

## Research Study Computer System Assessment Checklist

### SITE: Alfred Health – Clinical Information System

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

No.	Question	Answer	IT Qualification Statement
1	Name of Systems Administrator	Chris Liew	IT Services department manages the system, and for the purpose of this audit, is represented by the IT Security & Business Continuity Analyst (03-9076 3299)
2	Is the system located in a secure area?	Yes	The clinical information system that houses the patient data is stored in robust secure data centre facilities located in offsite custom-built locations.
3	Is access limited to authorised staff only?	Yes	Only authorised users are allowed into the system. Authorisation is via written request approved by department managers. The type of access commensurate with job duties.
4	Is the system password protected?	Yes	Only authorised users can access the system with their unique account and password.
5	Does each authorised individual have their own unique password?	Yes	Each user is provided with an individual unique account ID and password. The first time one logs in, there's a prompt to change the password to his/ her own.
6	Is the system backed up at regular intervals?	Yes	The system is backed up regularly, including to a secondary system, located in another data centre.
7	Are the backups kept in a separate, secure location?	Yes	The secondary data centre is in a separate and secure location. Backups are also stored off-site.
8	Has the retrieval system been tested and is satisfactory?	Yes	A full failover was carried out in Mar-2008, and one planned this year. A component of the system (CPDI) was failed over recently. (Jul-2010)
9	Does the computer system capture changes made to the data? Does an audit trail exist?	Yes	All activities to the clinical information system including viewing and modifying records are logged. Reports are available to interrogate who accesses specific patient information. Old audit trail logs greater than 30 days are overwritten, and the process to recover from backup is technically possible but requires significant resources.
10	Can the audit trail be easily viewed and copied?	Yes	Only authorised personnel are allowed to access the audit trail. These are made available to managers on request. HIS department has two reports that search the audit trail for activities for a period of time, and for activities for specific patients.
11	If the software version changes, how will historical data be read?	Yes	Changes to the software version does not impact the historical data. Historical data is still accessible. This requirement is important, as we keep all patient information from the first version (2000).
12	If applicable, are operating instructions in place?	Yes	Usage instructions and training material for end-users (documents and video format) are available in the intranet.

## Research Study Computer System Assessment Checklist

No.	Question	Answer	IT Qualification Statement
			Support instructions are available to the IT support staff in the internal department folders and wiki. The system has online Help Menu the vendor has a centralised online support repository of information with dedicated customer logins.
13	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. However, change management process is currently being reviewed and being improved. <i>Data validation (eg, range checks, etc) is carried out during entry by end-users for data integrity. However, some fields are free text and data may be 'garbage' in some instance. Regular reviews are conducted to ensure the accounts are cleaned up and risk assessments are conducted (eg, Emergency module review).</i>
14	Do you have system validation documentation?	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.
15	Is there a system-generated audit trail?	Yes	See response to Question 9 above.
16	Is there documented training for persons that use and maintain the system?	Yes	See response to Question 12 above.
17	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.
18	Does the system contain complete records (data, metadata, audit trail, and, as applicable, e-signatures)?	Yes	This question is partially answered in Question 9 above. As for e-signatures, the system log record the individual's name, date, and meaning of signature.
19	Is there a process to copy records for regulatory agency inspections?	Yes	There is a process to allow auditor access to specific patients' records. External Auditor access is managed by Health Information Services.
20	What are your electronic record collection and retention practices?	Yes	As per Alfred Health Records Management and Archiving Policy (compliant with various Public Record Office Victoria – VERS and Health Records Act)
21	Are there adequate backup, recovery and contingency procedures for data and metadata?	Yes	See response to Question 6 above.
22	Are there procedures and controls for physical security,	Yes	See response to Question 2 above.

## Research Study Computer System Assessment Checklist

No.	Question	Answer	IT Qualification Statement
	ensuring a controlled environment?		
23	Are there procedures and controls for user access security?	Yes	See response to Question 3 – 5 above.
24	Are there procedures to manage and document changes to the system?	Yes	There is a change management system that documents changes. Individual practices include version control and documentation within the codes.
25	Is there protection from viruses, hackers, etc.?	Yes	A robust industry grade solution is in place with Intrusion Detection/ Protection System, and layered anti-malware security infrastructure.
26	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. We have a maintenance window once a month for two to four hours.
27	Is the system documentation maintained appropriately?	Yes	See response to Question 12 above
28	Are electronic signatures used?	Yes	Electronic signatures are required for electronic order management of diagnostic services and for clinical documentation. Users are prompted to validate these actions by entering their account id password.
29	If e-signatures are used, are there written procedures to hold people accountable for their signature?	Yes	This is deemed to be encapsulated in their employment contract, professional ethics and their acceptance of conditions of use acceptance screen which places responsibility in the use of their individual ID and password.
30	If e-signatures are used, do e-signatures include individual's name, date, and meaning of signature?	Yes	See response to Question 18 above.
31	Are there unique identifiers and passwords to access the system?	Yes	Each user is provided with an individual unique account ID and password. The first time one logs in, there's a prompt to change the password to his/ her own.
32	Are there measures in place to keep passwords confidential (not shared)?	Yes	The IT Security Policy mandates that passwords must not be shared. Password management policy and procedures are in place, eg, enforced password change, lock-out on a number of unsuccessful attempts, etc.
33	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, ICU and ED to facilitate operations.
34	Is access to certain functions controlled based upon the user's role (e.g., read, write, change, delete)?	Yes	Systems positions are aligned with job roles. The initial account creation form must stipulate the job position, signed off by the department manager.
35	Is there a list of individuals authorised to access each function?	Yes	A reporting tool can generate the list of individuals authorised for each position type.

## Research Study Computer System Assessment Checklist

No.	Question	Answer	IT Qualification Statement
36	Is there an audit trail for capturing changes to information in the system?	Yes	All activities to the clinical information system including viewing and modifying records are logged. Reports are available to interrogate who accesses specific patient information. Old audit trail logs greater than 30 days are overwritten, and the process to recover from backup is technically possible but requires significant resources.
37	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 Question 36 above. <i>(sample available)</i>
38	Are the audit trail entries date- and time- stamped?	Yes	See response to Question 7 above.
39	Does the audit trail indicate who made a change?	Yes	All transactions recorded in the audit trail have at least the user ID, data/ time stamp and action.
40	Is the audit trail protected from modification by users?	Yes	Only authorised personnel are allowed to access the audit trail. These are made available to managers on request.
41	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.
42	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	See response to Question 6 above.
43	Can this backed up data be restored?	Yes	See response to Question 8 above.
44	Has the restoration of backup data been tested?	Yes	See response to Question 8 above.
45	Are electronic signatures used in the system?	Yes	See response to Question 28 above.
46	Are electronic signatures protected from intentional or unintentional misuse?	Yes	Access to system configuration and database has to be authorised.
47	When a signature is applied to a record, is it protected from cutting and pasting to other records?	Yes	The signature is in the form of account ID and password – the password is hidden and once entered, the password cannot be accessed by another user to be re-used for another record.
48	Are the name of the signer and the meaning of the signature displayed?	Yes	The action by the signer is stored in the system (using user ID and password) as a record of who carried out the action. If necessary a second user is required to co-sign, eg, placing an order for the patient on behalf of the doctor.
49	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.

## Research Study Computer System Assessment Checklist

No.	Question	Answer	IT Qualification Statement
50	Will the sponsor CRA (clinical research associate) be able to access the data for monitoring?	Yes	A unique account can be created for the CRA to gain access to the data.
51	Is the system capable of restricting the CRA's access to ONLY those patient records of sponsor trial participants?	Yes	
52	Is there documentation maintained on installation and training?	Yes	See response to Question 12 above.
53	Is there documentation maintained on system maintenance and upgrades?	Yes	See response to Question 12, 13 and 14 above.
54	Is there a policy for addressing the availability of data for a defined retention period?	Yes	See response to Question 20 above.

Review carried out by



Name: CHRIS LIEW  
Designation: IT Security & Business Continuity Analyst

09-08-2010

Date

Verified as correct based on the IT qualification statements



Name: MARK GARDINER  
Designation: CIO

10-08-2010

Date