Computer system compliance with FDA 21 CFR Part 11

The Information system of the Cliniques universitaires Saint-Luc is not formally certified FDA 21 CFR Part 11. However, in our management of the information system, we apply procedures and rules that lead us to the respect of the recommendations and the regulations. This document summarizes our level of compliance with the FDA 21 CFR Part 11 criteria.

Internal Policy

A variety of hospital policies and procedures require staff to secure their usernames and passwords ("ID/PW") against unauthorized use.

Here are some simple steps that can be taken to achieve this:

- *Never ever share your password with anyone, including family members, students, supervisors, support staff, or others.*
- *Never keep your password in a computer file, on your desk or in other obvious or easily accessible locations.*
- *When developing passwords, do not use dictionary words, foreign words, simple transformations, repeated words, names of people, keyboard sequences, phone numbers, or words with vowels removed, even if the system might allow this. Do use a line from a song or verse together with mixed cases, punctuation marks, and numbers.*
- *Change your password frequently, at least every three (3) months, even if not prompted or required to do so by the system.*

Epic Electronic Health Record System Compliance with 21 CFR Part 11

CuSL and staff use electronic applications to maintain records and create signatures necessary to support clinical care and human research activities. Sponsors occasionally request certification of compliance with 21 C.F.R. Part 11 ("Part 11") or alternatively certification that systems covered by Part 11 will be used for these activities.

This notice provides information about the Hospital's use of Epic Electronic Health Record System (EHR) with Part 11 requirements.

FDA Approach

The FDA released another Guidance for Industry on the Use of Electronic Health Record Data in Clinical Investigations in July 2018: (https://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM501068.pdf).

In this guidance the FDA reiterated that "Under the ONC Health IT Certification Program, certified EHR technology would be in compliance with applicable provisions under 45 CFR part 170. EHR technology with certified capabilities generally has clear advantages, because many of the certification requirements are aimed toward ensuring interoperable data sharing and enabling processes to keep electronic data confidential and secure. In particular, all EHR technology certified under the ONC Health IT Certification Program is required to meet certain privacy and security protection requirements for an individual's health information (see 45 CFR 170.314(d)(1) through (8) and 45 CFR 170.315(d)(1) through (11)). FDA encourages the use of such certified EHR systems together with appropriate policies and procedures for their use."

Epic Compliance

Epic Electronic Health Record System is ONC Health IT certified. Epic has historically been one of the first EHR developers to have ambulatory and inpatient software applications certified against industry standard criteria. For current certification information, see: http://www.epic.com/docs/mucertification.pdf

The FDA has stated that "use of such certified EHR technology is encouraged and, if used, would give FDA confidence during inspections that the EHR data is reliable and that the technical and software components of privacy and security protection requirement have been met."

In addition, based on an internal analysis, there are no known issues that currently suggest that CuSL's Epic Electronic Health Record System together with the hospital's electronic authentication system, is not compliant with Part 11 requirements.

The FDA has not published certification criteria or a certification process for Part 11. Moreover, the FDA Guidance for Industry on Electronic Source Data in Clinical Investigations (September 2013) states, **"The FDA does not intend to assess the compliance of EHRs with Part 11."** As a result of this guidance, Epic has no plans to certify their EHR to Part 11.

Given the lack of specific detailed certification criteria, the FDA's own industry guidance, and Epic's position with respect to the FDA Guidance, the CuSL is unable to provide any absolute representation or warranty of compliance to Part 11.
The CuSL Information Security and Privacy committee believes that CuSL's Epic system is compliant with Part 11 requirements.

CuSL researchers performing FDA-regulated studies may rely on this compliance statement or may print out and physically sign required documents and maintain these with other required research records. FDA has specified that it will exercise "enforcement discretion" where electronic records and signature are committed to physical writings and appropriately countersigned to assure security and non-repudiation.

Compliance level - Summary

Criteria	Compliance Level
Validation of systems	**YES** We respect a quality approach based on ITIL and ISO27000 recommendations.
Logical and Physical Security	System access for development servers and application servers is strictly controlled through both logical and physical security procedures and methods. Epic provides a method for controlling access rights and levels. System is built using an architecture that makes unauthorized access very difficult and controllable. We implemented adequate procedures and processes for logical and physical security, such as back- up of data, safe storage, virus protection, data loss protection and disaster recovery. Computers are kept in secure, locked rooms, with restricted access, protected from fire, flooding,... and with correct climate conditions for system and storage. A mirror site is available. We have DRP and BCP procedures in case of breakdown or system failure. We have regular backups (tape and disk, frequency: 1/day, storage on–site and dual location). Procedures are regularly tested.
Ability to generate accurate and complete copies	**YES**
Protection and retention of records	**YES** Respect of legal rules Respect of Belgian Public Health Services recommendations
Limiting system access to authorized individuals	**YES** – Orbac approach – individual account – specific rules for logical access control We have a user account management process for creating, managing and revoking user accounts. The following controls are in place to limit access : - Unique user accounts with user ID and password. - Locks user account after several failed logs in attempts - Automatically timed-out after inactive periods Only authorized individuals can access, use and sign records. Audit trail is performed.
Written policies	**YES** – confidentiality policy and good practices code

Criteria	Compliance Level
Audit trail	**YES** The system has an audit trail. Creation, modification and deletion actions are recorded with the date and time of the operator's entries and with the ID of the user who performed the action. The audit trail cannot be modified by the user. Access to the system and control of access to sensitive log information is done by a security officer. Inspector or sponsor auditor can view the audit trail, on-demand, with his own read-only individual user account.
Operational system checks to enforce step and events	**YES** We realize consistency checks in the system to ensure that data transferred from other systems (radiology data, laboratory data) match with the correct patient.
Electronic sign of record, authority checks	**YES** By login ID and password. With timestamping and hash of dataset. Handwritten signatures equivalence
Education and training	**YES** An up-to-date user documentation is available on-line. A training can be realized on demand or in a welcome program. We ensure that technical persons implementing, maintaining or using the Epic technology have the appropriate training and that the requirements have been identified, implemented, and appropriately documented.
Proper documentation	**YES** Online documentation for the software CMDB approach for the computer system

Compliance level - Detail

1.1. Introduction

21 CFR Part 11 is an FDA (Food & Drug Administration) regulation, applicable since 1997, which specifies how electronic records or data and electronic signatures should be managed.

The 21 CFR Part 11 regulation defines the criteria by which electronic records and signatures will be considered equivalent to paper records and handwritten signatures. The regulation applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted as part of the requirements for any record described in the FDA regulation

1.2. Scope

(a) The regulations in this part set forth the criteria under which FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, in accordance with any records requirements set forth in agency’s regulations. This part also applies to electronic records submitted to the agency under the requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency’s regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) When electronic signatures and associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to handwritten signatures, initials, and other general signatures required by agency regulations, unless specifically excluded by one or more regulations effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, as provided in §11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and related documentation maintained under this part must be readily accessible and subject to inspection by FDA.

1.3. 21 CFR Part 11 requirements summary

21 CFR Part 11 states that the risk of manipulation, misinterpretation, and alteration without documentation of justification is greater with computerized records management than with handwritten records and that these instances are more difficult to detect with electronic records/signatures than with traditional paper records/handwritten signatures. Additional control measures are therefore necessary.

Requirement	Description
Validation	All systems must be validated to ensure accurate, reliable and consistent processing in accordance with expected performance.
Audit Trails	Systems must provide secure, computer-generated, time-stamped audit trails to record the actions of creating, modifying or deleting electronic records.
Retention, protection, reproducibility and recovery of recordings	Systems must be able to store, protect and quickly recover records for the entire defined data retention period. They must be able to reproduce records in an electronic and readable form.
Control of documents	Controls must exist for access to system execution and maintenance documentation, review, distribution and use.
Access security	Systems must limit access to qualified and authorized personnel only. In open systems, additional security measures must be taken to ensure access security (see also 21 CFR Part 11.30).
Electronic signature	Systems must provide measures to ensure that use is limited to the original holders only and that any attempted use by third parties is detected and promptly reported. Non-biometric systems must use two separate identification mechanisms (user ID/password). The user ID and password must be entered prior to a signature session and at least the password must be entered for each subsequent signature during the same session. Electronic signatures must not be reused or reassigned. The purpose of an electronic signature must be clearly stated. Finally, systems must include measures to prevent forgery of electronic signatures by standard tools. Written procedures must be in place to hold individuals accountable for actions taken under the cover of their electronic signature.
Certificat for the FDA	Written certification that all electronic signatures used are as binding as traditional handwritten signatures must be provided to the regional FDA office.

1.3.1. Point 01 : System Validation

Specification	
11.10(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records 11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency… 11.10(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period	Information system (IS) is developed with quality approach and good practices. Recognised approach is given in ITIL and ISO27000 recommandations. Regulary self-inspection audits are operated to demonstrate compliance with the internal SMSI procedures and controls. IS can be able to identify changes to electronic records in order to detect invalid or altered records. In practice, adequate audit trail is implemented. All significant modifications are recorded, including timestamping, user identifier, old/new value and comment. Not authorized modifications are prevented by the system via the secure access function. Archived records are secured via checksum mechanism, allowing to detect not authorized modifications. IS allows electronic data to be accessed in human readable form, to export data and any supporting regulatory information. Specify retention periods in accordance with legal rules are guaranteed, regardless of upgrades to operating environment. IT organisation maintain defined, proven and secured backup and recovery processes.

1.3.2. Point 02 : System access security

Specification	
11.10(d) Limiting system access to authorized individuals.	By managing profiles, the administrator ensures that only people who have a legitimate business need to use the system can have physical access to the system (e.g. server, system console). Users have an individual, non-transferable login as recommended. The system has logging functions for actions related to access security such as login, logout (manual and automatic), incorrect login, incorrect password, user blocked after a predefined number of consecutive login attempts with an incorrect password, password change by the user. Users are prompted to log out when they leave their workstation. The system triggers a screen saver after a defined period of inactivity. It is necessary to re-encode

	the password to reactivate the session. After a long period of inactivity, the session is automatically closed. The principle is extended to logical access to information.

Comments :
The IS offers a user profile management system that makes it possible to define access, addition, modification, archiving, masking and deletion rights, etc., by application, by module and by document. This approach makes it possible to clarify the responsibility and access of system users. Each document is associated with one or more profiles, which guarantees the appropriate confidentiality of the data.

User management managed by AdminSec and Epic is based on an ORBAC approach:

- Based on the user groups, the authorizations and authorization levels are defined in the Adminsec user management.
- The individual users and their assignment to user groups are defined in the AdminSec user management. This information is then passed via interfaces to Epic to create the user with the appropriate profile.

This meets the following requirements for access security:

- Centralized user management (creation, deactivation, blocking, unblocking, group assignment) by the administrator in conjunction with Payroll
- Unique user ID/password combination
- Passwords are encrypted in the database
- Definition of access rights for groups and users
- Access dependent on site area and authorization levels
- Password validity management: the user is forced to change his password after a definable period of time and the password can only be reused after n generations
- The system forces the user to define a new password the first time he/she logs in (initial password)
- The user is automatically locked out after a definable number of failed login attempts and can only be unlocked by the administrator
- Automatic disconnection after a definable period of time during which no action is taken on the keyboard or mouse
- An end date for the validity of a user profile can be defined, especially for employees with fixed-term contracts

In addition, the IS has logging functions for actions related to access security such as login, logout (manual and automatic), incorrect login, incorrect password, user blocked after a predefined number of consecutive login attempts with an incorrect password, password change by the user.

1.3.3. Point 03 : Audit trail

Specification	
11.10(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	IS has secured audit-trail, which cannot be modified by a user. Changes made during production are added to the audit trail by the system itself and include timestamp information, user ID, old and new value and comment. The logs can be generated, viewed or exported for any audit.

Comments
All critical data changes are tracked (user + date/time of modification):

- Validation of a workflow step (logging, upload, consultation)
- Execution, verification of an action
- Creation, modification of an event
- Event effectiveness check
- Audit, audit report, audit plan approval
- Creation, archiving, verification, approval and publication of documents
- Document versioning management
- Traceability of the consultation of published documents
- Traceability of document printing

These records are in fact secured by the system itself. Each user session is recorded in the system and standard reports allow to visualize all the actions performed during these sessions.

Changes made in the context of user management (such as defining new users, blocking users, etc.) are recorded by the AdminSec audit trail.

The following section describes how the Epic system supports the practical implementation of 21 CFR Part 11 requirements for the audit trail during runtime operations. This section also presents the tools that the system provides to the user for tracing changes in the engineering system.

Access to Epic is allowed only to properly identified and authenticated individuals.

Process data (e.g. process values, process alarms, or control messages) are saved without the user being able to make changes.
The relevant changes made by the user during the execution of his operations in the process visualization system are recorded in an audit trail.

The sole purpose of user access is for the server to generate events relating to the files: creation, opening, approval/disapproval, revocation. These events are linked to the medical records as well as stored on the Epic audit trail.

Each event linked to a file and/or a document carries the identification of the user who generated this event.

The metadata concerning the life cycle of a file and/or document cannot be modified. Each recorded event is accompanied by a time stamp and the electronic signature of the process and the authenticated user.

The transmission of documents to the archive is automatic and transparent to the user. This upload is done under the control of the upload server, which then creates an archiving event, which is recorded in the file and listed in the server's database where the document can be viewed and retrieved.

The archiving system uses its own databases, each alteration (insertion, modification, deletion) of data is successively traced in a log file and includes the time stamp of the operation, the identity of the user responsible for the operation, the operation performed with his data. The data in this log file are never modified: the data are accumulated (versioning).

1.3.4. Point 04 : Operational Control

Specification	
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Controls are established to ensure that the system's date and time are correct. Dates and times of systems are synchronized to the date and time provided by international standard-setting agencies (Begian agency). In addition to internal safeguards built into a computerized system, external safeguards are put in place to ensure that access to the computerized system and to the data is restricted to authorized personnel. Procedures and controls are 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 are implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on information data and software. Backup and recovery procedures are designed to protect against data loss. Alternative storage exists in a separate building from the original records.
11.10(j) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	A signature workflow, a transaction conditioned on a batch status, bring an assurance of confidence in the use of a computerized system. For the validation of the source of data, the presence of the card is necessary. The signature is effective only if the user give his password.

1.3.5. Point 05 : Education and training

Specification	
11.10(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Users have the education, training and experience necessary to perform their assigned tasks. Specific trainings are provided to users in specific upgrades or operations by qualified employee.
11.10(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	All users sign a confidentiality policy and a good practices code in usage of the computing tools.

1.3.6. Point 06 : Documentation management

Specification	
11.10(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The integrity of the data and the integrity of the protocols are maintained when making changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement. Previously specific changes are validated in test and validate environment. All changes to the system are documented.

1.3.7. Point 07 : Electronic signature

Specification	
Digital signature means an electronic signature based upon crytographic methods of originator authentification, computed by using a set of rules and a set of parameters such that the identify of the signer and the integrity of the data can be verified.	Digital signatures are used. Electronic records contains the following related information - User ID of the signer - date and time of signing - a meaning status of the signing (approval, review,...) The above information is shown on displayed and printed copies. The electronic signature is unique to an individual. The identity of any user is verified before electronic signature etablishment. Individual logins in addition of password is used for signature process.

1.3.8. Point 08 : Closed / Open System

Specification	
Closed or Open System. Additionnal procedures and controls shall be included	The system is considered as a closed system. Only the accredited persons have access to computed systems. Procedures and processes guarantee the preservation and the appropriate use of the mechanisms of access to the data and signature of documents.

Glossary

Audit trail
An audit trail is a process that captures details such as additions, deletions, or alterations of information in an electronic record without obliterating the original record. An audit trail facilitates the reconstruction of the course of such details relating to the electronic record.

Biometrics
Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

Certified Copy
A certified copy is a copy of original information that has been verified, as indicated by a dated signature, as an exact copy having all of the same attributes and information as the original.

Computerized System
A computerized system includes computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information.

Direct Entry

Direct entry is recording data where an electronic record is the original means of capturing the data. Examples are the keying by an individual of original observations into a system, or automatic recording by the system of the output of a balance that measures subject’s body weight.

Electronic record
Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Folder
Electronic Folder means a computer data compilation of any symbol or series of symbols created, modified, maintained, archived, backuped or distributed by a computer system.

Electronic signature
Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Handwritten signature
Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

Digital signature
Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Original data:
Original data are the values that represent the first recording of study data. FDA is allowing original documents and the original data recorded on those documents to be replaced by copies provided the copies are identical and have been verified as such (see FDA Compliance Policy Guide # 7150.13).

Source Document
Source Documents: Original documents and records including, but not limited to, 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 and complete, 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.

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

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

Transmit
Transmit is to transfer data within or among clinical study sites, contract research organizations, data management centers, sponsors, or to FDA.