SITE: Alfred Health – Clinical Information System (CIS)

Summary of Key Questions in regards to Electronic Medical Records and Clinical Trials

Alfred Health supports many clinical research study projects approved by Alfred Health's Ethics Committee, and these projects require access to the Electronic Medical Records system (Cerner Millennium). In order to validate such research, the EMR system must comply with FDA CFR 21 Part 11 requirements. Note that this review version is compliant with April 2018. This assessment is required for each research project upon request, and this document is filed with the Ethics Committee.

Review Date: July 2021

No.	Question	Answer	IT Qualification Statement
1	**SYSTEM/ SITE CONTACT**		
1.1	System Evaluated System Version	Alfred Health CIS 2018.03.05 Edition	Clinical Information System Cerner Millennium
1.2	Name of Systems Administrator/ Information Security Contact/ Coordinator	Chris John Chris Liew	Manager, Manager EMR, Operations, Development and Support, Information Development Division, (tel: 03-9076 3988 email: c.john@alfred.org.au), is *responsible for developmental and operational performance and meets with Cerner weekly.* Information Development Division (IDD) supports the system functions and connectivity. All information security audits and access controls are coordinated by the Manager, Technology Risk & Information Security (tel: 03-9076 3299 email: c.liew@alfred.org.au)
2	**PHYSICAL SECURITY**		
2.1	Is the system located in a secure area? Is the computer hardware kept in a secure location? Are there procedures and controls for physical security, ensuring a controlled environment?	Yes	The clinical information system that houses the patient data is remote-hosted in an offsite robust and secure data centre facilities within Australia. Physical access is managed by vendor Cerner.
2.2	If satellite sites are used, how do satellite sites access the system? Do all satellite sites have direct access to the EMR system?	 Yes	Satellite sites have secure extended network connectivity and are logically part of the network. Access is via Citrix virtual desktop portal.

No.	Question	Answer	IT Qualification Statement
3	**ACCESS SECURITY**		
3.1	Is access limited to authorised staff only? Is access to the EMR system restricted for staff by unique, identifiable login?	Yes	Only authorised users are able to access the system. Authorisation is via a formal request (paper or electronic) approved by Alfred Health (AH) department managers. The type of access commensurate with job duties. Access is also granted to honorary appointees and contracted parties authorised by the organisation. Sep-2020: Remote access by monitors (including from overseas) are allowed with cost recovery (per year) from the sponsor. Due to COVID-19 response, trial monitors are allowed remote access to comply with source data verification. State researchers are given remote access if they already have authorised clinical access.
3.2	Is the system password-protected?	Yes	Only authorised users can access the system with their unique username and password. Limited uses of generic accounts are only to areas with compensating controls in place, after a risk assessment and special approval is provided.
3.3	Does each authorised individual have their own unique User ID & password?	Yes	Each user is provided with an individual unique username and temporary password. The first time one logs in, the system prompts the user to change their password.
3.3a	Are the following controls in place to limit access to the system? • Automatically log off user after idle periods • Locks user account after several failed login attempts	 Yes Yes	 Time-outs & lockouts are implemented in all areas. (high dependency areas have extended time-outs) 3 failed attempts are allowed.
3.4	Are there procedures and controls for user access security? Is there a process for issuing and revoking user access?	Yes	See response to Q 3.1 to 3.3a above. All requests are logged and managed in the HEAT incident & service request management system. There is a process to create new access, modify access and to terminate access when the user exits the organisation. In the case of contracted staff, their access is automatically disallowed on the contract end date. Users are disabled after a period of inactivity that can be re-enabled on request. The system also retains an audit trail of detailed access to system components. Sep-2020: Remote access by trial monitors is controlled by RSC via the patient list and operationally limited due to resource requirements to a few days.
3.5	Is there a list of individuals authorised to access each function?	Yes	The various levels of security functions and views are documented in the Alfred Security Data Collection Worksheet (DCW). A reporting tool can generate the list of individuals authorised for each position type. Oct-2018: Positions are added and removed based on business requirements, managed by EMR Core & Security.

No.	Question	Answer	IT Qualification Statement
3.6	Will the sponsor Clinical Research Associate (CRA) be able to access the data for monitoring?	Yes	A unique account is created for the CRA to gain read-only access to the EMR. Only consenting patients' data can be accessed by the CRA. The process is managed by the Clinical Research Study Coordinator (RSC), with a formal request form that must be accompanied by an Ethics Certificate or Alfred Health authorisation letter; and study end-date.
3.6a	Are sponsor personnel (ie, Clinical Monitor, Compliance Auditor) allowed to have read-only access to the EMR system?	Yes	See response to Q 3.6 above. The 'position' created is for Auditor, Researcher or Monitor using the same access principle outlined in Item 3.6 above.
3.7	Is the system capable of restricting the CRA's access to ONLY those patient records of sponsor trial participants?	Yes	The assignment of consenting patients' records to the CRA is carried out by the sponsoring department clinical representative (RSC) for the specific research project.
3.8	Is access read-only and limited to subjects on sponsor trial studies?	Yes	The access is 'read-only'. For the second part of the question, see response to Q 3.7 above.
4	**BACKUPS & RECOVERY**		
4.1	Is the system backed up at regular intervals?	Yes	System backups including offsite storage to a secured environment. A standby database is synchronized to the production database approximately every 15 minutes.
4.2	Are there adequate backup, recovery and contingency procedures for data and metadata? In case of system failure, what backup procedures are available and how are they accessible?	Yes	Contractual arrangement as part of Cerner-AH contract with data backup and recovery procedures. Data is backed up regularly based on a backup schedule and using disk-to-disk & backup tape medium. There is a DR system housed in a secondary data centre at a separate and secure remote location. For business continuity, offline 24/7 downtime viewer laptops at strategic locations around the hospitals provide contingency fallback option with up-to-minute data during system downtime.
4.3	Is the data in the system backed up (either via a network connection or external hard drive, for example) in case of system failure or loss of data at an appropriate frequency?	Yes	Contractual arrangement as part of Cerner contract with Alfred Health.
4.4	Are the backups kept in a separate, secure location?	Yes	Backups are stored off-site. Arrangement as part of Cerner contract.
4.5	Has the retrieval system been tested and is satisfactory?	Yes	Testing is part of Cerner contract.

No.	Question	Answer	IT Qualification Statement
4.6	Can this backup data be restored?	Yes	Cerner Technology Centre recovery procedures.
4.7	How often are backups made? How long are they retained by the site?	Not applicable	Arrangement as part of Cerner contract. Currently, clinical records are maintained indefinitely.
5	**AUDIT TRAIL**		
5.1	Does the computer system capture changes made to the data? Is there a system-generated audit trail? Are all changes retained by the system?	Yes	All activities to the clinical information system including viewing and modifying records are logged at all times. Reports are available to interrogate user access to specific patient information and system configuration changes. Old audit trail logs can be recovered from backup but would require a longer period for the recovery process.
5.2	Is the original information as well as the new information still available after the change is made? (Attach example if appropriate)	Yes	See response to Q 5.1 above. (sample available) Clinical documentation retains a complete history of old and new data.
5.3	Are the audit trail entries date and time-stamped?	Yes	All audit trail entries are logged based on activity with date and time stamp.
5.4	Does the audit trail indicate who made a change?	Yes	All transactions recorded in the audit trail have at least a user ID/ name, date/ time stamp and action.
5.5	Is the audit trail protected from modification by users?	Yes	Authorised personnel are allowed to access/ read the audit trail.
5.6	Can the audit trail be edited?	No	It is a system function that is built by the software and protected even from the system administrators.
5.7	Are the audit trail and other security settings protected from being turned off?	Yes	It is a system function that is built by the software and protected even from the system administrators.
5.8	Does the system contain complete records (data, metadata, audit trail, and, as applicable, e-signatures)?	Yes	This question is partially answered in A 5.1 above. As for e-signatures (validation via password challenge for electronic ordering), the system log records the individual username, date, and purpose for the authorisation. Single Sign-On with Tap-On-Tap-Off is available for AH clinical staff.
5.9	Can the audit trail be easily viewed and copied?	Yes	Some audit trails are viewable to end users but only authorised personnel have access to the backend audit trail. Patient-specific audit tools are only available to Health Information Services personnel (to ensure data integrity) for auditing use.
5.10	If the software version changes, how will historical data be read?	Yes	Software version changes do not impact the historical data. Historical data are still accessible. This requirement is important, as we keep all patient information from the commencement of the system since 1999.

No.	Question	Answer	IT Qualification Statement
5.11	Can data be modified once saved in the system?	Yes	An audit trail is maintained for all activity including modifications and a copy of the original data value is retained.
5.12	Does the audit trail contain? ○ Old data value ○ New data value ○ Name of person making the change ○ Date & time of change	Yes	A sample can be provided on request. Strike through or Addenda are viewable when changes are made to clinical documentation.
6	**DOCUMENTATION & TRAINING**		
6.1	If applicable, are operating instructions in place? Have the site personnel been trained in the use of the computer system? Is there documentation maintained on installation and training? Does the EMR system have a User Manual?	Yes	Usage instructions and training material for end-users (documents and video format) are available on the intranet. EMR Quick Reference Guides are available via the eCoach icon. Support instructions are available to the IT support staff in the *WIKI* and on the vendor Cerner's website (uCERN). New inductees are trained to prepare them to use the system. Some specific audience groups have face-to-face training during orientation (Medical Interns and Students), but all other roles are 'trained' locally by Educators or Super Users in a mentoring model with the addition of online training modules.
6.2	Is there documented training for persons that use and maintain the system?	Yes	See response to Q 6.1 above. There is a sign-off sheet for all training attendees to formally attest their attendance. System maintenance as per our contract with Cerner.
6.3	Is the system documentation maintained appropriately?	Yes	System documentation located in the WIKI is accessible by IT personnel and protected from general users. Vendor Cerner's website (uCERN) is tightly controlled and accessible to only authorised AH personnel.
6.4	If applicable, has validation been performed and documented.	Yes	System testing is normally carried out in the development environment prior to implementation in the production environment. Validation of the change in the production environment is also performed after it is implemented. Change management is used to control changes made to production – overseen by Alfred Health's Change Review Group (CRG) for Cerner-related changes or the Change Advisory Board (CAB) for other changes. *User acceptance and data validation (eg, range checks, etc) is carried out during entry by end-users for data integrity. Validation is also conducted by Health Information Services as part of the batch scanning workflow. Other departments and teams are also involved for validation where required.* *Regular reviews are conducted to ensure that end-user access accounts are cleaned up and risk assessments are conducted. Periodic penetration testing had been carried out to identify system/ network vulnerabilities.*

No.	Question	Answer	IT Qualification Statement
6.5	Do you have system validation documentation? Is documentation of the system validation available?	Yes Yes	There are test plans and documentation for validation and user acceptance tests carried out for new systems and major system upgrades. This is to ensure the systems meet the required functional objectives.
6.6	Is there documentation maintained on system maintenance and upgrades?	Yes	See response to Q 6.1 – 6.5 above.
6.7	How will the site train the Clinical Research Monitor in the use of the EMR system?	Yes	The RSC will train (and provide documentation as necessary) the CRA or Monitor at the first session for which they require EMR access.
7	**RECORD COLLECTION, STORAGE & RETENTION**		
7.1	Is there a process to copy records for regulatory agency inspections?	Yes	There is a process to allow internal or external Auditor access to patients' records for the purpose of audit compliance. External Auditor access is managed by IDD, upon formal request by the relevant business unit (e.g. Clinical Governance Unit, Finance or Clinical Director) and authorised by ED, IDD.
7.2	What are your electronic record collection and retention practices? Does the site have a written data storage/ archival policy for the EMR system?	Yes	As per Alfred Health Records Management and Archiving Policy & Guideline (compliant with various Public Record Office Victoria – VERS and Health Records Act 2001) that covers paper and electronic medical record.
7.3	Is there a policy for addressing the availability of data for a defined retention period? Is the electronic data routinely archived as per legal record retention requirements?	Yes No	See response to Q 7.2 above. All electronic patient records have been retained since 1999.
7.4	Can archived electronic medical records be retrieved for a regulatory inspection after the study is closed?	Not applicable	All study EMR can be retrieved from the live data as no archival was carried out.
7.5	Are the medical records recorded on paper, in an electronic system or a combination of both?	☐ Electronic ☐ Paper ☒ Both	These are mostly electronic, some notes and forms are handwritten, and later scanned into the clinical information system.
7.6	Is the data entered directly into a computer system or is there a paper record created first from which they are transcribed/ scanned.	☐ Electronic ☐ Paper first ☒ Both	As above, some notes and forms are handwritten, and later scanned into the CIS. Radiology feeds reports directly into the CIS via HL7 and some diagnostic reports feed in as an AXRM/ CPDI Cold Feed.

No.	Question	Answer	IT Qualification Statement
8	**SYSTEMS & OPERATIONS SECURITY**		
8.1	Are the computer [system] date and time-controlled?	Yes	Time synchronisation exists across all integrated systems to ensure time-stamps are correct, and database records are sequenced correctly. This is also required for correct timestamp in the audit trail.
8.2	Are there procedures to manage and document changes to the system?	Yes	There is a formal change management system that receives, manages, rejects or approves changes. Operational practices include version control and documentation within the codes.
8.3	Is there protection from viruses, hackers, etc.?	Yes	The system is within a secured health network including Cerner. A robust industry-grade solution is in place with layered firewalls and anti-malware security infrastructure.
8.4	Are there Device and/ or Operational Checks as appropriate?	Yes	Operational checks, monitors and alerts are on-going to ensure the system is operational 24x7. An operational Security Operations Centre had been implemented for the environment in Oct20. We have a maintenance window once a month for 2 to 4 hours.
8.5	How are modifications/ system enhancements handled?	Yes	All changes are managed within the organisation's Change Management process, working in tandem with the Cerner's change process. Changes to the software version do not impact historical data, which remains accessible.
9	**ELECTRONIC SIGNATURE**		
9.1	Are electronic signatures used in the system? Does the system allow "signing" of documents electronically? How is the signing done? (eg, ID & password, electronic pen, fingerprint, ID card swipe, etc)	Yes	Electronic signatures are required for electronic order management, referrals, point-of-care scanning and clinical documentation. For electronic orders, users are prompted to validate by entering their password. Password Challenge (ID & password) or Single Sign-On (Tap-On-Tap-Off) with 4-digit PIN At the start of a session, both password & SSO (with 4-digit PIN) challenges will be carried out. The user will be challenged once every 12 hours for the PIN.
9.2	When a signature is applied to a record, is it protected from cutting and pasting (signature) to other records?	Not applicable	It is not applicable due to the electronic signature method used.
9.3	If e-signatures are used, are there written procedures to hold people accountable for their signature?	Yes	This is encapsulated in their employment contract, professional ethics and their acceptance of IT Acceptable Use Policy screen which places responsibility in the use of their individual User ID and password.
9.4	If e-signatures are used, do e-signatures include individual's name, date, and meaning of signature?	Yes	The system logs record the individual's name, date, and purpose/ meaning of signature.
9.5	Are there unique identifiers and passwords to access the system?	Yes	Each user is provided with a unique user ID and password. The first time one logs in, the system prompts the user to change their password.

No.	Question	Answer	IT Qualification Statement
9.6	Are there measures in place to keep passwords confidential (not shared)?	Yes	The IT Security Policy mandates that passwords must not be shared. This is reinforced in the Information Security Awareness campaigns; and login banner which requires each user to accept before accessing Alfred Health network. Password management policy and controls are enforced, e.g, regular password change, lock-out on a number of unsuccessful attempts, etc.
9.7	Does the system automatically suspend or log off a user after a specified period of inactivity?	Yes	This function is available in all areas, and is set to longer periods in physically secured locations, eg, Legal Support, HIS, ICU, Alfred E&TC and Sandringham ED to facilitate operations.
9.8	Is access to certain functions controlled based upon the user's role (e.g., read, write, change, delete)?	Yes	System access positions are designed according to job roles and an Access Control Matrix (ACM) is maintained for this purpose. New account applications must stipulate the job position and discipline, and must be authorised by the staff's department manager.
9.9	Are electronic signatures protected from intentional or unintentional misuse?	Yes	See partial response to Q 9.3 above. They form part of the audit trail that is system protected.
9.10	When a signed record is altered, is the signature made invalid?	Yes	The altered record must be re-signed. However, the system retains a complete audit trail of all electronic signatures.
9.11	Is the signature printed (with signer's name, date & time when signature was done) on the document when it is printed?	Yes	The system has several printing options including an option to print an audit trail including the author's details.
10	**OTHERS**		
10.1	What source data is held on a computer for patients likely to participate in the study?	Not applicable	Original record within the clinical system is the source data. No data is extracted to an external computer for the purpose of the study.
10.2	Is the use of external sources of data (eg, IV pump, vital signs, bedside devices) validated before it is entered into the EMR system?	Yes	The patient is validated by the clinician using his/her individual ID, and the type of data capture is validated before the information is entered into the EMR system.

No.	Question	Answer	IT Qualification Statement
10.3	If using Limited Supervised Access/ Printouts:		
	• Do the paper printouts display the full user ID or name, date & time?	Yes	Evidence available on request.
	• Are printouts signed/ dated by the site staff to confirm that they are a complete and true representation of the data in the system?	No	Only on request by the Sponsor's representative. *Alfred Health Ethics Policy:* *"Researchers/ Auditors/ Monitors must not print any patient information or use screen prints, use USBs or other forms of data transfer to take information off-site. The RSC reserves the right to check that these devices have not been used. The RSC may print certain documentation and de-identify patient information."*
	• Is site prepared to resource over the shoulder access?	Yes	Request by clinical research study manager will be required to extend the access. The CRA's access would be end-dated so that after the study period, the access will no longer be active.

Consultation:
Bullie Sibanda (Data Governance Officer)
Robin Dhillon (Project Manager)
John Moore (Team Lead Blue Team, EMR)
Howard Booth (Manager, Clinical Documentation, EMR)
Merryn Bassett (Clinical Documentation Coordinator, EMR)
Neave, Katrina (IDD Adoption & Change Manager)
Mark Firth (IDD Training Manager)
Melissa Yong (IDD Testing Manager)
Yann Pasnin (Deputy CTO, IDD)
Kim Heath (CTO, IDD)
Chrisa Alexiou (Deputy Director, HIS, Outpatients)
Annie Gilbert (Director, Data Governance & Security, IDD) – Chief Privacy Officer
Nicole Rosenow (Senior Research Governance Officer, Research and Ethics)
Rowan Frew (Ethics Manager, Research and Ethics)
Angela Henjak (Senior Manager, Office of Ethics & Research Governance)

Review prepared by
Name: Chris Liew Date: 29/04/2021 1536h
Designation: Manager, Technology Risk & Information Security

Verified as correct based on the above IT qualification statements

Name: Chris John Date: 06/05/2021 0902h (email)
Designation: Manager, EMR, Operations, Development & Support

Name: Maryanne Liddell Date: 02/07/2021 1252h (email)
Designation: Chief Information Officer, IDD