NOVEMBRE 2020

PROTECTION DES DONNÉES DE SANTÉ

ENJEUX ET BONNES PRATIQUES

Livre blanc

doshas consulting

SOMMAIRE

Introduction 5

1. Cadre juridique des données de santé 7

1.1. La Loi du 4 mars 2002 8

1.2. Les référentiels de sécurité et d'interopérabilité 8

1.3. L'identifiant National de Santé (INS) 8

1.4. Le règlement eIDas 9

1.5. Le RGPD 9

1.6. Hébergement des données de santé 10

2. Impacts sur les organisations de santé 17

2.1. Impacts RGPD en termes de gouvernance SI 17

2.1.1. Sécurité des données : articulation RGPD / HDS 19

2.1.2. Déclaration des incidents 22

2.1.3. Analyse de risques SI /AIPD 24

2.2 Impacts sur la sécurisation du SI 25

2.2.1. Processus de mise en production 25

2.2.2. Base de recette / base de Formation 27

2.3 Impacts juridiques 27

2.3.1. Sur les contrats de travail 27

2.3.2. Sur les contrats avec les fournisseurs 27

2.3.3. Sur les contrats HDS 28

2.3.4. Sans oublier les obligations RGPD 28

Perspectives et enjeux à venir 31

Annexes 35

Qui sommes-nous ? 39

1. Doshas consulting 39

2. Nos retours d'expérience sur la protection des données de santé 40

3. Ils nous font confiance 42

2019	**392**	**300**	**70**
2018	**327**	**247**	**47**
	incidents déclarés sur le portail des signalements	structures ont déclaré au moins un incident	demandes d'accompagnement

14	**11**	**16**	**8**
6	**2**	**15**	**3**
incidents ont fait l'objet d'un suivi particulier de la part du FSSI	incidents ont été pris en charge par l'ANSSI	ont été communiqué à l'ANSM	incidents ont fait l'objet d'une alerte à la DGS / CORRUSS

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

ANSSI

ansm Agence nationale de sécurité du médicament et des produits de santé

DGS Direction générale de la Santé

Source : AGENCE DU NUMÉRIQUE EN SANTÉ

INTRODUCTION

En mai dernier, la compagnie aérienne *EasyJet* est victime d'une cyberattaque « exceptionnelle » à la suite de laquelle les données personnelles de 9 millions de clients ont été dérobées. Dans le contexte de la crise du coronavirus, les systèmes d'information ont joué un rôle important dans la gestion de la crise et la résilience face à la pandémie, rendant ainsi les organisations de plus en plus exposées au risque de cyberattaques (télétravail, accès aux SI de l'entreprise à distance, accès Wifi, etc.).

Selon Jean-Claude LAROCHE, DSI Enedis,
Président du cercle cybersécurité du Cigref

« La gravité et le nombre des attaques contre les systèmes numériques ne cessent de prendre de l'ampleur. Les grandes institutions et entreprises intensifient leurs actions de protection et se préparent à la crise, mais elles ne peuvent pas pour autant banaliser un tel contexte ».

Si l'augmentation des cyberattaques n'épargne aucun secteur d'activité, le domaine de la Santé enregistre des risques plus élevés et des conséquences qui peuvent s'avérer graves sur la prise en charge des patients, comme le montrent les chiffres publiés par l'agence du numérique en santé (ANS), en juillet 2020 *(cf figure page 4)*.

S'il est clair que la protection des données est un réel enjeu pour tous les acteurs du secteur de la Santé, la foisonnante et complexe réglementation, cependant indispensable, peut facilement conduire à mettre plusieurs organisations en situation de non-conformité réglementaire ; et en risques de manière opérationnelle.

Dans ce livre blanc, nous proposons d'appréhender l'environnement réglementaire avec une vision pratique à travers les trois parties suivantes :

1. Le cadre juridique concernant les données de santé

2. Les impacts sur les organisations qui manipulent des données sensibles

3. Les perspectives et enjeux à venir

Qu'est qu'une donnée personnelle ?

« Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent une ou des personnes, celles-ci doivent en conserver la maîtrise ».

Source : https://www.cnil.fr/fr/definition/donnee-personnelle

Qu'est qu'une donnée de santé ?

Le RGPD, qui définit précisément pour la première fois les données de santé : « Les données à caractère personnel concernant la santé physique ou mentale, passée, présente ou future, 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 ».

Cette définition comprend, par exemple :

- Les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle.
- Les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source)

Cette définition - large - montre la multitude d'acteurs qui peuvent être amenés à traiter des données de santé, parfois sans même le savoir.

Au travers de nos expériences (une vingtaine d'accompagnements d'acteurs sur la thématique de l'hébergement des données de santé), nous avons constaté que plusieurs sociétés n'étaient pas forcément très au clair sur la protection des données de santé qu'elles manipulaient dans certains processus métier voire une absence de protection adaptée.

En effet les données de santé sont sensibles, et la réglementation en encadre les modalités de collecte et de stockage.

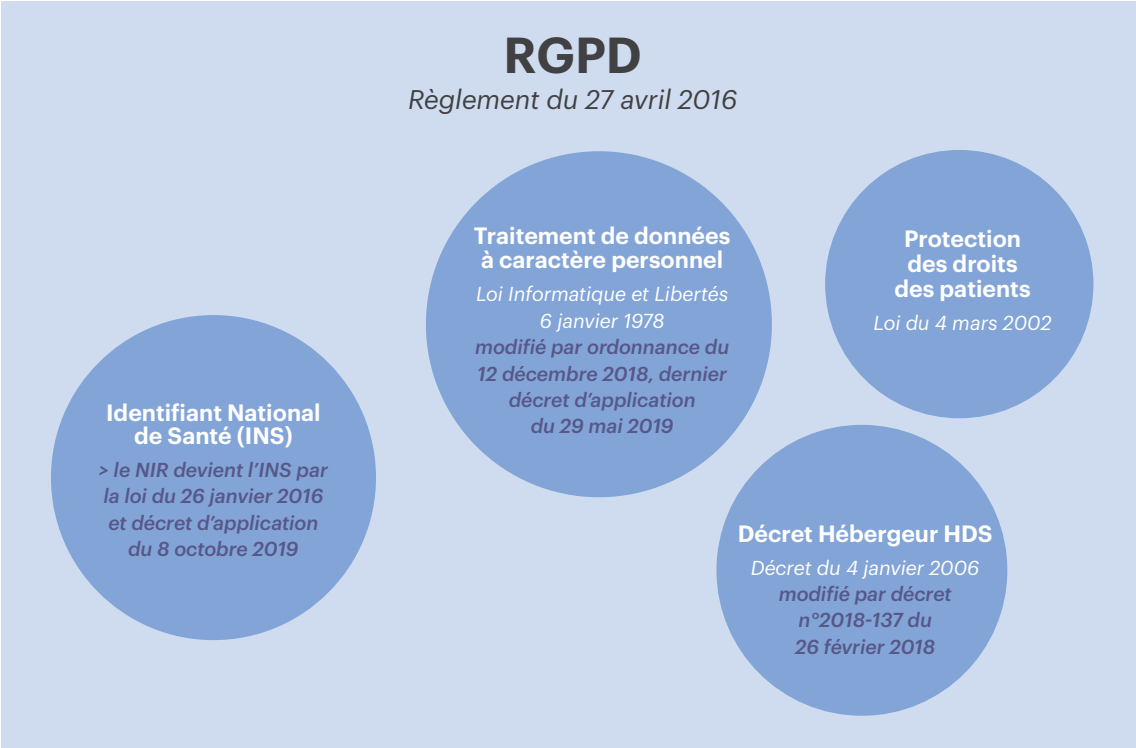
1. CADRE JURIDIQUE DES DONNÉES DE SANTÉ

L'entrée en application du Règlement Général Européen sur la protection des données (RGPD), le 25 mai 2018, marque une date importante dans la protection des données de santé, définies pour la première fois dans ce texte normatif.

Cependant, ce cadre est loin d'être le premier texte de loi encadrant la protection des données de santé :
- Ce cadre juridique est **évolutif** et s'adapte aux évolutions technologiques.
- La réglementation est **stratifiée et multidimensionnelle**.

Il faut être ainsi en mesure de pouvoir identifier et déterminer précisément la règlementation applicable en termes de protection des données.

Le schéma ci-dessous synthétise l'articulation du cadre juridique de la protection des données de santé.



1. LA LOI DU 4 MARS 2002

Cette loi dite « Kouchner » est relative aux droits des malades et à la qualité du service de santé. Elle concerne plusieurs points :
- Le droit d'accès aux soins et le principe de non-discrimination,
- L'information et le consentement libre et éclairé du patient,
- Le droit d'accès au dossier médical.

La loi du 4 mars 2002 affirme aussi qu'afin de garantir la confidentialité des informations médicales, leur conservation sur support informatique, leur transmission par voie électronique entre professionnels, ces derniers sont soumis à l'application des règles du décret pris en Conseil d'État après avis de la CNIL.

2. LES RÉFÉRENTIELS DE SÉCURITÉ ET D'INTEROPÉRABILITÉ

La confidentialité des données de santé à caractère personnel conservées sur support informatique ou transmises par voie électronique est réglementée par l'article L.1110-4-1 du CSP. En effet, les modalités de sécurisation des échanges doivent :

- Respecter les **référentiels** d'authentification émis par les autorités et ayant pour but de déterminer les fonctions de sécurité nécessaires aux traitements informatiques des données de santé (paliers d'authentification, sécurité physique des matériels, accès aux traitements, procédures de traçabilité...).
- Mettre en œuvre les principes du RGPD avec le maintien dans le secteur de la santé de formalités préalables à accomplir (ces conditions sont à examiner au cas par cas en fonction des projets et du porteur de projet).

3. L'IDENTIFIANT NATIONAL DE SANTÉ (INS)

En février 2007, la CNIL interdisait l'utilisation du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques NIR, plus communément appelé numéro de sécurité sociale en tant qu'identifiant de santé.

Mais en 2016, et dans le cadre de la loi de modernisation de notre système de santé, l'article 1111-8-1 du code de la santé publique CSP a été modifié pour permettre l'utilisation du NIR, et à défaut le numéro identifiant d'attente NIA, comme Identifiant National de Santé (INS) des personnes pour leur prise en charge à des fins sanitaires et médico-sociale et ce dans les conditions prévues à l'article L.1110-4 du CSP relatif au secret médical.

L'identifiant national de santé (INS) permet d'identifier les patients et de fiabiliser le référencement des données de santé et des données personnelles des usagers. Nécessaire au développement de la santé numérique en France, l'INS est une donnée personnelle protégée par la Loi Informatique et Libertés (par conséquent, son utilisation est contrôlée par la CNIL).

Concrètement, l'entrée en application de l'INS au 1er Janvier 2021 (décret n°2019-1036 du 8 octobre 2019), signifie que les acteurs de santé devront :
- Mettre en place l'INS dans les systèmes d'information de santé et se former à ses modalités d'utilisation,
- Intégrer l'INS à leurs modes d'organisation, particularités de fonctionnement et maturité en identitovigilance.

À noter : À contrario ceux sur qui ne pèsent pas cette obligation n'ont pas le droit de l'utiliser. Une analyse juridique est donc nécessaire dans ce cas-là.

4. LE RÈGLEMENT EIDAS

Le règlement n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDas », est un règlement européen qui a été adopté le 23 juillet 2014 par le Parlement Européen et le Conseil de l'Union Européenne.

L'objectif de ce règlement est de mettre en place un cadre juridique à même de susciter une confiance accrue dans les transactions électroniques au sein du marché intérieur. Le règlement eIDas s'applique à l'identification électronique et aux services de confiance. Il accorde également une valeur juridique aux documents électroniques.

5. LE RGPD

Le règlement général pour la Protection des données (RGPD) renforce la protection des données de santé considérées comme **sensibles**. Ce texte est donc directement applicable en France.

Le principe est celui de l'interdiction du traitement des données de santé relatives à une personne identifiée ou identifiable et de leur commercialisation sans finalité précise (article 9 RGPD - § I et II). En effet, l'exploitation est possible :

- Si la personne concernée est informée et donne son consentement « clair et explicite » (RGPD, art. 7).

- Si elle est rendue nécessaire aux fins de la **médecine préventive**, des **diagnostics médicaux**, de l'**administration de soins ou de traitements**, ou de la **gestion de services de santé** et mis en œuvre par un **membre d'une profession de santé**, ou par une autre **personne soumise à l'obligation de secret professionnel**.
- Si elle est conforme à la loi Informatique et Libertés et justifiée par l'intérêt public (éviter la propagation des maladies, dans le cadre d'une recherche publique, etc.) après avis motivé et publié de la CNIL ou si les données de santé sont rendues anonymes.

Le RGPD allège certaines formalités auprès de la CNIL comme la déclaration préalable des fichiers ou la délivrance d'une autorisation (sauf pour la recherche). En contrepartie, le RGPD se base sur le **principe « d'accountability »** en responsabilisant davantage l'ensemble des acteurs traitant des données de santé. En effet, ces acteurs doivent **être en mesure de prouver à tout moment leur conformité aux exigences du RGPD**.

À noter : l'Article L. 1111-8 CSP : VII.prévoit que « tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal ».

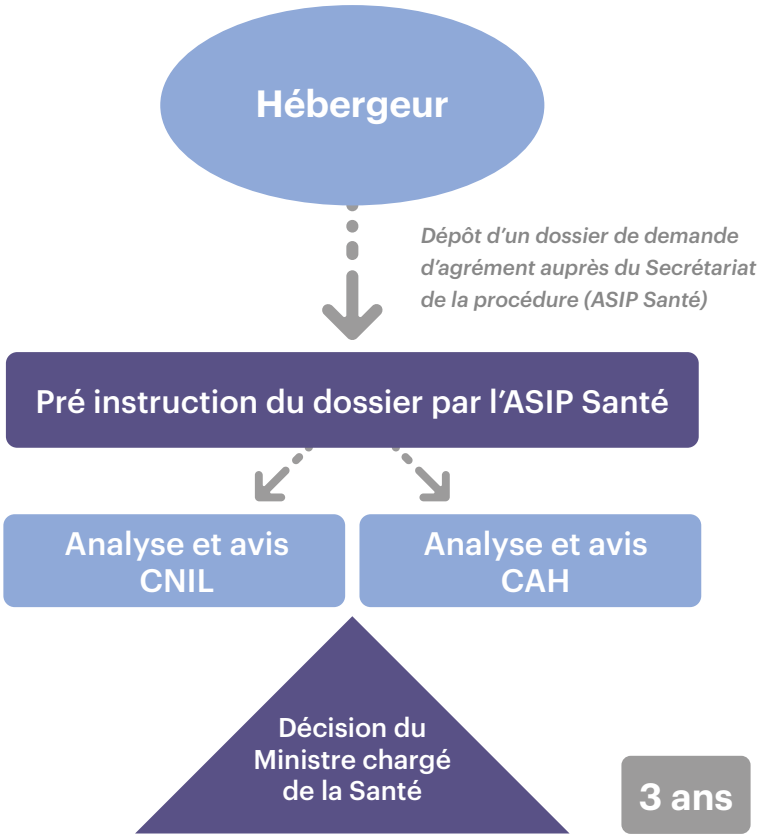
Nous constatons que :
- Le RGPD impose des changements importants pour tout acteur manipulant une donnée de santé.
- Les différents impacts de la mise en conformité sont multiples notamment en termes :
  > de Gouvernance
  > d'organisation
  > Juridique
  > de sécurité du Système d'Information

6. HÉBERGEMENT DES DONNÉES DE SANTÉ

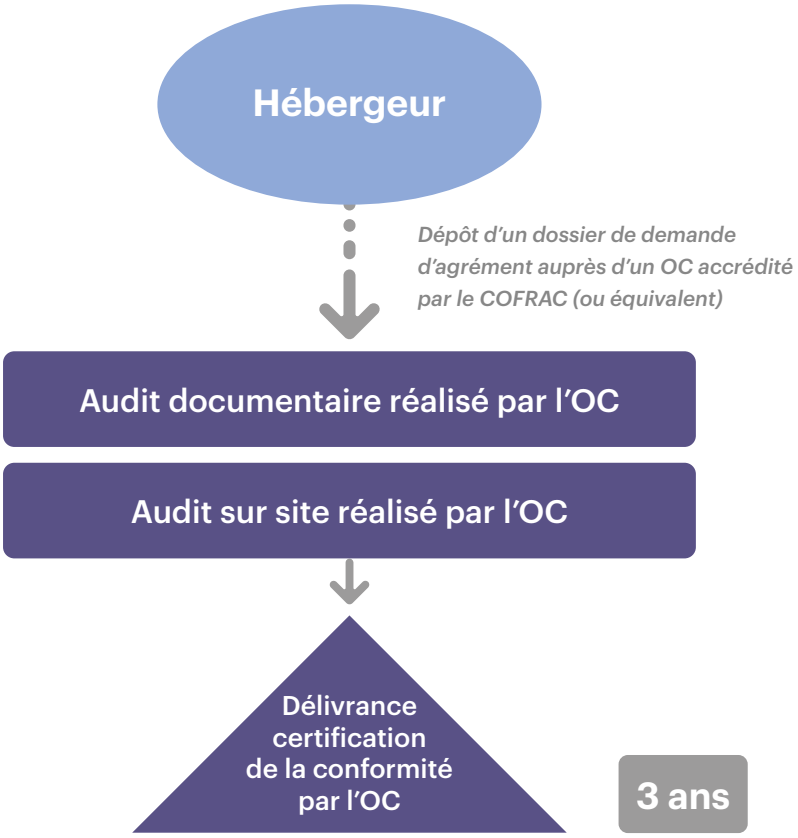
Par hébergement de données de santé à caractère personnel, on désigne l'activité qui consiste à stocker les données (notion de coffre-fort électronique) recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social :

- Pour le compte de personnes physiques ou morales, responsables de traitement au sens de la loi n°78-17 du 6 janvier 1978, à l'origine de la production ou du recueil de ces données.
- Pour le compte du patient lui-même.

Procédure d'agrément



Procédure de certification



L'ancienne procédure d'agrément

Jusqu'au 1er avril 2018, un HDS devait obtenir l'agrément du ministre chargé de la Santé sur la base d'un dossier remis à l'ASIP-Santé et après avis de la CNIL et du comité d'agrément des hébergeurs. L'agrément était donné pour une durée de trois ans.

Le dossier portait sur la capacité financière du candidat, le type de prestation proposé, le niveau de sécurité et les conditions du respect des principes de la protection des données personnelles et des droits des personnes. En outre, le contrat HDS était analysé au regard du contrat type proposé par l'hébergeur avec les tiers (en détaillant notamment les responsabilités respectives des parties prenantes).

Un impact organisationnel fort était que l'HDS devait notamment disposer d'un « médecin de l'hébergeur » soit parmi son personnel soit sous forme de prestation de service. Ce médecin hébergeur était chargé d'accompagner les demandes d'accès à leur dossier par les patients, et d'assurer que l'éthique médicale était respectée dans la mise en œuvre des procédures d'hébergements.

Certification depuis le 1er avril 2018

Depuis le 1er avril 2018, un hébergeur souhaitant obtenir l'autorisation d'héberger des données de santé doit obtenir la certification d'un organisme certificateur accrédité par le COFRAC (comité français d'accréditation) ou tout organisme équivalent au niveau européen.

Le schéma suivant montre les principaux impacts du passage d'un agrément à une certification HDS :

En 2018, la réglementation a changé, passant d'un agrément HDS à une certification HDS

1	Les hébergeurs disposant déjà d'un agrément doivent passer à la certification avant la fin de validité de leur agrément.
2	La certification est délivrée par des organismes de certification agréés (anciennement l'ASIP Santé / ANS pour l'agrément).
3	Renforcement des exigences afin d'obtenir la certification (certification ISO 27001, exigences issues des normes ISO 20000 et ISO 27018, exigences spécifiques définies par l'ANS).
4	2 types de certification : - Certification pour hébergeur physique (hébergement des données). - Certification pour hébergeur infogéreur (supervision des données)

INFOGÉRANCE : CHARNIÈRE DE LA VALEUR AJOUTÉE D'UN HÉBERGEUR DE SANTÉ

Une des ambitions de la procédure de certification était d'apporter plus de transparence et de clarté sur la nature et le périmètre des offres HDS proposées par les hébergeurs certifiés.

Toutefois, des incertitudes subsistent concernant le périmètre des activités HDS – en particulier l'activité 5 : « administration et exploitation du système d'information contenant les données de santé». Cette activité a fait l'objet de nombreux débats, sa suppression a même été évoquée. Finalement, une définition est proposée dans le cadre de l'évolution des référentiels HDS.

Comment est-ce que nous comprenons cette activité chez Claranet ?
Bien que les six activités HDS sont clairement dissociées dans les textes, techniquement, il est difficile pour un hébergeur d'apprécier ces activités de façon isolée. Aussi, lorsque la suppression de l'activité 5 a été évoquée, il a fallu démontrer que cette activité était la pierre angulaire, le liant entre les différentes activités HDS. Ce fut d'ailleurs le thème d'un groupe de travail au sein du Syntec Numérique qui a permis de valider une position commune sur le contenu et la compréhension de cette activité 5.

C'est dans le périmètre de cette activité 5 que l'hébergeur doit notamment garantir un niveau de service et de support adapté à la sensibilité des données de santé, de façon à garantir ses clients, en cas de survenance d'un incident ayant un impact sur la disponibilité et la continuité du service d'hébergement de données de santé.

Au regard du cœur de métier d'un hébergeur et de l'objectif poursuivi par cette activité 5, l'administration et l'exploitation de l'application métier par l'hébergeur comprend les prestations suivantes :
- La gestion des incidents et des demandes avec un service support adapté aux besoins des clients - les établissements de santé ont par exemple besoin d'un support en 24/7. Cette gestion doit être capable d'appréhender l'incident sur toutes les couches de la plateforme et/ou du système d'information (du datacenter au middleware et aux bases de données), et ce, quel que soit l'hébergeur certifié sur les couches « hébergeur infrastructure » (activités 1 et 2) ; elle doit permettre d'escalader à un éditeur en cas de problème applicatif.
- L'aide à la gestion des déploiements applicatifs, avec des processus de sécurisation additionnels (scan de vulnérabilité par exemple).
- L'aide à la gestion sécurisée des déploiements en mode « devops » (conteneurisation, intégration et déploiement continu).
- Le maintien en condition sécurité et de manière managée de la plateforme et/ou du système d'information, par outillage sécurité spécifique.
- La gestion de la performance de la plateforme et/ou du SI (dans l'adhérence infra-application).
- La gestion globale de la continuité (pas uniquement réseau et datacenter), management des PCA (plans de continuité d'activité) et PRA (plans de reprise d'activité), gestion de crise.
- La gestion de la réversibilité et de la migration du service.

KAHINA HADDAD
Chef de projet conformité | CICS

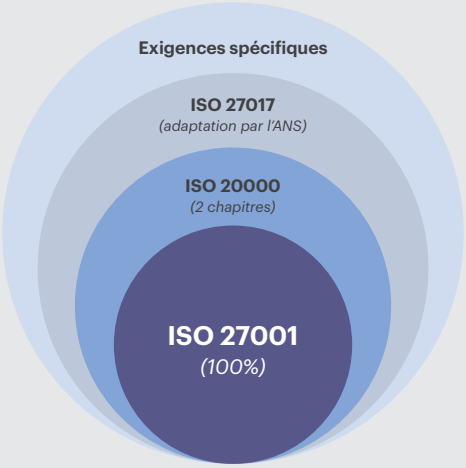
& CHRISTOPHE JODRY
Directeur des offres et responsable de production BU Healthcare

claranet

Procédure de certification HDS

La procédure de certification repose sur une évaluation de conformité au référentiel de certification. Le schéma suivant résume le référentiel de certification :

Certification HDS = Certification 27001 complétée



Le processus de certification est le suivant :

Lors de l'audit, l'organisme certificateur vérifie, notamment l'équivalence des éventuelles certifications ISO 27001 ou ISO 20000 déjà obtenues par l'hébergeur.

L'hébergeur dispose de trois mois après la fin de l'audit sur site pour corriger les éventuelles non-conformités majeures et faire auditer ses corrections. Passé ce délai et sans action de l'hébergeur, toute la procédure d'audit sur site devra être de nouveau réalisée.

Le certificat est délivré pour une durée de trois ans, par l'organisme certificateur et chaque année, un audit de surveillance est réalisé.

Retour d'expérience

La précédente procédure HDS, l'agrément laissait libre le choix du périmètre de responsabilités entre l'hébergeur et l'hébergé, ce qui a donné lieu à des définitions de périmètres différentes entre les hébergeurs rendant ainsi la compréhension et la comparaison des offres compliquées, avec des positionnements tarifaires très variables.

Aujourd'hui, on assiste à une « standardisation » des offres puisque le référentiel est le même. Les offres varient cependant selon les hébergeurs HDS, notamment selon les variables suivantes :

*- **En fonction des services de l'hébergeur** proposé. Ces services peuvent être de nature :*

> Technique (ex. : même technologie de base de données, etc.),

> Fonctionnelle (ex. : mutualisation de modules comme la facturation, authentification forte, plateforme « mobilité », etc.),

> Services rendus par l'hébergeur (ex. : SLA selon les usages, supervision déléguée, etc.).

*- **En fonction du risque** :*

> Clauses back to back dans les contrats HDS (périmètre de responsabilité et dans le contexte RGPD).

*- **En fonction du coût** :*

> Coûts de réversibilité,

> Coûts de migration.

2. IMPACTS SUR LES ORGANISATIONS DE SANTÉ

L'ensemble des textes de loi évoqués dans les parties précédentes implique que les organisations de santé doivent appliquer le cadre législatif contraignant et qui impose plusieurs ajustements en matière d'organisation interne ainsi que le recours - le cas échant - à un hébergeur de données externe (agréé ou certifié HDS).

1. IMPACTS RGPD EN TERMES DE GOUVERNANCE SI

L'un des impacts forts du RGPD est l'obligation (obligatoire dans la majorité des cas) d'avoir un **délégué à la protection de données (DPD) ou data protection officer (DPO)**. Les organisations publiques sont toutes concernées par cette obligation, tandis que les organisations privées sont potentiellement concernées, selon qu'elles mettent ou non en œuvre un traitement de données sensibles « à grande échelle ». Pour les organisations de santé privées, il semble évident que la présence d'un DPO est obligatoire.

La fonction de DPO peut être confiée à un prestataire sur la base d'un contrat de service.

- Pour le secteur privé :
Il est possible de désigner un DPO mutualisé au niveau du groupe.

- Pour le secteur public :
Il est possible de désigner un seul DPO pour plusieurs organismes ou autorités.

Zoom

Profil du DPO

Désigner un DPO est un signal positif, même pour les entreprises qui n'y sont pas obligées, et permet de se doter d'un référent de la conformité.

Le DPO doit pouvoir :
- Démontrer une connaissance approfondie en matière de protection des données,
- Démontrer une connaissance approfondie des processus métiers,
- Avoir un intérêt pour les systèmes d'information,
- Être indépendant,
- Démontrer une capacité de communication,
- Être au fait des évolutions technologiques.

On note aussi l'obligation de signaler auprès de la CNIL tout incident de sécurité impliquant des données personnelles (obligation qui s'ajoute à l'obligation actuelle de signalement des incidents de sécurité des systèmes d'information de santé prévue à l'article L.1111-8-2 du code de la santé publique).

Source : CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Retour d'expérience

À travers nos expériences, nous avons relevé certains points de vigilance :

- La désignation d'un DPO ne doit pas exclure une prise de conscience générale et aux différents niveaux décisionnels de l'organisation des risques liés à la protection des données.

- Cette même désignation ne devrait pas exclure la conduite d'une analyse de risques lorsqu'il s'agit de prestataires externes ou de sous-traitants.

- Dans certains cas, nous avons constaté que le DPO n'avait pas une bonne appréhension de la donnée de santé, notamment dans les compagnies d'assurance ou de mutuelle. À titre d'exemple, les données recueillies dans les questionnaires de santé pour la prévoyance ou l'assurance emprunteur relèvent bien du cadre de la protection des données sensibles, elle exonère cependant d'un hébergement HDS mais nécessite la mise en place de mesures de protection des données complémentaires.

- Nous avons également noté un manque de sensibilisation de toutes les équipes opérationnelles au quotidien ce qui peut conduire à des écarts importants entre les procédures et les réalités opérationnelles.

1.1. SÉCURITÉ DES DONNÉES : ARTICULATION RGPD / HDS

Les réglementations HDS et RGPD sont **complémentaires**. La réglementation HDS renforce les mesures de sécurité à appliquer et rend leur mise en œuvre obligatoire avant toute opération d'hébergement.

Les mesures issues du RGPD sont donc renforcées en ce qui concerne :
- **L'instauration** d'une obligation en amont pour les hébergeurs de données de santé à caractère personnel d'obtenir une certification à cet effet avant tout hébergement des dites données,
- **Le renforcement des exigences** de sécurité applicables aux hébergeurs de données de santé à caractère personnel.

En plus de la complémentarité, ces deux réglementations présentent donc également une logique de **conformité continue**. La mise en œuvre d'une certification HDS pourra ainsi servir d'outil de convergence de la conformité à la réglementation RGPD.

Retour d'expérience

À travers nos expériences, nous avons relevé certains points de vigilance :

- Lors de la préparation d'une démarche de certification HDS, nous avons constaté que les impacts du RGPD n'étaient pas toujours pris en compte par un hébergeur (au-delà de l'aspect données sensibles) après l'entrée en vigueur le 25 mai 2018.

- Lors d'un audit de conformité RGPD, nous avons constaté qu'une organisation utilisait des données de santé sans les protéger. Plus précisément, l'organisation utilisait des objets connectés sans protéger les données qui s'échangeaient « en clair » par ces technologies. Notre recommandation, dans ce cas, est d'utiliser des outils de chiffrement de données entre l'objet et un serveur HDS en ne transmettant que les numéros de série des objets connectés et en aucun cas un identifiant patient dont le rapprochement avec l'identité du patient n'est réalisé qu'au niveau du serveur HDS.

- Nous avons également constaté qu'à des fins de formation des professionnels de santé, des appels de télémédecine étaient réécoutés sans anonymisation. S'il n'est pas prévu dans les contrats de réécouter les appels téléphoniques, le consentement du patient doit être recueilli en amont.

CYBER-ASSURANCE POUR LES ÉTABLISSEMENTS DE SANTÉ : L'ALÉA DU RISQUE RESTE À VÉRIFIER !

Les nouvelles récentes démontrent chaque mois que le secteur de la santé par les données qu'il détient intéresse vivement les cyber-pirates. Malgré le caractère vital des missions de ce secteur, il ne faut par ailleurs pas compter sur l'éthique des pirates. Même au plus fort de l'épidémie de Covid ces derniers ont mené des attaques virulentes à son encontre.

Chaque professionnel ou établissement de santé peut se heurter schématiquement à deux type d'attaques majeures :

- **Un sinistre court et intense** de type Ransomware : il bloque son exploitation, génère pertes et frais supplémentaires importants, et entraîne même des conséquences indirectes mais non moins dramatiques pour les établissements de santé comme des pertes humaines (Une cyber-attaque récente touchant une clinique à Düsseldorf a empêché la tenue d'une intervention dans les temps, entrainant le décès d'une patiente).

- **Un sinistre long** : les données des patients sont subtilisées puis exploitées par les cyber-pirates ou les receleurs des informations vendues. Dans un tel cas, il ne faut pas sous-estimer l'impact du mécanisme de notification qui accroit nécessairement les risques de réclamations. Les conséquences sont lourdes pour l'organisation qui n'aurait pas su sécuriser ces données. Les réclamations sont à la hauteur des préjudices potentiels des patients. Puisqu'en raison de la nature des données violées les patients se retrouvent eux-mêmes en risque vis-à-vis d'une usurpation d'identité, d'une divulgation publique de pathologie pouvant desservir leur vie sociale ou professionnelle.

Au-delà de procédures longues et coûteuses pour indemniser les tiers, l'autorité administrative compétente, **la CNIL, peut diligenter une enquête et aller jusqu'à sanctionner à terme**.

Dans le cas précédent il s'agit de la mise en jeu de la responsabilité de l'organisation – personne morale. Mais ces attaques peuvent être révélatrices d'un tout autre sinistre trop souvent oublié : la mise en jeu de la responsabilité personnelle du ou des dirigeants. Ainsi, si malgré les enjeux et obligations, il s'avère qu'ils n'avaient pas fait le nécessaire pour protéger les systèmes et données stockées, cela pourrait constituer une faute de gestion.

Nous le voyons à travers ces exemples les enjeux sont clairs, ils sont **financiers, opérationnels, juridiques et réputationnels**.

Les assureurs ont développé des produits permettant de répondre à ces problématiques. Ils incluent notamment :
- la garantie des pertes d'exploitations,
- celle des conséquences d'attaques par ransomware,
- un volet assurance dommages au tiers,
- et surtout une assistance solide incluant l'accès à des experts en cyber-sécurité, dont recherche de faille et reconstitution des données, mais également en communication de crise et bien entendu juridiques.

Pour ce qui est des dirigeants des contrats spécifiques existent également.

Toutefois et compte tenu des enjeux, avant de proposer ces garanties, **les compagnies opèrent une nécessaire sélection du risque**.

L'organisation souhaitant s'assurer doit démontrer qu'elle a su, au regard des enjeux, mettre en place les « premières défenses » en disposant des moyens techniques et des politiques appropriés. L'assurance ne sert en effet qu'à transférer la partie du risque, certes conséquente, que l'organisation elle-même ne pourrait assumer avec ses propres moyens en cas de crise.

Un contrat d'assurance ne peut pas résoudre les déficiences avérées.
Si les données et leurs accès ne sont pas sécurisés, dans les cas extrêmes il n'y a plus d'aléa, et sans aléa il ne peut y avoir d'assurance. Par ailleurs, sans sauvegardes de qualité, le travail des experts est nécessairement plus compliqué, long et onéreux ; sans conservation des logs (journaux d'évènements) les recherches de failles suivent le même chemin.

Les professionnels de la cyber-sécurité et les assureurs spécialistes constatent avec préoccupation, un déficit, **non de compétences des DSI** (qui méritent à n'en pas douter plus d'écoute de la part des dirigeants), **mais de moyens et de formations des utilisateurs**.

À ce jour, trop d'établissements, pour ne pas dire une majorité, sont dépourvus des moyens de base : systèmes parfois obsolètes, solutions de sauvegarde non pertinentes vis-à-vis des attaques par ransomware et parfois éloignées des standards de la certification HDS, accès à distances des praticiens non sécurisés, transferts de données non cryptées, etc.

Les conséquences sont évidentes : **beaucoup ne sont pas préparés à faire face à une cyber-attaque** et ne répondent pas aux règles édictées par le RGPD. En conséquence :
- une bonne partie ne peuvent s'assurer faute d'être assurables,
- une autre à travers des appels d'offres mal calibrés ou conscients de la qualité du risque qu'ils constituent sont insuffisamment garantis,
- enfin les établissements ayant pu développer une politique complète de management de leur risque cyber sont encore trop rares, mais ils existent.... tout comme les solutions.

Le secteur de la cyber-sécurité dispose d'audits spécialisés pouvant aider à **cartographier les risques** et **définir une stratégie efficace** devant s'exprimer in fine dans un plan de continuité d'activité intégrant les cyber-évènements. Des solutions techniques pertinentes sont proposées pour sécuriser les données et systèmes critiques, contrôler les accès et les flux. De même la **formation des personnels et praticiens – essentielle - sur l'hygiène en cyber-sécurité** peut simplement s'effectuer par des sessions d'**e-learning** (par exemple : nous avons développé pour des structures de moins de 10 millions d'euros de chiffre d'affaires ou de budget de fonctionnement, un outil dédié que nous proposons à nos assurés - la CyberClear Academy by Hiscox).

Une bonne défense vis-à-vis des cyber-attaques, si elle n'est pas suivie et mise à jour régulièrement, pourrait **s'avérer obsolète en quelques années si ce n'est quelques mois**. Nous constatons sur ce point une meilleure agilité des structures privées, le « tempo » des marchés publics face à une menace aussi évolutive, mériterait d'être revu, du moins les hôpitaux mériteraient de bénéficier de plus de moyens.

Pour les dirigeants, la cyber-sécurité nécessite une vigilance perpétuelle, le temps de la prise de conscience est passé, elle a eu lieu, celui de l'action s'impose et ils peuvent être accompagnés.

FRÉDÉRIC ROUSSEAU
Responsable de marché Cyber / Head of Cyber

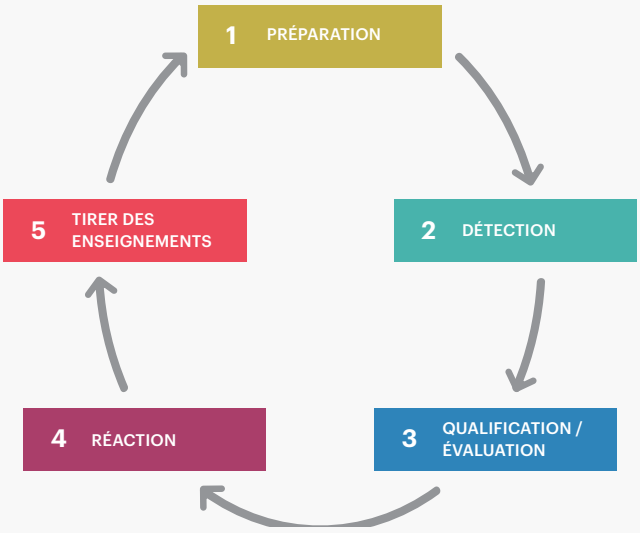
HISCOX ASSURANCES | Penser à tout, et surtout à vous

1.2. DÉCLARATION DES INCIDENTS

Selon une étude menée par l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), une organisation, quel que soit son secteur d'activité, met, en moyenne, environ 196 jours pour détecter un incident de sécurité. Ainsi, l'enjeu est d'introduire plus de réactivité dans la déclaration d'incidents en mettant en œuvre un ensemble de guides et de processus en interne prenant appui sur la méthodologie décrite dans la norme ISO 27035–1 : 2016, norme internationale sur la gestion des incidents.

Les différentes réglementations citées dans les parties précédentes impactent la gestion interne d'un incident.

CYCLE DE VIE D'UN INCIDENT DE SÉCURITÉ



Préparation :
En définissant par exemple une organisation autour de la gestion du risque qui liste les rôles et les responsabilités > Rôle du DPO imposé par le RGPD.

Détection :
En utilisant des outils conformes au RGPD.

Qualification / Évaluation :
En comparant aux critères préalablement définis et aux référentiels RGP et eiDas.

Réaction :
En notifiant la CNIL.

Retour d'expérience

À travers nos expériences, nous avons relevé certains points de vigilance :

- La CNIL pouvant diligenter un contrôle sur site, il convient de se préparer en amont, et d'être accompagné le cas échéant lors de ce type d'audit.

LE RGPD :
S'OUTILLER POUR SÉCURISER SON ACTIVITÉ

Les données de santé de vos patients ? C'est leur identité. C'est votre patrimoine. Ils vous font confiance. Vous devez garantir la protection et la sécurité de leurs données personnelles. Avec le RGPD, donnez-vous les moyens de vos ambitions en sécurisant et en consolidant votre niveau de service rendu aux patients. N'attendez plus pour adopter une démarche responsable à l'égard de vos patients !

S'outiller... pour aller plus vite

Mettre en conformité vos activités de traitement de données de santé, c'est tout d'abord décrire et documenter vos opérations sur les données dans un Registre. Par où commencer ?

Vous DPO, optimisez votre temps avec une solution vous guidant dans votre démarche, vous permettant d'automatiser des étapes, et d'homogénéiser vos approches.

S'outiller... pour aller plus haut

Le DPO a pour rôle d'orchestrer les chantiers de la conformité au RGPD de son organisme. Comment avoir une vision d'ensemble et garder une cohérence d'action ?

Vous DPO, prenez de la hauteur de vue, mettez en place une stratégie globale en adéquation avec les risques liés à l'activité de votre organisme, planifiez, priorisez, et passe à l'action. Avec des indicateurs d'activité, communiquez sur vos avancées et diffusez une culture respectueuse des données personnelles.

S'outiller... pour aller plus loin

La mise en conformité, c'est aussi vérifier la cohérence, la qualité et la conformité des informations recueillies, pour renforcer les dispositifs de protection et de sécurité des données. Comment vous assurer durablement de la protection des données personnelles au sein de votre organisation ?

Vous DPO, entrez dans une démarche d'amélioration continue sans perdre de vue les objectifs. Avec une approche intégrée et globale des problématiques du RGPD, vous pourrez alors être véritablement efficaces, vers la conformité !

S'outiller... pour aller mieux

Vos patients, vos clients, vos partenaires, les institutionnels, tous ont des attentes fortes : quelles garanties leur apportez-vous dans le traitement des données personnelles ? Et vous êtes-vous bien assurés de celles qu'apportent vos fournisseurs ?

Vous DPO, pour avancer serein dans l'écosystème dans lequel vous évoluez, assurez sur toute la chaîne la sécurité juridique de vos opérations sur les données personnelles, et justifiez de votre conformité, avec un espace de centralisation des obligations documentaires.

Pour en savoir plus : https://www.adequacy.app/

CLAIRE DE LA FOUCHARDIÈRE
Consultante Data Protection | RGPD

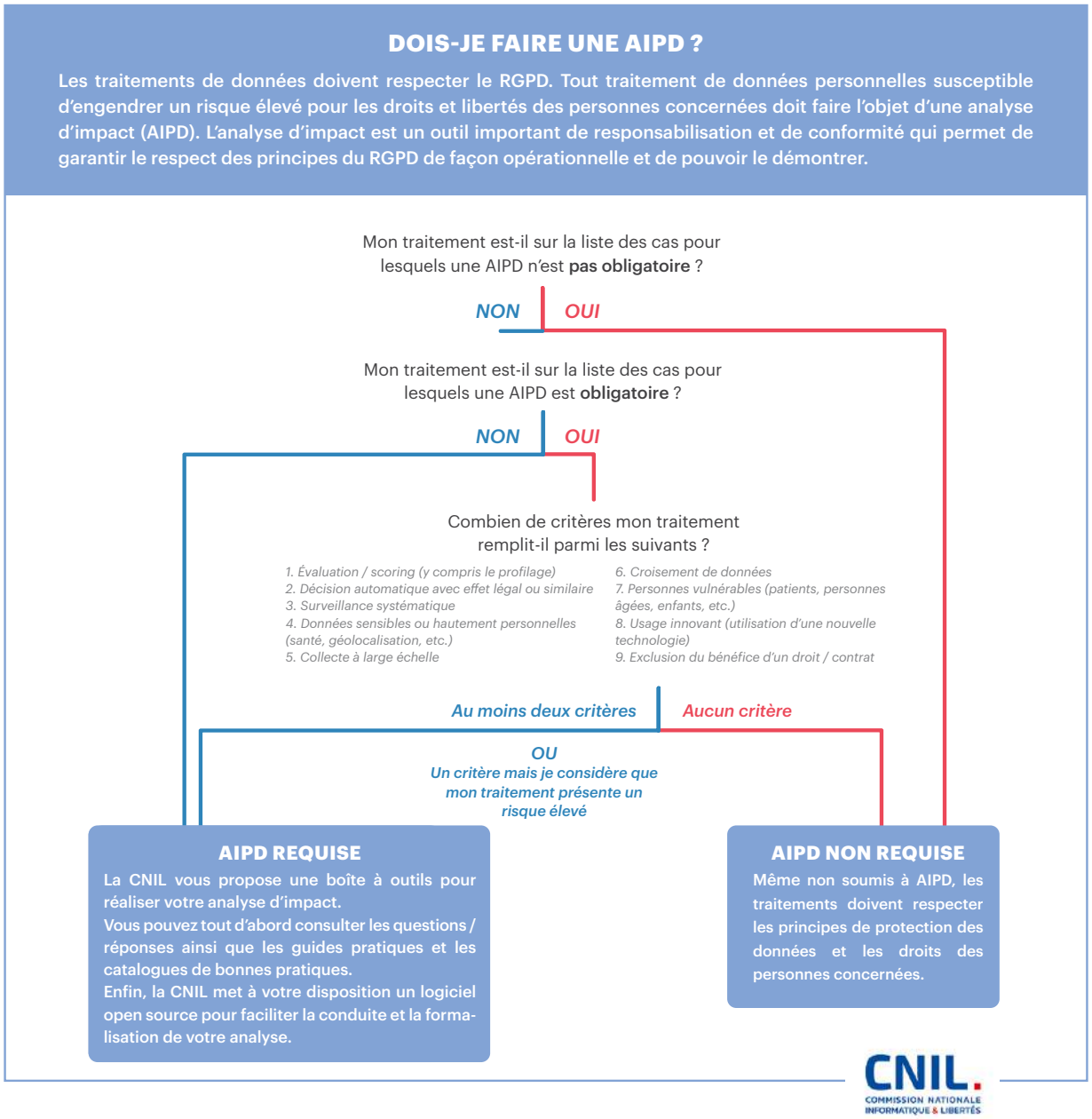
ADEQUACY

1.3. ANALYSE DE RISQUES AIPD

Qu'est-ce qu'une analyse d'impacts relative à la protection des données (AIPD) ?

L'AIPD est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au Règlement Général sur la Protection des Données (RGPD).
Elle est obligatoire pour les traitements susceptibles d'engendrer des risques élevés.

Comment savoir s'il faut faire une AIPD ?



L'AIPD se décompose en trois parties :

1/ Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels.

2/ L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques.

3/ L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

Retour d'expérience

D'après nos expériences, nous constatons que :

- Les analyses de risques ne sont pas toujours réalisées en amont de la mise en place d'une nouvelle application dans le SI d'une organisation et peuvent être à l'origine des failles dans la protection des données.

- La plupart du temps, le facteur humain est le « maillon faible » de toutes les procédures. Il convient donc de sensibiliser en permanence les acteurs des processus de l'organisation impliquant des données sensibles au travers des outils de sensibilisation comme les serious game.

2. IMPACTS SUR LA SÉCURISATION DU SI

2.1. PROCESSUS DE MISE EN PRODUCTION

S'agissant des logiciels s'exécutant sur des serveurs, il est conseillé d'utiliser des outils de détection des vulnérabilités (logiciels scanners de vulnérabilité, comme par exemple : Harfanglab, ComputableFacts) pour les traitements les plus critiques afin de détecter d'éventuelles failles de sécurité. Des systèmes de détection et prévention des attaques sur des systèmes ou serveurs critiques peuvent aussi être utilisés.

Ces tests doivent être menés de façon régulière et avant toute mise en production d'une nouvelle version logicielle.
L'une des précautions est d'effectuer les développements informatiques et les tests dans un environnement dédié distinct de celui de la production selon les bonnes pratiques ITIL, en veillant à ce que les jeux de données soient des données fictives ou anonymisées.

Retour d'expérience

D'après nos expériences, nous recommandons de bien définir les rôles et les responsabilités des différents intervenants entre l'organisation responsable du traitement, ses équipes techniques DSI, l'éditeur de l'application et l'hébergeur de données de santé HDS, qui peut mettre en place des processus spécifiques de mise en production pour éviter que les développeurs n'aient accès à des informations sensibles. Cela évite qu'un développeur restaure une base de production à partir d'une base de formation par exemple.

Contribution

EXEMPLE DE SOLUTION DE CYBERVIGILANCE

Les cyber-attaques contre les organismes de santé sont devenues une tendance lourde de ces dernières années[1]. Les prestataires de soins de santé ont en leur possession de très nombreuses données sensibles ce qui fait d'eux une cible privilégiée des cyber-attaquants[2].

Les entreprises investissent du temps et des ressources significatives dans la mise en place de contrôles de sécurité : pare-feux, VPN, isolement des applications et des bases de données dans des containers, etc. Cependant, peu d'entre elles testent et valident l'efficacité des contrôles de sécurité mis en place.

Il est cependant possible pour une entreprise d'évaluer l'efficacité des procédures de sécurité appliquées à une infrastructure ou à une application accessible en ligne en utilisant une plate-forme de tests d'intrusions automatisés. Par exemple, une plate-forme telle que ComputableFacts[3] utilise la méthodologie et les outils des cyber-attaquants pour simuler des attaques permettant de tester la vulnérabilité d'une entreprise aux ransomewares.

Ces plates-formes permettent aux entreprises d'effectuer des simulations de cyber-attaques en continu ou à la demande sans affecter les systèmes évalués : les vulnérabilités détectées ne sont pas exploitées mais reportées à l'entreprise. L'objectif ultime de ces attaques simulées est de mettre en évidence les lacunes et vulnérabilités de l'entreprise pour lui permettre de comprendre quelles tactiques, techniques et procédures d'attaque constituent une menace et dans quelle mesure les contrôles de sécurité mis en œuvre offrent une protection adéquate.

CYRILLE SAVELIEF
Directeur Associé

computable**facts**

(1) https://www.aha.org/center/emerging-issues/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed
(2) https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
(3) https://computablefacts.com/

2.2. BASE DE RECETTE / BASE DE FORMATION

Les bases de recette et bases de formation des personnels ne devraient pas utiliser les données personnelles des patients. Il faudrait que les données utilisées par ces bases soient mises en anonymat de manière professionnelle, en utilisant par exemple des algorithmes d'anonymisation.

Retour d'expérience

D'après nos expériences, nous constatons qu'il ne suffit pas de remplacer l'identifiant d'une personne pour l'anonymiser. Il convient d'utiliser des algorithmes d'anonymisation, ou pseudonymisation.
Il nous est arrivé également de retrouver sur des captures d'écrans utilisées dans des manuels utilisateurs... des identités de patients ou clients réels.

3. IMPACTS JURIDIQUES

3.1. SUR LES CONTRATS DE TRAVAIL

Dans les contrats de travail des salariés susceptibles d'accéder à des données de santé dans le cadre de leurs activités, il convient de s'assurer que les contrats prévoient des clauses de confidentialité.

Dans le cadre de nos missions, il est possible que nos consultants (salariés ou experts partenaires) interviennent sur des données personnelles de santé. Aussi, nous nous assurons que des clauses de confidentialité sont signées entre le cabinet et les intervenants (au travers un d'engagement de confidentialité spécifique) d'un côté et avec notre client de l'autre ; en outre, nous intervenons toujours sous la responsabilité d'un médecin inscrit à l'ordre (soit chez nos clients, soit dans notre communauté d'experts).

3.2. SUR LES CONTRATS AVEC LES FOURNISSEURS

Dans le cadre, par exemple, de contrats cloud avec des fournisseurs proposant des contrats d'adhésion standardisés, une entreprise française qui envisage d'avoir recours à ce genre de services doit être très rigoureuse et réaliser une analyse de risques.

L'entreprise a la responsabilité de s'assurer que le fournisseur offre des garanties en termes de protections des données personnelles.

Retour d'expérience

Lors de l'une de nos missions, nous avons constaté que les employés d'une plateforme téléphonique de support utilisateurs étaient basés hors territoire européen, ils pouvaient donc avoir accès à des données de santé à caractère personnel.

Nous avons donc :
- Limité les données auxquelles les employés avaient accès à celles nécessaires pour les activités de support téléphonique,
- Fait signer des clauses de confidentialité aux employés selon le cadre local (en transposant les obligations européennes en veillant aux « frottements juridiques », le cas échéant),
- Fait héberger les données sur des serveurs HDS à distance, accessibles uniquement par connexion sécurisée, et en s'assurant de l'auditabilité des traces de connexion.

3.3. SUR LES CONTRATS HDS

Les contrats HDS sont régulés par le décret du 1er avril 2018 qui liste, au nouvel Article R1111-11 CSP, ce que doivent contenir les contrats relatifs à l'hébergement, y compris en ce qui concerne la sécurité des données et l'accès aux données.

3.4. SANS OUBLIER LES OBLIGATIONS RGPD

Indépendamment d'un contrat HDS avec un organisme externe ou de contrats avec des fournisseurs chez lesquels transitent des données personnelles ou sensibles, il est de la responsabilité d'un responsable de traitement de définir les responsabilités de toutes les parties prenantes en termes de respect des exigences du RGPD.

Dans le cadre d'un contrat de sous-traitance, les organisations de santé doivent rester particulièrement vigilants, définir leurs propres exigences techniques et juridiques et conduire des analyses de risques.

Le recours à un hébergeur HDS n'exonère donc pas le responsable du traitement de ses relations avec ses autres fournisseurs ou sous-traitants.

DONNÉES DE SANTÉ : SAUVEGARDES, ARCHIVAGES, EXTERNALISATION HDS

La légitime conservation sécurisée des données de santé

Les données de santé produites en quantité au sein des structures de soins représentent sans conteste la mémoire persistante de la santé numérique : prescriptions médicales, résultats d'analyse biologique, comptes rendus de réunions pluridisciplinaires, bilans thérapeutiques du patient, feuilles de soins électroniques, résultats d'imagerie médicale, dossiers de suivi longitudinale du patient, données produites par les objets connectés... Dès lors, la conservation et la protection de cette mémoire apparaît fondamentale aux yeux des patients, des soignants et des pouvoirs publics. Il appartient ainsi aux responsables de traitement de recourir à des dispositifs de protection à l'état de l'art comme la sauvegarde et l'archivage dans le respect de la Politique de Sécurisation des Systèmes d'Information (PSSI) en vigueur.

La sauvegarde (back-up) :

Comment restaurer les données endommagées ?

Parce que le risque Zéro n'existe pas, que les sinistres comme l'incendie, le dégât des eaux, le vandalisme ou le vol sont possibles, que les arrêts de production coûtent chers et que les utilisateurs ne tolèrent désormais plus l'indisponibilité des services numériques (qu'ils soient métiers, bureautique, messagerie, téléphonie ou internet), la mise en place d'une politique de sauvegardes contrôlée et adaptée aux risques identifiés est devenue une obligation. L'état de l'art préconise d'ailleurs une sauvegarde 3-2-1, c'est-à-dire la réalisation de 3 copies minimum pour une même donnée sur 2 supports différents avec 1 sauvegarde hors site.

« 60 % des données sensibles dans le cloud sont stockées dans des documents Office et ne sont pas sauvegardées à 75 % ».

L'archivage : Comment stocker à long terme ?

Si la sauvegarde permet de gérer l'urgence et de restaurer des données fiables au plus vite afin de relancer la production, elle n'a pas vocation à conserver des données sur une longue période. Au-delà d'un an, il apparaît intéressant de supprimer les données d'origine pour se tourner vers des dispositifs d'archivage sur des systèmes moins coûteux comme des bandes, des disques capacitifs, voir des systèmes spécifiques ad hoc en cloud public. Afin de récupérer la donnée, le logiciel de recherche d'archives se doit d'être performant ; en disposant de l'archivage à valeur probante, il apporte une richesse fonctionnelle supplémentaire permettant, dans le respect des lois, de garantir l'authenticité, intégrité et l'intelligibilité des documents archivés. En d'autre terme, cela permet de prouver que le document archivé n'est pas un faux.

L'externalisation chez un hébergeur certifié HDS

L'externalisation des sauvegardes et/ou des archives est considérée comme faisant partie des best practices de sécurité de l'information. Loin d'être une option, le recours à un hébergeur certifié HDS est donc le complément indispensable à ajouter à tout bonne politique de sauvegarde/archivage et constitue également un excellent point de départ en matière de Plan de Reprise d'Activité (PRA). L'interconnexion sécurisée, rapide et fiable de la structure de soins avec l'hébergeur est un autre élément sur lequel il ne faut pas transiger.

SÉBASTIEN DEON,
Directeur des Offre e-Santé

Adista
Accélérateur de confiance en santé numérique

PERSPECTIVES ET ENJEUX À VENIR

Vol des données de santé : à qui profite le crime ?

Au-delà des risques pour la sécurité des soins exposés dans ce livre blanc, on peut se demander quels intérêts sont à l'oeuvre derrière la récupération massive des données de santé. En effet, à moins d'être un « VIP », les données de santé du citoyen lambda n'intéressent que l'équipe de soins à l'hôpital ou en ville pour la coordination des soins.

Les assureurs, souvent accusés de vouloir récupérer des données de santé à des fins de « sélection du risque », sont souvent pointés du doigt. Notre connaissance profonde de ces acteurs économiques nous fait clairement conclure au fantasme populaire :
- d'une part, parce que la santé est un « risque court » et qu'à ce titre, les montants financiers sont importants en « flux » (avec une saisonnalité liée à l'état de santé de la population, modulo les périodes de pandémie et de confinement), mais pas en « stock » (contrairement à la prévoyance ou à la retraite dont les provisions financières pèsent lourds dans les bilans financiers de ces organisations) ;
- et d'autre part, parce que les assurances et mutuelles sont soumises à une réglementation très contraignante, sous surveillance de l'autorité de contrôle prudentiel et de résolution (ACPR) - intégrée à la Banque de France. Nous savons par exemple que la convention AERAS, acronyme de « S'Assurer et Emprunter avec un Risque Aggravé de Santé » depuis 2007, est appliquée scrupuleusement par l'ensemble des assureurs emprunteurs du marché en France.

En revanche, on peut se poser la question de l'intérêt de certains Etats souhaitant jouer un rôle sur la scène internationale, et qui soutiennent leurs entreprises à travers l'intelligence économique. Prenons l'exemple de la recherche médicale : les données des patients lors des études cliniques constituent une véritable mine d'or pour les sociétés travaillant sur les médicaments ou les vaccins. En particulier dans la période actuelle, les centres de recherches des hôpitaux et des organisations publiques ou privées sont des cibles de choix. Nul besoin d'une attaque par des hackers surdoués, des étudiants poursuivants leur cursus dans nos universités ou centres de recherche peuvent assez facilement accéder aux données de cohortes de patients et les copier ; elles sont ensuite exploitées au sein de publications et d'études qui représentent un important levier d'influence internationale. Pour résumer, la santé et ses données sont devenues un enjeu géopolitique mondial.

Données de santé : un subtil équilibre entre protection et innovation

Le partage et l'exploitation des données de santé est au cœur des enjeux du développement de la santé numérique et des solutions de médecine augmentée. En effet, des solutions de plus en plus personnalisées mettent le patient au cœur du parcours de soins grâce à des technologies qui reposent sur le traitement massif des données de santé, telles que les objets connectés, l'intelligence artificielle, etc. Si l'innovation en santé paraît nécessaire pour répondre aux enjeux de nos sociétés (vieillissement des populations, recrudescence des maladies chroniques, urbanisation des modes de vie, ...), la protection des données qui en découle et la mise en place d'un cadre juridique adaptés à la réalité du terrain sont tout aussi indispensables.

En effet, bien que la réglementation française semble contraignante, celle-ci est un facteur de confiance pour les patients, usagers et citoyens.
Cette confiance, nécessaire au développement de nouvelles technologies en santé numérique, passe par la protection des données de santé. En 2017, selon un sondage Odexa réalisé pour le Think Thank Healthcare Data Institut (HDI), plus de 80% des répondants se disent favorables – sous conditions – au partage de leurs données de santé à des fins de recherche médicale et de mesure des parcours de soins et des produits de santé. Parmi les conditions citées par les sondés, on retrouve l'anonymisation mais aussi le droit à l'information et le droit constant à l'opposition à l'utilisation de leurs données. Ces conditions, qui ne sont pas sans rappeler les principes de privacy by design du RGPD, montrent comment le cadre juridique peut instaurer un climat de confiance entre les professionnels de santé et les patients et favoriser ainsi le développement de l'innovation.

Par ailleurs, la réglementation peut aussi être une opportunité pour les entreprises qui, en la respectant, acquièrent une réelle appréhension des risques et peuvent ainsi développer leurs offres en accord avec l'environnement complexe qui les entoure. Si le RGPD alourdit les obligations à la charge des entreprises, il uniformise aussi ces obligations à l'échelle Européenne. Les entreprises en conformité en France sont donc préparées à se lancer sur le marché Européen.

Notons par ailleurs que le cadre juridique est amené à évoluer dans les années à venir afin de s'adapter aux innovations technologiques (blockchain par exemple). Ces évolutions de la réglementation sont d'autant plus indispensables que plusieurs questions restent sans réponses tranchées : quelle valorisation (pas uniquement économique) des données de santé ? Quel droit d'usage voire monétisation les individus peuvent-ils avoir sur leurs données ?

Pour toutes ces raisons, il est important pour les entreprises d'être à jour sur l'évolution du cadre juridique et d'œuvrer tout d'abord à se mettre en conformité. Ce processus et ses impacts aussi nombreux que variés, détaillés dans les parties précédentes, montrent que la protection des données de santé est loin d'être une simple case à cocher. C'est un réel changement de paradigme à même de devenir un avantage compétitif pour les entreprises et acteurs qui sauront en tirer parti.

N'attendez pas la loi - ou l'incident de sécurité - pour protéger vos données et celles de vos patients.

IMPACT DU « PRIVACY SHIELD » SUR LES DONNÉES DE SANTÉ

Par une décision du 16 juillet 2020 , la Cour de Justice de l'Union Européenne (CJUE) a invalidé le « bouclier de protection des données » (dit « privacy shield ») entre l'Europe et les États-Unis, au motif d'une protection des données sur le sol américain jugée inadéquate et insuffisante. Le contexte est le suivant tel que décrit sur le site de la CNIL : « La CJUE a invalidé la décision d'adéquation « Privacy Shield », adoptée en 2016 par la Commission européenne suite à l'invalidation du « Safe Harbor », **qui permettait le transfert de données entre l'Union européenne et les opérateurs américains adhérant à ses principes de protection des données sans autre formalité**. » Dès son entrée en vigueur ce texte a suscité de nombreuses réserves au regard des libertés et droits fondamentaux des personnes concernées. Cette invalidation annoncée de longue date n'est donc pas surprenante.

Le RGPD prévoit plusieurs outils juridiques pour encadrer le transfert de données à caractère personnel vers des pays en dehors de l'UE. Les décisions d'adéquation, comme l'accord Privacy Shield, constituent l'un des principaux outils de transfert. **En l'absence d'une telle décision d'adéquation, le responsable du traitement ou le sous-traitant doit mettre en place des garanties appropriées prévues à l'article 46 du RGPD pour encadrer le transfert envisagé**. Parmi ces garanties, figurent notamment les Clauses Contractuelles Types (CCT) adoptées par la Commission. La CJUE a validé la décision de la Commission européenne relative aux clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants établis dans des pays tiers. Néanmoins, cette validation est conditionnelle. Il semble qu'il faille a minima **les compléter par des mesures complémentaires** tels que des **mesures particulières de chiffrement** (lorsque cela est possible en fonction du cas d'usage concerné).

Dans le domaine de la santé

Les données de santé étant particulièrement sensibles, cette évolution du cadre juridique est particulièrement préoccupante, notamment pour le choix de l'hébergeur des données pour des traitements nécessitant le recours à un prestataire tiers. **Ce choix fait actuellement l'objet de controverses concernant le Health Data Hub (HDH)**, entrepôt **national** de données **pseudonymisées**, composé notamment des données de l'assurance maladie, des données de facturation hospitalière, des causes médicales de décès, des données médico-sociales des personnes handicapées et d'un échantillon de données de remboursement des organismes complémentaires et dont l'hébergement a été confié en avril 2020 à la société américaine Microsoft.

Le Conseil d'État s'est déjà prononcé une première fois en référé le 19 juin 2020, à l'égard de l'arrêté du 21 avril 2020 qui autorise la plateforme « Health Data Hub » à récolter différentes données de santé pour la gestion de l'urgence sanitaire et l'amélioration des connaissances sur le covid-19. Il a estimé qu'il « n'apparaît pas que l'arrêté (...) porte une atteinte grave et manifestement illégale au droit au respect de la vie privée et au droit à la protection des données personnelles ». Un nouveau recours a été déposé le 18 septembre 2020 par un collectif de 18 organisations et personnalités en mettant en avant l'illégalité du transfert de ces données de santé, personnelles, sensibles et couvertes par le secret médical vers les États-Unis.

Cette situation générée par la décision de la CJUE de juillet dernier **entraîne des conséquences qui ne sont encore que partiellement mesurées au plan juridique** ainsi que d'importants rapports de force entre les États-Unis et l'Union européenne concernant le transfert des données personnelles en dehors de notre espace juridique et la souveraineté numérique.

FLORENCE EON-JAGUIN
Avocate associée

WITHLAW
SOLUTIONS JURIDIQUES DE SÉCURITÉ

Arrêt en grande chambre de la CJUE du 16 juillet 2020 dans l'affaire C-311/18 (dite « Schrems II »)
http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0
https://www.cnil.fr/fr/invalidation-du-privacy-shield-la-cnil-et-ses-homologues-analysent-actuellement-ses-consequences
https://pad.interhop.org/s/BJ2cxGT4v#

DATA

ANNEXES

Quelle(s) durée(s) pour la conservation des données de Santé ?

Conformément au RGPD et à la loi Informatique et Libertés, une donnée ne peut être conservée indéfiniment. En effet, les données de santé ont « un cycle de vie » correspondant à des phases de traitements successives :

> La conservation en base active :
- C'est la durée nécessaire à la réalisation de l'objectif ayant justifié la collecte des données. Cette durée est, en général, de deux ans maximum pour les entreprises.
- Concrètement, les « données en base active » sont facilement accessibles dans l'environnement de travail immédiat des professionnels de santé.

> Archivage intermédiaire :
- Les données ne sont plus utilisées pour atteindre l'objectif ayant justifié leur collecte mais présentent un intérêt administratif ou remplissent une obligation légale pour l'organisme.
- Ces données ne sont pas accessibles par tous les opérationnels mais uniquement par les professionnels habilités et de manière ponctuelle.

> Archivage définitif :
- En raison de leur valeur, certaines données sont archivées de manière pérenne et définitive.

Les durées de conservation des données de santé (hors recherche scientifiques) sont variables selon le type d'archivage. Les durées de conservations sont régies par la loi dans la plupart des cas, il appartient donc au responsable de traitement de vérifier et mettre en oeuvre la durée de conservation conforme à ces obligations ou recommandations.

La CNIL a résumé ces durées de conservation dans le tableau repris sur les pages suivantes.

RÉFÉRENTIEL CNIL

Activités de traitements	Détails	Durée de conservation en base active	Durées de conservation en base intermédiaire	Fondements juridiques Textes de références	Date de mise à jour
Prise en charge des patients par les établissements de santé (dossier patient)	/	Pendant la durée de la prise en charge opérationnelle du patient (au cours d''une consultation, de l'hospitalisation, ou de la réalisation d'un examen) puis 20 ans à compter du dernier passage pour soin (dernier séjour du patient ou consultation externe au sein de l'établissement). Cas particuliers: Décès SI le patient décède moins de 10 ans après son dernier passage dans l'établissement, son dossier est conservé pendant une durée de 10 ans à compter de la date du décès. Mineur Lorsque la durée de conservation du dossier s'achève avant le 28e anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dossier transfusionnel La mention des actes transfusionnels pratiqués et, le cas échéant, la copie de la fiche d'incident transfusionnel qui doivent figurer dans le dossier médical en vertu du l) du 1° de l'article R. 1112-2 du code de la santé publique doivent y être conservées pendant une durée de trente ans à compter du dernier passage du patient Recours et contentieux Ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison	Il appartient au responsable de traitement d'évaluer, notamment pour les cas particuliers (ex : décès du patient, déménagement du patient, etc.) l'opportunité d'archiver certaines données en base intermédiaire.	*Article R. 1112-7 du code de la santé publique (CSP)*	18/06/2020
Gestion des cabinets médicaux et paramédicaux	/	5 ans à compter de la dernière intervention sur le dossier du patient	15 ans sur un support distinct dans des conditions de sécurité équivalentes à celles des autres données enregistrées dans l'application	*Référentiel « Gestion des cabinets médicaux et paramédicaux »*	18/06/2020
Gestion d'une pharmacie d'officine	Dossier patient	3 ans à compter de la dernière intervention sur le dossier	15 ans	*Norme simplifiée n°52*	18/06/2020
	L'ordonnancier	N/A[1]	10 ans	*Article R. 5125-45 du CSP*	18/06/2020
	Les copies d'ordonnance de médicaments classés comme stupéfiants ou relevant de la réglementation des stupéfiants	N/A	3 ans	*Article R. 5132-35 du CSP*	18/06/2020
	Le registre comptable des médicaments stupéfiants, les documents attestant de leur destruction	N/A	10 ans à compter de leur dernière mention	*Article R. 5132-36 du CSP*	18/06/2020
	Les bons de traçabilité des lots de médicaments ou autres produits pharmaceutiques acquis	N/A	5 ans	*Article R. 5124-58 du CSP*	18/06/2020
	Le registre des médicaments dérivés du sang	N/A	40 ans	*Article R. 5121-195 du CSP*	18/06/2020

[1] N/A : non applicable

Légende :

Les durées prévues par les textes cités sont des durées obligatoires imposées par la réglementation.

Les durées prévues par les textes cités sont des durées recommandées par la CNIL, qui ne revêtent pas un caractère obligatoire.

LES DURÉES DE CONSERVATION

Traitements dans le domaine de la santé (hors recherches)

Activités de traitements	Détails	Durée de conservation en base active	Durées de conservation en base intermédiaire	Fondements juridiques Textes de références	Date de mise à jour
Laboratoires d'analyse de biologie médicale	Dossier patient	5 ans à compter de la dernière intervention sur le dossier	15 ans	*Norme simplifiée n°53*	18/06/2020
	Relevé chronologique des analyses effectuées par le laboratoire ou transmises à un autre laboratoire (pour les laboratoires d'analyses de biologie médicale soumis aux dispositions de la loi du 11 juillet 1975)	N/A	10 ans		
	Résultats nominatifs des analyses (pour les laboratoires d'analyses de biologie médicale soumis aux dispositions de la loi du 11 juillet 1975))	N/A	5 ans		
	Dossiers et livres de registre (pour laboratoires réalisant des analyses dans les établissements de santé)	Voir la durée pour les établissements de santé			
	Analyses génétiques (comptes rendu d'analyses et commentaires explicatifs)	Le temps de la réalisation des comptes rendus et des commentaires explicatifs des analyses	30 ans	*Article R. 1131-20 du CSP*	
Gestion par les opticiens lunetiers de leur activité professionnelle	/	5 ans	15 ans	*Norme simplifiée n°54*	18/06/2020
Télétransmission des feuilles de soins	Double électronique des feuilles de soins et des accusés de réception	3 jours ouvrés en cas de paiement direct de l'assuré 8 jours ouvrés lorsque l'assuré bénéficie d'une dispense d'avance de frais	Conservation du double électronique et des accusés réception pendant 90 jours à compter de la transmission des feuilles de soins par voie électronique par le professionnel, l'organisme ou l'établissement ayant effectué des actes ou servi des prestations remboursables	*Article R. 161-47 du code de la sécurité sociale (CSS)*	18/06/2020
	Décomptes de remboursement de la sécurité sociale	N/A	Conservation pendant 2 ans des décomptes de remboursement de l'assurance maladie et maternité. Le délai court : - pour les prestations de l'assurance maladie : à compter du premier jour du trimestre suivant celui auquel se rapportent lesdites prestations - pour les prestations de l'assurance maternité : à compter de la date de la première constatation médicale de la grossesse.	*Article L. 332-1 du CSS*	

Légende :

Les durées prévues par les textes cités sont des durées obligatoires imposées par la réglementation.

Les durées prévues par les textes cités sont des durées recommandées par la CNIL, qui ne revêtent pas un caractère obligatoire.

RÉFÉRENTIEL CNIL

Activités de traitements	Détails	Durée de conservation en base active	Durées de conservation en base intermédiaire	Fondements juridiques Textes de références	Date de mise à jour
Dossier pharmaceutique	Les données mentionnées à l'article R. 1111-20-2-I-1° relatives au bénéficiaire	Jusqu'à la clôture du dossier	N/A	*Article R. 1111-20-11 du CSP*	18/06/2020
	Les données mentionnées à l'article R. 1111-20-2-I-2° relatives à la dispensation des médicaments	4 mois à compter de la date de saisie	32 mois	*Article R. 1111-20-12 du CSP*	
	Les données mentionnées à l'article R. 1111-20-2-I-2° relatives à la dispensation de vaccins	21 ans à compter de la date de saisie			
	Les données mentionnées à l'article R. 1111-20-2-I-2° relatives à la dispensation de médicaments biologiques	3 ans à compter de la date de saisie			
	Les traces de refus de création ou de clôture d'un dossier pharmaceutique	36 mois	N/A	*Article R. 1111-20-3-1 du CSP*	
Dossier médical partagé (DMP)	/	Le temps de l'utilisation du dossier par le patient	10 ans à compter de la clôture du dossier	*Article L. 1111-18 du CSP*	18/06/2020
Dépistage organisé du cancer du sein, du cancer colorectal et du cancer du col de l'utérus mis en oeuvre par les structures de gestion conventionnées	/	Les données relatives à la prise en charge des personnes concernées sont conservées par les structures en charge de la mise en oeuvre des programmes de dépistage des cancers jusqu'à la fin du suivi, décidée par la personne elle-même ou son médecin. Ces durées doivent être conformes aux dispositions législatives et réglementaires en vigueur.	Conservation possible pour les données strictement nécessaires à l'accomplissement d'obligations légales pendant une durée fixée, ou, si les données présent un intérêt administratif (ex: contentieux)	*Arrêté du 22 février 2019* *Arrêté du 19 mars 2018* *Arrêté du 4 mai 2018*	18/06/2020
Vigilances sanitaires	/	Conservation en base active pendant la durée d'utilisation courante des données	Durée légale ou réglementaire applicable à chaque vigilance En l'absence de précision légale ou réglementaire, les données ne peuvent en principe être conservées au-delà d'une période de 70 ans à compter de la date du retrait sur le marché du médicament, du dispositif ou du produit.	*Référentiel « vigilances sanitaires »*	18/06/2020

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Légende :

Les durées prévues par les textes cités sont des durées obligatoires imposées par la réglementation.

Les durées prévues par les textes cités sont des durées recommandées par la CNIL, qui ne revêtent pas un caractère obligatoire.

QUI SOMMES-NOUS ?

1. DOSHAS CONSULTING

Cabinet de conseil indépendant fondé par Didier Ambroise, Doshas Consulting se positionne depuis 7 ans comme un acteur engagé dans la transformation numérique de la santé. Précurseur dans le domaine de la santé numérique, le cabinet bénéficie d'une cinquantaine de références dans l'écosystème de la santé et de la protection sociale.

Portée par une conviction stimulante et communicative, la force de Doshas Consulting est de fédérer les meilleures compétences et expertises pour faciliter la co-construction de projets innovants.

Pour accompagner aujourd'hui la construction du monde d'après, Doshas Consulting intervient sur différents aspects de la cybersécurité, l'innovation et la santé numérique.

Le cabinet propose notamment des offres adaptées concernant :

- **Le programme Ma Santé 2022**
- **La Gouvernance des données de santé**
- **La Protection de la donnée (RGPD, HDS, cyberscurité)**

2. NOS RETOURS D'EXPÉRIENCE SUR LA PROTECTION DES DONNÉES DE SANTÉ

À ce jour, nous avons accompagné **une vingtaine d'acteurs dans toutes les étapes de protection des données de santé** :

- **Démarche d'agrément ou de certification HDS** d'établissements de santé, de groupes mutualistes sur le périmètre innovation santé et e-Santé, des infogéreurs ou hébergeurs « secs » souhaitant devenir « Hébergeur de données de santé ».
- **Sécurisation des données de santé** pour des organisations de santé (établissements, professionnels de santé libéraux, associations de patients, fondations de santé) tant **du point de vue RGPD que HDS**.
- Industriels de la santé (éditeurs de logiciel, sociétés relevant des Dispositifs Médicaux) sur le **choix d'un partenaire hébergeur HDS**.
- **Analyses de risques** cyber pour des établissements de santé et des industriels pharmaceutiques ou du DM .

Doshas Consulting est le seul cabinet conseil disposant d'une **approche globale « protection de la donnée de santé »**, nous avons notamment co-organisé avec nos partenaires le 5 février 2020 la première édition du CyberCamp Santé en croisant à la fois les aspects **juridiques, médicaux, IT, Sécurité et innovations** en matière de **cybervigilance**.

CYBERCAMP Santé

Aftermovie de l'événement : https://bit.ly/CyberCampSante

Depuis Septembre 2020, nous commercialisons un **Serious Game** pour l'ensemble des acteurs de la Santé et de la protection social pour sensibiliser et former les utilisateurs comme les directions à la CyberSécurité. Ce Serious Game, appelé **MediRisk**, a été éprouvé auprès de DSI, RSSI et DPO en santé, mais également auprès d'avocats santé, assureurs et des agences nationales de santé.

MEDIRISK

SERIOUS GAME DE SENSIBILISATION ET DE FORMATION AUX RISQUES CYBER DANS LES ÉTABLISSEMENTS DE SANTÉ

OUTILS DE SIMULATION POUR AGIR ET RÉAGIR EN TEMPS RÉEL

POURQUOI UN SERIOUS GAME SUR LE RISQUE CYBER ?

1. **Sensibiliser...** et former vos équipes (comité de direction, soignants, RSSI) à l'hygiène numérique rapidement et à moindre coût, ce qui permet de diminuer les risques et conséquences d'actes cyber malveillants,

2. **Se préparer...** aux cyberattaques en analysant les différentes menaces, leurs impacts sur votre activité et les meilleures réponses à apporter,

3. **Entraîner...** une cellule de crise cyber au-delà des formes classiques dans le secteur de la santé (Plan blanc, dispositif ORSAN, dispositif ORSEC...).

3 SCÉNARIOS DE CRISE

. Centre hospitalier
. Laboratoire Estrazy
. Réseau Médicis

MEDIRISK COMPREND :

Un livret de règles, un plateau de jeu, des fiches scénarios, des cartes Menaces, Conséquences et Moyens...

Offre exclusive Doshas Consulting . Crédits : Doshas Consulting, Medirisk, iStock . IPNS Ne pas jeter sur la voie publique

01 84 20 07 83 | www.medirisk.game

3. ILS NOUS FONT CONFIANCE

Conception : Doshas Consulting
Responsable de la publication : Didier Ambroise
Rédaction : Didier Ambroise et Rim Mrabet
Création graphique et réalisation : Doshas Consulting
Crédits : iStock, Shutterstock et Doshas Consulting

153 boulevard Haussmann 75008 PARIS

01 84 20 07 83

contact@doshas-consulting.com

www.doshas-consulting.com

Retrouvez notre actualité sur les réseaux sociaux

@DoshasConseil

Page entreprise

Chaîne YouTube