The ICH GCP sets out that study sponsor monitors must review the medical records of study participants against the data captured for the trial (case report form). This process is termed Source Document Verification. Access to the medical record is critical to demonstrate the data captured for analysis in clinical trials are accurate in that they are a true record of the observations made by the investigating clinician and diagnostic results. The purpose of this document is to illustrate compliance of the integrated electronic Medical Record (ieMR) with ICH GCP and should be administered to sponsor monitors requesting confirmation.

Question	Answer
Security and validation	
1. Name, version and date of the electronic system	CERNER; PowerChart Release date: 01/12/2013 Version number: 2015.26
2. Is the electronic system validated?	Cerner is ISO (International Organisation for Standardisation) 9001:2008 Quality Management System certified. The National Body representing Australia for ISO is Standards Australia.
3. Is the validation report available and reviewed by the site monitor?	Yes, the individual can access https://chpl.healthit.gov/#/search and type 'Cerner Corp'.
4. Is iEMR compliant with all requirements as defined in ICH GCP Section 4.9 and any applicable national or regional standards/regulations?	Yes.
5. Does the site maintain a record of the electronic system version that was in use during the conduct of the clinical trial, including version dates, documented and auditable validation of changes made during the conduct of the clinical trial?	Yes.

6. Is there antivirus software installed and updated regularly on all computers used to access or maintain data used for clinical trials?	Yes. Anti-Virus (AV) software is used, as appropriate, throughout the hosted environment and pattern file updates are deployed daily. Inbound data is scanned in real-time, and system drives are scanned on a weekly basis. In addition to keeping virus signatures up to date, the AV software and scan engines are updated to maintain and improve their effectiveness.
Audit trail	
7. Does the system have an audit trail for data that tracks what, who and when entered in the iEMR, including modifications?	Yes, CERNER Millennium provides the technical safeguard audit controls (per CFR 164.312) to produce secure, computer-generated time-stamped audit trails to independently record the date, time, and author of any data creation, change or deletion. New audit trail information does not overwrite previous information. Audit log information is retained with the record and accessible to authorised users.
8. Is this audit trail protected against being turned off and modification?	Yes.
9. Does this system include controls that limit the ability to change system standard settings to authorised persons?	Yes.
Passwords	
10. Are unique User IDs and confidential passwords required to access the system?	Yes.
11. Does the system automatically log off and require a password for logging back in?	Yes, the system will log the user off after 30 minutes of inactivity. Each individual device will activate a sleep mode that requires a log in to be entered.
12. Does the system automatically prevent access after a defined number of failed access attempts?	Yes, the system will deliver a prompt stating the user has failed 3x attempts. The account will then be locked requiring administrator support to unlock.
13. Does the system keep a log of unauthorised access attempts?	Yes.
14. Are passwords periodically changed?	Yes, passwords must be changed once in a 90-day period.
System back up	
15. Is the data in the system periodically backed up?	Yes, a real time backup is always completed.
16. Can backed up data be restored?	Yes.

17. Where is the retained data stored?	Real-time sync to the Disaster Recovery data centre in Sydney. In addition, regular backups to tape are stored offsite at a secure facility.
18. Has the backup process been verified (tested) by either the vendor or the site, providing assurance of backup integrity, and verification documentation is readily available for inspection by an auditor?	Yes.
19. Is there a documented process for continuing operations if the system is not accessible?	Yes. There are downtime procedures in place that comply with regulations set by the hospital and health service and system regulations. This includes recovery processes following emergency or unexpected shutdown.
Maintenance	
20. Is there a site/institutional or departmental procedure for change and system incident management in place and are these changes documented?	Yes.
21. If/when the iEMR is upgraded, is additional testing performed?	Penetration testing is conducted by CERNER security professionals who have appropriate industry certifications and credentials.
Data retention	
22. Is the data retention period compliant with local regulations?	Yes.
23. Does the system produce accurate and complete copies of the patient data, including a audit trail and coded data in an understandable format?	Yes.
System administration	
24. Are user active and inactive accounts reviewed?	Yes.
25. Is there a list of user accounts identifies when access is granted and revoked?	Yes. However, Queensland Health does not have permission to provide all user details.
26. Is there a process for revoking user access?	Yes.
User	

27. Is training needed to obtain a user account?	Yes.
28. Are training records stored?	Yes.
29. Does your site allow the sponsor representative to remotely access the iEMR from outside your site/facility/office?	Yes.
Data privacy	
30. Do site monitors have 'read only' rights?	Yes.
31. Are there restrictions in place for site monitors monitoring trial subjects/patients?	Yes, site monitors are assigned a role on the study within PowerTrials, limiting access to medical records where participants have provided consent and are enrolled into the study.
Further information	
Source documents	

Metro South Health Digital Hospital Support Module, April 2018, v2

Cerner Security Program

Date effective: 13/10/2020

Review date: 13/10/2022

Contact	
Metro South Research Compliance Officer - PowerTrials	MSH-PowerTrials@health.qld.gov.au
Metro South Digital	MSHDigital@health.qld.gov.au