Accélérer le démarrage des essais

Recommandations à destination des promoteurs

Avis /autorisation réglementaire | **Faisabilité** | **Convention** | **Mise en place 1er centre** | **Inclusion 1er patient**

Renforcer la sécurité des outils et des données

Authentification multifacteur

Recommandations CNIL rélatives à l'authentification multifacteur
(publiées le 20 mars 2025)

Pourquoi est-ce obligatoire ?

La CNIL exige une authentification renforcée pour les accès à des données sensibles. La MFA (authentification multifacteur) réduit les risques d'usurpation, de phishing et d'accès non autorisé..

Elle doit être adaptée au niveau de risque du traitement :

- données directement identifiantes ;
- données pseudonymisées.

Quel outil de double authentification utiliser ?

La CNIL ne recommande pas un outil unique, mais des catégories de facteurs considérées comme suffisamment robustes selon le niveau de risque.

Exemple d'outils : les applications d'authentification (Google Authenticator, Microsoft Authenticator, FreeOTP, Authy...) ou les clés physiques de sécurité (Yubikey, Titan Key...).

Les codes par SMS ou email sont tolérés uniquement pour des usages à risque faible, car moins robustes.

Pour quels logiciels la MFA est-elle obligatoire ?

Pour tout système donnant accès à des données sensibles, en particulier des données de santé : eCRF/EDC, IWRS, ePRO, portails promoteurs/investigateurs, plateformes de monitoring à distance, espaces de randomisation, etc.

- Données directement identifiantes : obligatoire.
- Données pseudonymisées : obligatoire d'ici 2 à 3 ans.

Peut-on utiliser un smartphone personnel ?

La CNIL précise que la solution recommandée est l'installation par le responsable de traitement d'une application TOTP (*time based one time password*) sur le téléphone de l'employé.

L'envoi de SMS sur le téléphone de l'employé est toléré par la CNIL mais ne présente pas les mêmes garanties de sécurité qu'un TOTP.

L'usage doit rester proportionné et non intrusif.

Que faire si un professionnel refuse d'utiliser son smartphone personnel ?

Le responsable de traitement doit s'assurer de la conformité au droit du travail, une alternative peut être proposée par le responsable de traitement : smartphone professionnel dédié, clé physique de sécurité, ou token matériel générant des OTP (*one time password*).

Le refus ne doit pas empêcher l'accès aux outils nécessaires.

Comment cela se passe en pratique ?

L'utilisateur installe une application d'authentification ou utilise une clé physique.

À chaque connexion :

- Il saisit son mot de passe,
- Puis un 2ème facteur :
  - Facteur possession :
    - Code temporaire venant d'un jeton matériel ;
    - Code temporaire venant d'un jeton logiciel ;
  - Facteur inhérence :
    - Caractère morphologique (Face ID, empreinte digitale…).

Le promoteur doit documenter la mesure dans son analyse de risques et son registre de traitement.

Que faire pour les questionnaires patients (ePRO) ?

La MFA doit rester proportionnée.

Attention à la fracture numérique : pour les patients, les solutions simples (code par email ou SMS) sont généralement acceptables, car le risque est moindre et l'usage doit rester accessible.

Qui est responsable de la mise en place ?

Le responsable de traitement (promoteur) doit garantir un niveau de sécurité adapté.

Les prestataires (éditeurs) doivent fournir des solutions conformes.