**Remote access, Monitor & Auditor Declaration Form**

ICH GCP requires and the principles of GCP expect direct access to trial participant medical/health records for the sponsor representatives. Remote direct access to the medical/health records of clinical trial participants allows source data review and source data verification to occur without the Monitor or Auditor having to visit the investigator site/institution.

It is understood that there are additional risks to privacy of participants when remote monitoring is undertaken. Therefore, all members of the RGIT who undertake monitoring and auditing using remote EHR access are required to read and sign the following document. Members of the RGIT should also ensure that they are up to date with all appropriate training, and have an understanding of the College process and definitions of a data breach: [Imperial College - Reporting data breaches](https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/data-breaches/).

When involved in remote monitoring or auditing the following should be undertaken with us as sponsor:

1. No documentation should be downloaded, printed or retained from the EHR.
2. Remote login in access to an EHR system at UK sites should only be undertaken from a physical location in the UK
3. The device through which remote login access to the EHR system is used should be provided by the sponsor (personal laptops should not be used). Devices must not be left unattended and accessible when logged in to the EHR system.
4. EHR should not be accessed in an open plan office without suitable privacy.
5. The EHR systems should not be access in a public space, or locations where there is a high risk that others could view sensitive information.
6. Login access is acceptable from home but should be done privately.
7. If the device is left unattended then the monitor/auditor, should ensure they are logged out of the EHR, and not just lock the device.
8. There should be no recording of any video calls where there is screen sharing of guided direct access of the EHR or when paper source documentation is taking place.
9. There must be no records of any trial participant information in any of the chat functions of the remote video calling system.
10. It is not permitted to take photographs of information displayed on the device, take screen shots, print or download from the EHR, or document any information that identifies a trial participant (including via email).
11. If the monitor/auditor needs to document any information from the medical records as necessary to record monitoring and audit activity then this can take place, but it should be ensured that the participant is only identified by their trial identification number.
12. User accounts and login information for any EHR should not be shared with any other persons.
13. The monitor/auditor should not share content of the EHR with any other persons. If this is required then it should be undertaken by the site.
14. The site should be informed as soon as the user of account of the monitor or auditor is no longer required.
15. All staff should undertake the College data protection training course and be aware of their responsibilities when dealing with participant data.
16. If a data breach occurs then the College Data Protection Office should be contacted as soon as possible (within 72 hours) using the Notification of Data Security Breach Form sent to [365-dataprotectionoffice@groups.imperial.ac.uk](mailto:365-dataprotectionoffice@groups.imperial.ac.uk) and the site informed as per their R&D contact details.

I have read and understood the above guidance

Signed…………………………..