Respect du RGPD dans les établissements de santé

Rapport d'enquête 2025

Introduction

Dans le cadre de notre mission de protection des droits des patients et de promotion de la transparence, notre association a conduit une enquête approfondie visant à évaluer le respect du Règlement Général sur la Protection des Données (RGPD) au sein des établissements de santé.

Entré en vigueur le 25 mai 2018, le RGPD impose des obligations strictes en matière de collecte, de traitement et de sécurisation des données personnelles, notamment dans le secteur de la santé où les informations sensibles abondent.

Cette enquête, menée entre [période à préciser], a couvert un échantillon de [nombre] établissements publics et privés à travers [région/pays]. Les résultats révèlent des manquements préoccupants qui compromettent la protection des données des patients.

Méthodologie

L'enquête a combiné plusieurs approches :

- Analyse des politiques de confidentialité et des procédures internes des établissements.
- Entretiens avec des responsables de la protection des données (DPO) et des membres du personnel.
- Étude des plaintes déposées par les patients auprès des autorités compétentes.
- Vérification des mesures techniques et organisationnelles mises en place pour sécuriser les données.

CONSTATS PRINCIPAUX

Les principaux constats

1

Absence ou insuffisance de formation du personnel

Dans plus de [pourcentage]% des établissements étudiés, le personnel soignant et administratif n'a pas reçu de formation adéquate sur le RGPD. Cette lacune entraîne des erreurs fréquentes, comme la divulgation non autorisée de données personnelles ou l'utilisation inappropriée de systèmes informatiques.

2

Manque de transparence envers les patients

Une majorité des structures auditées ([pourcentage]%) omet d'informer clairement les patients sur l'utilisation de leurs données, en violation de l'article 13 du RGPD. Les formulaires de consentement sont souvent absents, incomplets ou rédigés dans un langage trop technique.

3

Failles dans la sécurisation des donnée.

Des systèmes informatiques obsolètes ou mal protégés ont été identifiés dans [pourcentage]% des cas. Plusieurs établissements ne respectent pas les standards minimaux de chiffrement ou de contrôle d'accès, exposant les dossiers médicaux à des risques de piratage ou de fuites.

4

Gestion défaillante des violations de données

En cas de breach (violation de données), seuls [pourcentage]% des établissements ont notifié l'autorité de protection des données dans les 72 heures, comme l'exige le RGPD. Certains incidents n'ont même pas été documentés ni signalés aux patients concernés.

Conséquences pour les patients

Ces manquements exposent les patients à des risques graves : usurpation d'identité, discrimination liée à la divulgation de données de santé, ou encore perte de confiance envers le système médical. Ils traduisent également un mépris des droits fondamentaux à la vie privée et à la protection des données, garantis par la législation européenne.

RECOMMANDATIONS

Recommandations

Face à ces constats alarmants, notre association propose les mesures suivantes :

1. **Renforcement de la formation** : Mettre en place des programmes obligatoires et réguliers pour sensibiliser le personnel au RGPD.

2. **Mise à jour des infrastructures** : Investir dans des systèmes sécurisés et conformes aux normes actuelles.

3. **Amélioration de la communication** : Fournir aux patients des informations claires et accessibles sur leurs droits et l'usage de leurs données.

4. **Contrôles réguliers** : Instaurer des audits indépendants pour garantir la conformité des établissements.

Ces recommandations tiennent compte du fait que la présence d'une charte ou politique de confidentialité sur le site web est un premier pas, mais insuffisant si son contenu ne respecte pas le RGPD ou ne correspond pas aux pratiques réelles.

Le chiffre de 73 % de non-conformité ou d'omissions met en évidence un problème systémique : trop souvent, ces documents servent de façade plutôt que de véritable engagement. En alignant formation, infrastructures, communication et contrôles sur une exigence de cohérence entre les déclarations en ligne et les actions concrètes, les établissements pourront restaurer la confiance des patients et se conformer pleinement à la législation.

Chacune de ces recommandations va être détaillée :

Recommandation n°1

Renforcement de la formation

Pour garantir une application effective du RGPD, il est impératif de mettre en place des programmes de formation obligatoires et réguliers à destination de l'ensemble du personnel (soignants, administratifs, informaticiens).

Ces sessions doivent inclure une sensibilisation aux exigences du RGPD, notamment sur la collecte, le traitement et la sécurisation des données personnelles.

Un accent particulier doit être mis sur l'interprétation et la mise en œuvre des chartes ou politiques de confidentialité publiées sur les sites web des établissements.

Notre enquête a révélé que, dans 73 % des cas, ces documents existaient mais présentaient des non-conformités (termes vagues, absence de mention des droits des patients) ou des omissions (durée de conservation des données, identité du DPO).

La formation doit donc également enseigner au personnel comment aligner les pratiques internes avec les engagements publics affichés, sous peine de créer une dissonance préjudiciable à la confiance des patients.

Objectif

Sensibiliser et former l'ensemble du personnel aux exigences du RGPD, y compris à l'application cohérente des chartes ou politiques de confidentialité publiées en ligne.

Moyens

- **Programmes de formation obligatoires :** Sessions animées par des experts en protection des données (juristes, DPO externes), couvrant les bases du RGPD, les droits des patients, et les bonnes pratiques de gestion des données. Une section spécifique portera sur l'analyse des chartes existantes, souvent non conformes dans 73 % des cas (ex. : absence de mention des droits d'opposition ou de portabilité).

- **Modules e-learning :** Mise à disposition d'une plateforme en ligne avec des quiz et mises en situation (ex. : comment réagir à une demande d'accès aux données d'un patient), accessible à tout moment pour les nouveaux employés ou comme rappel annuel.

- **Ateliers pratiques :** Simulations de cas réels (ex. : rédiger une réponse conforme à une charte corrigée) pour le personnel administratif et soignant.

Calendrier

- **0-3 mois :** Élaboration des contenus avec des experts et lancement d'un programme pilote dans 10 % des établissements.
- **3-12 mois :** Déploiement à l'échelle nationale, avec au moins une session en présentiel par employé et accès au e-learning.
- **12 mois et au-delà :** Formation annuelle obligatoire, avec évaluation des connaissances via un test certifiant.

Recommandation n°2

Mise à jour des infrastructures

Les établissements doivent investir dans des systèmes informatiques sécurisés et conformes aux normes actuelles (chiffrement des données, authentification renforcée, pare-feu modernes).

Ces améliorations techniques sont essentielles pour protéger les données sensibles des patients, mais elles doivent aussi refléter les promesses faites dans les politiques de confidentialité en ligne.

Dans 73 % des cas, les chartes consultées mentionnaient des mesures de sécurité "adaptées" ou "renforcées", mais ces engagements étaient contredits par des infrastructures obsolètes ou mal protégées.

Une politique de confidentialité non suivie d'effets concrets constitue une violation du principe de transparence du RGPD. Nous recommandons donc un audit technique préalable pour identifier les écarts entre les déclarations publiques et la réalité, suivi d'un plan de modernisation ciblé.

Objectif

Aligner les systèmes informatiques sur les normes de sécurité actuelles et les engagements des chartes en ligne, souvent contredits par des failles techniques.

Moyens

- **Audit technique** : Réalisation par des cabinets spécialisés en cybersécurité pour identifier les vulnérabilités (ex. : absence de chiffrement, serveurs obsolètes), avec un focus sur les écarts entre les promesses des chartes (73 % non conformes ou incomplètes) et la réalité.

- **Investissements ciblés :** Acquisition de logiciels de gestion sécurisés (ex. : dossiers patients électroniques avec authentification multi-facteurs), mise à jour des serveurs, et installation de pare-feu avancés. Budget estimé : 50 000 à 200 000 € par établissement selon sa taille.

- **Partenariats publics-privés :** Subventions gouvernementales ou collaboration avec des entreprises technologiques pour réduire les coûts.

Calendrier

- **0-6 mois** : Audit complet des infrastructures dans tous les établissements concernés.
- **6-18 mois** : Mise en œuvre progressive des mises à jour (priorité aux établissements les plus vulnérables).
- **18-24 mois** : Vérification post-implémentation par un second audit pour certifier la conformité.

Recommandation n°3

Amélioration de la communication

Les établissements doivent fournir aux patients des informations claires, accessibles et exhaustives sur leurs droits (accès, rectification, suppression des données) et sur l'utilisation de leurs informations personnelles,

conformément à l'article 13 du RGPD. Cette obligation s' étend aux chartes ou politiques de confidentialité présentes sur leurs sites web.

Notre constat montre que, bien que 73 % des établissements disposent d'une telle charte, elles sont souvent incomplètes (absence de base légale explicite pour le traitement des données) ou rédigées dans un jargon juridique incompréhensible pour le grand public.

Nous préconisons une révision systématique de ces documents par des experts en protection des données, avec une attention particulière portée à la lisibilité et à l'exhaustivité (mention des finalités, des destinataires, des délais de conservation).

Une version simplifiée pourrait être proposée en complément pour les patients moins familiers avec ces questions.

Objectif

Garantir une information claire et accessible aux patients, en révisant les chartes ou politiques de confidentialité pour corriger les 73 % de non-conformités ou omissions.

Moyens

- **Révision des chartes :** Embauche de consultants juridiques pour réécrire les politiques en ligne, en incluant les mentions obligatoires (finalités du traitement, identité du DPO, délais de conservation, procédures en cas de violation) absentes ou floues dans 73 % des cas.

- **Double format :** Publication d'une version complète conforme au RGPD et d'une version simplifiée (ex. : infographie ou FAQ) pour les patients, disponible sur le site web et en version papier dans les établissements.

- **Campagne d'information :** Affichage dans les salles d'attente, courriels aux patients, et tutoriels vidéo expliquant leurs droits (ex. : comment demander la suppression de données).

Calendrier

- **0-4 mois :** Révision et validation des nouvelles chartes par des experts.
- **4-8 mois :** Mise en ligne des versions corrigées et distribution des supports simplifiés.
- **8-12 mois :** Campagne de sensibilisation et collecte des retours patients pour ajustements.

Recommandation n°4

Contrôles réguliers

Pour assurer une conformité continue, des audits indépendants doivent être instaurés, réalisés par des organismes externes ou des autorités compétentes comme la CNIL.

Ces contrôles devraient inclure une vérification spécifique des chartes ou politiques de confidentialité disponibles sur les sites web, afin de s'assurer qu'elles reflètent les pratiques réelles de l' établissement et respectent les exigences du RGPD. Le fait que 73 % de ces documents présentent des non-conformités ou des omissions (par exemple, l'omission des procédures en cas de violation de données) souligne l'urgence de cette mesure.

Les résultats de ces audits devraient être rendus publics dans un souci de transparence et assortis de plans d'action correctifs avec des délais stricts pour les établissements en infraction.

.

Objectif

Assurer une conformité durable via des audits indépendants, avec un focus sur la cohérence entre les pratiques et les chartes en ligne.

Moyens

- **Audits externes :** Contrats avec des organismes certifiés (ex. : cabinets d'audit ou associations spécialisées) pour évaluer annuellement chaque établissement. Ces audits incluront une analyse des chartes web (73 % problématiques) et des tests pratiques (ex. : simulation de violation de données).

- **Sanctions et suivi :** Transmission des résultats à la CNIL avec demande de sanctions en cas de non-conformité persistante, assortie d'un plan d'action imposé (ex. : délai de 6 mois pour corriger les écarts).

- **Publication des résultats :** Rapport annuel public résumant les progrès et les manquements, pour maintenir la pression sur les établissements.

Calendrier

- **0-6 mois :** Mise en place d'un cadre d'audit avec les autorités et sélection des organismes.
- **6-18 mois :** Premier cycle d'audits complet dans tous les établissements.
- **18 mois et au-delà :** Audits annuels systématiques, avec rapports publics chaque mars.

Justification

Ces recommandations s'appuient sur des moyens réalistes (expertise externe, outils numériques, financements mixtes) et un calendrier progressif pour permettre une mise en œuvre sans paralyser les établissements.

La prise en compte des chartes non conformes (73 %) renforce l'urgence d'agir sur la cohérence entre les engagements publics et les pratiques internes, un enjeu clé pour restaurer la confiance des patients.

CONCLUSIONS

Conclusions

L'enquête menée par notre association citoyenne et de défense des patients met en lumière des manquements inquiétants, voire systémiques, dans le respect du Règlement Général sur la Protection des Données (RGPD) au sein des établissements de santé. Ces lacunes ne se limitent pas à de simples écarts administratifs ou à des erreurs isolées : elles révèlent une négligence profonde dans la gestion des données personnelles, un domaine pourtant crucial dans le secteur médical où la confidentialité et la trust sont des piliers fondamentaux. Les failles identifiées – qu'il s'agisse de systèmes informatiques vulnérables, de chartes de confidentialité inadéquates dans 73 % des cas, ou d'un manque criant de formation – exposent les patients à des risques concrets : piratage de leurs dossiers médicaux, utilisation abusive de leurs informations sensibles, voire atteinte à leur vie privée par des fuites non maîtrisées. Ces dérives ne sont pas seulement des infractions réglementaires : elles constituent une menace directe à la sécurité, à la dignité et à l'autonomie des individus, sapant la relation de confiance essentielle entre les patients et le système de santé.

Face à cette situation alarmante, nous adressons un appel urgent aux autorités compétentes, en particulier à la Commission Nationale de l'Informatique et des Libertés (CNIL), pour qu'elles intensifient leurs efforts de contrôle et adoptent une posture plus ferme. Des inspections régulières, des sanctions dissuasives – financières ou juridiques – et des injonctions claires doivent être mises en œuvre sans délai pour contraindre les établissements fautifs à se conformer aux exigences du RGPD. Il ne s'agit pas seulement de punir, mais de prévenir : chaque violation non corrigée est une porte ouverte à de nouvelles atteintes aux droits des citoyens. Nous demandons également que les résultats de ces contrôles soient rendus publics, afin que les patients puissent eux-mêmes juger de la fiabilité des structures qu'ils fréquentent.

Association SENTINELLE DUARTE - loi 1901
https://www.sentinelle-duarte.fr

Conclusions

Par ailleurs, nous invitons les citoyens à jouer un rôle actif dans cette bataille pour la protection de leurs données. Rester vigilants, c'est se renseigner sur leurs droits – accès, rectification, suppression – et les exercer pleinement. C'est aussi signaler sans hésiter toute anomalie, qu'il s'agisse d'une communication floue sur l'usage de leurs informations, d'une charte en ligne douteuse, ou d'une suspicion de fuite de données, auprès des établissements ou directement à la CNIL. Cette mobilisation collective est essentielle pour faire pression sur les acteurs de la santé et les pousser à assumer leurs responsabilités. Enfin, notre association s'engage à poursuivre son travail de veille et d'accompagnement, en mettant à disposition des ressources pédagogiques et un espace de signalement pour soutenir les patients dans cette démarche.

En somme, les manquements constatés ne sont pas une fatalité : ils peuvent et doivent être corrigés par une action concertée des pouvoirs publics, des établissements de santé et des citoyens eux-mêmes. Le respect du RGPD n'est pas une option, mais une obligation morale et légale, garante d'un système de santé digne de ce nom. L'heure n'est plus aux constats, mais à l'action : nous ne pouvons tolérer que la protection des données personnelles reste un vœu pieux dans un secteur où chaque faille peut avoir des conséquences humaines irréversibles.

SENTINELLE DUARTE

Association loi 1901

http://www.sentinelle-duarte.fr