Indiana University Health Electronic Health Records in Support of Research

Overview

Clinical Research at IU Health is governed by implementation of approved Institutional Review Board (IRB) protocols. The IU Health Enterprise Data Warehouse and Regenstrief Institute Data Core provide access to all data captured via Electronic Health Records at IU Health with IRB approval.

Information Services maintains Electronic Health Records (EHR) at IU Health via the following major systems: Cerner (ambulatory, surgery, radiology, Emergency Department, hospital based and home health, pathology, and population health), and Fuji Synapse (PACS).

These 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 IU Health 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 IU Health 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 the IS Clinical Research team via email: clinicalresearchsystems@iuhealth.org

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:

System Certifying Organization

Cerner - CCHIT, ICSA Labs
Fuji Synapse PACS - CCHIT

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

IU Health 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 IU Health 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 20 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

IU Health 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 after the defined time period.

Privacy Monitoring

Audit Access to EHR records from the Cerner environment is monitored using the Iatric Haystack Patient Privacy Monitoring System. Haystack utilizes Machine Learning technology to proactively examine access to EHR data for appropriateness. The Privacy team reviews potential incidents identified by Machine Learning. The Privacy team also conducts proactive reviews of high-profile patients such as athletes, politicians, or people in the news. Inappropriate access by IU Health team members is grounds for termination under policy HR-100, the Corrective Action Policy.

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. Cerner does not have the capability currently to delete individual records.

Distributed Technologies

If distributed verification and validation technologies, such as Blockchain, are used in a system, they are required to comply with the security language in the Indiana University Health, Inc. Verification and Validation Using Distributed Computing Requirements document, and the use of this technology must be reviewed and approved by Information Security before usage. Cerner has agreed to these terms as part of their contract with IU Health.

System Infrastructure

Virus protection

IU Health computers currently use Symantec Endpoint Protection and Cisco Anti-Malware Protection (AMP). There is currently a project to migrate from Symantec to Elastic Endgame Endpoint Detection and Response (EDR). Anti-virus, EDR, and AMP are all updated at least daily.

Network

The IU Health and IU 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 Access

Remote users can connect at various network speeds depending on their location and capabilities utilizing either Virtual Private Network (VPN), Citrix, or Virtual Desktop Infrastructure (VDI) connections. All remote access to either IU Health or IU School of Medicine networks requires the use of Duo two-factor authentication.

Firewalls

The IU Health network is protected by site and perimeter firewalls, intrusion detection systems, and security monitoring. Cisco Identity Services Engine (ISE) is also utilized to help identify and protect against unauthorized devices on the network.

Desktop Operating Systems

The majority of IU Health desktops are currently running Windows 7. A project is underway to upgrade to Windows 10. The VDI infrastructure runs Windows 10.

Automatic updates

IU Health desktops and VDI images receive regular software updates via the Microsoft SCCM desktop configuration management product.

Internet Browsers

IU Health desktop computers are running Internet Explorer 11, Google Chrome, and Mozilla Firefox.

Adobe Acrobat Support

Adobe Reader is installed on all desktops.

EHR Installation

EHR installation and upgrade projects and initiatives are driven by the IU Health Chief Health Information Officer and appropriate executive leadership and sponsorship.

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 at version that is no more than 24 hours old. Cerner is contractually obligated to maintain appropriate backups and test them at least twice annually.

DR Plan

IU Health maintains active and passive disaster recovery systems using redundant power, networks, environments and data storage networks.

Governance Approval: Indiana University Health

AHC Privacy and Security Council

September 11, 2019