

Webinaire ANAT

19 novembre 2026



RGPD ESSAIS CLINIQUES

Webinaire ANAT

DPO, RGPD et cadres internationaux post-Safe Harbor

19 novembre 2026, 18h-19h

Sylvain Chemtob & Fleur Labrunie
Cabinet Phénix Privacy

Au programme

01 Les principes du RGPD utiles au quotidien

Qui décide, ce qu'est une donnée personnelle, ce qui se passe quand les données quittent l'Europe

25 min

02 Recherche en santé : les questions à se poser

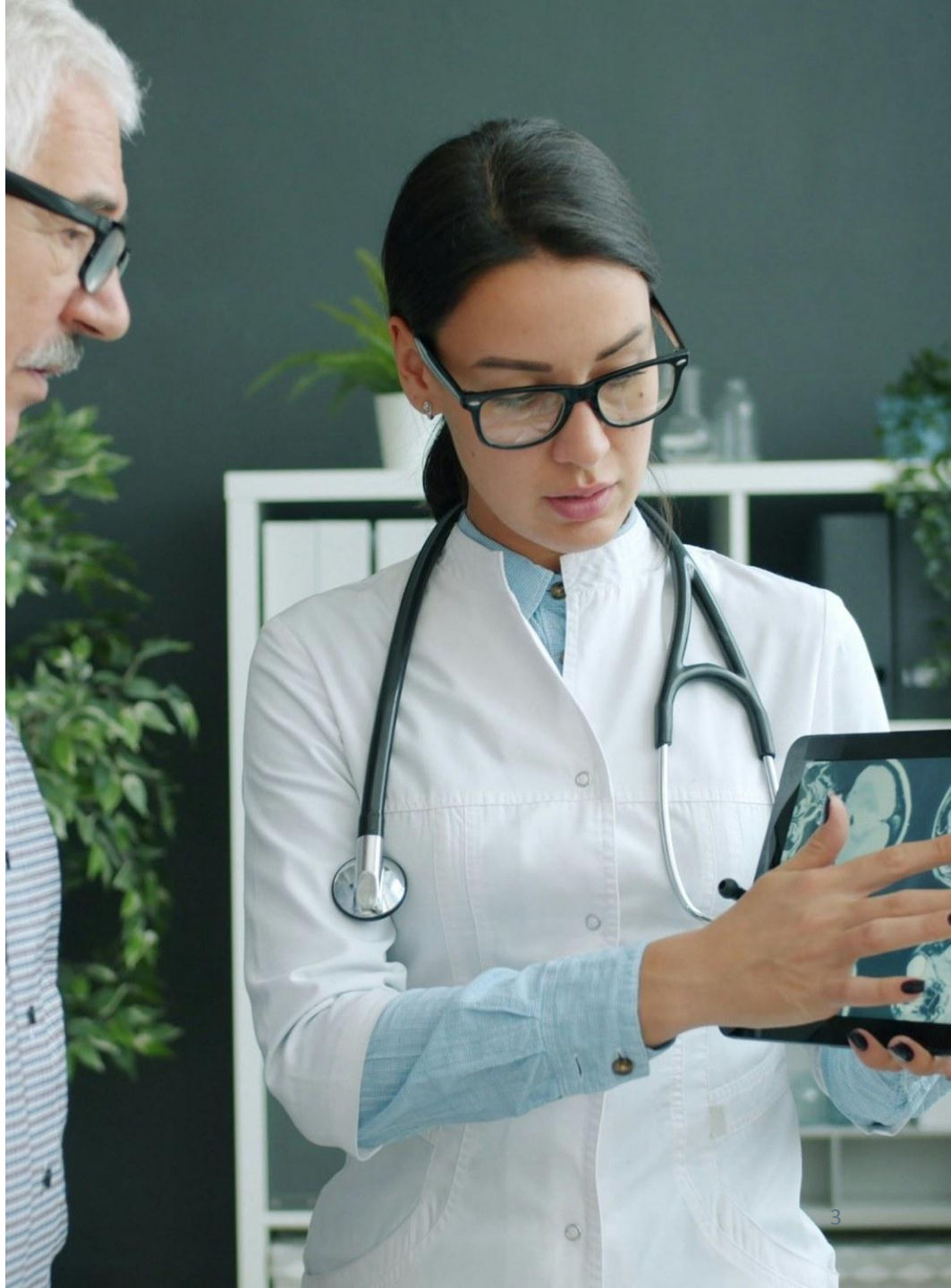
Les méthodologies de référence (MR) révisées en 2026, le monitoring à distance, le code patient, la sanction IQVIA

25 min

03 Vos questions

Transferts, contrats, prestataires, sécurité

10 min



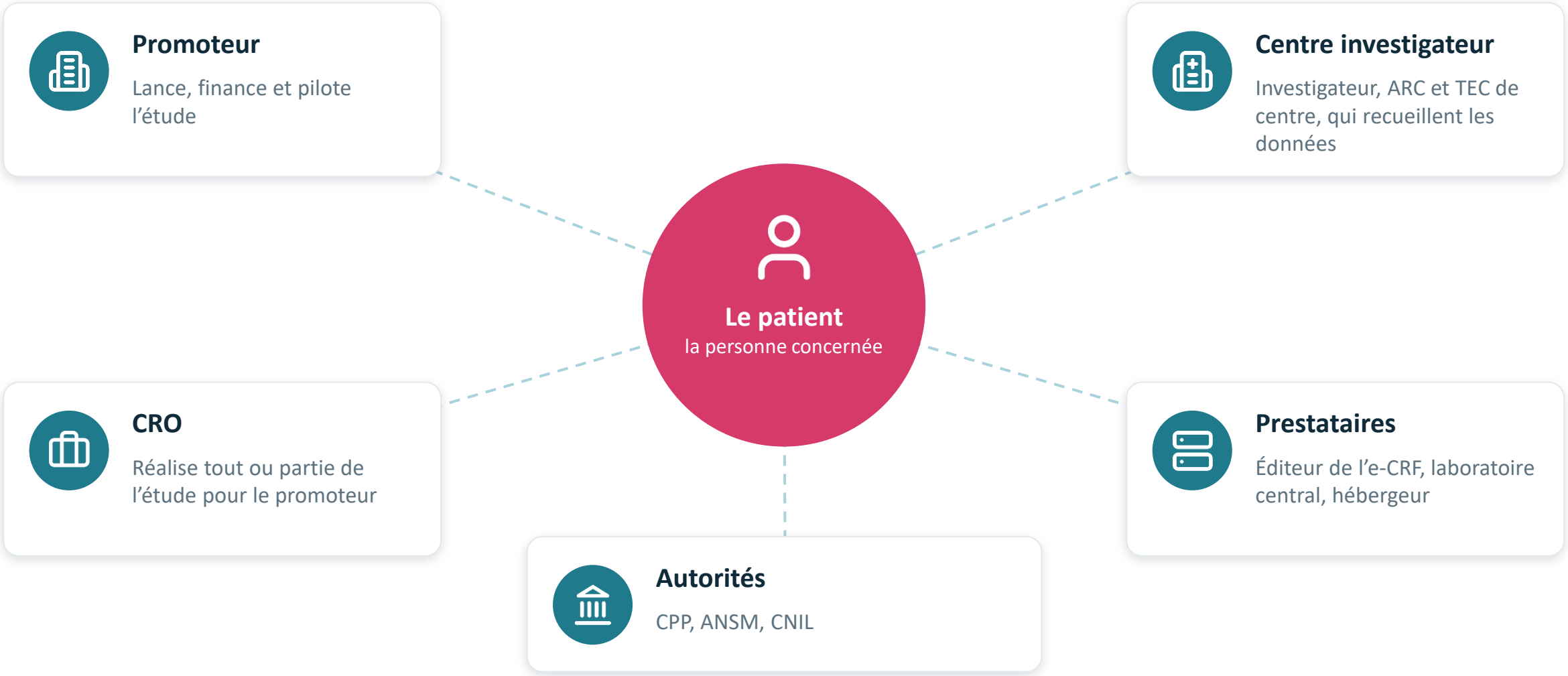


01

Les principes du RGPD utiles au quotidien

Qui décide, ce qu’on protège, où vont les données, comment on les sécurise

Une étude, beaucoup d’acteurs autour des mêmes données



Qui décide, qui exécute ?

Responsable de traitement

Décide pourquoi et comment les données sont traitées. Il porte la responsabilité.

Exemple

Le promoteur

RGPD, art. 4.7

Sous-traitant

Traite les données pour le compte du responsable, sur ses instructions et avec un contrat.

Exemple

La CRO, l'éditeur de l'e-CRF, le centre investigateur

RGPD, art. 28

Responsables conjoints

Décident ensemble et se répartissent les obligations dans un accord.

Exemple

Deux co-promoteurs

RGPD, art. 26 ; dans les MR depuis 2026

La question utile pour un ARC ou un TEC : pour le compte de qui je travaille sur ces données ? La réponse dit à qui remonter une question ou un incident.

Le DPO et ceux qui travaillent avec lui

Ses missions (RGPD, art. 39)

Informer et conseiller
les équipes, les chefs de projet, la direction

Contrôler
que les règles sont appliquées sur le terrain

Conseiller sur les analyses d'impact
pour les traitements à risque, comme la recherche

Faire le lien avec la CNIL
et servir de contact aux personnes concernées

Autour de lui

RSSI
la sécurité

DSI
les outils

Juridique
les contrats

Achats
les prestataires

Projet
chefs de projet, ARC, TEC

Qualité
les procédures

Le promoteur, la CRO et l'hôpital ont souvent chacun leur DPO.



Donnée personnelle : bien plus que le nom

« Toute information se rapportant à une personne physique identifiée ou identifiable », directement ou indirectement.

RGPD, art. 4.1



Dans une étude, par exemple

- Nom et prénom
- Numéro d'inclusion
- Date de naissance
- Dates de visite
- Résultats d'analyses
- Images IRM ou scanner
- Enregistrement de la voix
- Adresse IP d'une appli patient

Les données de santé sont une catégorie particulière

Leur traitement est interdit par principe (art. 9). La recherche fait partie des exceptions, dans un cadre précis : en France, une méthodologie de référence de la CNIL ou une autorisation.

Pseudonymisé n’est pas anonyme

Identifiante

Nom, prénom, date de naissance

RGPD applicable

Pseudonymisée

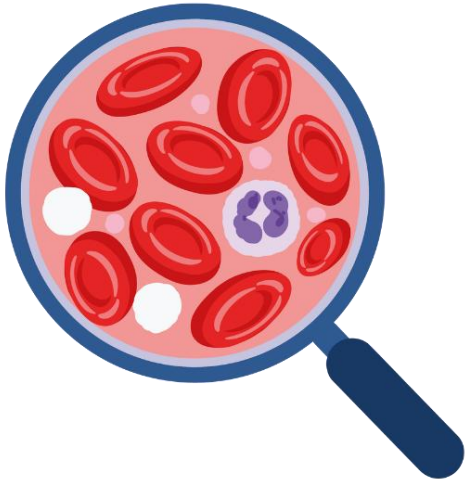
Un numéro remplace le nom. La table de correspondance existe quelque part.

RGPD applicable

Anonyme

Plus aucun moyen raisonnable de retrouver la personne

Hors RGPD



Ce qui compte, c’est la possibilité de réidentifier la personne avec des moyens raisonnables.

RGPD, art. 4.5 et considérant 26

Le RGPD suit les personnes, pas les serveurs



Il protège les personnes situées dans l’Union

Il s’applique aux organismes établis dans l’UE, et à ceux qui, hors UE, ciblent ou suivent des personnes situées dans l’UE (art. 3).

Données qui sortent de l’UE = transfert

Hébergement, consultation ou support depuis un pays tiers : il faut un cadre (art. 44 et suivants).

La protection doit voyager avec les données

Sécurité, droits des personnes, recours devant une autorité indépendante.

Encadrer un transfert : trois voies

1

Art. 45

Pays adéquat

La Commission européenne reconnaît un niveau de protection équivalent. Les données circulent sans formalité supplémentaire.

Exemples
Suisse, Japon, États-Unis pour les seules entreprises certifiées DPF

2

Art. 46

Garanties appropriées

Un contrat ou des règles internes apportent les garanties, complétées si besoin par des mesures techniques comme le chiffrement.

Exemples
Clauses contractuelles types, règles d’entreprise contraignantes

3

Art. 49

Dérogations

Cas particuliers, à interpréter strictement. Pas adaptées aux flux réguliers d’une étude.

Exemples
Consentement explicite à un transfert ponctuel

États-Unis : trois cadres successifs

2000

Safe Harbor

Décision d'adéquation de la Commission

2015

Invalidé

CJUE, Schrems I (C-362/14)

2016

Privacy Shield

Nouvelle décision d'adéquation

2020

Invalidé

CJUE, Schrems II (C-311/18)

2023

Data Privacy Framework

Décision du 10 juillet 2023

2025

Validé, puis contesté

Tribunal de l'UE, 3 sept. 2025 (T-553/23). Pourvoi pendant (C-703/25 P)

Le point qui fâche, à chaque fois

L'accès des services de renseignement américains aux données, et les recours offerts aux Européens. Le recours contre le DPF conteste l'indépendance de la juridiction créée pour eux (la Data Protection Review Court) et la collecte en masse.

Sécuriser : des mesures techniques et organisationnelles



Chiffrement
des données stockées et échangées

Double authentification
mot de passe et code sur téléphone (MFA)

Habilitations
chacun n'accède qu'à ce dont il a besoin

Journalisation
tracer qui fait quoi, et relire les traces

Sauvegardes
régulières et testées

Bons gestes
poste verrouillé, pas d'export ni de clé USB personnelle

MFA, chiffrement et journalisation figurent désormais dans l'annexe sécurité des MR (MR-SEC09, 12 et 14).



02

Recherche en santé : les questions à se poser

Ce que les méthodologies de référence révisées en 2026 changent pour un ARC ou un TEC

Ce qui change depuis mai 2026

19 mars 2026

Adoption

Nouvelles MR-001 et MR-003, et deux annexes : sécurité, contrôle qualité

23 mai 2026

Application

Pour les recherches qui démarrent à partir de cette date

1er janvier 2027

MFA, outils web

Double authentification pour les outils accessibles par le web, dont la plupart des e-CRF

Mai 2027

Recherches en cours

Plan d'actions sécurité mis en œuvre au plus tard

1er janvier 2028

MFA, autres outils

Pour les outils non accessibles par le web

Autre nouveauté : les recherches menées en partie ou entièrement à l'étranger entrent dans le champ des MR.



Monitoring à distance : deux formats autorisés



Visioconférence

- Un professionnel du centre reste présent pendant toute la session
- Le centre partage à l'écran les seuls documents sources nécessaires
- Ni prise en main à distance, ni partage de fichiers, ni enregistrement ou retranscription automatique



Plateforme sécurisée

- Le centre dépose les documents sur une plateforme intermédiaire
- Chiffrement, double authentification, journalisation surveillée par le centre
- Documents conservés le temps du contrôle, pas plus

Source : annexe contrôle qualité des MR, version mai 2026

Dans les deux cas, les mêmes règles

Compte nominatif

Lecture seule

Accès limité dans le temps

Lieu clos, sans passage (recommandé)

Ni capture d'écran, ni impression, ni export

Un doute sur une donnée ? Vérification sur site

Patient informé dès l'inclusion

Patient opposé : aucun contrôle sur ses données

Hors du champ de l'annexe : le contrôle à distance par accès direct au dossier patient informatisé (§ 7).

Le code patient change de règles

À proscrire

`JD-120385`

Initiales et date de naissance

Attendu

`7KQ2-94XF`

Tiré au hasard, sans lien avec la personne

MR-CNS-02

Pas d’initiales, de date de naissance, d’identifiant de soins, ni de numéro d’inclusion ou de tube, même tronqués

MR-CNS-03

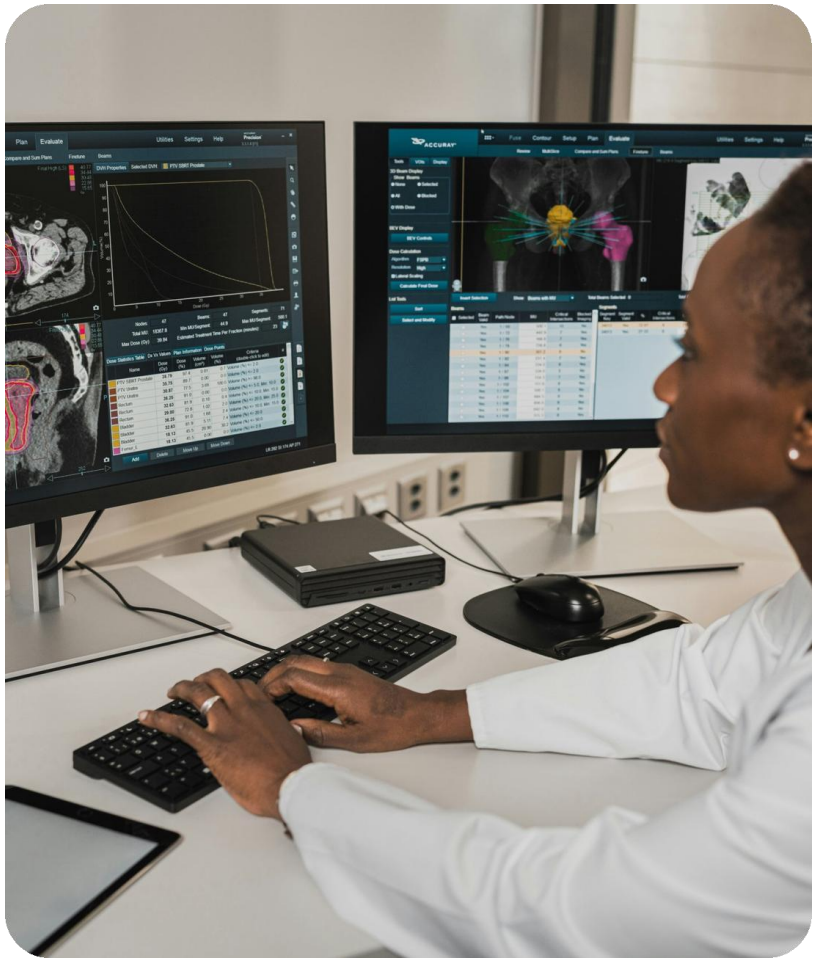
Code tiré au hasard, ou calculé par hachage avec une clé secrète

MR-CNS-04

Table de correspondance gardée seulement si strictement nécessaire, accès limité à quelques personnes habilitées

Et chez vous ? Combien d’études en cours codent encore les patients avec leurs initiales ?

Regarder depuis les États-Unis, c’est déjà transférer



Un moniteur du promoteur, basé aux États-Unis, suit une visioconférence de monitoring

Il ne télécharge rien. Il regarde l’écran partagé

Pour la CNIL, c’est déjà un transfert hors UE, même en simple visualisation (annexe contrôle qualité, § 35)

Conséquences

Outil hébergé dans l’UE, l’EEE ou un pays adéquat (CQ-DIST-JUR-4). Transfert encadré : DPF si l’entreprise américaine est certifiée, sinon clauses contractuelles types.

Le contre-exemple : la sanction IQVIA

5 M€

Amende infligée par la CNIL à IQVIA Operations France le 26 mai 2026 (SAN-2026-008), pour deux entrepôts de données de santé

Injonction de se mettre en conformité sous six mois, sous astreinte de 10 000 € par jour de retard

- Pas de double authentification pour accéder à l'un des entrepôts
- Journaux de connexion non analysés
- Information des patients inexacte
- Droit d'opposition sans procédure effective

« Nos données sont anonymes » : refusé

IQVIA invoquait l'arrêt SRB de la Cour de justice (4 septembre 2025). Pour la CNIL, les données sont pseudonymes : identifiant unique par patient, données très détaillées, croisement possible avec des données publiques. La réidentification reste possible par des moyens raisonnables.

Six questions à se poser sur une étude

1 Pour le compte de qui je traite ces données ?

2 Mon accès est-il nominatif, en lecture seule, avec double authentification ?

3 Le patient a-t-il été informé du monitoring à distance ?

4 Le code patient contient-il des initiales ou une date de naissance ?

5 Quelqu'un consulte-t-il les données depuis un pays hors UE ?

6 Un incident ? Je préviens tout de suite : le responsable de traitement a 72 heures pour notifier la CNIL (art. 33)



Vos questions

Transferts, contrats, prestataires, sécurité, monitoring : à vous



Phénix Privacy