1.3/

Voici des **mesures concrètes** pour mettre la Clinique en conformité (point « Actions à entreprendre » du Rapport de conformité légale du dossier *Clinique Pasteur – Atelier pro SIO2*).

Gouvernance & preuves de conformité

* **Nommer un DPO** (obligatoire pour un établissement de santé traitant à grande échelle des données sensibles) et lui donner les moyens d’agir.
* **Tenir un Registre des activités de traitement (RoPA)** et le maintenir à jour (soins, facturation, études, RH…).
* **Réaliser une AIPD (DPIA)** pour les traitements à risque élevé (données de santé, études, registres/entrepôts).

Bases légales, information & consentement

* **Qualifier la base légale** : soins (art. 9.2.h RGPD), recherche/intérêt public (art. 9.2.j) ou consentement explicite lorsque requis ; **rédiger les mentions d’information** remises aux patients.
* Pour les **études** : se **rattacher à une Méthodologie de Référence CNIL (MR-001/MR-004 selon le cas)** et documenter consentement ou modalités de réutilisation.

Contrats & hébergement

* **Encadrer les sous-traitants par des clauses RGPD (art. 28)** et liste des accès.
* Si l’hébergement est externe, **choisir un prestataire certifié HDS** (exigence du cadre e-santé français). ([Agence du Numérique en Santé](https://esante.gouv.fr/produits-services/hds?utm_source=chatgpt.com))

Sécurité technique & organisationnelle

* **Contrôles d’accès** (RBAC, comptes nominaux, MFA), **journalisation/traçabilité des accès**, **chiffrement** des données en transit/au repos, **sauvegardes chiffrées** et testées, **segmentation réseau** et **gestion des correctifs**.
* **Cloisonner les environnements** (dev/recette/prod) et **durcir les postes** (EPP/EDR).
* **Remplacer les fichiers papier/Excel** par des applications/BDD sécurisées ; sécuriser les archives physiques (armoires fermées, politique de destruction).

Données de recherche (schéma fourni dans l’annexe)

* **Pseudonymiser** les données d’étude : conserver la clé d’identification séparée ; structurer la base *Etudes/Inclusions* pour éviter tout accès aux identités non nécessaires. (Aligné avec MR-004/MR-001.)

Durées de conservation & purge

* **Dossier médical** : définir une politique conforme (**20 ans** après le dernier passage, avec règles spécifiques mineurs/décès) et **automatiser la purge/anonymisation** à échéance. ([Légifrance](https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036658351/?utm_source=chatgpt.com))

Droits des personnes

* Mettre en place un **processus de gestion des droits** (accès, rectification, limitation, opposition/portabilité quand applicable), formulaires, délais et point de contact (DPO).

Gestion d’incident

* **Procédure de notification des violations** : journal interne, analyse de risque, **notification à la CNIL sous 72 h** et, si risque élevé, information des patients. Former une cellule de réponse. ([RGPD](https://gdpr-info.eu/art-33-gdpr/?utm_source=chatgpt.com))

Sensibilisation & politique interne

* **Former** tous les personnels (soins, admin, IT) au RGPD et à la sécurité santé ; adopter une **charte informatique** et **procédures** (accès, mots de passe, BYOD, messagerie, partage).

Ces actions, priorisées (DPO/RoPA/AIPD → sécurité/HDS → transparence/consentement → conservation → droits/incidents → formation), répondent au **« petit 3 – Actions à entreprendre »** attendu pour la mise en conformité.