PROTECTION DES DONNÉES DE SANTÉ : LA CHECKLIST DE MISE EN CONFORMITÉ

Lorsque le Règlement général sur la protection des données (RGPD) et le Data Protection Act (DPA) sont entrés en vigueur en 2018, les entreprises entretenant des relations commerciales avec des citoyens de l'Union européenne et du Royaume-Uni ont dû agir dans l'urgence pour se conformer aux exigences de confidentialité imposées par ces nouvelles réglementations. Depuis, plusieurs autres législations européennes sur la protection des données ont été proposées et/ou mises en application : la Loi sur la gouvernance des données, le Règlement sur les données, la Directive sur la sécurité des réseaux et des systèmes d'information (SRI) et, plus récemment, le Règlement pour un espace européen des données de santé (EHDS).

D'où la question que tous les acteurs de la santé se posent : comment rester conforme à un cadre réglementaire si dense et si changeant ? En appliquant les bonnes pratiques reconnues, mais aussi en utilisant des technologies garantes de la conformité des processus et de la sécurité des données de santé, maintenant et pour longtemps*.

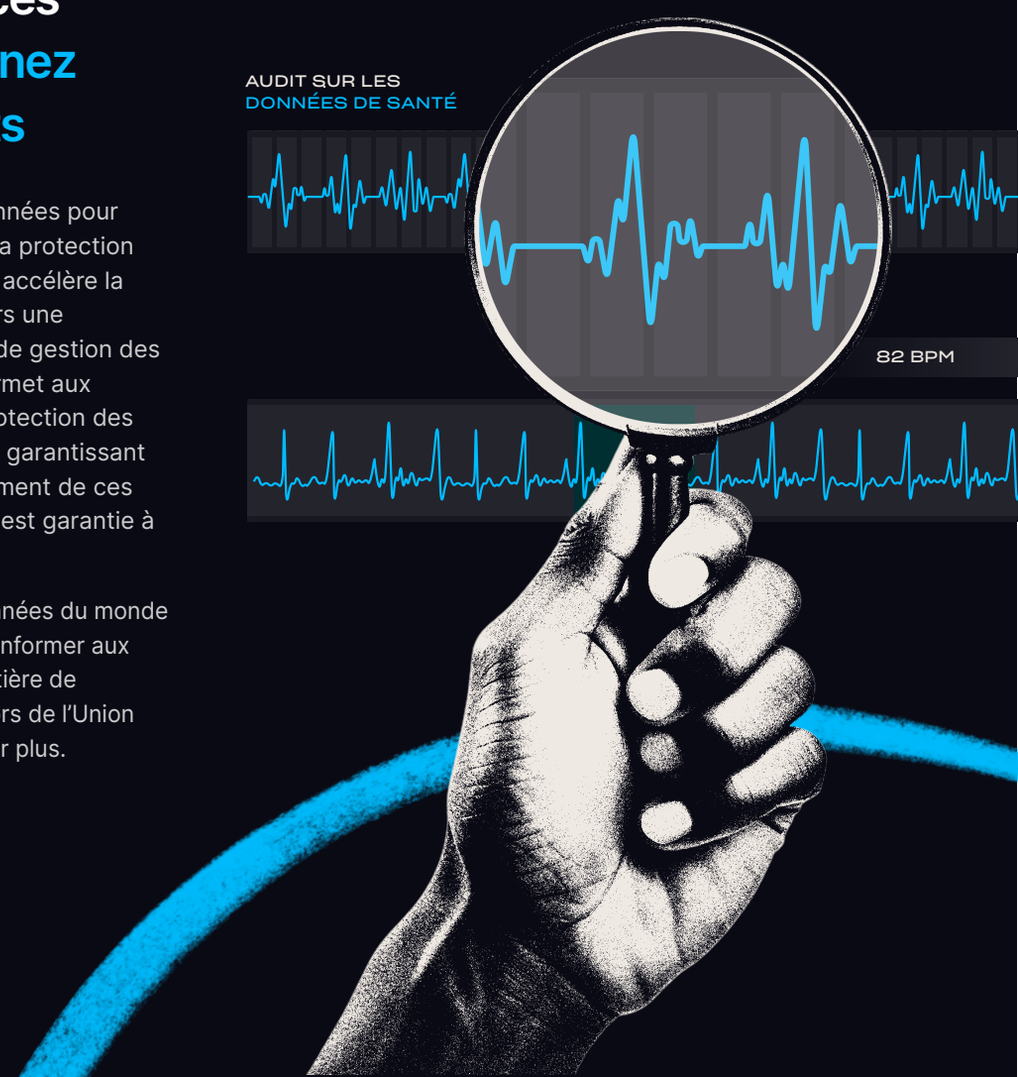
* NB : rien dans ces pages ne constitue un conseil d'ordre juridique. Nous vous recommandons de vous adresser à un avocat spécialisé dans le domaine de la protection des données, qui vous aidera à respecter les lois actuelles et futures en fonction de votre situation spécifique.

Respectez les exigences réglementaires et gagnez du temps sur les audits

Avec Rubrik, renforcez la sécurité des données pour mieux répondre aux réglementations sur la protection des données de santé. Rubrik simplifie et accélère la mise en conformité réglementaire à travers une plateforme unique, équipée de fonctions de gestion des données sur site et dans le cloud. Elle permet aux utilisateurs d'automatiser les règles de protection des données et les délais d'expiration, tout en garantissant une complète transparence sur l'emplacement de ces données et la manière dont la conformité est garantie à l'échelle de toute l'infrastructure.

Fidèle à sa mission de sécurisation des données du monde entier, Rubrik aide les organisations à se conformer aux réglementations actuelles et futures en matière de protection des données, au sein et en dehors de l'Union européenne. Contactez-nous pour en savoir plus.

Scannez pour en savoir plus



DONNÉES DE SANTÉ : LES 7 ÉTAPES DE LA CONFORMITÉ RÉGLEMENTAIRE

rubrik

1 Identifiez les rôles et les responsabilités

Définissez clairement les rôles et les responsabilités par écrit, en expliquant qui est responsable de chaque étape du processus de mise en conformité. Il s'agit par exemple de déterminer qui sera chargé d'identifier la manière dont les données de santé sensibles sont collectées et utilisées, comment les politiques et les contrôles facilitent l'utilisation et la distribution des données à caractère personnel, et comment les patients peuvent demander l'accès à leurs données de santé ou la suppression de celles-ci.

2 Procédez à une analyse des écarts de conformité

Étudiez les politiques actuelles de protection des données et leur mise en œuvre afin d'identifier les finalités du traitement, le type de données de santé que vous traitez, l'identité et les lieux de connexion des collaborateurs internes et des tiers autorisés à y accéder (p. ex. Epic, Cerner, McKesson, BigHealth), les mesures prises pour protéger ces données, et la durée de conservation prévue avant effacement automatique, le cas échéant. Comparez vos résultats aux exigences réglementaires actuelles et futures afin d'identifier les domaines d'action prioritaires.

3 Élaborez votre plan d'action

Établissez une liste des priorités, des étapes et des actions indispensables au respect des réglementations actuelles et futures en matière de protection des données de santé, en tenant compte de plusieurs critères : loi, sécurité, responsabilité, gouvernance et droit à la vie privée.

4 Obtenez l'adhésion de vos dirigeants

Sensibilisez les membres du conseil d'administration pour vous assurer de leur soutien dans la mise en place des changements nécessaires au respect des réglementations sur la protection des données. Les acteurs de la santé ont le devoir de prendre toutes les mesures nécessaires pour assurer la sécurité des données de santé, de leur propriété intellectuelle et autres données critiques. Ce n'est qu'à cette condition qu'ils pourront éviter de lourdes amendes, sans parler des atteintes à la réputation et des pertes de vies humaines.

5 Sensibilisation

Sensibilisez tous les collaborateurs de votre structure de santé (utilisateurs, équipes informatiques, dirigeants, etc.) aux changements imposés par les réglementations applicables et à leur propre responsabilité dans la protection des données. Les établissements de santé doivent former leurs employés à tous les aspects des principes de protection et des politiques internes de gestion des données pour garantir le respect les réglementations tout en préservant les données sensibles qui leur sont confiées.

6 Repensez les cadres de gouvernance de l'information

Veillez à la conformité de vos cadres de gouvernance de l'information (GI). Politiques de rétention, d'accès et de suppression des données ; procédures de gestion, de classification et de stockage ; protocoles de reprise après sinistre et de sécurité des informations sensibles sur supports numériques ou papier… effectuez une grande remise à plat de vos politiques GI. Cela passe notamment par une surveillance proactive pour identifier les vulnérabilités potentielles, les compromissions de données, les accès trop permissifs ainsi que les tentatives et procédures d'accès non autorisé, afin de vous conformer aux exigences actuelles (et futures).

7 Auditez, auditez, auditez

En établissant un calendrier d'audits réguliers, vous garantissez le respect des réglementations tout en protégeant les données sensibles confiées à votre organisation. Pour réaliser des audits réguliers, mais aussi simplifier et accélérer la conformité aux réglementations, envisagez de déployer une plateforme unique dotée de fonctions de gestion des données sur site et dans le cloud. Elle permettra aux utilisateurs d'automatiser les règles de protection des données et les délais d'expiration, tout en garantissant une complète transparence sur l'emplacement de ces données et la manière dont la conformité est garantie à l'échelle de toute l'infrastructure.