Northern NSW & Mid North Coast Local Health Districts
Cancer Trials Network

21 CFR 11 Electronic Records;
Electronic Signatures

MOSAIQ™ Assessment Worksheet

- Final Version 3.2; March 2012 -

System Name:	**MOSAIQ™**	System Location:	345 Pacific Highway Coffs Harbour NSW 2450
Assessment Type: *(check all that apply after completing pg. 7)*	✓ Electronic Records ✓ Electronic Signatures ✓ Closed System ☐ Open System	Director, Area Cancer Services:	Dr Tom Shakespeare Northern NSW & Mid North Coast Local Health Districts
		Assessor 1: Assessor 2: Assessor 3: Assessor 4: Assessor 5:	David Goulding – IT Infrastructure Manager Stuart Greenham – Area Manager Radiation Therapy Nicole Raschke – Manager, Cancer Trials Network Klaus Daro – Project Officer Oncology Information management System Joshua Herden – Quality and Information Management Radiation Therapist
Start Date	March 2012	End Date:	

APPROVAL OF ELECTRONIC RECORDS ASSESSMENT RESULTS

The approval signatures below mean that the signers:

- Have read this document, and based upon their understanding of this document and the signer's education, training, and experience, can find no substantive errors or omissions, and
- Attest that the assessment described by this worksheet accurately summarises the current capability of the computerised system described in this assessment to fulfil the applicable requirements of 21 CFR Part 11[1].

Assessor 1 Name (print)	*Assessor Signature*	*Date*
Assessor 2 Name (print)	*Assessor Signature*	*Date*
Assessor 3 Name (print)	*Assessor Signature*	*Date*
Assessor Name 4 (print)	*Assessor Signature*	*Date*
Assessor Name 5 (print)	*Assessor Signature*	*Date*

[1] The complete 21 CFR Part 11 Code of Federal Regulations document can be found at: http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm

TABLE OF CONTENTS

Background

There is an increasing use of computerised systems in clinical trials to generate and maintain source data and source documentation on each clinical trial subject. Such electronic source data and source documentation must meet the same fundamental elements of data quality (e.g., attributable, legible, contemporaneous, original, and accurate) that are expected of paper records and must comply with all applicable statutory and regulatory requirements. The US FDA's acceptance of data from clinical trials for decision-making purposes depends on the FDA and other regulatory authority's ability to verify the quality and integrity of the data during an on-site inspection and audit. (21 CFR 312, 511.1(b), and 812).

Whilst it is recognised that the Northern NSW and Mid North Coast Local Health District's (NNSW & MNC LHD) computerised systems are not physically located in the US and therefore not under FDA regulations, many research studies that NNSW & MNC LHD Clinical Trial Units take part originate in the US. The data obtained for the marketing of products through the FDA requires that the computerised systems used comply with the FDA regulations.

Purpose

The purpose of this worksheet is to:

- Specify the criteria under which electronic records, electronic signatures, and handwritten signatures executed to electronic records are considered equivalent to paper records and handwritten signatures executed on paper in accordance with 21 CFR Part 11[2] (the Regulation),
- Evaluate a computerised system versus the established requirements of the Regulation, and
- Document the evaluation of the computerised system.

Definition of Terms[3]

Closed System[4]

An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Inspection

The act by a regulatory authority(ies) of conducting an official review of documents, facilities, records, and any other resources that are deemed by the authority(ies) to be related to the clinical trial and that may be located at the site of the trial, at the sponsor's and/or contract research organisation's (CRO's) facilities, or at other establishments deemed appropriate by the regulatory authority(ies).

Open System[4]

An environment in which system access is not controlled persons who are responsible for the content of electronic records that are on the system.

Regulatory Authority

---

[2] Guidance for Industry. Computerised Systems Used in Clinical Investigations. http://www.fda.gov/cder/guidance/7359fnl.pdf

[3] All definitions taken from ICH Guidelines for Good Clinical Practice (E6) *Step 4* version dated 10 June 1996 http://www.ich.org/ with the exception of those noted.

[4] Guidance for Industry. 21 CFR Part 11; Electronic Records; Electronic Signatures. Glossary of Terms

Bodies having the power to regulate. In the ICH GCP guideline the expression Regulatory Authorities includes the authorities that review submitted clinical data and those that conduct inspections. These bodies are sometimes referred to as competent authorities

Source Data

All information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the reconstruction and evaluation of the trial.

Source Documents

Original documents, data, and records (e.g., hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate copies, microfiches, photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at the pharmacy, at the laboratories and at medico-technical departments involved in the clinical trial).

FDA 21 CFR 11 Recommendations

In summary the recommendations set forth by the FDA 21 CFR 11 document provides guidance on the following:

A. Study Protocols

This recommendation refers to the study protocol developed by the sponsor of a clinical trial and is not relevant to this assessment document.

B. Standard Operating Procedures

There should be specific procedures and controls in place when using computerised systems to create, modify, maintain, or transmit electronic records, including when collecting source data at clinical trial sites. Standard operating procedures (SOPs) should be maintained either on-site or be remotely accessible through electronic files as part of the specific study records, and the SOPs should be made available for use by personnel and for inspection by FDA.

C. Source Documentation and Retention

When original observations are entered directly into a computerised system, the electronic record is the source document. Under 21 CFR 312.62, 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be maintained under part 312, § 511.1(b), and part 812, for a period of time specified in these regulations. This requirement applies to the retention of the original source document, or a copy of the source document.

D. Internal Security Safeguards

1. Limited Access

Access must be limited to authorised individuals (21 CFR 11.10(d)) and may be accomplished by the following recommendations:

- Individual accounts for users
- Log-in attempt limits and recording of unauthorised access log-in attempts
- User accounts are password or other access key restricted
- Passwords or access keys should be changed regularly
- One log-in at a time per user
- Users should log off at the end of their session, or an automatic log off for long idle periods

2. Audit Trails

Audit trails or other security methods used to capture electronic record activities should describe when, by whom, and the reason changes were made to the electronic record. Original information should not be obscured through the use of audit trails or other security measures used to capture electronic record activities.

3. Date/Time Stamps

Controls should be established to ensure that the system's date and time are correct. The ability to change the date or time should be limited to authorised personnel, and such personnel should be notified if a system date or time discrepancy is detected. Any changes to date or time should always be documented. Documentation of time changes that systems make automatically to adjust to daylight savings time conventions are not necessary.

E. External Security Safeguards

External safeguards should be put in place to ensure that access to the computerised system and to the data is restricted to authorised personnel.

Procedures and controls should be put in place to prevent the altering, browsing, querying, or reporting of data via external software applications that do not enter through the protective system software.

Controls should be implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on data.

F. Other System Features (Relevant to this paper only)

1. System Controls

Sufficient backup and recovery procedures should be designed to protect against data loss. Records should regularly be backed up in a procedure that would prevent a catastrophic loss and ensure the quality and integrity of the data. Records should be stored at a secure location specified in the SOP. Storage should typically be offsite or in a building separate from the original records.

Maintenance of backup and recovery logs is recommended to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

2. Change Controls

The integrity of the data should be maintained when making changes to the computerised system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation. The effects of any changes to the system should be evaluated and some should be validated depending on risk. Changes that exceed previously established operational limits or design specifications should be validated. Finally, all changes to the system should be documented.

G. Training of Personnel

Those who use computerised systems must determine that individuals (e.g., employees, contractors) who develop, maintain, or use computerised systems have the education, training and experience necessary to perform their assigned tasks (21 CFR 11.10(i)).

Training should be provided to individuals in the specific operations with regard to computerised systems that they are to perform. Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerised system and with any changes to the system.

It is recommended that computer education, training, and experience be documented.

System Classification Section

Determine if the computerised system is required to comply with 21 CFR 11.

NOTE: 'Scenario' numbers refer to those in **Table 1** (page 8) and indicate which section of 21 CFR 11 are relevant providing direction for which portion(s) of the **Assessment Section** (pages 9 – 13) requires to be completed.

Question #	Question	Answer	OBS/REC #
C.1	Does this computerised system create, modify, maintain, archive, retrieve, or transmit any electronic records(s) that are required to demonstrate compliance with FDA regulations? *(NOTE: Even if "parallel" paper records exist, answer "yes". All electronic records that are maintained in viewable condition must comply)*	☐ No — Stop here, Part 11 compliance is not required. ✓ Yes — Continue with next question	1
C.2	Is the computerised system an "Open System" or a "Closed System"? *(Note: See the Definitions section)*	☐ Open System ✓ Closed System	
C.3	Does the computerised system require electronic signatures on the electronic records? *Q1. If the records are printed out, would or do you need to sign them"* *Q2. Do you save 'John Smith' as a field in the file / database and expect it to be right on the form, printout, and/or archive?* *Q3. If I sign 'John Smith' does that mean I have attested that I did or saw something, or that I'm authorising some action?* *If any of these answers is yes, e-signatures are required.*	☐ No — Scenario #1 Applies Skip to C.5 ✓Yes — Continue with the next question	
C.4	Classify the electronic signature that this system uses: (Check all that apply) ▪ Handwritten signature executed to electronic record ▪ Biometric ▪ Identification code / password ▪ Token / password	✓Scenario #2 Applies ☐ Scenario #3 Applies ✓Scenario #4 Applies ☐ Scenario #5 Applies Continue with next question	
C.5	Update the "Assessment Type" on the cover sheet. Update the "Assessment Section" to indicate which 21 CFR 11 sections are N/A according to the chosen Scenario Number and Table 1. Complete the "Assessment Section"		

Table 1 – Applicable Sections of 21 CFR 11

Scenario #	Attributes	21 CFR 11 Sections									
		11.1; 11.2; 11.3	11.10	11.30	11.50	11.70	11.100	11.200(a)	11.200(b)	11.300(a), (b), (d)	11.300(c), (e)
	CLOSED SYSTEMS										
1	Electronic Record Only (without signature)	✓	✓	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**
2	Handwritten Signature Executed to Electronic Record	✓	✓	**N/A**	✓	✓	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**
3	Electronic Signature Based upon Biometrics	✓	✓	**N/A**	✓	✓	✓	**N/A**	✓	**N/A**	**N/A**
4	Electronic Signature Based upon ID Code & Password	✓	✓	**N/A**	✓	✓	✓	✓	**N/A**	✓	**N/A**
5	Electronic Signature ID Code & Token	✓	✓	**N/A**	✓	✓	✓	✓	**N/A**	**N/A**	✓

Assessment Section

1. Ensure that all non-applicable parts have been checked "N/A" before commencing this assessment. (Refer to the **Classification Section** and **Table 1**)

2. Record "Assessment Results" as conformances (C) or non-conformances (NC). Any non-conformances require an Observation or Recommendation (OBS/REC #). Observations/Recommendations can be written in Appendix A referring to the number in this table.

Sub – Part B: Electronic Records

Req't #	21 CFR 11 Requirements	Assessment Results	OBS/REC #
11.10: CONTROLS FOR CLOSED SYSTEMS			
R.1	**Validation** – The computerised system shall be validated in accordance with applicable Corporate Standards and regulatory requirements to ensure……		
R.1.1	- Accuracy [11.10 (a)]	✓ C ☐ NC ☐ N/A	
R.1.2	- Reliability [11.10 (a)]	✓ C ☐ NC ☐ N/A	
R.1.3	- Consistent intended performance [11.10 (a)]	✓ C ☐ NC ☐ N/A	
R.1.4	- Ability to discern invalid or altered records [11.10 (a)]	✓ C ☐ NC ☐ N/A	
R.2	**Inspectability** – Procedures and controls shall be designed and implemented to include the ability to…..		
R.2.1	- Generate accurate and complete copies of records in both human and electronic from for inspection, review, and copying [11.10 (b)]	✓ C ☐ NC ☐ N/A	
R.2.2	- Protect records to enable their accurate and ready retrieval throughout the records retention period [11.10 (c)]	✓ C ☐ NC ☐ N/A	
R.3	**Security** – Security procedures and controls shall be designed and implemented to include:		
R.3.1	- System access shall be limited to authorised individuals [11.10 (d)]	✓ C ☐ NC ☐ N/A	
R.3.2	- Operational system checks shall enforce the proper sequencing of steps in a process (as appropriate) [11.10 (f)]	✓ C ☐ NC ☐ N/A	
R.3.3	- Authority checks shall ensure that only authorised individuals can:		
R.3.3.1	Use the system [11.10 (g)] (Logical access)	✓ C ☐ NC ☐ N/A	
R.3.3.2	Electronically sign a record [11.10 (g)]	✓ C ☐ NC ☐ N/A	
R.3.3.3	Access the operation or computer system input or output device [11.10 (g)]	✓ C ☐ NC ☐ N/A	
R.3.3.4	Alter a record [11.10 (g)]	✓ C ☐ NC ☐ N/A	
R.3.3.5	Perform the specified operation [11.10 (g)]	✓ C ☐ NC ☐ N/A	
R.3.4	- Device or terminal checks shall determine validity of the source of input or operation (as appropriate) [11.10 (h)]	✓ C ☐ NC ☐ N/A	
R.4	**Audit Trails** – Procedures and controls shall be designed and implemented for audit trails to:		
R.4.1	- Be secure [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.2	- Be computer-generated [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.3	- Be time- and date-stamped [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.4	- Independently record the date/time of operator entries and actions that…		
R.4.4.1	Create electronic records [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.4.2	Modify electronic records [11.10 (e)]	✓ C ☐ NC ☐ N/A	

R.4.4.3	Maintain electronic records [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.4.4	Delete electronic records [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.5	- Ensure that changes to electronic records shall not obscure previously recorded information [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.6	- Ensure that audit trail records shall be maintained for at least as long as the retention of the underlying records [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.4.7	- Ensure that audit trail records shall be available for review and copying [11.10 (e)]	✓ C ☐ NC ☐ N/A	
R.5	**Personnel Qualifications** – Determination that the following persons have the education, training, and experience to perform their assigned tasks:		
R.5.1	- Developer(s) of the computerised system [11.10 (i)]	✓ C ☐ NC ☐ N/A	
R.5.2	- Maintainer(s) of the computerised system [11.10 (i)]	✓ C ☐ NC ☐ N/A	
R.5.3	- User(s) of the computerised system [11.10 (i)]	✓ C ☐ NC ☐ N/A	
R.6	**Accountability and Responsibility for Actions** – Establishment of, and adherence to, written policies and/or procedures that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification [11.10 (j)]	✓ C ☐ NC ☐ N/A	
R.7	**Systems Documentation Controls** – Establishment and use of appropriate controls over systems documentation including:		
R.7.1	- Adequate controls over the documentation for system operation and maintenance, to include:		
R.7.1.1	Distribution of documentation [11.10 (k)(1)]	✓ C ☐ NC ☐ N/A	
R.7.1.2	Access to documentation [11.10 (k)(1)]	✓ C ☐ NC ☐ N/A	
R.7.1.3	Use of documentation [11.10 (k)(1)]	✓ C ☐ NC ☐ N/A	
R.7.2	- Revision and change control procedures to maintain an audit trail that documents the time-sequenced development and modification of the systems documentation [11.10 (k)(2)]	✓ C ☐ NC ☐ N/A	

Req't #	21 CFR 11 Requirements	Assessment Results	OBS/REC #
11.30: CONTROLS FOR OPEN SYSTEMS			
R.8	**Controls for Open Systems –** Open systems used to create, modify, maintain, or transmit electronic systems shall employ procedures and controls designed to ensure the following attributes for those electronic records from the point of their creation to the point of their receipt:		
R.8.1	- Authenticity [11.30]	☐ C ☐ NC ✓ N/A	
R.8.2	- Integrity [11.30]	☐ C ☐ NC ✓ N/A	
R.8.3	- Confidentiality, as appropriate [11.30]	☐ C ☐ NC ✓ N/A	
	Such procedures and controls shall include:		
R.8.4	- Those identified in 11.10, as appropriate [11.30]	☐ C ☐ NC ✓ N/A	
R.8.5	- Use of digital signature standards, as appropriate [11.30]	☐ C ☐ NC ✓ N/A	
11.50 SIGNATURE MANIFESTATIONS			
R.9	Signature manifestations – Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		
R.9.1	- The printed name of the signer [11.50 (a)(1)]	✓ C ☐ NC ☐ N/A	
R.9.2	- The date and time when the signature was executed [11.50 (a)(2)]	✓ C ☐ NC ☐ N/A	
R.9.3	- The meaning of the signature [11.50 (a)(3)]	✓ C ☐ NC ☐ N/A	
	All items identified in 11.50 (a)(2), and 11.50 (a)(3) above shall be:		
R.9.4	- Subject to the same controls as for electronic records [11.50 (b)]	✓ C ☐ NC ☐ N/A	
R.9.5	- Included as part of any human readable form of the electronic record (such as electronic display and/or printout or report) [11.50 (b)]	✓ C ☐ NC ☐ N/A	
11.70: SIGNATURE / RECORD LINKING			
R.10	**Signature/Record Linking –** Electronic signatures, and handwritten signatures executed to electronic records, shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means [11.70]	✓C ☐ NC ☐ N/A	

Sub-Part C: Electronic Signatures

Req't #	21 CFR 11 Requirements	Assessment Results	OBS/REC #
11.100: GENERAL REQUIREMENTS FOR ELECTRONIC SIGNATURES			
R11	General Requirements		
R11.1	- Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else [11.100 (a)]	✓ C ☐ NC ☐ N/A	
R11.2	- The identity of the individual shall be verified prior to the organisation establishing, assigning, certifying, or otherwise sanctioning that individual's electronic signature [11.100 (b)]	✓ C ☐ NC ☐ N/A	
R11.3	- Persons using electronic signatures shall, prior to or at the time of such use, certify to the FDA that the electronic signatures used in the computerised system on or after August 20, 1997 are intended to be the legally binding equivalent of traditional handwritten signatures [11.100 (c)]	✓ C ☐ NC ☐ N/A	2
R11.4	- The certificate shall be submitted in paper form and signed with a traditional handwritten signature to the appropriate FDA Office specified in the Regulation [11.100 (c)(1)]	✓ C ☐ NC ☐ N/A	2
11.200: ELECTRONIC SIGANTURE COMPONENTS AND CONTROLS			
R12	**Electronic Signatures Not Based on Biometrics** – Electronic signatures that are not based on biometrics shall:		
R12.1	- Employ at least 2 distinct identification components such as an identification code and password [11.200 (a)(1)]	✓ C ☐ NC ☐ N/A	
R12.2	- When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components. Subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual [11.200 (a)(1)(i)]	✓ C ☐ NC ☐ N/A	
R12.3	- When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components [11.200 (a)(1)(ii)]	✓ C ☐ NC ☐ N/A	
R12.4	- Be used only by their genuine owners [11.200 (a)(2)]	✓ C ☐ NC ☐ N/A	
R12.5	- Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other that its genuine owner requires collaboration of two or more individuals [11.200 (a)(3)]	✓ C ☐ NC ☐ N/A	
R.13	Electronic Signatures Based On Biometrics		
R13.1	Electronic records based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners [11.200 (b)]	☐ C ☐ NC ✓ N/A	
11.300: CONTROLS FOR IDENTIFICATION CODES / PASSWORDS			
R14	**Controls for Identification Codes/Passwords** – Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity, including:		

R14.1	- The combination of identification code and password shall be unique [11.300 (a)]	✓ C ☐ NC ☐ N/A	
R14.2	- Identification code and password issuances shall be periodically checked, recalled, or revised (e.g., to cover such events as password aging) [11.300 (b)]	✓ C ☐ NC ☐ N/A	
R14.3	- Procedures and controls shall be designed and implemented for devices which bear or generate identification code or password information to:		
R14.3.1	Electronically deauthorise devices that have been lost, stolen, or potentially compromised [11.300 (c)]	✓ C ☐ NC ☐ N/A	
R14.3.2	Issue temporary or permanent replacements using suitable, rigorous controls [11.300 (c)]	✓ C ☐ NC ☐ N/A	
R14.4	- Transaction safeguards shall be implemented to:		
R14.4.1	Prevent unauthorised use of identification codes and passwords [11.300 (c)]	✓ C ☐ NC ☐ N/A	
R14.4.2	Detect any attempt at unauthorised use of identification codes and/or passwords [11.300 (d)]	✓ C ☐ NC ☐ N/A	
R14.4.3	Report in an immediate and urgent manner any attempt at unauthorised use of identification codes and passwords to the system security unit, and, as appropriate, organisational management [11.300 (d)]	✓C ☐ NC ☐ N/A	
R14.5	- Initial and periodic testing of devices that bear or generate identification code or password information [11.300 (e)]	✓C ☐ NC ☐ N/A	

Appendix A: Observations and Recommendations

OBS/ REC #	Req't #	Observation / Recommendation
1		The computerised systems of the North Coast Cancer institute is not located and does not operate within the jurisdiction of the United States FDA authority therefore would not be obligated to meet the FDA specific criteria nevertheless the software complies with the criteria so noted through compliance with Australian regulatory equivalents.
2	11.3 & 11.4	Refer to Appendix B for a copy of the letter signed by the Director, Area Cancer Services sent to the FDA attesting to the legality of electronic signatures in Mosaiq™ in April 2012.

Appendix B: Electronic Signature FDA Certification Letter

Health
Mid North Coast
Local Health District
Cancer Trials Network
Health
Northern NSW
Local Health District

Food and Drug Administration
The Office of Regional Operations
12420 Parklawn Drive
RM 3007 Rockville, MD 20857

3rd April, 2012

Dear Sirs,

Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that all electronic signatures of employees of Northern NSW & Mid North Coast Local Health Districts contained within the electronic medical record system, Mosaiq™ are the legally binding equivalent of traditional handwritten signatures as verified by the assessors of Mosaiq™.

Associate Professor Thomas Shakespeare
Director, Area Cancer Services
Northern NSW & Mid North Coast
Local Health Districts

Mid North Coast Local Health District
Port Macquarie Health Campus
PO Box 126
Port Macquarie NSW 2444