ELECTRONIC SYSTEM VALIDATION

SYSTEM: INTERNET

How does the site access the Internet?	LAN / WAN
Is there a proxy server?	Yes HTTP – Port : 8080
Does the proxy server use proxy authorization?	Yes
Do you have a firewall?	Yes
Does the system have a virus detection / protection program?	Yes
Will your internet access allow the site monitor to go online using their laptop?	No
If satellite sites are used, how do satellite sites access the system?	Through a Citrix gateway or secured VPN

SYSTEM : ELECTRONIC MEDICAL RECORDING AND MAINTENANCE

System name	Epic Hyperspace
System version	November 2022
System description	EPIC EMR
System validation	EPIC is certified by the Office for the National Coordinator for Health Information Technology (ONC)
Validation documentation	Available
Department using the system	Nearly all departments (medical, paramedical, nursing, pharmacy, laboratories, medico-technic and administrative)
EMR system administrator	P. Colin
Who is the system owner?	Hospital IT department

Specification data capture: is the medical record recorded on paper, in an electronic system or a combination of both?	Predominantly electronic system. Some scanned docs.
What kind of electronic medical record system is it for?	EPIC Entreprise
What processes are in place should there be a failure of the electronic medical record system? - backup medium - backup frequency - storage	Business Continuity Access system (read-only version). backup : disk frequency : 1/day storage : on-site/ secure dual location
Is the data in the system regularly backed up in case of system failure or loss of data?	Yes
Has the restoration of data been tested?	Yes
In case of EMR software updates, is there a process to verify that this update will not have a negative impact on the data in the system?	Yes, the release process includes at least testing in 3 environment before PRD (REL, POC, TST)
How are modifications and system updates handled/validated?	Following Epic release-to-production procedure
How are problems concerning the electronic medical systems such as system failure solved and documented?	Incidents in ITIL tracking system, created and documented
Is there someone at the site who maintains the computers and/or the computer network?	Yes - Contact name : Pierre Colin - Contact phone : +32 – 2 –7642318 - Contact email : Pierre.Colin@saintluc.uclouvain.be

ELECTRONIC MEDICAL USER ACCESS & SECURITY

Do you have a written procedure for management of EMRs/eSource including for account creation and management for electronic records systems?	Yes
Are users required to complete training before providing access to the EMR/eSource system?	Yes
Is there a record of the names of authorized personnel, their titles and their access privileges?	Yes

Is access to the electronic medical record system restricted to staff by unique identifiable login and password?	Yes Limiting system access to authorized individuals. Orbac approach – individual account – specific rules for logical access control We have a user account management process for create, manage and revoke user account. 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
Is the system protected from unauthorized access?	Yes
Are uses IDs **and** passwords required to access the system?	Yes
Are the passwords kept confidential?	Yes
Do passwords periodically expire, requiring use of a new password?	Yes
Which password protections are in place (alpha/numeric letters, minimum length, password expiration, limited log-in attempts)?	Password must be changed at least after 6 months, locks user account after several failed logs in attempts. Complexity and lengths of the passwords has been adapted in 2023. Recommendations to users : 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.
Are there any procedures or consequences when misuse of the login and/or password is established?	Yes. Possible reactivation after analyse by the Access Management board.
Is there an automatic log off to protect the workstation during periods of inactivity?	Yes
Locks the computer after several failed attempts?	Yes
Is the electronic medical record system protected from modifications by users?	Yes
Is access to certain system functions controlled based upon the user's role? (read, write, change, delete)	Yes

ELECTRONIC MEDICAL RECORDING AND ACCESS TO THE DATA

Are electronic signatures used in the system?	Yes
Are electronic signatures protected from editing (cutting/pasting)?	No
When signed record is altered is the signature made invalid and replaced?	Yes
Are electronic signatures protected from intentional or unintentional misuse?	Yes
Does the electronic record identify? - The person who first observed the data? - The person who entered the data in the system? - The person who attested that the data is correct?	 No Yes Yes
Is the signature supported by an encrypted digital or electronic certificate that allows verification of its authenticity by others who might use or receive the record? (e.g. Public/Private Key Encryption)	No cryptographic signature in EPIC
Does any printed or electronic copy of a signed record include all the elements of the signature and audit trail?	Yes
Is there a way to easily identify data that has been changed? (e.g. Flag, different colour on the screen...)	Yes
Is there an **audit-trail** of all changes made to electronic medical record system that maintain a record of?	Yes

- the original data	Yes
- the changed data	Yes
- who made the change	Yes
- the reason for the change	No (depends on the data type). A comment section is available to document and explain the encoded data that are changed.
- who approved the change	Yes
- date (YMD) and time (HM) of any change	Yes
- do users have direct access to the audit trail?	Yes, partially
- Is it possible to retrieve data about the read history of system users?	Yes
- How is audit trail generated?	By the system
- Can the audit trail be edited or turned off?	No
- Is the electronic audit trail secure?	Yes
- Will the audit trail be retained as long as the electronic record is required to be stored?	Yes
- Can audit trail be printed completely ?	Yes
If an admin support/study nurse/study coordinator enters data for an investigator, is the data reviewed/validated by the investigator?	Yes
If yes, is the investigators' review/validation documented in the system?	Yes
Can data be printed completely?	Yes
Are copies of the EMR certified with name, date and signature?	Yes

ELECTRONIC MEDICAL RECORDING: DATA CONTROL BY MONITORS

How will the monitor verify source data?	The monitor will be given a separate ID/password to review electronic medical records at a computer terminal
Will the password used by the monitor give him/her read-only access?	Yes
Will the password used by the monitor give him/her only access to the electronic medical records of the patients included in the trial?	Yes
Could an audit trail be provided to confirm only records of study specific subjects have been accessed by Site Monitor?	Yes
Do passwords periodically expire, requiring use of a new password?	Access valid for a period of 1 year.
Is there a relevant site SOP about access for monitors?	Yes
Should the monitor complete/sign a document for EMR access?	Yes
Does the EMR system include scanned original paper document? Is the scanning and uploading of paper originals completed using a formalised, documented procedure, including as a minimum the following requirements: - Scanned documents are certified as copies through QC checks that verify scan quality, legibility, completeness, page counts, etc. - Copies are maintained chronologically, legibly (including maintaining colour coding) and in a searchable format. - There is supporting documentation that includes what documents were transferred, when and how the scanning took place and by whom (i.e. metadata)	Yes Yes
Can these paper documents be accessed by the monitor for verification? If no, can a copy of the relevant site SOP be made available to the monitor?	No. Original records are destroyed Yes
How does a monitor know when a document has been changed in the EMR?	There is an audit-trail of all changes made to electronic medical record system generated by the system. It is possible to retrieve data about the read history of system users.
Will the audit trail be accessible to monitors and auditors/inspectors in a readable format?	Yes

ELECTRONIC MEDICAL RECORDING : ARCHIVING OF THE DATA

Does the site have a data storage/archival policy for the electronic medical record system?	Yes
Duration of data storage?	30 years
Can archived electronic medical records be retrieved for a regulatory inspection?	Yes

ELECTRONIC MEDICAL RECORDING : PROCEDURES AND TRAINING

Do the site employees of the hospital receive training concerning the electronic system?	Yes
Is the training documented?	Yes – could be provided upon request to auditors who have an agreement with EPIC to view IP protected information
Does the site have an up to date statement/declaration concerning the retaining of personal information?	Yes, for all users (internal and external)
Does the site have written SOPs for software installation, qualification and quality control?	Yes - could be provided upon request to auditors who have an agreement with EPIC to view IP protected information
Does the site have written SOPs for data handling?	No
Does the CRA receive training when logging-in for the first time?	Yes. A training guide is available in the system, in French and English. CRA access and read this guide at the first log-in. After reading the guide, the CRA signs a training certificate (also available in the system) that is kept on TMF.