DONNÉES PERSONNELLES SENSIBLES

Alors que toutes les informations qui identifient ou peuvent être utilisées pour identifier un individu doivent être protégées contre les accès non autorisés, il existe une norme plus élevée en ce qui concerne les données sensibles. Les données sensibles sont des informations qui, si elles sont rendues publiques, peuvent entraîner des dommages importants tels que la discrimination, le vol d'identité ou la fraude financière. Vous trouverez ci-dessous quelques directives à suivre lorsque vous traitez des données sensibles.

SACHEZ POURQUOI VOUS L'AVEZ

- Connaître et documenter la ou les raisons pour lesquelles vous avez besoin de données sensibles avant de les collecter
- Ne collectez pas de données sensibles dont vous n'avez pas besoin
- Demandez à votre avocat de groupe si vous avez besoin d'un consentement avant de collecter des données sensibles
- N'utilisez pas de données sensibles à des fins nouvelles ou différentes sans vérifier auprès de votre avocat de groupe
- Complétez une DPIA avant de mettre en œuvre ou de modifier un fournisseur, un outil ou un processus qui utilise ou collecte des données sensibles

SÉCURISEZ-LE PHYSIQUEMENT

- Stockez les données sensibles dans un endroit sécurisé avec un accès limité
- Ne laissez pas les données sensibles sur votre bureau ou sans surveillance
- Examinez régulièrement les fichiers et sachez de quels types de données sensibles vous disposez
- Ne partagez pas les données sensibles avec quiconque n'est pas autorisé à les avoir ou n'a pas besoin de les connaître
- Ne faites pas de copies inutiles de données sensibles
- Eliminer les données sensibles par déchiquetage
- Ne prenez pas de photos de votre espace de travail si des données sensibles peuvent être consultées

SÉCURISEZ-LE ÉLECTRONIQUEMENT

- Stockez, transférez et traitez uniquement des données sensibles dans et sur des appareils, logiciels, serveurs et sites Web approuvés par l'informatique
- Ne conservez pas et n'accédez pas à des données sensibles sur des appareils personnels à moins d'avoir été préalablement approuvés par le service informatique
- Utilisez des mots de passe forts ou un cryptage lors du transfert ou du stockage de données sensibles
- Ne partagez pas et ne mettez pas à disposition vos identifiants de connexion ou vos clés de cryptage
- Ne stockez pas de données personnelles sur votre disque dur ou votre ordinateur de bureau
- Limitez les autorisations et l'accès aux données sensibles dans la mesure du possible
- N'accédez pas aux données sensibles à partir d'une connexion Wi-Fi publique non sécurisée

MINIMISER LA RÉTENTION

- Ne conservez pas les données sensibles indéfiniment
- Attribuer une période de conservation à toutes les données sensibles lors de leur réception
- Ne sauvegardez pas de données sensibles sur un appareil ou un site à moins qu'elles n'aient été approuvées au préalable par le service informatique

SIGNALER DES PROBLÈMES

- Soyez à l'affût des activités suspectes
- Ne répondez pas aux demandes de données sensibles par e-mail ou par téléphone, sauf si vous avez confirmé la légitimité de la demande par d'autres moyens
- Utilisez la page Evénements à signaler pour signaler tout problème, préoccupation ou violation de données sensibles
- Ne tardez pas à signaler les incidents impliquant des données sensibles

NOUS SOMMES RPM ET NOTRE SUCCÈS DÉPEND DE CHACUN DE NOUS SUIVANT LA BONNE VOIE ET ADOPTANT NOTRE VALEUR DE 168® POUR PRENDRE LES BONNES DÉCISIONS.

CONTACTEZ-NOUS : DATAPROTECTION@RPMINC.COM