LIVRE BLANC

RGPD : UN CADRE GENERAL QUI S'IMPOSE À TOUS LES ESMS

widip
Very Informatics People

EDITO

La SCOP WIDIP, est engagée depuis 2005 dans l'accompagnement des etablissements et services médico-sociaux sur l'évolution et la pérennité de leur patrimoine numérique. Hébergeur de serveurs, operateur réseau et intégrateur de logiciels, WIDIP a développé un haut niveau d'expertise dans la sécurité des systèmes d'information des établissements médico-sociaux et leur transition numérique.

Le sujet du Règlement général de protection des données (RGPD) souvent vécu comme une contrainte est au contraire l'occasion aux établissements de repenser leur stratégie numérique. Ce Livre Blanc sur le RGPD est un chapitre du livre à paraître en octobre, ***Etablissements et services médico-sociaux, réussir la transition numérique,*** co-écrit par Marc Perotto, Directeur Général de la SCOP WIDIP et Isabelle Bourdon, Maître de conférences à Polytech Montpellier.

QUI EST WIDIP :

WIDIP est une entreprise de services numériques (ESN) qui a développé une très forte expertise dans la mise en oeuvre de cloud privé (IAAS) interne ou externe pour les ESMS. Son offre s'appuie sur quatre datacentres et sur une équipe d'informaticiens certifiés Cisco, Citrix, Fortinet, Microsoft, Vmware. Une assistance téléphonique basée à Grenoble complète le dispositif.

WIDIP intervient également sur des prestations d'expertise et de conseil concernant la sécurité des systèmes d'information.

SOMMAIRE

1 Les grands principes du nouveau règlement..... 6

2 Quelles données, utilisées à quelles fins, par qui et combien de temps ?..... 8

3 Respecter ses obligations : la feuille de route RGPD 12

Nommer un délégué à la protection des données 12

Tenir un registre des traitements 14

Informer les personnes et recueillir leur consentement 15

Instaurer des procédures garantissant la sécurité et la confidentialité des données 16

Réaliser une analyse d'impact relative à la protection des données (AIPD) 18

Sécuriser ses relations avec ses partenaires et prestataires 19

Sensibiliser les salariés et bénévoles 20

Signaler tout incident de sécurité 20

Intégrer le respect de la vie privée dès la conception du système 21

RGPD

Une stratégie par étape pour adapter les pratiques

La protection des données personnelles et médicales fait partie de la culture des établissements et services médico-sociaux. Pour autant, le Règlement général de protection des données (RGPD) en vigueur depuis 2018 semble à beaucoup une contrainte supplémentaire. Et si ce nouveau cadre juridique était à l'inverse l'occasion de réfléchir à sa stratégie, notamment en matière de transition numérique ? Le chantier s'avère moins éprouvant qu'il n'y paraît – si l'on s'organise.

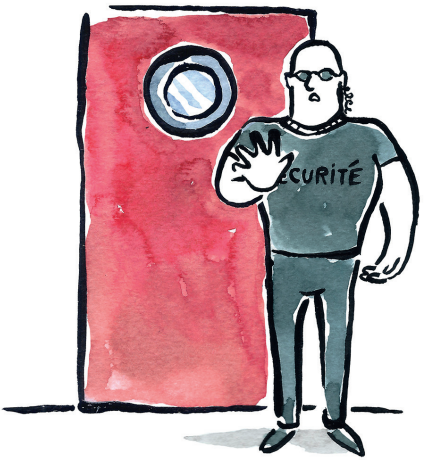
Le chiffre est révélateur : un an après son adoption, le RGPD était – plus ou moins – appliqué par la moitié seulement des 341 ESMS interrogés par l'Uniopss[1].

Cette enquête de 2019, qui n'a pas valeur de sondage, témoigne des obstacles rencontrés pour aborder cet important virage. Manque de budget, de temps et de méthode, mais aussi de formation et d'information, absence de service chargé du système d'information, complexité de la réglementation et de l'articulation entre protection des données, secret professionnel et mise en œuvre pratique du droit des usagers : de quoi faire reculer les plus motivés.

[1] Enquête auprès de 341 ESMS de toutes tailles réalisée par l'Uniopss, qui regroupe 25 0000 structures privées à but non lucratif et une centaine de fédérations et associations nationales des secteurs du social, du médico-social et de la santé.

Pourtant, un rapide coup d'œil à l'actualité devrait donner l'élan nécessaire pour se lancer. Pas un mois ne s'écoule sans qu'une cyberattaque n'alerte sur la vulnérabilité informatique des établissements médicaux et médico-sociaux. Certes, le RGPD ne concerne pas seulement les données électroniques, mais c'est souvent là que sont les failles. L'Agence du numérique en santé a recensé près de 700 incidents de sécurité « graves ou significatifs » entre octobre 2017 et fin 2019, dont 43 % avaient une origine malveillante.

Mieux protéger des données personnelles toujours plus menacées : tel est le défi à relever, qui exige une véritable « hygiène numérique », selon l'Agence nationale de la sécurité des systèmes d'information (Anssi). Le RGPD est l'une des deux boîtes à outils pour y parvenir ; l'autre étant la politique de sécurité des systèmes d'information.



LES GRANDS PRINCIPES DU NOUVEAU RÉGLEMENT

Appliquer le RGPD, c'est mettre en œuvre quelques principes prioritaires : le renforcement du contrôle sur le stockage, le traitement et le partage des données collectées par les organisations ; l'amélioration des procédures de sécurité et du contrôle des citoyens sur leurs données. En bref : meilleure transparence, meilleure traçabilité et meilleure détection des défauts de protection.

Ces principes se traduisent en droits pour les citoyens :

- **LE DROIT D'ACCÈS À L'INFORMATION :** chacun a le droit d'accéder à ses informations, de vérifier où elles sont stockées et si le traitement est conforme, dans les 30 jours suivant sa demande. Le consentement éclairé est nécessaire si les données collectées n'ont pas de lien direct avec le service fourni.

- **LE DROIT DE RECTIFICATION :** en cas d'inexactitude ou d'erreur dans les données personnelles, celles-ci doivent être corrigées dans les 30 jours suivant la réclamation.

- **LE DROIT À L'OUBLI :** tout citoyen peut demander l'effacement de ses données s'il estime qu'il n'y a pas lieu de continuer à les utiliser ou s'il retire son consentement.

- **LA GESTION DU CYCLE COMPLET :** chaque étape du parcours des données est soumise à obligation. Leur collecte doit reposer sur leur utilité, leur stockage doit être sécurisé, leur usage traçable et leur destruction prévue.

- **LA NOTIFICATION DE VIOLATION DE DONNÉES :** toute violation des données doit être signalée dans les 72 heures aux personnes concernées et aux autorités.

DÉFINITIONS

• DONNÉES À CARACTÈRE PERSONNEL :

Toute information relative à une personne physique, permettant de l'identifier directement ou indirectement : nom, prénom, adresse postale, adresse électronique, adresse IP, photo, empreinte digitale, etc.

• DONNÉES PERSONNELLES EN SANTÉ :

Données relatives à la santé physique ou mentale d'une personne physique (y compris la prestation de services de soins de santé), qui révèlent des informations sur l'état de santé de cette personne : antécédents médicaux, numéro ou élément attribué à une personne pour l'identifier à des fins de santé, informations issues de l'examen d'une partie du corps, etc.

• TRAITEMENT DE DONNÉES PERSONNELLES :

Toute opération réalisée sur des données personnelles, par quelque procédé que ce soit : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, diffusion, rapprochement, verrouillage, effacement, destruction.

Exemples : fichier d'usagers, fichier des adhérents de l'association, bandes de vidéosurveillance, dossiers nominatifs, logiciel de paie.

Point central du nouveau règlement : l'inversion de la logique déclarative. Avant, il suffisait de signaler tout traitement de données par une déclaration préalable à la CNIL. Désormais, chaque organisme est responsable de sa conformité au règlement et doit mettre en place un processus permanent de protection, régulièrement mis à jour. En cas de contrôle de la CNIL, il doit pouvoir fournir les preuves de ce processus. Et la commission dispose d'un pouvoir de sanction dissuasif avec des pénalités très lourdes.

D'où l'impératif d'un contrôle strict sur la gestion de l'accès aux données conservées et sur leur utilisation, ainsi que sur la localisation de leur stockage. Cela passe par la sensibilisation et la formation des collaborateurs, l'évaluation des pratiques et sans doute leur réaménagement, sans oublier la mise à jour des politiques de sécurité.

QUELLES DONNÉES, UTILISÉES À QUELLES FINS, PAR QUI ET COMBIEN DE TEMPS ?

Les établissements ou services médico-sociaux peuvent utiliser des données « sensibles » – les données de santé à caractère personnel –, sous réserve qu'elles soient nécessaires aux finalités de leurs interventions. Parmi la liste établie par la CNIL, retenons les données d'identification du bénéficiaire de l'accompagnement (et de ses représentants légaux), celles de son entourage et des personnes concourant à sa prise en charge sociale et médico-sociale ; les informations relatives à sa vie personnelle (composition du foyer, habitudes de vie

nécessaires à l'organisation de la vie quotidienne, centres d'intérêt, etc.) ; son parcours professionnel et de formation ; ses conditions de vie matérielles ; ses données de santé ; l'évaluation sociale et médico-sociale ; mais aussi la vie sexuelle et les opinions religieuses dans certains cas.

Outre ces données spécifiques, les ESMS sont amenés à collecter et traiter des données personnelles liées à leur activité courante : images de vidéosurveillance, informations concernant les salariés, les fournisseurs et les prestataires, données personnelles des adhérents, administrateurs, bénévoles et donateurs, données relatives aux visiteurs, informations financières.

Le RGPD est ferme sur ce point : les données doivent être « adéquates, pertinentes et non excessives » au regard des finalités de leur collecte et de leurs traitements. C'est le « principe d'utilité », au cœur de la démarche. Toutes les informations ne sont pas utiles. Les opinions politiques d'un candidat ne regardent pas son employeur potentiel. De même, les images de vidéosurveillance ne peuvent en aucun cas servir à contrôler le travail du personnel.

On devine que pour les ESMS, les objectifs légitimes sont liés à leurs missions de suivi et d'accompagnement des bénéficiaires, ainsi qu'à la gestion des structures et des personnes. La CNIL détaille sur son site le périmètre autorisé.

De la même façon, il faut identifier les personnes ou services susceptibles de collecter et de traiter des données personnelles. Lorsque différents services d'un établissement sont concernés, seules certaines personnes doivent être autorisées à accéder à ces données.

À titre d'exemple, les personnes concourant à la prise en charge et au suivi des bénéficiaires, celles appelées à intervenir dans la gestion financière et successorale de leur patrimoine, les organismes instructeurs et payeurs de prestations sociales, entre autres, peuvent accéder aux données personnelles des usagers dans les limites de leurs attributions légales, et chacun pour ce qui le concerne. De son côté, le service Ressources humaines collecte et traite uniquement des données relatives aux salariés.

Attention, les classeurs papier sont des traitements de données personnelles au même titre que les fichiers informatiques !

Enfin, les informations doivent être conservées dans des délais jugés raisonnables – lesquels varient en fonction de la nature des données et les finalités poursuivies. En bref, selon la CNIL, deux ans après le dernier contact avec la personne prise en charge, les données collectées et traitées pour les besoins du suivi de celle-ci doivent être sorties des bases actives. Les justificatifs qui n'ont plus d'utilité doivent être détruits. En cas de décès de la personne, tout doit être supprimé de façon sécurisée.

SE POSER LES BONNES QUESTIONS

1. De quelles données ai-je vraiment besoin pour atteindre l'objectif fixé ?
2. Ai-je bien distingué les données obligatoires des données facultatives ?
3. Les données que je recueille sont-elles objectives ?
4. Pourrai-je en toute transparence, donner accès à toute personne qui en fait la demande à l'ensemble des données que je détiens sur elle ?
5. Est-ce que je recueille des données sensibles ? Ai-je le droit de collecter ces données ?
6. Est-ce justifié au regard de mes missions ? Puis-je faire autrement ?
7. L'information est-elle au service du projet personnalisé ? De l'usager ?
8. Est-elle profitable à l'usager ? Respecte-t-elle son intérêt, ses droits ?
9. Cette information est-elle précieuse ? A-t-elle du sens ?
10. Est-elle nécessaire aux intervenants ? A tous ? Seulement à certains ?

RESPECTER SES OBLIGATIONS : LA FEUILLE DE ROUTE RGPD

Les principes étant posés, voici l'heure de leur mise en œuvre opérationnelle. Le règlement européen impose des nouveautés à mettre en œuvre pas à pas.

1) NOMMER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (OU DATA PROTECTION OFFICER – DPO)

Première étape : désigner la personne chargée d'orchestrer la politique de protection des données et des droits des personnes. Le délégué à la protection des données a pour mission :

1. l'information et le conseil auprès du responsable du traitement, du sous-traitant le cas échéant, et des collaborateurs ;

2. le contrôle du respect de la réglementation : tenue du registre, réalisation d'études d'impact, formalisation des procédures, etc. ;

3. la coopération et la communication avec la CNIL.

Le DPO doit bien connaître l'établissement et son métier pour adapter ses actions. Outre de solides connaissances en droit, la personne choisie doit avoir une vision transversale des processus et de l'organisation, et être capable d'une analyse indépendante. Si elle exerce d'autres missions dans la structure, celles-ci ne doivent pas présenter de conflit

d'intérêts avec sa tâche de DPO : elle ne doit pas être amenée à déterminer les moyens et les finalités d'un traitement de données personnelles, ce qui la conduirait à devenir « juge et partie ». Par exemple, les fonctions de directeur administratif et financier ou de directeur des systèmes d'information ne sont pas compatibles avec la mission de DPO.

Le délégué, rattaché à la direction, doit disposer des moyens nécessaires à l'exercice de sa mission : temps, formation, budget. Important : il n'est pas responsable, d'un point de vue civil ou pénal, de l'éventuelle non-conformité des procédures de l'établissement. La responsabilité incombe au responsable de traitement – le directeur de l'établissement ou du service médico-social – ou au sous-traitant.

On peut désigner son délégué au sein de sa structure, mais aussi à l'extérieur (consultant indépendant ou cabinet spécialisé), voire le mutualiser entre plusieurs établissements. C'est le choix qu'a fait la Mutualité française de l'Isère. « Nous lançons notre démarche RGPD, et nous allons désigner un délégué à la protection des données, explique son directeur général, Laurent Van Herreweghe. Nous avons choisi de travailler avec un prestataire, que nous partageons avec les autres branches de la Mutualité française de la région : c'est une démarche commune. »

Certains établissements créent une cellule chargée de suivre ces questions, regroupant le DPO, un responsable de la sécurité informatique, un juriste, un administratif, un médecin. Une bonne façon de diffuser en interne la culture de la protection des données.

2) TENIR UN REGISTRE DES TRAITEMENTS

Deuxième étage de la stratégie RGPD : la cartographie des traitements de données opérés, à consigner dans un registre dédié.
Ce registre doit, pour chaque type d'informations personnelles, préciser les traitements effectués, leur finalité, les catégories de personnes concernées, les durées de conservation, le mode de sécurisation, les sous-traitants concernés. À noter : la CNIL fournit un modèle de registre de traitement à imiter sans complexe.

Il faut aussi penser à formaliser, mettre à jour et conserver les documents suivants :

- réponse aux demandes d'effacement des données ;
- demande d'accord exprès pour le consentement sur les traitements ;
- communication des droits de vos salariés et résidents

(accès, rectification, opposition, effacement, portabilité) ;
- signalement aux personnes concernées et à la CNIL en cas de violation de données.

La documentation interne doit permettre d'attester la conformité de la structure aux principes du RGPD en cas de contrôle de la CNIL. Registre, mentions d'information, preuves du recueil du consentement, contrats avec les sous-traitants doivent être à jour. Il faut être capable de justifier chaque mesure prise, et de la faire évoluer si nécessaire. Il s'agit désormais de raisonner en continu, en conservant toutes les traces des décisions.

3) INFORMER LES PERSONNES ET RECUEILLIR LEUR CONSENTEMENT

La réglementation n'impose pas aux établissements et services médico-sociaux le recueil du consentement des personnes, si la collecte et le traitement de leurs données personnelles servent exclusivement à leur prise en charge sanitaire ou sociale : c'est la règle de l'usage limité et pertinent au regard de la finalité.
En revanche, le consentement exprès de la personne ou de son représentant légal est obligatoire pour toute collecte et tout traitement de données personnelles à d'autres fins que la prise en charge.

L'information des usagers et des salariés reste toutefois obligatoire, « dans un langage compréhensible et selon des modalités appropriées et adaptées à leur état », indique la CNIL. Cette information doit comporter l'identité du responsable de traitement, la finalité poursuivie par le traitement, les destinataires des données et les droits des

personnes (droits d'opposition pour motifs légitimes, d'accès et de rectification).
Il faut également informer les personnes du caractère obligatoire ou facultatif de leurs réponses, ainsi que des conséquences éventuelles d'un défaut de réponse ou de l'exercice de leur droit d'opposition. Cette information doit figurer sur les formulaires de collecte.
Enfin, la structure doit désigner le service auprès duquel les personnes peuvent exercer leurs droits d'opposition, d'accès et de rectification. Sans oublier le contact du délégué à la protection des données.

4) INSTAURER DES PROCÉDURES GARANTISSANT LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES

Chaque établissement ou service doit prendre toutes les précautions pour préserver la sécurité et la confidentialité des données personnelles en son sein. C'est-à-dire respecter les obligations suivantes :

1. mesures permettant de garantir la confidentialité des données échangées (chiffrement par exemple) pour toute transmission via un canal non sécurisé (Internet notamment) ;

2 authentification des personnes habilitées avant tout accès à des données personnelles (identifiant et mot de passe personnels, autre moyen d'authentification sécurisé) ;

3 mécanisme de gestion des habilitations, garantissant que les personnes habilitées n'ont accès qu'aux seules données nécessaires à la réalisation de leurs missions. Définition et formalisation d'une procédure assurant la bonne mise à jour des habilitations ;

4 mécanismes de traitement automatique garantissant que les données à caractère personnel sont systématiquement supprimées à l'issue de leur durée de conservation, ou font l'objet d'une procédure d'anonymisation rendant impossible toute identification ultérieure ;

5 traçabilité des accès afin de permettre la détection d'éventuelles tentatives frauduleuses ou illégitimes. Traçabilité spécifique des accès aux données considérées comme sensibles, avec horodatage, identifiant de l'utilisateur, données concernées. Conservation des données de journalisation pendant six mois glissants à compter de leur enregistrement, puis destruction ;

6 externalisation de l'hébergement de données de santé personnelles dans les conditions prévues dans le code de la santé publique ;

7 en cas de production de statistiques, anonymisation pour éviter toute identification, même indirecte, des personnes concernées.

Sans oublier bien sûr les mesures de sécurisation d'accès aux locaux et une politique sérieuse de sécurité informatique (stations de travail, réseaux, serveurs, etc.).

5) RÉALISER UNE ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES (AIPD)

Voilà sans doute le chantier le plus complexe imposé par le RGPD : il s'agit d'analyser les risques que chaque traitement de données personnelles fait peser sur les droits et libertés des personnes. Lorsque ces risques sont élevés, une analyse d'impact relative à la protection des données est exigée. C'est le cas des traitements de données personnelles mis en œuvre par les ESMS aux fins de suivi des bénéficiaires. Par exemple, l'usage d'un dispositif de télémédecine, ou un traitement portant sur les dossiers des résidents d'un établissement devront faire l'objet d'une étude d'impact.

D'autres traitements, concernant la gestion générale de la structure (relations fournisseurs, gestion des ressources humaines hors profilage, etc.), ne sont en revanche pas soumis à l'analyse d'impact : la CNIL en fournit la liste précise.

L'analyse d'impact comporte quatre parties. En premier lieu, la description des opérations de traitement envisagées et des finalités du traitement, ainsi que l'intérêt légitime poursuivi par le responsable du traitement. Ensuite, une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités. Enfin, l'évaluation des risques pour les droits et libertés des personnes concernées. Laquelle sera complétée par les mesures envisagées pour

faire face à ces risques.

Pour tout traitement soumis à AIPD, la consultation du délégué à la protection des données (DPO) ainsi que des personnes concernées est obligatoire.

Il faut en outre prévoir la révision de l'analyse d'impact, en fonction des évolutions du risque présenté par les opérations de traitement.

BON À SAVOIR :

La CNIL a édité un guide et un logiciel pour réaliser son analyse d'impact, disponibles sur son site.

6) SÉCURISER SES RELATIONS AVEC SES PARTENAIRES ET PRESTATAIRES

La responsabilité de la structure quant à la protection des données personnelles s'étend à ses relations avec ses prestataires et sous-traitants. S'assurer que ceux-ci respectent les obligations liées au RGPD est indispensable : il faut donc inscrire ces dispositions dans les contrats avec les partenaires (officine, services d'ambulance ou de transport, prestataire informatique, etc.).

Attention : la CNIL rappelle que l'usage d'outils ou de logiciels développés par des tiers pour un traitement de données personnelles est sous la responsabilité du responsable de traitement, qui doit notamment vérifier que ces outils ou logiciels respectent les obligations légales.

QUEL HÉBERGEMENT POUR LES DONNÉES DE SANTÉ ?

Faire appel à un prestataire pour l'hébergement, le stockage ou le traitement des données est une solution intéressante, garantie d'un haut niveau de conception et de sécurisation du système d'information.

Vigilance toutefois : le sous-traitant doit impérativement disposer d'un agrément ou d'une certification « HDS » (Hébergement de données de santé), garantissant qu'il met en œuvre toutes les procédures de protection de la vie privée des personnes, de confidentialité et de sécurité des données.

7) SENSIBILISER LES SALARIÉS ET BÉNÉVOLES

Il revient à l'employeur de sensibiliser ses collaborateurs, salariés ou bénévoles, aux questions relatives à la protection des données personnelles et de les informer de leurs obligations et de leurs droits. Chacun doit identifier le délégué à la protection des données.

Si nécessaire et si possible, des formations au RGPD peuvent être dispensées aux salariés. C'est l'occasion aussi d'organiser des moments de réflexion collective sur les enjeux déontologiques de ces questions et sur les pratiques des professionnels. Par exemple, quel partage d'information légal et légitime au bénéfice des personnes accompagnées ?

8) SIGNALER TOUT INCIDENT DE SÉCURITÉ

La loi impose de notifier toute violation de données à caractère personnel. Il faut alerter les personnes concernées ainsi que la CNIL dans les 72 heures après avoir pris connaissance de

l'incident. Mieux vaut donc s'y être préparé, et avoir sous la main des documents prêts à cet usage.

9) INTÉGRER LE RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION DU SYSTÈME D'INFORMATION

Le RGPD impose une profonde remise en cause des pratiques. Voilà les directeurs d'ESMS responsables de la sécurité informatique nécessaire au respect de la protection des données. Il leur faut donc prendre en compte la question de la vie privée dès la conception de leur système d'information, suivant le principe de la « Privacy by design ». Qui plus est, il faut intégrer le niveau de conformité qui permet, par défaut, d'assurer un niveau très élevé de protection avant le lancement de tout nouveau traitement : c'est ce qu'on appelle « Privacy by default ».

Finis donc les échanges de données personnelles sur les personnes prises en charge via des messageries non sécurisées, ou les listes de coordonnées sur des tableaux Excel accessibles à tous. Finis aussi les postes de travail et les serveurs locaux non sécurisés.

Le chantier est vaste : il s'agit de mettre à plat tous les processus informatiques. C'est-à-dire de réfléchir à son organisation, à ses besoins métier et aux obstacles à lever. Une bonne occasion de repenser sa stratégie et les moyens d'améliorer ses méthodes au service des usagers.

QUEL HÉBERGEMENT POUR LES DONNÉES DE SANTÉ ?

1 • Avez-vous recensé les données personnelles collectées et les traitements effectués ?

2 • Les personnes concernées sont-elles informées des traitements ?

3 • Combien de temps conservez-vous les données personnelles des personnes prises en charge ?

4 • Avez-vous formalisé des documents correspondant à vos obligations ?

5 • Avez-vous nommé un DPO ? Vos collaborateurs et les personnes prises en charge le connaissent-ils ?

6 • Qui héberge vos données ? Les datacenters sont-ils localisés dans l'Union européenne ? Le prestataire ou l'éditeur qui héberge des données de santé est-il certifié « HDS » ?

7 • Avez-vous réalisé une analyse d'impact des traitements de données sur la vie privée ?

8 • Savez-vous tracer et identifier les accès aux données et à leurs traitements ? Conservez-vous un historique de ces accès ?

9 • La sécurité des données est-elle intégrée à vos contrats de sous-traitance ?

10 • Vos échanges électroniques de données personnelles sont-ils sécurisés ?

11 • Avez-vous sensibilisé vos collaborateurs au respect de la réglementation relative aux données personnelles ?


y a
quelqu un ??

GUIDE PRODUIT PAR WIDIP, FOURNISSEUR DE SOLUTIONS NUMÉRIQUES POUR LE SECTEUR MÉDICO-SOCIAL

Very Informatics People