EMR assesment risk _ Orbis V 8.5.22

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

INTRODUCTION

Afin de faciliter le remplissage des EMRQ nécessaire pour la recherche clinique, ce document procurera un questionnaire type de l'APHP concernant le DPI ORBIS.

Electronic Medical Records Questionnaire (EMRQ)

Details of the Site Representative providing EMRQ Responses:	- **APHP**
Name of the EMR/Electronic Data System	- **ORBIS 8.5.22**

Questionnaire

This questionnaire applies to an electronic (computerized) system used for collecting and storing Electronic Medical Records (EMR, also known as Electronic Health Record (EHR)) in clinical investigations. For the purpose of this questionnaire, an EMR may include patient's medical history, diagnoses, treatment plans, progress notes, letters to patients, immunization dates, allergies, radiology images, pharmacy records and laboratory and test results. This data may be entered manually or collected electronically and may subsequently be transcribed to a paper Case Report Form (CRF) or transferred to an Electronic Data Capture (EDC) system e.g. Sponsor eCRF.

An EMRQ must be completed for each EMR system used at the site, which hold study specific data.

Please note that this assessment of the investigator site's EMR system is a critical component of assessing source documentation systems for the conduct of clinical trials and determining compliance with ALCOA plus (CCEA) principles (i.e. Attributable, Legible, Contemporaneous, Original, Accurate; and Complete, Consistent, Enduring, Available) and any other local regulations. Completion of this EMRQ is necessary to support site selection or on-going study participation.

EMR/Electronic Data System and Training	YES	NO
Provide the below information on EMR/electronic data system:		
EMR/electronic data system Manufacturer : **Dedalus**		
EMR/electronic data System Model Number / Name : **ORBIS**		
EMR/electronic data System Version Number : **08052200.06000.FR**		

1. Is the EMR/electronic data system certified by the ONC (the Office of the National Coordinator for Health Information Technology, US sites) or any authorized body (non-US sites)?	☐	☒
2. Do you confirm that the EMR/electronic data system is compliant with all requirements as defined in ICH GCP E6 (R2) Section 4.9 and any applicable national or regional standards / regulations?	☒	☐
3. Is there a site/institution or departmental description of system and procedure that addresses the use of an EMR/electronic data system (including training) and site source data collection? (Site Monitor or SMA will request a copy for review)	☒	☐
4. Are all users (internal site employees and external people e.g. Site Monitors) trained on using the EMR/electronic data system, if applicable?	☒	☐
Access and Controls	**YES**	**NO**
5. Are the following controls in place to limit access to the EMR/electronic data system? [Check all that apply]		
a. Unique individual user accounts (User Identification [UID] & password)	☒	☐
b. Site processes do not allow sharing of User Identification (UID) / password to access the system	☒	☐
c. Locks user account after several failed log in attempts	☒	☐
d. Automatically log off user after an idle period	☒	☐
e. System access is granted based on segregation of duties and responsibilities, Least-privilege rules applied (i.e. users should have the fewest privileges and access rights for them to undertake their required duties for as short a time as necessary.	☒	☐
f. Overview of current and previous access, roles and permissions available	☒	☐
g. Access no longer required or no longer permitted is removed	☒	☐
h. Is procedure for password policies implemented (length, complexity, expiry, login attempts, and logout reset)?	☒	☐
6. Will external reviewers e.g. Site Monitors, Regulatory Inspectors (such as FDA, EMA) or auditors, be provided with restricted access to the trial participants only (i.e. subjects who signed an informed consent form for the clinical trial being monitored)?	☐	☒
If yes, external reviewers will be provided direct, restricted access via read-only guest user accounts including full access to source data and audit trails for trial participants only.		
If no, how do these reviewers review/verify electronic source data in the system?		
• **No access:** Certified copies will be provided.	☐	☒
○ If certified copies are provided, will Site Monitor be allowed to do interval comparison of EMR/electronic data to certified copies of source data?	☐	☒
• **Indirect access:** Over the shoulder review of study staff. Study staff will use their own user account. Please note person must remain with the Site Monitor during the visit and be navigating the EMR/electronic data system.	☐	☒
• **Unrestricted read-only access:** Site Monitor required to sign a Confidentiality Disclosure Agreement (CDA).	☒	☐
• **Other, please specify:** Site monitor has access to the list of patients included in all the clinical trial of the site.		
6.1 Remote Access: Will Site Monitors be permitted to access the EMR/electronic data remotely (off-site)? • When remotely connecting to systems over the internet, a secure and encrypted protocol (virtual private network (VPN) and/or hypertext transfer protocol secure (HTTPS)) should be used.	☐	☒
If yes, will Site Monitors be provided with direct, restricted access via read-only guest user accounts including full access to source data and audit trails for trial participants only?	☐	☐

If no, please specify below the reason why remote EMR/electronic data access can not be provided. Remote connection for Site monitors is not allowed by CNIL in france		
Audit Trail	**YES**	**NO**
7. Is the creation, deletion and modification of electronic source data tracked in a secure, computer generated audit trail?	☒	☐
If yes:		
• Is the following information included in the audit trail or a feature of the audit trail to ensure that changes to the data are traceable?		
○ Date and time of operator (user) action (timestamp)	☒	☐
○ User Identification (UID) / name who performed the action	☒	☐
○ If modified, data before the change and data after the change	☒	☐
○ Reason for change (where applicable)	☐	☒
○ It should not be possible for normal users to deactivate the audit trail (protected against change, deletion and access modification)	☒	☐
○ The audit trail should be stored within the system	☒	☐
○ The audit trail should be visible at data point level	☒	☐
○ Possible to export the audit trail in dynamic data file	☒	☐
○ A procedure should be in place to address the situation when a data originator wants to correct incorrectly recorded data	☒	☐
• Can a Site Monitor, Regulatory Inspector or Auditor view the audit trail in a human readable format (i.e. is the information within the audit trail visible for review so that the person making the change can be identified)?	☒	☐
○ If yes, Site Monitor should request to see the audit trail documentation in order to assess what would be available to the Site Monitor, Regulatory Inspector or Auditor.	☒	☐
• Is audit trail linked to the associated record?	☒	☐
7.1 Can site staff view in real time which trial participants' records are reviewed by the Site Monitor?	☐	☒
If no, is process in place to manage non-trial participants' potential confidentiality breach?	☒	☐
Protection, Storage, Security and Archiving	**YES**	**NO**
8. Can accurate and complete copies of electronic source data be generated from the system?	☒	☐
9. Are any paper source data scanned and original source not retained?	☒	☐
If yes, do you have a process to generate and verify certified copies?	☐	☒

If yes, how do you verify that the scanned copy is a certified copy? Please specify the method below:		
• Manual verification	☒	☐
• Validated automatic electronic method	☐	☒
• **Other, please specify:** _____		
10. Are any records transcribed from audio/video files or other media into EMR/electronic data system?	☐	☒

If yes, is documented process available outlining how data transcribed from audio/video source is verified and certified for accuracy and integrity?	☐	☐
11. Do you have a contingency plan in place?	☒	☐
If yes, please specify:		
• Making data back up at an appropriate frequency	☒	☐
• Disaster recovery plans	☒	☐
• Emergency mode operations	☒	☐
12. After the trial is closed, are electronic source data, metadata and the audit trail archived in a secure manner available for human readable and restorable access during the records retention period (please refer to ICH GCP E6 (R2) 4.9.5 and local regulation related to records retention).	☐	☒
13. Is there any other information relating to your EMR/electronic data system that you believe the clinical trial sponsor should be made aware of?	☐	☒
14. Are there appropriate physical security measures in place for your computerised system, servers, communication infrastructure and media containing clinical trial data?	☒	☐
If yes, please specify:		
a. Is physical security set up for your computerised system, servers to include:	☒	☐
o Is physical access limited to the necessary minimum?	☒	☐
o Is risk of flooding minimized?	☒	☐
o Is there pest control?	☒	☐
o Is there fire protection?	☒	☐
b. Is a firewall set up?	☒	☐
c. Is use of bi-directional devices (e.g. USB devices) controlled?	☒	☐
d. Is anti-virus software installed, activated and security patches applied?	☒	☐
e. Is intrusion detection and prevention system implemented as well as penetration testing conducted in regular intervals?	☒	☐
f. Is a system for monitoring internal activity implemented (i.e. to detect unusual or risky user activities)?	☒	☐

Approvals

I have completed and/or reviewed the above questionnaire and to the best of my knowledge attest that the information provided is an accurate and true summary of the compliance of the Electronic Medical Record / Electronic data system and procedures that will be used in the conduct of the clinical trial.

Signataires

Didier PERRET *Responsable Sécurité du Système d'Information APHP (RSSI)*	Quentin DEMANET *Direction de la Recherche Clinique et de l'Innovation APHP (DRCI)*
ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS c=FR, st=Paris (75), o=AP-HP, ou=1750712184, title=Personnel santé ou social, sn=PERRET, givenName=DIDIER, cn=3750712184/4024242 2025.10.06 15:00:29 +02'00'