Protocolo de seguridad de la conexión remota para el entorno de monitorización de ensayos clínicos

Este documento define los controles de seguridad que deben seguirse, para la monitorización remota y autónoma de ensayos clínicos por los monitores de los promotores o CRO, con el fin de permitir el seguimiento y supervisión de los ensayos fuera del Centro del estudio en las actuales circunstancias excepcionales derivadas de la pandemia generada por el COVID19.

Las configuraciones propuestas, tienen como objetivo ofrecer al monitor la posibilidad de realizar la verificación de datos de manera remota, de forma análoga a las actividades que podría realizar presencialmente, a la vez que garantizar la máxima calidad e integridad de los datos de los pacientes del ensayo.

El alcance incluye la revisión de los datos en el Cuaderno de Recogida de Datos, historia médica electrónica y resto de documentos fuente que no están en la historia como las hojas de enfermería, tablas de farmacia, etc. Se asume que toda esta información estará disponible en formato digital.

1. Requerimientos de Administración de Acceso para un monitor

- El Monitor solicitará una cuenta de acceso a la Organización, donde resida el sistema de gestión de datos de pacientes, para la realización del ensayo clínico que cada Centro designe.
- El Monitor firmará y remitirá a dicha Organización el "Acuerdo de confidencialidad", que incluye la prohibición de descargar, imprimir, fotografiar o capturar (por cualquier) medio la información confidencial a la que se le va a dar acceso.
- Una vez otorgada la autorización por el responsable que administre el sistema de gestión de datos de pacientes de la Organización designado por cada Centro, se podrá realizar el acceso conforme al protocolo siguiente:
    - El departamento de IT de la Organización creará la cuenta.
    - Se proporcionará usuario y contraseña, al que se recomienda añadir autenticación de doble factor (2FA). Si la autenticación se realiza mediante aplicativo móvil, el dato del número deberá estar en posesión de la organización previamente al proceso de autenticación.
    - Los requisitos de contraseña para el sistema de gestión de datos de pacientes deberán cumplir con los estándares de complejidad de la industria: se recomienda una longitud mayor de 7 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
    - La cuenta deberá otorgar al monitor acceso únicamente de lectura sobre la información requerida del paciente participante en ese ensayo, dentro del sistema de gestión de datos de pacientes.
    - Se define el tiempo (fecha de comienzo/fin) que la cuenta del monitor estará activa para acceder al sistema. Este proceso se rige por una política aprobada por la Organización.
    - El monitor se conecta en el entorno web mediante su navegador habitual.
    - No se podrá acceder al sistema de gestión de datos de pacientes, a través de conexiones NO cifradas.

2. Arquitectura y Conexión propuesta:

- Infraestructura/software a través del portal seguro vía servicios **Citrix** (on Premise), en "Cloud" o equivalente.
- Deberá asegurar que el monitor remoto acceda a la Organización mediante una conexión **https** y **servicios de autenticación fuerte** y por el otro lado se establecerá una conexión segura Cloud-Servicios corporativos mediante una máquina "Conector".
- La solución deberá de poder manejar conectividad remota con PCs y otros dispositivos móviles como IPads.

3. Cifrado:

- Ha de garantizarse la confidencialidad e integridad de los información tratada, tanto almacenada en los sistemas de gestión de información, como en tránsito por la red, por lo que deberá recurrirse a mecanismos de cifrado:
  - Información "**en la línea de transmisión**" mediante cifrado basado en certificados TLS 1.2 o superior.

4. Gestión de "Logs" y auditoría:

El centro ha de disponer de gestión de logs y auditoría:

- Deberá posibilitar la revisión periódica de usuarios, para asegurar que estén configuradas al nivel de privilegio adecuado y activas las cuentas que deban estarlo (eliminando el personal que haya causado baja y su cuenta siga activa). La periodicidad dependerá de cada Organización.
- Las interacciones del usuario con el sistema de gestión de datos de pacientes se deberán registrar y almacenar en un entorno seguro durante 5 años.
- Los registros de anotaciones deberán incluir suficiente información para rastrear la actividad de un individuo / usuario con una marca de tiempo, incluyendo accesos, modificaciones, inserciones y búsquedas realizadas.
- El sistema de gestión de datos de pacientes deberá proporcionar una pista de auditoría completa de la navegación que realiza la cuenta del monitor, ya que no se permitirá realizar cambios en el registro de los pacientes.
- Antes del inicio de las actividades de monitorización se deberá realizar una auditoría previa de la adecuación de los sistemas de todos los intervinientes. Esta auditoría se ha de realizar con periodicidad de al menos un mes o cuando surja algún incidente.

5. Gestión de vulnerabilidades:

- El sistema de gestión de datos de pacientes deberá estar desarrollado utilizando estándares de codificación seguros y estar protegido contra ataques de aplicaciones web.

6. Requerimientos del Monitor:

- **Equipo:** El equipo proporcionado por el Promotor al monitor deberá reunir medidas de seguridad y protección frente a ataques externos:
  - El disco duro deberá estar cifrado.
  - Deberá tener instalado, operativo y adecuadamente configurado un sistema antivirus que actualizará las firmas diariamente.
  - Deberá tener instalado un firewall correctamente configurado de acuerdo a la política de seguridad definida por el promotor.
  - Deberá tener instaladas las últimas actualizaciones del sistema operativo.
  - Deberá manejar las políticas de IT del promotor/CRO.
  - El acceso deberá estar protegido por contraseña o patrón de desbloqueo robusto.
  - Deberá ser un equipo dedicado utilizado en exclusiva para las tareas de ensayo realizadas por cuenta de los promotores.
  - Todos los servicios e interfaces de conexión que no sean necesarios deberán estar deshabilitados.
  - El perfil de trabajo configurado en los equipos para los usuarios monitores carecerá de privilegios de administración.
- **Personal:** Cada monitor utilizará el equipo (PC y/o IPad) que le haya facilitado el propio **promotor/CRO**. El monitor deberá:
  - Evitar instalar y utilizar aplicaciones que no hayan sido formalmente aprobadas por el promotor.
  - Revisar y eliminar periódicamente la información residual que pueda haber quedado almacenada en el dispositivo, como archivos temporales o documentos descargados.
  - Finalizados los trabajos de ensayo sobre los sistemas de gestión de datos del paciente de la Organización, debe procederse al cierre de la sesión contra el servidor de acceso remoto
  - Se deberá comprobar a priori la conectividad del equipo con la URL de la Organización: revisar si el Puerto de Acceso que proporciona la Organización pueda crear un problema en la red del **promotor/CRO, y que se tenga que manejar una excepción para que la URL** pase los firewalls del **promotor/CRO**.

Importante

- La solución ofrecida por la Organización **no permitirá instalar ningún componente** de software en el equipo del monitor proporcionado por el promotor/CRO.
- Se sugiere a la Organización no haga cambios sin previo aviso al **promotor/CRO** y mantener activos los puertos estándares para recibir llamadas desde el exterior.

- **Entorno de Trabajo:**
  - El lugar de trabajo deberá reunir unas condiciones mínimas de privacidad, como en un recinto de acceso limitado (casa), evitando que otras personas puedan tener acceso.
  - Si fuera preciso trabajar desde espacios de acceso público, se adoptarán medidas de protección adicionales para preservar la confidencialidad de la información tratada como el uso de filtros de privacidad en las pantallas de los dispositivos.
  - Ha de evitarse trabajar con información en soporte papel y nunca proceder a su eliminación sin el empleo de mecanismos seguros (destructora de papel)
  -
  - Se deberá trabajar desde redes cifradas, nunca desde redes wifi gratuitas y/o libres.
  - Ante cualquier anomalía que pueda afectar a la seguridad de la información y la protección de los datos tratados el monitor debe comunicarlo al punto de contacto establecido en la Organización