Shred-it®
Une Solution Stericycle®

Élimination sécurisée des données. Protégez vos patients et l'environnement

Un guide sur la sécurité de l'information

Nous protégeons ce qui compte.

Sommaire.

Introduction.

La protection des données sensibles est plus qu'une obligation légale.

Bien que nous soyons tous familiers avec la législation sur le RGPD et ses directives en constante évolution en matière de protection des données, en raison du grand nombre de documents en circulation au sein d'une établissement de santé, décider ce qu'il faut détruire peut être un défi.

Les risques peuvent être importants si des informations sensibles sur les patients ou des données commerciales sont mal conservées, éliminées de manière inappropriée, ou compromises.

Que vous soyez un prestataire du NHS ou une organisation de soins de santé privée, la responsabilité incombe à chacun de traiter et de protéger les données personnelles conformément aux principes rigoureux de la protection des données. Continuez votre lecture pour découvrir les risques potentiels auxquels vous pourriez être confronté et comment assurer la protection de votre organisation, de vos patients et de vos collaborateurs tout en contribuant à lutter contre la crise climatique.

La loi et la destruction sécurisée des fichiers confidentiels.

Réagir rapidement aux évolutions législatives et aux conseils en matière de protection des données peut être un défi. Plus nous conservons d'informations, plus il peut être difficile de rester conforme.

Les nouveaux projets de loi et les orientations réglementaires en matière de traitement, de stockage et de protection des données personnelles des citoyens de l'UE et de la France peuvent rapidement impacter les processus internes de gestion des documents des entreprises et organisations

- La Loi sur la protection des données
- Le règlement général sur la protection des données (RGPD)
- La commission Nationale Informatique & Libertés (CNIL)
- Droit d'accès à ses données personnelles

Reporter la destruction de documents obsolètes, conserver des papiers indéfiniment ou les stocker, voire les éliminer dans des bacs de recyclage, peut exposer votre organisation aux violations de données et aux sanctions financières.

La Commission Nationale Informatique & Libertés recommande la destruction sécurisée pour éliminer les documents papier. En travaillant avec des professionnels de la destruction d'informations, vous vous assurez que votre organisation bénéficie d'une chaîne de contrôle sécurisée pour vos informations sensibles et qu'elle est en conformité avec les règles de protection des données en constante évolution.

Comprendre les risques.

Les violations de données et le recyclage sans destruction sécurisée préalable peuvent avoir un impact sur votre activité.

Pertes financières

Les violations de données peuvent entraîner des pertes financières en raison des coûts de notification des personnes affectées, des amendes de la Commission Nationale Informatique & Libertés; et de la mise en conformité aux exigences réglementaires.

Atteinte à la réputation

Outre l'interruption des activités, une violation de données pourrait réduire la confiance des clients et nuire à votre réputation.

Responsabilité juridique

Vos sites peuvent être tenus de verser une indemnisation aux personnes concernées par une violation de données.

Élimination non sécurisée

Laisser des documents dans un bac de recyclage non sécurisé peut sembler respectueux de l'environnement, mais des informations importantes et confidentielles peuvent être compromises si elles sont récupérées dans ce bac.

Nous protégeons ce qui compte.

Erreurs de sécurité des données pouvant compromettre les informations confidentielles.

Les informations confidentielles stockées dans les dossiers des patients, les notes de rendez-vous, les radiographies et les dossiers d'IRM doivent être protégées contre les tiers malveillants et détruites lorsqu'elles ne sont plus nécessaires.

Laisser vos données exposées

Protégez et sauvegardez toujours les informations privées lorsqu'elles sont visibles dans les espaces publics : par exemple, les informations sensibles non classées laissées sur les bureaux et les écrans d'ordinateurs portables clairement visibles par tous.

Accumuler des disques durs

Au lieu de stocker ou de mettre au rebut vos anciens disques durs, clés USB, CD, etc., déchiquetez et détruisez vos supports numériques et électroniques en toute sécurité afin que toute récupération de données soit impossible.

Déchiqueteuses de bureau

Les déchiqueteuses de bureau monopolisent le temps précieux d'un collaborateur et génèrent des coûts de manutention importants. De plus le risque que les collaborateurs aient accès à des documents hautement sensibles auxquels ils ne devraient normalement pas accéder est alors présent.

Manque de formation des employés

Selon une étude[1], 58 % des entreprises craignent que leurs employés ne connaissent pas les meilleures pratiques pour prévenir une violation de données - aidez vos employés à mieux comprendre leur rôle dans la sécurisation de votre entreprise.

Défis auxquels font face établissements de santé.

La protection des informations sensibles devient de plus en plus complexe pour les établissements de santé et les entreprises, suscitant des préoccupations quant aux conséquences qu'une violation de données pourrait avoir sur leurs patients et clients.

Une étude indépendante portant sur la perception de 500 chefs d'entreprise en France a mis en évidence des préoccupations concernant la sécurité des données sensibles et les risques potentiels de violations.

En ce qui concerne le RGPD et la conformité réglementaire, les personnes interrogées évoquent la complexité des réglementations et des exigences en matière de protection des données, tout en reconnaissant la nécessité impérieuse d'améliorer la sécurité des données.

Les résultats de l'étude ont révélé que :

87%

des personnes interrogées estiment qu'il est difficile de protéger les données sensibles de leur entreprise

41%

des personnes interrogées ont été victimes d'une violation de données au sein de leur entreprise

64%

des personnes interrogées craignent que l'on n'accorde pas assez d'importance à la sécurité des informations physiques

71%

craignent l'impact qu'une violation de données aura sur leurs clients

*Données internes à Shred-it

Développement durable: aligner la protection des données sur les objectifs de neutralité carbone

La plupart des organismes de soins de santé se sont fixés des objectifs destinés à agir contre le changement climatique et à les aider à atteindre la neutralité carbone. Pour atteindre ces objectifs, il est essentiel d'utiliser des pratiques sûres et durables dans tous les aspects de vos activités.

La durabilité est fermement inscrite à l'ordre du jour national et le public se tourne de plus en plus vers les organisations pour aider à résoudre les problèmes environnementaux majeurs.

La loi française Climat et Résilience vise à :

- Réduire les émissions de gaz à effet de serre d'au moins 55 % d'ici à 2030

L'une des façons pour le secteur de la santé de se mobiliser et d'assumer ses responsabilités consiste à adopter une approche équilibrée de la réduction des émissions de gaz à effet de serre, tant au sein des organisations que dans l'ensemble de ses chaînes d'approvisionnement. De nombreuses organisations de soins de santé disposent désormais de politiques ESG qui comprennent des détails sur les mesures qu'elles prennent pour améliorer les résultats environnementaux.

La destruction et le recyclage sécurisés des données complètent les initiatives en matière de développement durable en faisant en sorte que le papier déchiqueté se retrouve dans l'économie circulaire. Les organisations peuvent respecter les réglementations en matière de protection des données et témoigner de leurs émissions relevant du champ d'application 3 relatives à la collecte et au déchiquetage du papier dans la catégorie Biens et services achetés.

Mesures concrètes : ce que vous pouvez faire dès maintenant.

Prenez des mesures immédiates pour protéger les informations confidentielles et intégrer des pratiques durables dans votre organisation. Explorez les points suivants qui peuvent faire l'objet d'une action:

Avis de confidentialité :

Élaborez un avis de confidentialité complet décrivant vos engagements en matière de protection des données et informant les individus de leurs droits.

Expliquez comment et pendant combien de temps les données personnelles seront conservées avant d'être éliminées ou détruites, y compris celles figurant dans les dossiers papier.

Politique de conservation :

Gérez les dossiers physiques et expliquez le processus de suppression/destruction.

Politiques sur le lieu de travail :

Mettez en œuvre des structures de travail robustes sensibilisant les employés à la sécurité de l'information.

Favorisez une culture de responsabilité et de vigilance.

Considérez la nécessité de politiques atténuant les risques de sécurité liés aux dossiers physiques.

Stockage sécurisé :

Protégez les informations sensibles en utilisant des solutions de stockage sécurisées comme des armoires fermées à clé, des zones d'accès restreint et un stockage numérique crypté.

Tenez compte des risques liés aux différents supports tels que le papier ou les disques durs.

Formation du personnel :

Investissez dans des programmes complets de formation du personnel pour sensibiliser les employés aux meilleures pratiques en matière de sécurité de l'information.

Donnez à votre personnel les moyens d'être le premier mécanisme de protection et assurez-vous que les politiques et les normes sont mises en œuvre et respectées.

Destruction sécurisée :

Associez-vous à un fournisseur de services de destruction sécurisée de confiance, tel que Shred-it.

Veillez à ce que vos documents confidentiels soient traités en toute sécurité, détruits de manière efficace et recyclés de manière responsable.

Comment un prestataire de services de destruction sécurisée peut vous aider

Une collaboration avec un prestataire de services de destruction sécurisée, tel que Shred-it, peut vous permettre de découvrir les meilleures pratiques en accord avec les engagements de votre organisation en matière de conformité et de durabilité, de manière rentable et sécurisée.

Collectes régulières ou ponctuelles

Déchiquetage sur site ou hors site

- Chaîne de contrôle sécurisée
- Certificat de destruction
- Recyclage de l'ensemble du papier déchiqueté

Shred-it®
Une Solution Stericycle®

Appelez le **0800 844 848**

Visitez notre site web: **shredit.fr**

Contactez-nous dès aujourd'hui et franchissez la prochaine étape vers la construction d'un cadre de sécurité de l'information résilient qui contribue à protéger la réputation de votre organisation, maintient la confiance, assure la conformité et participe à votre démarche vers la neutralité carbone.

[1]:Rapport sur la protection des données Shred-it 2022

[2]: Données internes à Shred-it, 2022

Nous protégeons ce qui compte.