UCSD
EPIC EMR System Features

Introduction

Electronic Medical Records (EMRs), also referred to as Electronic Health Records (EHRs) in clinical research, are digital versions of a patient's traditional paper chart. They are designed to be patient-centric, offering real-time records that are securely accessible to authorized users within a healthcare organization. This document specifically addresses UCSD's EPIC system, a comprehensive digital platform used for the collection and storage of electronic medical records.

UCSD's EPIC system includes features that are rapidly evolving to incorporate more research-specific functionalities. Although the current version cannot fully support a wide spectrum of clinical trials—from FDA-regulated first-in-human studies to comparative effectiveness research—on its own, it remains compliant with the 2018 FDA Guidance on electronic source data. As an Office of the National Coordinator (ONC) certified EHR, EPIC aligns with the FDA's "eSource" guidance, ensuring adherence to high standards of data integrity, security, and traceability.

EPIC's robust audit log capabilities meticulously record all modifications to electronic health records. Its comprehensive logging includes timestamps, user identification, and detailed descriptions of any changes made. The system ensures that original content is preserved, upholding the legal requirements that differentiate EHRs from general research information systems. EPIC treats research data with the same level of security and integrity as clinical information stored within the EHR.

Research teams may use this tool to provide information to potential sponsors on UCSD EPIC EMR system's suitability as a source documentation platform for conducting your clinical research study. The system is designed to comply with the comprehensive data integrity requirements of ALCOA+ and CCEA principles (Attributable, Legible, Contemporaneous, Original, Accurate; and Complete, Consistent, Enduring, Available) required by industry. By ensuring data reliability, security, and compliance with regulatory standards, the UCSD EMR system supports the integrity of clinical trial data documented in the platform.

The details provided here are for reference purposes only. Using any of the features, such as providing access to EPIC for monitoring activities, is optional. Each study team should evaluate and utilize the features of the UCSD EPIC EMR system according to their specific practices and needs. It is important for research teams to assess how these features align with their protocols and procedures to ensure they meet their study's requirements.

EMR System and Training	YES	NO
1. Is the EMR system certified by the ONC (the Office of the National Coordinator for Health Information Technology, US).	☒	☐
EMR Manufacturer: **Epic Systems (Verona, WI)**		
EMR System Model Number: **Epic Hyperspace**		
EMR System Version Number: **August 2023 release**		
2. The UCSD EPIC EMR system is compliant with all requirements as defined in ICH GCP Section 4.9 and any applicable national or regional standards / regulations?	☒	☐
3. Is there a site/institution or departmental procedure that addresses the use of an EMR system (including training) and site source data collection**?** Yes, there is Epic Research specific training and documentation. This can be obtained from the Epic training team. This does not specifically cover "site source data collection" per see.	☒	☐
4. Are all users internal and external site employees trained on using the EMR system, if applicable?	☒	☐
If yes, is the training documented? It is maintained on an internally accessible website -- https://pulse.ucsd.edu/departments/EMR/ResourceLibrary/Pages/Epic-Update.aspx	☒	☐
EMR Audit Trial	**YES**	**NO**
5. Audit trails is available upon request of a regulatory agency or sponsor audit or inspection. Yes, study-specific request for raw data or access log report can be created by the EHR department upon request.	☒	☐
6. The EMR system has a computer generated "time stamp" which records the date, time of operation, the person who performed all entries, changes, and deletions in the patient electronic record.	☒	☐
7. Reason for change (no, unless the user, indicated reason for change)	☐	☒
8. Site staff can view in real time which trial participants' records are being reviewed by the Site Monitor (while on site).	☐	☒
If no, is process in place to manage non-trial participants' potential confidentiality breach? Yes, the Health System compliance has procedures to manage breaches including this type.	☒	☐
EMR Access and Controls	**YES**	**NO**

9. Access to electronic health record systems is limited to authorized users	☒	☐
10. Authors of e-records are identifiable	☒	☐
11. Unique user accounts (User ID & password)	☒	☐
12. Site processes do not allow sharing of user ID/password to access the system	☒	☐
13. Locks user account after several failed log in attempts	☒	☐
14. Automatically log off user after an idle period	☒	☐
15. Will external reviewers e.g. Site Monitors, Regulatory Inspectors (such as FDA) or auditors, be provided with restricted access to the trial participants only (i.e. subjects who signed an informed consent form for the clinical trial being monitored)? Yes, restricted access can be provided via read-only guest user accounts including full access to source data for trial participants only. However, this decision is made at the study level as the PI and/or staff may not allow this practice within their research team.	☒	☐
16. Other available options for monitors to review/verify electronic source data in the system?		
• **Certified copies** can be provided.	☒	☐
○ If certified copies are provided, will Site Monitor be allowed to do interval comparison of EMR to certified copies of source data? With help of CRC with previous notification to the study staff.	☒	☐
• **Indirect access:** Over the shoulder review of study staff. Study staff will use their own user account. CRC will navigate system and will remain with the Site Monitor during the visit.	☒	☐
• **Unrestricted access:** Site Monitor required to sign a Confidentiality Disclosure Agreement (CDA). No unrestricted access will be provided.	☐	☒
17. Remote Access to monitors to access the EMR remotely (off-site) will not be permitted.	☐	☒
If no, reason for not providing remote EMR access to monitors/auditors. It is not a currently approved procedure by our health system compliance office, primarily due to valid authentication related remote access as well as ensuring access is by an individual who is doing so within the jurisdictional boundaries of the United States (a HIPAA requirement).		
Protection, Storage and Archiving	**YES**	**NO**
18. Can accurate and complete copies of electronic source data be generated from the system?	☒	☐

19. Are any paper source data scanned and original source destroyed?	☐	☒
20. Are any records transcribed from audio files into EMR system? Response is study specific. However, note that UCSD is starting a pilot use of "ambient artificial intelligence" that will indeed be able to transcribe audio files. The audio files themselves will be automatically destroyed/deleted (within 30min of the transcription). If in the future this feature is utilized, a contingency plan to ensure source data should be put in place (e.g. data backups, etc.)	☐	☐
21. After the trial is closed, are electronic source data and the audit trail available for access during the records retention period (please refer to ICH GCP 4.9.5 and local regulation related to records retention).	☒	☐
EMR Archiving	YES	NO
Electronic records are stored in accordance with ICH GCP Section 4.9 and relevant local regulations	☒	☐
In the event of any technological changes, the site will ensure that adequate hardware is maintained to access records throughout the required retention period. Users will be regularly informed about updates or changes to the Electronic Health Records System (EHRS), along with providing documentation on how to use the updated features, if applicable.	☒	☐
Physical EMR Security	YES	NO
Institution has an electronic system back up mechanism to protect patient electronic records in case of unexpected events. The EMR system has real-time recovery through an offsite disaster recovery instance.	☒	☐