CATALIS
RECHERCHE CLINIQUE QUÉBEC

Surveillance à distance des données
Document d'orientation

Version 15 octobre 2021

Table of Contents

1. Contexte

La crise pandémique a créé des difficultés d'accès aux installations, rendant beaucoup plus complexe la réalisation d'activités de surveillance à distance dans le cadre d'essais cliniques.

Afin de faciliter la mise en œuvre de solutions, CATALIS Québec a coordonné la mise en œuvre d'un guide des **meilleures pratiques pour la surveillance à distance des données** dans les établissements de santé et de services sociaux.

2. Objectif

L'objectif de ce document est de fournir des lignes directrices en matière de solutions de rechange et de recommandations pour la planification, la mise en œuvre et l'exécution d'activités de surveillance à distance des données dans le cadre de la surveillance des processus et des livrables d'essais cliniques. Les aspects suivants de la surveillance à distance des données constituent l'objet de ce document

- Accès à distance aux dossiers médicaux électroniques
- Accès à distance aux documents sources en format papier (note : Veiller à ce que la numérisation des documents sources en format papier soient conformes aux bonnes pratiques de sécurité de l'information (environnement sécurisé et restreint), considérant le niveau de sensibilité des données)
- Processus de copie certifiée conforme
- Considérations générales relatives à la surveillance à distance des données

3. Introduction

Aux fins de ce document, le processus de surveillance à distance des données a été défini de manière à inclure six (6) phases majeures comme illustrées à la *figure 1* ci-dessous):

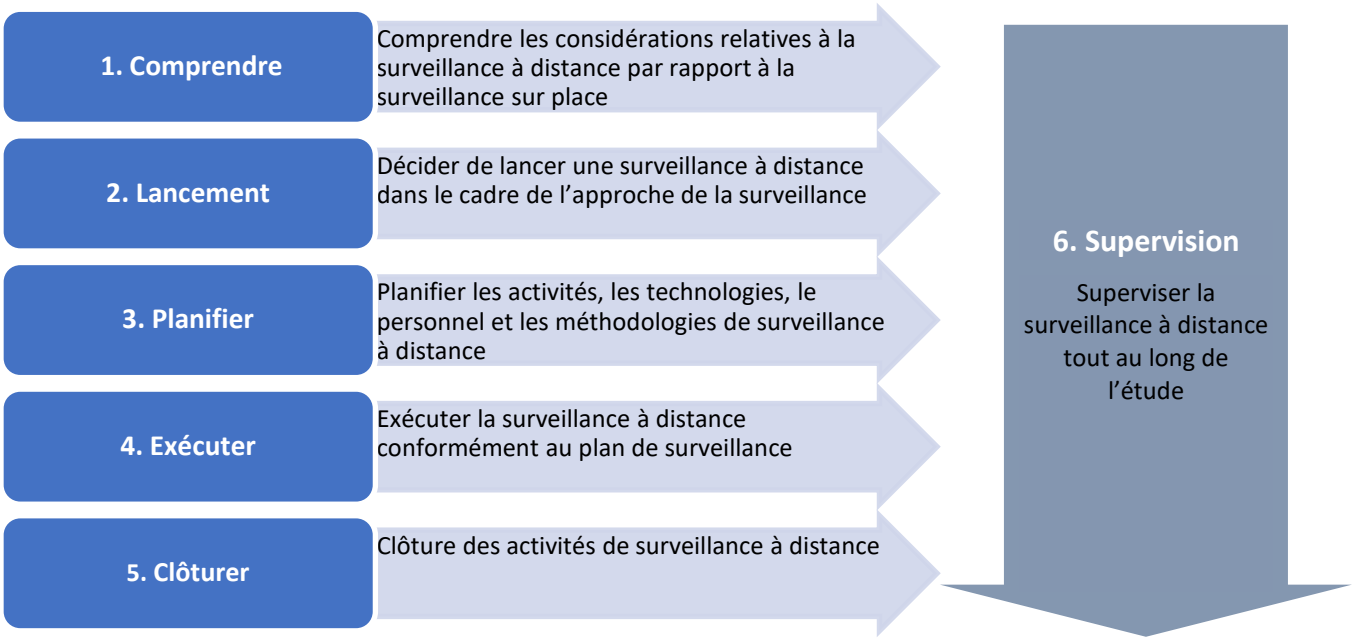

Figure 1. Aperçu du processus de surveillance à distance des données

4. Comprendre les considérations relatives à la surveillance à distance des données

Avant de commencer toute activité de surveillance à distance des données, les aspects suivants doivent être considérés et évalués pour s'assurer que ce type d'approche est viable et que les activités à distance demeureront conformes aux règlements et aux exigences de l'essai.

4.1 Exigences des intervenants de l'étude

Il faut consulter plusieurs parties prenantes clés et répondre à des besoins particuliers lors de la mise en œuvre de solutions de surveillance à distance des données, par exemple :

- L'approbation de l'**établissement** est-elle requise?
- L'approbation du **BCH** (bureau de certification et d'homologation du MSSS) est-elle requise?
- L'approbation du **représentant de la conformité/qualité** est-elle requise?
- Étant donné que chaque promoteur peut avoir des exigences différentes, quelles sont les exigences spécifiques du **promoteur**?
    - Type de systèmes de téléconférence acceptables
    - Exigences en matière d'anonymisation
    - Exigences en matière de certification
    - Exigences en matière de sécurité de l'information
    - Solutions de dossiers partagés
    - Peut nécessiter une nouvelle surveillance lors d'une visite de surveillance subséquente sur place

  Le promoteur est ultimement responsable de veiller à ce que toute autre méthode utilisée pour un EDS ou une VDS à distance réponde à la fois à la réglementation et à toute ligne directrice spécifique sur la COVID-19 émise par les autorités locales ou nationales concernant le travail et la surveillance à distance.
  Le promoteur peut envisager d'utiliser une approche standard pour évaluer l'adéquation de la surveillance à distance des données, comme demander à un centre de remplir un questionnaire de surveillance des risques à distance, puis acheminer pour approbation avant la visite, afin d'assurer une compréhension commune de l'approche de surveillance à distance des données.

- L'approbation du **responsable de la sécurité de l'information (RSI)** est-elle requise? Tenez compte notamment des éléments de sécurité suivants et des défis potentiels pour établir un accès au site et avec le moniteur en toute sécurité :
    - Utilisation du service F
    - Anonymisation
    - Gestion des identités et des accès, incluant la journalisation des accès
    - Sécurité de la solution de surveillance à distance des données
    - Destruction sécuritaire des informations inutiles
    - L'emplacement physique du demandeur d'accès
    - Sécurité du materiel informatique du demandeur d'accès (antivirus, wifi, etc.)

- L'approbation du **service des technologies de l'information (TI)** est-elle requise? Tenez compte des éléments de TI suivants et des défis potentiels pour établir un accès au site et avec le moniteur en toute sécurité :
    - Pare-feu pour l'établissement et le promoteur

- Installations de jetons ou d'applications
- Conflits avec d'autres programmes/applications de l'établissement et du promoteur
- Ordinateurs dédiés à la surveillance à distance des données afin de ne pas limiter les ordinateurs du coordonnateur de l'étude

- Si les travaux sont réalisés dans plusieurs **services**, peuvent-ils tous utiliser les solutions exactes au sein de l'établissement? Tenez compte des répercussions suivantes :
  - Charge de travail et ressources
  - Heure
  - Essais à venir
  - Limitations techniques

- Communiquez avec le **comité d'éthique de la recherche (CER)** pour déterminer les exigences suivantes :
  - Le CER doit-il être avisé? Et quand?
  - Est-il possible d'obtenir une approbation qui est générique et qui peut être utilisée pour tous les essais?
  - Le CER doit-il être avisé chaque fois qu'une visite de surveillance à distance des données a lieu?
  - Est-ce que le contenu du formulaire de consentement éclairé (FCE) autorise l'accès à distance aux dossiers médicaux des sujets?
  - Si le contenu du FCE limite l'accès aux dossiers médicaux au sein de l'établissement seulement, le FCE nécessite-t-il une mise à jour ou le consentement du sujet peut-il être obtenu verbalement?
  - Le FCE nécessite-t-il une mise à jour?
  - Votre CER exige-t-il toujours le consentement oral du sujet si le FCE autorise l'accès à distance, et quel est le processus de consentement oral?

  Remarque : Les clauses juridiques standard multicentriques du MSSS pour les formulaires d'information et de consentement destinés aux essais cliniques et publiés en 2021, ne limitent pas l'accès aux dossiers médicaux des sujets au sein de l'établissement seulement :

  - Pour la surveillance, le contrôle, la sûreté, la sécurité et l'approbation réglementaire d'un médicament à l'étude, votre dossier d'étude ainsi que vos dossiers médicaux pourraient être examinés par une personne mandatée par des organismes de réglementation canadiens ou internationaux, comme Santé Canada, ainsi que par des représentants autorisés du promoteur de l'étude, de l'établissement ou du comité d'éthique de la recherche. Toutes ces personnes et tous ces organismes auront accès à vos données personnelles, mais ils adhèrent à des ententes de confidentialité.

- Existe-t-il une entente de confidentialité signée par l'**associé de recherche clinique (ARC)**?
  - Si aucune entente de confidentialité n'est en place, est-ce toujours acceptable et est-ce que ça répond aux exigences légales?

- Si une entente de confidentialité est en place, doit-elle être mise à jour afin de tenir compte des aspects de surveillance à distance des données?

4.2 Conservation des dossiers

- Si des documents sources en format papier sont numérisés et surveillés par l'ARC, seront-ils archivés pendant 25 ans avec les autres documents de l'étude?
- Les documents numérisés ne comprendront-ils que des documents sources en format papier essentiel ou l'ensemble de ces documents?
  - Si oui, existe-t-il un processus écrit en place, vérifié et assorti d'une formation pour ceux qui exécutent le travail?
- Vaut-il la peine que les documents sources en format papier soient numérisés (c.-à-d. des copies certifiées conformes) par le service d'archivage et importés dans le DME, comme méthode potentielle pour assurer une conservation appropriée?
- À titre de mesure de précaution, l'ARC effectuera-t-il un examen des documents sources originaux une fois sur place pour confirmer que les documents sources précédemment surveillés ont été complétés (c.-à-d., l'ARC a surveillé tous les documents sources [BPC 4.9.0 de la CIH])? Le fait de s'assurer que des copies certifiées sont en place réduira la nécessité d'un tel examen de surveillance secondaire.

4.3 Documents sources censurés par rapport à ceux qui sont non censurés

- Il est recommandé d'utiliser des documents sources censurés uniquement en cas de circonstances exceptionnelles, car il pourrait ne pas être possible de confirmer la traçabilité des dossiers du sujet examiné. C'est-à-dire que le processus de surveillance des documents sources censurés pourrait nécessiter une vérification secondaire par le moniteur de la source non censurée, afin de démontrer la traçabilité.
- Lorsque vous utilisez des modèles de documents sources, envisagez de ne pas ajouter les renseignements personnels du sujet, n'incluez que le numéro de sélection ou de répartition aléatoire du sujet.
- Lorsque vous fournissez des documents sources censurés, il est fortement recommandé qu'un processus écrit sur la façon de censurer des documents soit en place.

4.4 Exigence en matière de confidentialité

- L'examen ou la vérification des données sources (EDS/VDS) à distance par un ARC doit être limité(e) à la consultation des dossiers des patients de l'essai du centre uniquement, afin de minimiser le risque de consulter les données d'autres patients.
- Les images de la source ne doivent pas être sauvegardées, enregistrées électroniquement, dupliquées ou imprimées par l'ARC. Les systèmes qui exigent que l'ARC télécharge des copies des documents sources (p. ex., systèmes de transfert de fichiers) ne doivent utiliser que des documents sources censurés, qui doivent être supprimés ou éliminés une fois que toutes les activités d'examen sont terminées. Les copies des documents sources fournis pour examen temporaire ne doivent être conservées dans un système que le temps nécessaire.
- Les appels de vidéoconférence provenant de zones publiques doivent être interdits, afin de minimiser le partage des données des patients avec du personnel non autorisé.
- Pour une solution de transfert de fichiers ou un dépôt de fichiers, tenez compte de l'emplacement des serveurs, des lois relatives à la protection de la vie privée suivies par les fournisseurs de services, de l'archivage, des sauvegardes, etc.

- Réfléchissez à la fréquence de rappel ou de formation de l'ARC sur le processus de déclaration en cas d'incident lié à la protection de la vie privée.
- Dans les situations où les centres ne sont pas en mesure d'accorder à l'ARC un accès limité uniquement aux sujets de l'étude :
    - Les établissements peuvent exiger de l'ARC qu'il signe un formulaire spécifique au centre, soit sous la forme d'un document autonome, soit intégré en tant qu'invite dans le système informatisé (p. ex., entente de confidentialité de l'établissement, ententes de politique de l'établissement) comme condition pour obtenir l'accès à leurs documents sources (papier ou électronique), à leurs locaux ou ailleurs.
    - Après chaque visite à distance, un processus pourrait être mis en place au centre pour examiner les pistes de vérification, afin de s'assurer et de confirmer que l'ARC n'a pas eu accès aux documents sources des sujets ne faisant pas partie de l'étude.

4.5 Technologie : Pare-feu et réseaux privés virtuels

- Certains systèmes informatiques ne sont pas approuvés par les pratiques du promoteur en matière de TI. Les recommandations et les considérations en matière de TI doivent être examinées, afin d'évaluer les risques des systèmes de surveillance à distance des données pour l'accès aux DME et aux systèmes permettant l'examen à distance d'autres activités de surveillance (p. ex., classeur des dossiers de l'essai du chercheur [CDEC] ou fichiers réglementaires, fournitures cliniques). Les applications doivent toujours être installées par le biais du centre logiciel du promoteur ou de Microsoft Store (et non téléchargées à partir d'Internet) ou des instructions fournies par le centre. L'objectif est d'atténuer les risques que des logiciels malveillants soient installés sur les ordinateurs portables du promoteur ou du centre.
- Les promoteurs peuvent utiliser leur propre réseau privé virtuel (RPV) pour sécuriser leur réseau. Dans certains cas, des limitations techniques empêchent l'installation d'applications de RPV et l'établissement de connexions sur les ordinateurs portables du promoteur. L'installation sur les iPad du promoteur comporte des risques de cybersécurité, comme l'établissement de connexions réseau gérées par des entités externes. Si l'établissement exige un programme de RPV, le promoteur peut vérifier si des programmes de bureau à distance peuvent être utilisés sur les ordinateurs portables du promoteur.
- Des applications de connexion à distance (c.-à-d. Citrix, VMware, etc.) ou des solutions de partage d'écran, comme WebEx ou MS Teams, pourraient être considérées pour partager les documents sources des patients avec les promoteurs. Cependant, il sera important que le pare-feu de l'établissement n'empêche pas l'ARC du promoteur d'accéder à la solution si de telles solutions sont envisagées. Il y a eu des cas de pare-feu empêchant le contrôle à distance de l'ARC du promoteur qui utilisait Microsoft Teams.
- Planifier et lancer des réunions par téléconférence à l'aide des applications WebEx ou Microsoft Teams du promoteur.
- Pour assurer une gestion efficace des dispositifs d'authentification, des méthodes de chiffrement comme l'authentification à facteurs multiples (AFM) et l'authentification à deux facteurs (A2F) doivent être utilisées.
- Les fonctions pour copier, coller, imprimer, télécharger et transférer des données doivent être désactivées lors du partage de la documentation source et une piste de vérification doit être en place.

4.6 Copies certifiées conformes

- Les documents sources en format papier sont numérisés et téléversés par le personnel du centre. Les documents sources numérisés doivent être des copies certifiées conformes des originaux (*conformément aux BPC 1.63 de la CIH : Une copie [quel que soit le type de support utilisé] du document original qui a été vérifiée [c.-à-d., par une signature datée ou par le fait d'avoir été générée par un processus validé] en vue de déterminer que les renseignements qui y figurent, y compris les données qui décrivent le contexte, le contenu et la structure, sont les mêmes que ceux de l'original).*
- Il faut évaluer les exigences de chaque promoteur en ce qui concerne l'acceptabilité des documents anonymisés (censurés) et la certification comme copies certifiées conformes des documents sources. Si le promoteur l'accepte, la surveillance des documents sources anonymisés ou certifiés copies conformes peut nécessiter une nouvelle surveillance lors d'une visite de surveillance subséquente sur place.
- Voici quelques méthodes potentielles de préparation de copies certifiées conformes :

4.6.1 Certification en vrac à l'aide d'un registre de certification

- Le registre de certification est personnalisé selon les préférences du centre en utilisant l'une des approches suivantes :
  a) Selon l'étude ou le sujet, le registre de certification est conservé dans le dossier de recherche de chaque sujet.
     i. La certification du dossier papier du sujet permet de certifier à la dernière page d'un dossier au lieu de certifier chaque page (le processus de certification est intégré). Le dossier devra tout de même être vérifié selon un processus de CQ conçu à cet effet.
  b) Selon l'étude, inclure un registre de certification en cours de ce qui est numérisé avec une colonne pour le numéro du sujet.
     i. Il peut être conservé dans le CDEC.
     ii. Téléverser le registre de certification avec chaque trousse de documents téléversée.

4.6.2 Certification de documents individuels à l'aide de signatures électroniques conformes

- En utilisant une application de signature électronique numérique conforme à la norme 21 CFR Part 11 (comme DocuSign Part 11, PDF [Adobe Pro Part 11], etc.) avec preuve de signature électronique sur les documents sources en format papier numérisés.

  Remarque :

  FDA : Les signatures électroniques qui sont destinées à être l'équivalent de signatures manuscrites, d'initiales et d'autres signatures générales requises par les règles données. Les signatures Part 11 comprennent les signatures électroniques utilisées, par exemple, pour documenter le fait que certains événements ou actions se sont produits conformément à la règle donnée (p. ex., *approuvés, examinés* et *vérifiés*) (https://www.fda.gov/regulatory-information/search).

- De plus, les systèmes informatiques utilisés pour créer, modifier et tenir à jour des dossiers électroniques et gérer les signatures électroniques sont également soumis aux exigences de validation. [Voir 21 CFR § 11.10(a)]. De tels systèmes informatiques doivent être validés pour garantir l'exactitude, la fiabilité, la constance des performances prévues et la capacité à discerner les dossiers non valides ou modifiés. (*General Principles of Software Validation; Final Guidance*

for Industry and FDA Staff [FDA, Center for Devices and Radiological Health, Center for Biologics Evaluation and Research, 2002]).

4.7 Coût et remboursement de la surveillance à distance des données

Le coût de la configuration d'une surveillance à distance des données peut varier et le centre devra tenir compte de la façon dont il peut gérer efficacement ces configurations. Voici des exemples de ce qui est fait actuellement :

- Certains centres chargent des promoteurs pour l'accès à distance aux DME. Les frais peuvent être à chaque visite à distance (maximum de 4 heures par MV) ou à un tarif annuel couvrant le coût de la licence du système à distance du centre (frais annuels par ARC ou par étude).
- Certains centres demandent des frais pour le rapprochement TMF par heure passée par le centre à aider le promoteur dans cette tâche.
- Peu de centres demandent des frais de pharmacie à distance, ce qui est remboursé à l'heure.
- Le service des finances du promoteur examinera et approuvera les coûts du centre pour chaque étude. Le remboursement peut être effectué à la réception d'une facture et payé à partir des fonds prévisionnels du budget du centre.
- Les budgets des nouveaux promoteurs peuvent maintenant inclure les frais de DME à distance dans le coût par patient.

5. Initiation de la surveillance à distance des données

Lorsqu'une décision d'utiliser une surveillance à distance des données est prise et approuvée par les parties prenantes, les éléments suivants doivent être évalués et complétés dans le cadre de l'initiation ou de la planification :

- Portée de ce qui sera surveillé à distance
- La méthode doit être formalisée et documentée
- Capacité à effectuer les activités
- Compétence pour effectuer les activités
- Technologie qui sera utilisée
- Responsabilités des parties prenantes à la surveillance
- Responsabilités du centre
- Responsabilités du promoteur
- Exigences en matière de confidentialité
- Conservation des dossiers
- Réalisation des entrevues
- Réalisation des examens des données, y compris les FCE, les EI, les écarts et d'autres données
- Examen de l'établissement
- Examen du produit expérimental
- Exigences en matière de suivi
- Projet pilote du processus de surveillance à distance des données

6. Planification de la surveillance à distance des données

Lors de la planification détaillée de l'approche de surveillance à distance des données des documents et des données de l'étude, diverses options doivent être évaluées en fonction des exigences d'accès. C'est le cas pour l'accès aux dossiers médicaux électroniques (DME) et aux documents sources en format papier; et des domaines tels que la méthode, la technologie, les personnes et les outils doivent être soulignés pour comprendre les exigences d'exécution des activités de surveillance à distance des données.

Une fois que l'approche de surveillance à distance ou sur place a été acceptée par les parties prenantes, les activités requises doivent être documentées en tant que révision du plan de surveillance, ou dans une procédure ou des instructions de travail. Une formation doit également être planifiée pour garantir l'efficacité et la compréhension des nouvelles méthodologies.

Les sous-sections suivantes décrivent les tactiques potentielles pour la planification de la surveillance à distance des données des DME et des documents sources.

Note : La conformité aux exigences en matière de sécurité de l'information des différentes méthodes d'accès aux données décrites à cette section sera vérifiée au cours des étapes décrites à la section 4 du document, incluant l'approbation par le RSI (incluant le service F) et le services TI de l'établissement, ainsi que l'approbation du BCH lorsque requise.

6.1 Accès à distance aux dossiers médicaux électroniques (DME)

Opportunité : *Mise en œuvre d'un accès à distance sécurisé aux DME non censurés pour effectuer une surveillance à distance des données.*

Défi : *Les DME non censurés contiennent des identifiants personnels du sujet. Par conséquent, l'accès à distance comporte un niveau de risques en matière de sécurité, puisque l'ARC (c'est-à-dire le moniteur, le système informatisé) n'est pas sous le contrôle total du centre de recherche surveillé. Par exemple, il existe des risques comme la présence d'un tiers qui peut consulter les données sur l'écran du système informatisé ou l'enregistrement de l'activité de surveillance par le moniteur. Le risque, bien qu'il soit toujours présent, est plus faible lorsque le moniteur est au centre de recherche.*

- L'accès aux documents sources non censurés est l'option privilégiée et la méthode la plus proche de ce à quoi l'ARC du promoteur (c.-à-d. le moniteur) aurait accès et examinerait pendant la réalisation physique de la visite de surveillance sur place.
- Dans le passé et actuellement, lorsque les ARCs effectuaient une visite de surveillance sur place, ils avaient accès aux DME à l'aide du matériel spécifié par le centre, comme un ordinateur portable ou de bureau avec des identifiants de connexion établis pour accéder aux DME. De plus en plus, les ARCs utilisent leur propre ordinateur portable pour accéder aux données sur place, les progrès en matière de sécurité leur offrant cet avantage.
- Cet accès sécurisé aux DME par voie électronique est identique à celui de la méthode de surveillance à distance des données (sans utiliser le matériel du centre, c.-à-d. ordinateur portable ou de bureau ou ordinateur portable de l'ARC). Par conséquent, l'ARC utilisera les mêmes identifiants de sécurité logicielle pour accéder aux DME à distance. Ainsi, les problèmes de sécurité logicielle sont très similaires.
- Cependant, il existe un degré de risque plus élevé en matière de sécurité physique, comme le partage de renseignements lors de la visite de surveillance à distance des données.

Voici une description de deux approches possibles pour l'accès aux DME pendant la surveillance à distance des données :

6.1.1 Accès direct aux DME

La méthode consiste à fournir un accès direct, sécurisé et en mode consultation seulement, aux documents des DME avec les éléments suivants :

Élément	Utilisation
Outil	• Un navigateur Web installé sur le système informatisé de l'ARC qui permet d'exécuter la connexion et l'application sécurisées. • Une connexion à distance sécurisée peut être effectuée par le biais d'un jeton ou d'une application sécurisée que l'ARC doit installer sur son propre système informatique (p. ex., Citrix, VMware, RPV, ISL Light)
Dispositif	• Un bureau virtuel, configuré par le centre de recherche et dédié à la visite de surveillance avec un accès limité aux DME. • L'ARC doit disposer d'un système informatisé permettant de télécharger l'application requise. • L'ARC pourrait avoir besoin d'un téléphone intelligent pour l'authentification à facteurs multiples, le cas échéant. • L'ARC et le centre de recherche devront avoir un accès Internet sécurisé et offrant une certaine bande passante pour gérer les activités de manière efficace.
Méthode et outil	• Une entente de confidentialité spécifique peut devoir être conclue avec le moniteur ou l'organisation déléguée, afin de mener les activités d'examen à distance.
Méthode	• L'ARC peut garder le contrôle du bureau virtuel, c.-à-d. les données des dossiers médicaux électroniques, se connecter aux DME à l'aide de ses identifiants et examiner les données des DME comme requis par le plan de surveillance.

Avantages et inconvénients de l'accès à distance direct aux DME	Avantages	Inconvénients
Examen autorisé des données sources à distance lorsque les visites sur place sont restreintes.	X	
Aucun impact sur les ressources ou le temps du coordonnateur de l'étude du centre (coordonnateur de l'étude) (l'ARC peut se connecter indépendamment pendant la visite à distance).	X	
Accès limité si tous les documents sources ne sont pas stockés dans les DME, c.-à-d. notes sources en format papier, dossiers papier d'autres fournisseurs, etc.		X
Facile à configurer avec le service des TI par le biais d'une application approuvée.	X	
Accès contrôlé et restreint pour la piste de vérification de l'ARC.	X	
Risque accru à la sécurité physique lié au partage des données.		X

6.1.2 Accès indirect aux DME

La méthode consiste à fournir un accès indirect, en mode consultation seulement, aux documents des DME avec les éléments suivants :

Élément	Utilisation
Outil	• Un système de téléconférence établi et contrôlé par le centre de recherche avec des capacités audiovisuelles, comme Web-Ex, Microsoft Teams, Zoom ou Zoom Healthcare, est utilisé pour planifier et établir une visite de surveillance avec le coordonnateur de l'étude, l'ARC et d'autres membres du personnel de l'étude, au besoin, y compris le chercheur principal. Le centre de recherche doit contrôler le logiciel de téléconférence pour s'assurer que le risque de partage des renseignements personnels est sous le contrôle du centre. • Un navigateur Web installé sur le système informatisé de l'ARC qui exécute le système de téléconférence.
Dispositif	• Un ordinateur doit être mis à disposition par le centre de recherche et dédié à la visite de surveillance, afin d'éviter la monopolisation de l'ordinateur du coordonnateur de l'étude et le risque de partage inapproprié de renseignements. L'ordinateur dédié doit être configuré de manière à ce qu'il soit isolé et donc non connecté au réseau ou au disque partagé de l'établissement. Limitant ainsi tout risque d'exposition à d'autres données confidentielles. • L'ARC doit disposer d'un système informatisé permettant de télécharger l'application requise, au besoin. • L'ARC pourrait avoir besoin d'un téléphone intelligent pour l'authentification à facteurs multiples, le cas échéant.

	• L'ARC et le centre de recherche clinique devront avoir un accès Internet sécurisé d'une certaine bande passante pour gérer les activités de manière efficace.
Méthode et outil	• Une entente de confidentialité spécifique peut devoir être conclue avec le moniteur ou l'organisation déléguée, afin de mener les activités d'examen à distance.
Méthode	• Une fois l'accès en lecture accordé, l'ARC peut naviguer dans l'ordinateur dédié à la séance de consultation des données électroniques, en se connectant aux DME à l'aide de ses identifiants et en examinant les données limitées des DME, selon les exigences du plan de surveillance.

Avantages et inconvénients de l'accès à distance indirect aux DME	Avantages	Inconvénients
Examen autorisé des données sources à distance lorsque les visites sur place sont restreintes.	X	
Répercussions sur les ressources du coordonnateur de l'étude (temps que le coordonnateur de l'étude passe à se connecter, à partager l'écran et à donner le contrôle)		X
L'ARC prend le contrôle de l'ordinateur du coordonnateur de l'étude.		X
L'ARC obtient un accès direct aux DME pour examen à l'aide des mêmes identifiants qu'il utiliserait sur place.	X	
Accès limité si tous les documents sources ne sont pas contenus dans les DME.		X
Limitations techniques potentielles en raison des pare-feu (centre qui n'est pas en mesure de donner le contrôle à l'ARC).		X

6.2 Accès à distance aux documents sources en format papier

Opportunité : *Mise en œuvre d'un accès à distance sécurisé aux documents sources en format papier non censurés pour effectuer une surveillance à distance des données.*

Défi : *Une source en format papier non censurée contient des identifiants personnels du sujet. Par conséquent, l'accès à distance comporte un niveau de risques en matière de sécurité, puisque l'ARC (c'est-à-dire le moniteur, le système informatisé) n'est pas sous le contrôle total du centre de recherche surveillé. Par exemple, il existe des risques comme la présence d'un tiers qui peut consulter les données sur l'écran du système informatisé ou l'enregistrement de l'activité de surveillance par le moniteur. Le risque, bien qu'il soit toujours présent, est plus faible lorsque le moniteur est au centre de recherche.*

- Lorsque les ARC se rendaient sur place, on leur donnait des dossiers papier, des tableaux contenant des informations sources pour effectuer l'examen et la vérification des documents sources. De plus en plus, l'utilisation de systèmes de saisie électronique des données est mise à profit. Cependant, il existe toujours un niveau élevé de sources en format papier utilisées pour les études cliniques.
- Pour l'accès à distance des documents sources en format papier, les centres de recherche pourraient envisager d'utiliser les approches suivantes :

6.2.1 Approche avec applications Web gérées par le centre (dépôt de centre d'essai)

La méthode consiste à fournir un accès sécurisé, en mode consultation seulement, à l'aide d'un système de saisie électronique des données avec les éléments suivants :

Élément	Utilisation
Outil	• Les exemples de dépôt de centre d'essai sont Florence, Veeva Site Vault, Clouds, CRIO. • Un navigateur Web (p. ex. Microsoft Edge, Google Chrome) installé sur le propre système informatique de l'ARC est accessible à partir du dépôt du centre d'essai.
Dispositif	• L'ARC doit disposer d'un système informatisé permettant de télécharger l'application requise, le cas échéant. • Pour les sources en format papier, le coordonnateur de l'étude doit avoir accès à un dispositif, comme un scanneur, pour produire une copie certifiée conforme. • L'ARC et le centre de recherche clinique devront avoir un accès Internet sécurisé d'une certaine bande passante pour gérer les activités de manière efficace.
Méthode et outil	• Pour les sources en format papier, le coordonnateur de l'étude doit avoir la capacité de confirmer la copie certifiée conforme par un processus reproductible ou un outil validé. • Une entente de confidentialité spécifique peut devoir être conclue avec le moniteur ou l'organisation déléguée, afin de mener les activités d'examen à distance.
Méthode	• Les ARCs reçoivent des identifiants de connexion pour se connecter au système sur Internet. Cette approche ne nécessite généralement pas l'installation de logiciels sur les ordinateurs portables et est entièrement gérée par le personnel du site. Les documents (copies électroniques ou numérisées) sont téléversés par le personnel du centre dans un dossier ou un espace d'application désigné et consultés dans l'application sans effectuer le téléchargement de documents, c.-à-d. que l'ARC accède aux dossiers ou fichiers d'intérêt et consulte les fichiers dans le système (sans téléchargement).

Avantages et inconvénients de l'approche avec dépôt de centre d'essai	Avantages	Inconvénients
Examen autorisé des données sources à distance lorsque les visites sur place sont restreintes.	X	
Incidence sur les ressources du centre si les sources en format papier doivent être numérisées, certifiées et téléversées		X
Le registre de certification ou la piste de vérification doit être maintenu pour la source papier numérisée		X

Si le centre utilise le format eTMF, il peut facilement transférer des fichiers pour examen en fournissant un accès eTMF direct pour empêcher tout travail supplémentaire.	X	
Il y a des coûts supplémentaires pour le dépôt de centre d'essai si le centre ne dispose pas d'une telle plateforme de saisie électronique des données.		X
Accès restreint contrôlé par le centre et piste de vérification pour la connexion du CRA au système	X	

6.2.2 Approche avec dossiers partagés contrôlés

La méthode consiste à fournir un accès sécurisé, en mode consultation seulement, à l'aide d'un système de dossiers partagés contrôlés contenant les documents sources, avec les éléments suivants :

Éléments	Utilisation
Outil	• Un dossier partagé contrôlé sur le système informatisé spécifiquement utilisé pour la visite de surveillance à distance des données peut être utilisé pour téléverser les documents sources en format papier numérisés. Les documents sources en format papier doivent être des copies certifiées conformes aux originaux (conformément aux BPC 1.63 de la CIH). • Un système de téléconférence (comme Microsoft Teams) est utilisé pour consulter les données sur les ordinateurs de bureau du centre par le biais d'un partage d'écran.
Dispositif	• L'ARC doit disposer d'un système informatisé permettant de télécharger l'application requise. • Pour les sources en format papier, le coordonnateur de l'étude doit avoir accès à un dispositif, comme un scanneur, pour produire une copie certifiée conforme. • L'ARC et le centre de recherche clinique devront avoir un accès Internet sécurisé d'une certaine bande passante pour gérer les activités de manière efficace.
Méthode et outil	• Pour les sources en format papier, le coordonnateur de l'étude doit avoir la capacité de confirmer la copie certifiée conforme par un processus reproductible ou un outil validé. • Une entente de confidentialité spécifique peut devoir être conclue avec le moniteur ou l'organisation déléguée, afin de mener les activités d'examen à distance.
Méthode	• Pendant le TC, l'ARC peut prendre le contrôle de l'ordinateur utilisé pour la surveillance par le biais du système TC, ou le coordonnateur de l'étude peut ouvrir les documents sources en format papier numérisés et les faire défiler en suivant les instructions de l'ARC.

Avantages et inconvénients de l'approche avec dossiers partagés	Avantages	Inconvénients
Examen autorisé des données sources à distance lorsque les visites sur place sont restreintes.	X	
L'ARC prend le contrôle de l'ordinateur du coordonnateur de l'étude (ne peut fonctionner que si ordinateur dédié est disponible)		X
Répercussions sur les ressources du centre puisque les sources en format papier doivent être numérisées, certifiées et téléversées (ce qui prend beaucoup de temps)		X
Aucun coût système supplémentaire puisque le centre dispose de cette infrastructure de gestion des documents.	X	
Le registre de certification ou la piste de vérification doit être maintenu pour la source papier numérisée		X

6.2.3 Approche avec téléconférence Web

La méthode consiste à fournir un accès sécurisé, en mode consultation uniquement, à l'aide d'un outil de téléconférence Web permettant de visualiser les documents sources, avec les éléments suivants :

Éléments	Utilisation
Outil	• Caméra Web d'un centre connecté à un ordinateur de bureau du centre • Un système de téléconférence est utilisé pour consulter les données sur les ordinateurs de bureau du centre grâce à un partage d'écran.
Dispositif	• L'ARC doit disposer d'un système informatisé permettant de télécharger l'application requise. • L'ARC et le centre de recherche clinique devront avoir un accès Internet sécurisé d'une certaine bande passante pour gérer les activités de manière efficace.
Méthode et outil	• Une entente de confidentialité spécifique peut devoir être conclue avec le moniteur ou l'organisation déléguée, afin de mener les activités d'examen à distance.
Méthode	• Le coordonnateur de l'étude peut partager les documents sources en format papier à l'aide de la webcam dans l'environnement de la téléconférence, afin que l'ARC puisse les lire.

Avantages/inconvénients de l'approche avec téléconférence Web	Avantages	Inconvénients
Examen autorisé des données sources à distance lorsque les visites sur place sont restreintes.	X	
Examen autorisé des documents papier et électroniques.	X	
Impact important sur le coordonnateur de l'étude et les ressources du centre.		X

Aucune assurance que les documents partagés sont complets.		X
Capacités de partage et risques limités, car moins faciles à contrôler.		X

7. Exécution d'une surveillance à distance des données

Au cours de l'exécution, les détails du processus réel doivent être affinés pour des visites de surveillance à distance des données efficaces :

- Combien de temps à l'avance l'ARC doit-il planifier la visite?
- L'ARC doit-il informer le centre de ce qui doit être numérisé?
- Existe-t-il une limite au nombre de pages à numériser?
- Existe-t-il une limite au nombre de jours qui peuvent être programmés?
- Existe-t-il une limite au nombre d'ARC qui peuvent participer?
- Une solution hybride à long terme de visites sur place et à distance?
- Faut-il prévoir une réunion de préparation avec le coordonnateur du centre pour s'assurer que la logistique appropriée est comprise et en place?
- Il est fortement suggéré d'effectuer un essai pilote ou de préparer une évaluation des risques d'une surveillance à distance des données avec un ARC, afin de confirmer que les instructions sont claires et faciles à suivre.
- Tenez compte des coûts associés aux solutions de surveillance à distance des données et des possibilités de les réduire tout en maintenant la conformité.
- Les solutions d'accès à distance devraient ou doivent être documentées dans des procédures opérationnelles normalisées (PON) ou des instructions de travail et toute modification peut avoir une incidence sur ces documents contrôlés.
- Lors de la réalisation des activités de surveillance, s'il y a des problèmes techniques empêchant la consultation des documents, comment gérer le retard?

8. Clôture de la surveillance à distance des données

L'amélioration continue peut être maintenue en partageant les leçons apprises par les différentes instances de surveillance, afin d'accroître l'efficacité dans la mise en place et l'exécution. Le CRC et l'ARC doivent documenter l'apprentissage et des réunions planifiées pour partager des améliorations potentielles doivent être établies, ce qui peut être bénéfique pour d'autres études nécessitant une approche similaire.

9. Supervision de la surveillance à distance des données

L'efficacité et la qualité du processus de surveillance à distance des données peuvent être vérifiées plus en détail au moyen de vérifications d'assurance de la qualité, c.-à-d. des vérifications du processus de surveillance, ou en tant que vérification de l'étude, en mettant davantage l'accent sur les activités de surveillance. Des vérifications supplémentaires peuvent être nécessaires pour s'assurer que le processus est bien conçu et que les résultats de la surveillance correspondent aux attentes du promoteur.

De plus, le personnel de l'étude devra s'assurer que les problèmes sont traités dès qu'ils sont identifiés. Étant donné que la surveillance à distance des données dépend de la technologie par rapport à la surveillance sur place, il existe des risques de problèmes techniques multiples qui

peuvent entraver le processus de surveillance, et même retarder la visite de surveillance à distance des données. De tels risques peuvent également être inclus dans le registre des risques de l'étude, afin de s'assurer que tous les membres du personnel de l'étude en sont conscients.

Enfin, le budget et les coûts peuvent également devoir être ajustés pour les efforts supplémentaires fournis par le centre, en attendant que les méthodes de surveillance à distance des données soient établies et améliorées au cours de l'étude.