Penn Medicine Electronic Health Records in Support of Research

Overview

Institutional Review Board (IRB) approval is required for implementation of Clinical Research protocols at Penn Medicine.

Generally, Penn Data Store (clinical data warehouse) provides access to all data captured via Electronic Health Records at Penn Medicine with IRB approval. Information Services maintains Electronic Health Records (EHR) at Penn Medicine via the following major systems, Epic (ambulatory), Allscripts / Siemens (hospital based), Cerner (Laboratory and Home Health), GE (Radiology) and EMTRAC (Emergency Department). By May 2015, EMTRAC will be replaced by Epic ASAP and GE Radiology will be replaced by Epic Radiant. In 2016 and 2017 Allscripts, Siemens and Cerner Home Health will be replaced by Epic. The EPIC systems have documentation on system usage and validation.

Documentation of the EHRs includes the following.

1. System requirements
2. Design and configuration
3. Accurate installation
4. Formal Change Control processes
5. System Policies

Source data for research may originate from an EHR. The data may be included in study information either manually or electronically. Such processes are documented according to each study IRB approval.

Based on comments from the FDA’s Office of Good Clinical Practice, the FDA does not expect study sites to provide validation of EHR systems or any evidence relevant to Part 11. While an EHR does contain digital signatures, EHRs at Penn Medicine are currently not designed to meet FDA 21 CFR 11 criteria for electronic signatures via third party authentication.

Controls exist and are enforced in Information Services at Penn Medicine to ensure confidence in the reliability, quality, confidentiality and integrity of the electronic health records.

In case of questions and/or concerns about this document, please contact Maha Dutt at the Office of Clinical Research (OCR) via Phone at 215-746-8334, Email: ocr@exchange.upenn.edu.

The remainder of this document will outline more detailed information needed by most industry research partners.

Certifications

The EHR systems listed above have been certified as follows:

<table>
<thead>
<tr>
<th>System</th>
<th>Certifying Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epic</td>
<td>CCHIT</td>
</tr>
<tr>
<td>Allscripts</td>
<td>CCHIT, Drummond Group Inc.</td>
</tr>
<tr>
<td>Siemens</td>
<td>CCHIT</td>
</tr>
<tr>
<td>Cerner</td>
<td>CCHIT, ICSA Labs</td>
</tr>
<tr>
<td>EMTRAC (internally developed)</td>
<td>Certification not required under Meaningful Use</td>
</tr>
</tbody>
</table>
User Training
All EHR users are required to complete mandatory user training modules prior to receiving system login credentials. Updates to system functionality are communicated to users via splash screens, screen savers, newsletters, web sites and web based training videos.

Training documentation is provided online through computer based training modules and web sites.

Testing
All system installations and regular upgrades to those systems are tested by Information Systems teams including end user representatives to ensure that the system works as expected.

User Support and Enhancement Requests
Penn Medicine operates a 24 hour, 7 day a week service desk that enables end users to report system problems or request enhancements. All problems and requests are tracked in a vendor supplied issue and request tracking system. Enhancement requests are prioritized by end user run prioritization committees.

User Identification and Security
All users are assigned their own unique logon IDs and strong passwords. Users are not permitted to share their login credentials. Users must first authenticate with the UPHS network before authenticating with the EHR system being accessed. Passwords expire no more than every 180 days. Passwords may not be reused. Users are locked out for a minimum of 30 minutes after 3 consecutive authentication failures. User network accounts that have not been accessed for 90 days are disabled. Disabled logon IDs must not be reused for a different user.

Inactive sessions time out after 15 minutes or less of inactivity for most users.

Data Integrity and Audit Trails
User ability to view and change data is tied to their role and department/location. All access to data is logged in a HIPAA compliant audit trail. Audit trails also record changes to all data and who made the changes. Audit trails are retained indefinitely. Some data cannot be changed without user re-authentication (approval of held orders for example).

Electronic Signatures
UPHS relies on the individual user’s logon credentials as their electronic signature. Full names of signers along with date and time of signature are stored in the EHR and are printed on appropriate documents. Documents that require electronic signature cannot be changed once signed unless their status is changed.

Record Accessibility and Review
Access to EHR data by external monitors can be arranged by contacting the assigned Principal Investigator. Access will be limited to the patients enrolled in the study. External monitors will have read only access and cannot modify data. External monitors cannot download data or print data from the EHR. Access to system audit trails by monitor can be arranged but is not generally provided. Read only access User IDs for monitors will expire automatically after 90 days or less.

Data Archive
EHR data is not currently physically deleted even if deleted by an end user using the application. Records are marked as deleted but remain in the database.
System Infrastructure

Virus protection
UPHS computers currently use Symantec Endpoint Protection. Virus and anti-Spyware signatures are updated regularly.

Network
The UPHS and School of Medicine networks are high speed local area networks. When connecting locally all users connect through a high speed wired or wireless connection. Remote users can connect at various network speeds depending on their location and capabilities.

Firewalls
The UPHS network is protected by perimeter firewalls and intrusion detection systems.
Remote users must connect to the UPHS network using and encrypted Virtual Private Network connection.

Desktop Operating Systems
The majority of UPHS desktops are currently running Windows XP. A project is underway to upgrade to Windows 7.

Automatic updates
UPHS desktops receive regular software updates via the Microsoft SCCM desktop configuration management product.

Internet Browsers
UPHS desktop computers are running Internet Explorer 8. The Windows 7 upgrade project includes an upgrade to Internet Explorer 9 or higher.

Adobe Acrobat Support
Adobe Reader is installed on all UPHS desktops.

EHR Installation
EHR installation and upgrade projects are driven by UPHS Corporate IS members along with vendor support as needed.

Backup
Each component of the EMR is backed up using a system of weekly full backups with nightly incremental backups such that we can restore to a version that is no more than 24 hours old. Backup media is stored off site with a secure outsourced provider. Tape restores are tested regularly.

Disaster Recovery Plan
UPHS maintains active and passive disaster recovery systems using redundant power, networks, environments and data storage networks.