-30.19
Disposal of Confidential and Restricted Information, IM 10-30.18
Sanctions for Privacy and Information Security Violations, IM 10-30.12
Use & Disclosure of Protected Health Information, IM 10-30.06
Protection and Security of Protected Health Information IM 10-30.13
Protection and Security of Research Health Information IM 10-30.14
Privacy and Information Security Training IM 10-30.05
VUMC Informatics Center Project Implementation Process Guidelines
Change Management Process
Business Continuity, IM 10-10.08
Research Participant Documentation: Billing Compliance, OP 40 10-15

Limiting system access to authorized individuals

Systems containing electronic personal health information (ePHI) at Vanderbilt University Medical Center (VUMC) generate audit logs and require unique user Identifiers (ID's) and passwords for access. These access ID's are only requested for, assigned to those with a need-to-know in order to complete his or her job duties, and for time limited access as needed. Reviewed and signed Confidentiality Agreements are required for users to obtain access. Users are reminded of their obligations for the use of information through regular training. Training includes reviews of pertinent policies related to confidentiality and information security including locking workstations or logging off the applications before they leave the workstation. VUMC has auditing capabilities and processes to review user access of ePHI. These processes include consistent sanctions requirements for all violations. Using the HIPAA Security Rule as a guide, the VUMC Informatics Center performs annual Risk Assessments and establishes any necessary work plans for continued improvements to current administrative, technical and physical safeguards.

Operational system checks

VUMC Informatics maintains a Quality Center whose staff performs pre-deployment and post-deployment applications testing on all clinical care software applications and systems. Testing includes automation of functional tests, negative testing, load testing, and infrastructure testing, all of which are documented. A variety of automated software tools are used in this process, which is performed using dedicated testing servers that mimic operational environments. After software successfully passes testing, modified applications are deployed to production servers and the Quality Assurance team performs post-deployment testing. This is a continuous process that is driven by user requirements for application changes as well as automated surveillance and input from user help desks.

Authority checks

Audit trail analysis, automated and semi-automated methods are used on an ongoing basis to perform authority checks to ensure that only authorized individuals can use systems, electronically sign a record, access software modules and computer system input or output devices, alter a record, or perform data manipulation operations.

Device checks

Device (e.g., terminal, router, printer) checks are a standard component of system status assessment used to determine the validity of the source of data inputs or operation instructions. Network security operations include time-stamped logging of device IP addresses and physical verification of device locations and proper functioning is performed as part of routine system maintenance.

Ensuring that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks

As noted above, training is provided by the Informatics Center and VUMC Privacy Office on rights and responsibilities in the use of clinical systems containing person-identifiable data, as well as application-specific user training for effective and appropriate use of systems. Developers within the Informatics

Center receive privacy training and their software and systems management skills are under continuous assessment and improvement through short courses, and in-service training.

Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures

Information Management Policy IM 10-20.04 Electronic Signature: For Documentation in the Medical Record defines a properly executed electronic signature as a legally binding means to identify the author or approver of each entry in the health record with all associated ethical, business, and legal implications. The policy further defines the requirements for application of an electronic signature to an entry in the medical record. Multiple Information Management Policies address accountability for actions initiated via electronic signatures; reference IM 10-20.15 (Additions and Corrections to Documentation in the Legal Medical Record), IM 10-20.08 (Carry Forward of Clinical Information in the Electronic Health Record), IM 10-20.13 (Provider Documentation Standards for Hospitalized and Observation Patients). Suspected violations of these policies are investigated by the VUMC Privacy Office, and corrective actions implemented based on Sanctions for Privacy and Information Security Violations policy guidelines. Violations are graded by severity, and sanctions up to and including dismissal are applied. These policies are enforced rigorously, and a small number of employee terminations for non-adherence to these policies have occurred each year.

Controls over systems documentation including change controls

Formal Standard Operating Procedures and developer documentation are maintained by the Informatics Center for all of the following:

- System setup/installation (including the description and specific use of software, hardware, and physical environment and the relationship)
- Validation and functionality testing procedures
- System operating manuals
- Data collection and handling (including data archiving, audit trails, and risk assessment)
- System maintenance (including system decommissioning)
- System security measures
- Change control - the Change Management utilizing IT Infrastructure Library (ITIL) to implement IT Service Management (ITSM) Framework
- Data backup, recovery, and contingency plans
- Alternative recording methods (in the case of system unavailability)
- Computer user training
- Roles and responsibilities of sponsors, clinical sites and other parties with respect to the use of computerized systems in clinical care and research

Electronic signatures

In VUMC clinical systems, electronic signatures and handwritten signatures executed to electronic records are linked to their respective records so that signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. User ID’s and passwords are required within VUMC network and two-factor authentication (user ID, password, and Secure ID challenge-response systems) is required for remote access. Each electronic signature is unique to one individual

and may not be reused by, or reassigned to, anyone else. Before VUMC establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, the organization verifies the identity of the individual.

Electronic signatures based upon use of user ID's in combination with passwords employ additional controls to ensure security and integrity. The controls include the following: (1) the uniqueness of each combined identification code and password is maintained in such a way that no two individuals have the same combination of identification code and password; (2) identification codes and/or passwords are periodically recalled or revised; (3) loss management procedures are documented and must be followed to deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification codes or password information; (4) transaction safeguards are used to prevent unauthorized use of passwords and/or identification codes, and to detect and report any attempt to misuse such codes; (5) devices that bear or generate identification codes or password information, such as tokens or cards, are tested initially and periodically to ensure that they function properly and have not been altered in an unauthorized manner.

VUMC maintains written policies holding individuals accountable and responsible for actions initiated under their electronic signatures. Annual HIPAA system security training that is required of all users includes a statement regarding the proper use of electronic signatures.

Audit Trails

As noted above, all systems containing electronic personal health information (ePHI) at Vanderbilt University Medical Center (VUMC) generate audit logs and require unique user Identifiers (ID's) and passwords for access. While synchronizing data across multiple applications, the electronic medical record system records every transaction with date and time stamp information. Audit trails are analyzed on a routine sampling basis as well as a for-cause basis in cases of complaints regarding possible inappropriate access to ePHI.

Copies of Records

Controls are in place to generate accurate and complete copies of the legal medical record as needed in accordance with the Health Data Categories Table (defined in IM 10-20.05 Definition of the Legal Medical Record and the Designated Record Set) for auditing and submission to outside regulatory agencies. Procedures are in place to allow on-site inspection, review, and copying of records in a human readable form using VUMC hardware and software systems for accessing records

Records Retention

Archival procedures, backup and disaster recovery policies, procedures and technologies are in place that meet statutory requirements for clinical systems documentation. As an early adopter of electronic medical records technologies, Vanderbilt prides itself on longitudinal electronic clinical records that have data extending back for many years; in some cases, for decades. There is continuous data replication to remote data centers, and regular scheduled movement of backup tapes to offsite secure data archives.