**ELECTRONIC SYSTEM VALIDATION: 06 OCTOBER 2020**

**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 |
| System version | 2020 |
| System description | EPIC EMR |
| System validation | EPIC is ONC certified |
| Validation documentation | Available – ONC certified |
| Department using the system | Nearly all medical, paramedical, nursing and administrative |
| EMR system administrator | J. Rossler |
| 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 Continuty Access system (read-only version).  backup : disk  requency : 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 |
| 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 : Olivier Jeuniau * Contact phone :  +32 – 2 –7642460 * Contact email : olivier.jeuniau@uclouvain.be |

**ELECTRONIC MEDICAL RECORDING AND ACCESS TO THE DATA**

|  |  |
| --- | --- |
| 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 serveral 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 |
| Are there any procedures or consequences when misuse of the login and/or password is established? | Yes. Possible reactivation after analyze 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 |
| 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 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?   * the original data * the changed data * who made the change * the reason for the change * who approved the change * date (YMD) and time (HM) of any change * do users have direct access to the audit trail? * Is it possible to retrieve data about the read history of system users? * How is audit trail generated? * Can the audit trail be edited or turned off? * Is the electronic audit trail secure? * Will the audit trail be retained as long as the electronic record is required to be stored? | Yes  Yes  Yes  No  No (depends on the data type)  Yes  Yes, partially  Yes  By the system  No  Yes  Yes |
| If an admin support/study nurse/study coordinator enters data for an investigator, is the data reviewed/validated by the investigator?  If yes, is the investigators’ review/validation documented in the system? | Yes  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 |
| Do passwords periodically expire, requiring use of a new password? | Access valid for a period of 1 year. |
| Does the EMR system include scanned original paper document?  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? | Yes  No  Yes |
| 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? | If the service asks, it can be done. |