Fiche Sécurité & Confidentialité — Secrétariat médico-social en EHPAD

Objet : Cadre du secret professionnel et de la confidentialité des dossiers résidents + recommandations CNIL sur l'IA générative avec des données administratives / de santé.
Poste concerné : Secrétaire médical(e) en EHPAD (établissement d'hébergement pour personnes âgées dépendantes — établissement médico-social).
Date de rédaction : 22 juillet 2026.

1. Le secret professionnel : un cadre pénal et déontologique

1.1 Le principe

Toute personne qui, par son état, sa profession ou une mission temporaire, est dépositaire d'une information à caractère secret est tenue au secret professionnel. La révélation de cette information est **punie d'un an d'emprisonnement et de 15 000 € d'amende** (art. 226-13 du Code pénal, Légifrance).

Le secret s'impose « en raison d'une fonction ou d'une mission temporaire » : le/la secrétaire médical(e) d'EHPAD, même non-soignant(e), est donc pleinement concerné(e). La Cour de cassation précise que le secret est **absolu** et qu'il s'impose à l'ensemble du personnel de l'établissement ; le délit est constitué même sans préjudice, même si l'information est de notoriété publique, et même si elle n'est communiquée qu'à une seule personne elle-même tenue au secret (Cass. soc., 1er déc. 2015, 14-22.133, Légifrance).

1.2 Le secret médical « partagé » (exception encadrée)

Les professionnels participant à la prise en charge d'une même personne peuvent échanger des informations, mais dans une **double limite** : (1°) les seules informations strictement nécessaires à la coordination/continuité des soins, à la prévention ou au suivi médico-social et social ; (2°) le périmètre de leurs missions (art. L. 1110-4 et L. 1110-12 du Code de la santé publique, Légifrance).

Tenter d'obtenir la communication d'informations couvertes par le secret en violation de l'article L. 1110-4 est lui-même **puni d'un an d'emprisonnement et de 15 000 € d'amende** (art. L. 1110-4 V CSP, Légifrance).

1.3 Ce que cela signifie concrètement pour le secrétariat en EHPAD

Le secrétariat accède aux données uniquement « dans la mesure nécessaire à l'accomplissement de ses missions » — typiquement la gestion des rendez-vous et l'administration — et **sous le contrôle du professionnel de santé** (CNIL, délibération n° 2020-081 du 18 juin 2020, Légifrance, principe énoncé pour la gestion de cabinet médical/paramédical et

transposable au secrétariat d'EHPAD, en complément du besoin d'en connaître issu des art. L. 1110-4 et L. 1110-12 CSP). Les données médicales stricto sensu ne sont accessibles au secrétariat que de façon très limitée.

> **À retenir :** le/la secrétaire n'a accès qu'aux informations dont il/elle a « besoin d'en connaître » pour sa mission, jamais à l'ensemble du dossier médical du résident.

2. Confidentialité et sécurisation des dossiers résidents

Les données de santé sont des **données personnelles sensibles**, particulièrement protégées par le RGPD (art. 9), la loi Informatique et Libertés (art. 8), le Code de la santé publique et le Code de l'action sociale et des familles (CNIL, « Données de santé : la CNIL rappelle les mesures de sécurité… » ; CNIL, « Qu'est-ce qu'une donnée de santé ? »).

2.1 Mesures exigées par la CNIL (dossier patient informatisé)

Mesure	Exigence
Besoin d'en connaître	Les données ne sont accessibles qu'aux personnes justifiant du besoin d'en connaître
Habilitations par métier	Chaque agent n'accède qu'aux dossiers/données correspondant à sa fonction (accueil → dossier administratif seul ; médecin → données médicales)
Équipe de soins	Habilitations calées sur l'art. L. 1110-12 CSP : seuls les professionnels impliqués dans la prise en charge accèdent aux données couvertes par le secret médical
Mode « bris de glace »	Accès d'urgence possible, mais tracé, surveillé, justifié et identifié
Traçabilité/journalisation	Qui s'est connecté, à quel moment, qui a accédé à quoi
Contrôles réguliers	Détection des accès frauduleux/illégitimes ; analyse automatique des journaux recommandée

(CNIL, rappel mesures de sécurité et confidentialité, 9 févr. 2024)

2.2 Hébergement des données (HDS)

Tout hébergement de données de santé à caractère personnel, **lorsqu'il est assuré par un prestataire externe / cloud pour le compte de l'établissement**, doit l'être par un prestataire **certifié HDS** (art. L. 1111-8 du Code de la santé publique ; Décret n° 2018-137 du 26 février 2018, Légifrance). L'établissement qui héberge lui-même son propre système d'information de santé n'est pas soumis à cette obligation de certification ; en revanche, tout recours à un prestataire/cloud pour traiter ou stocker une trame contenant des données de santé identifiantes exige un hébergeur HDS et un contrat de sous-traitance.

2.3 Communication à des tiers autorisés (famille notamment)

Avant toute réponse à un tiers, vérifier la demande écrite, le fondement légal, la qualité du tiers, le respect du secret professionnel, la sécurisation de l'échange et la traçabilité (CNIL, guide « Tiers autorisés »).

La famille n'est pas automatiquement destinataire des informations du résident. La communication ne se fait que selon un cadre applicable : consentement du résident (ou de son représentant légal / tuteur), personne expressément habilitée, obligation légale, ou partage strictement nécessaire à la prise en charge dans les limites de l'art. L. 1110-4 CSP.

3. Recommandations CNIL sur l'usage de l'IA générative avec des données de santé / administratives

La CNIL recommande une **vigilance maximale** sur les données soumises à un système d'IA générative (CNIL, Q/R sur l'utilisation d'un système d'IA générative).

3.1 Principe : ne pas saisir de données personnelles

- « Éviter autant que possible la saisie de données personnelles. »
- Les utilisateurs ne devraient soumettre que des informations qu'ils sont **autorisés à partager**.
- **Ne jamais partager** d'informations confidentielles (données personnelles, données de l'administration, données couvertes par un secret comme le secret médical ou des obligations de déontologie) dans un service grand public.

3.2 Précautions techniques et organisationnelles

- **Choisir le système selon le besoin** et le niveau de risque.
- Pour des données personnelles ou sensibles : privilégier un déploiement **« sur site » (on premise)** ou une infrastructure sécurisée par **contrat de sous-traitance** (avec hébergeur HDS).
- **Désactiver la réutilisation des données d'usage** par le fournisseur (s'opposer à la réutilisation, voire à l'enregistrement de l'historique).
- Ne jamais reproduire telles quelles les sorties de l'IA.
- Précéder l'usage d'une **analyse des risques** et d'une stratégie de gouvernance ; associer le **DPO** et réaliser une **AIPD** le cas échéant.
- Encadrer l'usage par une **charte interne** (usages autorisés/interdits), former les utilisateurs et mener des contrôles réguliers.

3.3 Le point critique pour une trame de planning

Une trame saisie dans une IA générative grand public expose les données à la **mémorisation/ré-infusion** par le modèle. La règle de prudence est donc de **ne pas saisir de données personnelles** dans un service grand public ; si un traitement par IA est malgré tout envisagé, privilégier une **trame générique ou réellement anonymisée.** À défaut d'anonymisation réelle (qui a un sens juridique strict), la **pseudonymisation** reste une donnée personnelle soumise au RGPD (CNIL, « Tenir compte de la protection des données dans la collecte et la gestion des données »).

> **Alerte CNIL :** « une pseudonymisation n'est pas une anonymisation : effacer les noms et prénoms des personnes concernées ne suffit pas à anonymiser les données » (CNIL, délib. n° 2020-081, Légifrance). Le simple masquage du nom n'exclut donc pas une donnée du régime des données personnelles.

4. Vérification de la trame de planning (étape 2) — points de vigilance

4.1 Trame non récupérée — vérification directe non réalisée

La trame de planning produite à l'étape 2 **n'a pas pu être retrouvée** dans les sessions antérieures indexées (recherche effectuée sur les sessions des semaines de juillet 2026 et sur `asset_index.md`). En l'absence du document réel, **la vérification ligne par ligne de l'absence de données identifiantes n'a donc pas pu être réalisée sur la trame effective.**

Pour réaliser cette vérification, deux options :

1. me transmettre la trame (coller le tableau ou joindre le fichier) pour un contrôle ligne par ligne ;
2. appliquer soi-même la **grille de contrôle ci-dessous** (§ 4.3) avant toute utilisation / saisie dans un outil d'IA.

4.2 Trame modèle générique (sans donnée personnelle, utilisable comme gabarit)

Cette trame ne contient **aucune donnée identifiante** de résident (gabarit générique, et non une trame « anonymisée » de données réelles — l'anonymisation a un sens juridique strict) :

Créneau / Jour	Type de tâche	Pôle / Service	Intervenant (fonction)	Lieu	Statut
Lun. 08:00–09:00	Accueil familles / RDV	Accueil	Secrétariat	Hall	Planifié
Lun. 09:30–11:00	Préparation plannings soins	Soins	Secrétariat médical	Bureau	En cours
Lun. 14:00–15:30	Relances transports / ambulanciers	Logistique	Secrétariat	Bureau	À faire
Mar. 10:00–12:00	Saisie courriers / courrier départ	Administration	Secrétariat	Bureau	Planifié
Mar. 14:00–16:00	Mise à jour agenda médecin coordonnateur	Soins	Secrétariat médical	Bureau	À faire
Mer. 09:00–10:30	Gestion rendez-vous spécialistes	Soins	Secrétariat médical	Bureau	Planifié
Mer. 11:00–12:00	Tri / classement dossiers administratifs	Administration	Secrétariat	Archivage	En cours
Jeu. 08:30–10:00	Télétransmission / facturation	Administration	Secrétariat	Bureau	À faire

Créneau / Jour	Type de tâche	Pôle / Service	Intervenant (fonction)	Lieu	Statut
Jeu. 14:00–15:00	Réunion équipe (synthèse anonymisée)	Soins	Secrétariat + cadre	Salle réunion	Planifié
Ven. 09:00–11:00	Relances consentements / documents à jour	Administration	Secrétariat	Bureau	À faire

Pourquoi elle est conforme : aucun nom/prénom de résident, aucune date de naissance, aucun n° de dossier, aucun n° de chambre, aucune pathologie, aucun n° de sécurité sociale, aucun identifiant. Les cellules décrivent des tâches, pas des personnes.

4.3 Grille de contrôle à appliquer à la vraie trame

À vérifier avant impression, partage ou saisie dans un outil d'IA :

- [ ] **Aucun nom ni prénom** de résident (ni complet, ni initiale seule si elle permet la réidentification).
- [ ] **Aucun n° de chambre** rattachable à un résident (le n° de chambre + un créneau = réidentification facile en EHPAD).
- [ ] **Aucune date de naissance**, âge précis ou n° de sécurité sociale.
- [ ] **Aucun n° de dossier / IEP / identifiant interne**.
- [ ] **Aucune mention de pathologie, traitement ou motif de soins** (données de santé couvertes par l'art. 226-13 CP et art. L. 1110-4 CSP).
- [ ] **Aucun nom de famille apparenté / tuteur** identifiable.
- [ ] Si pseudonymisation (code résident type R-01) : le fichier de correspondance code ↔ identité est stocké **à part**, sous accès restreint, jamais dans la même trame.
- [ ] La trame ne circule que par canal sécurisé et est stockée sur un outil conforme (HDS pour les données de santé).
- [ ] Les habilitations d'accès au fichier suivent le « besoin d'en connaître » et sont tracées.

4.4 Points de vigilance spécifiques à signaler

1. **N° de chambre = donnée identifiante en EHPAD.** Dans un établissement de 120 résidents, le couple « chambre + créneau » identifie souvent directement la personne : à exclure de toute trame saisie en IA.
2. **Pseudonymisation ≠ anonymisation (rappel CNIL).** Remplacer « Mme Dupont » par « Résidente A » ne suffit pas si « Résidente A » reste rattachée à sa chambre, son âge ou son motif de RDV.
3. **Saisie en IA grand public = risque de ré-infusion.** Même une trame pseudonymisée saisie dans un outil grand public peut être mémorisée et ré-émise : respecter les recommandations CNIL (on premise / HDS, désactivation de la réutilisation des données d'usage, charte interne, DPO/AIPD).

4. **Secret partagé strictement limité.** Le secrétariat ne reçoit que ce qui relève de sa mission (gestion des RDV, administration) ; toute diffusion d'éléments médicaux hors équipe de soins est constitutive du délit de l'art. 226-13 CP.
5. **Traçabilité obligatoire** des accès et des communications à des tiers autorisés (famille, autorités).

Sources

- Art. 226-13 du Code pénal — De l'atteinte au secret professionnel (Légifrance)
- Art. L. 1110-4 du Code de la santé publique (Légifrance)
- Art. L. 1110-4 et L. 1110-12 CSP — Secret partagé / équipe de soins (Légifrance)
- Cass. soc., 1er décembre 2015, 14-22.133 — Secret médical absolu (Légifrance)
- CNIL, délibération n° 2020-081 du 18 juin 2020 — Accès du secrétariat, pseudonymisation ≠ anonymisation (Légifrance)
- CNIL — Données de santé : mesures de sécurité et confidentialité d'accès au dossier patient (9 févr. 2024)
- CNIL — Qu'est-ce qu'une donnée de santé ?
- CNIL — Q/R sur l'utilisation d'un système d'IA générative
- CNIL — Tenir compte de la protection des données dans la collecte et la gestion des données
- CNIL — Tiers autorisés : guide pratique et recueil de procédures
- Certification HDS — art. L. 1111-8 du Code de la santé publique (Agence du Numérique en Santé)
- Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé (Légifrance)