Mémento
à l'usage
du directeur
d'établissement de santé

Connaître vos risques pour mieux y faire face

Cybersécurité **édition 2017**

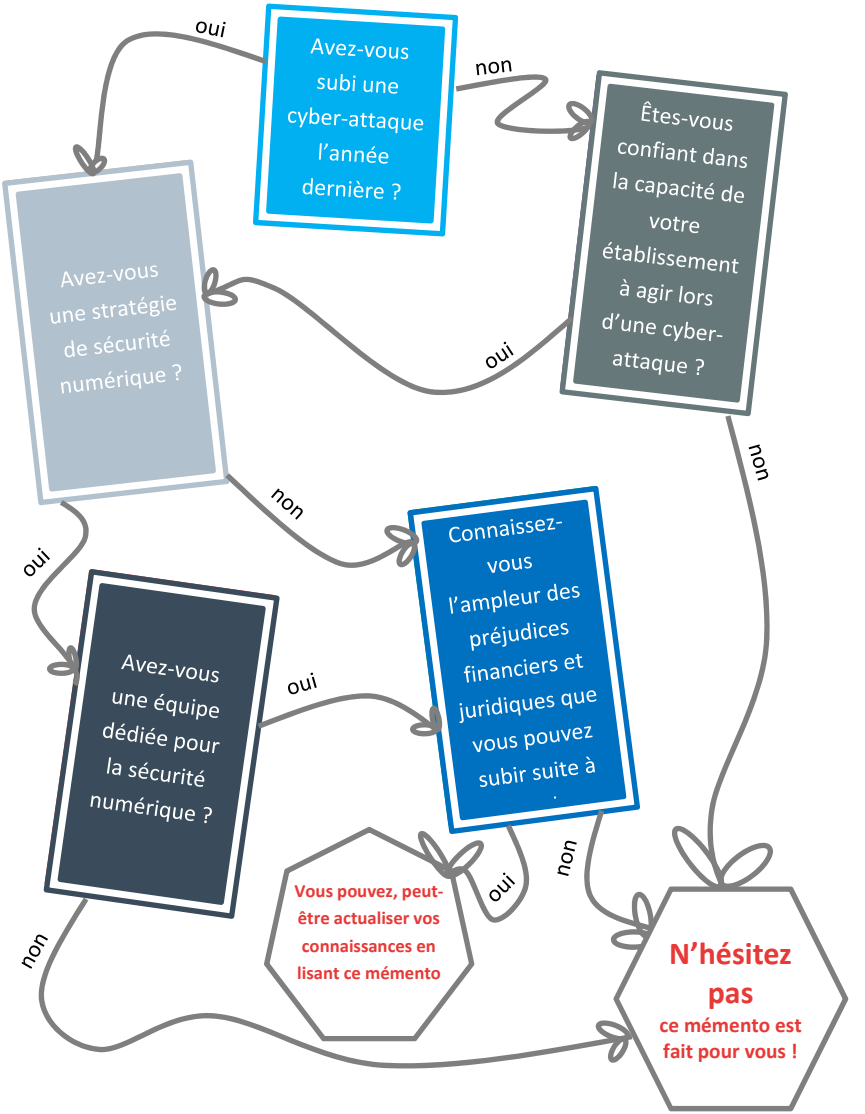
Vulnérabilités
Protection de la donnée
Gouvernance
Pilotage et contrôle

DIRECTION GÉNÉRALE DE L'OFFRE DE SOINS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE CHARGÉ DE LA SANTÉ

HÔPITAL NUMÉRIQUE

Ce guide est-il fait pour vous ?



Le mot de la directrice générale de l'offre de soins

Cécile COURREGES

L'organisation de l'offre de soins doit pouvoir évoluer en permanence et s'adapter aux besoins du patient et aux nouveaux enjeux de santé publique. Pour renforcer, par exemple l'accès territorial aux soins, il faut pouvoir tirer tout le bénéfice des technologies de l'information et des communications. Le numérique favorise en effet l'échange, le partage, et donc le décloisonnement entre les différents acteurs.

Il favorise la prise en charge ambulatoire en contribuant à des organisations plus efficientes et réduit les distances en permettant de développer la télémédecine. Il porte également, au cœur de toutes ces masses de données stockées, un immense potentiel d'information.

Tous ces nouveaux outils, ces nouvelles organisations, ne peuvent se déployer au quotidien que si les patients et les professionnels de santé leur accordent une pleine confiance.

Or, dans un environnement où la numérisation s'accélère et devient omniprésente, de nouveaux risques apparaissent. Il est donc essentiel d'être en situation de pouvoir les comprendre, les évaluer afin de mieux les maîtriser. Les méthodes et outils de la sécurité numérique ne manquent pas, mais ils perdent toute efficacité s'ils ne sont pas soutenus en permanence. Cela relève notamment du management des établissements de santé (directeur, directeur des soins, directeur des ressources humaines, président de commission médicale d'établissement) de les promouvoir et d'en accompagner la mise en œuvre.

Le présent mémento a pour objectif d'éclairer les décideurs sur la sécurité des systèmes d'information, d'en préciser les enjeux, le contexte réglementaires et les actions clés à mettre en œuvre. Un mémo-quizz « plan d'actions ssi » disponible à la fin du document propose des repères afin de faciliter la mise en œuvre de plans d'action.

Bonne Lecture,

Cécile Courrèges

En Bref

Les systèmes d'information sont des outils de partage et d'échange incontournables, au bénéfice des patients, des professionnels et du système de santé. Il est donc crucial de garantir leur sécurité pour maintenir la confiance des patients dans le système de santé et celle des professionnels dans les outils qu'ils utilisent chaque jour. Il convient pour cela d'**installer une véritable démarche de gestion du risque numérique**. Celle-ci vise à traiter ces risques, c'est-à-dire les réduire, les éviter, les partager ou les accepter, en étant pleinement conscient de ses vulnérabilités et ayant apprécié tout l'impact d'un potentiel accident de sécurité.

Il s'agit également de prendre toute la mesure du **véritable patrimoine d'informations** que représentent les données du système d'information parmi lesquelles les données de santé sont les plus sensibles. Le **nouveau règlement européen** pour la protection des données définit ce que sont ces « données à caractère personnel concernant la santé » et il établit tout un **cadre de protection** qu'il convient d'appliquer à partir du 25 mai 2018, en particulier en désignant un **délégué à la protection des données personnelles**.

La protection du système d'information et de ses données est un travail de tous les jours et qui concerne tout le monde, un travail par lequel on doit pouvoir **garantir la disponibilité des données, leur intégrité, leur confidentialité, et apporter la preuve des seuls usages autorisés**. A ce titre, la notion d'hébergement des données de santé requiert le respect d'une règlemention stricte et précise.

Si le premier pas vers la réduction des risques est une prise de conscience collective, le **soutien de la Direction est le principal facteur clé de succès** et de constance dans l'action. Celle-ci doit, d'ailleurs, rester réaliste pour ne pas décourager les différentes parties prenantes. Elle doit s'exprimer dans le cadre d'une véritable **politique de sécurité de l'établissement**, élaborée par un **reponsable sécurité du système d'information, dûment mandaté**.

Dans ce travail, l'établissement de santé trouve ses grandes orientations au sein même des référentiels nationaux produits dans le cadre de **la politique générale de sécurité des systèmes d'information de santé** (PGSSI-S) élaborée par l'ASIP Santé, dans l'atteinte des **prérequis du programme Hôpital Numérique**, et dans le **plan d'action sur la sécurité des systèmes d'information**.

Enfin, grâce au tout nouveau **dispositif de signalement des incidents de sécurité des systèmes d'information de santé**, mis en place depuis le 1er octobre 2017, il dispose désormais d'un accompagnement opérationnel face à un incident grave de sécurité de son système d'information.

Table des matières

Vulnérabilité

Protection de la donnée

Gouvernance

Pilotage et contrôle

1 L'univers numérique qui entoure le patient s'accroît sans cesse

Vulnérabilité

Dans la perspective de la mise en œuvre de la stratégie nationale de santé, les technologies numériques constituent un levier majeur pour la modernisation de notre système de santé. Les programmes nationaux aussi bien que les initiatives locales conduisent à une transition numérique qu'il convient d'accompagner le mieux possible pour en tirer tous les bénéfices sans s'exposer à de nouveaux risques.

Les programmes nationaux et les orientations de politique publique soutiennent la transition numérique dans le secteur de la santé, citons à titre d'exemple :

- Le programme Hôpital Numérique
- Les projets Territoire de soins numériques
- La mise en place des Groupements Hospitaliers de Territoire dans le cadre de la loi de modernisation de notre système de santé

La transition numérique touche tous les secteurs d'activité, aussi bien ceux en lien direct avec la production des soins, que ceux liés aux fonctions support nécessaires au bon fonctionnement de l'hôpital

■ Le monde numérique envahit notre quotidien

Les risques les plus élevés concernent aujourd'hui les données. Elles représentent un véritable patrimoine, de plus en plus convoité. Il devient donc essentiel d'identifier les vulnérabilités qui concernent votre établissement afin de réduire les risques numériques auxquels ces données peuvent être exposées.

■ Face à un risque évoluant sans cesse, la prise de conscience est essentielle

Il est important de gérer le risque comme un élément vivant et évoluant sans cesse. Le but de ce guide est de vous aider à en percevoir tous les enjeux et à vous orienter dans la mise en place des outils de pilotage, les actions d'audit et de suivi. Le but de la gestion des risques doit rester la protection du patient, de vos équipes, et de vous-même.

L'environnement immédiat du patient est aussi numérique

Les technologies du numérique sont omniprésentes dans l'environnement immédiat du patient. On les trouve aussi bien dans la mesure des constantes biologiques que dans l'application des plans de soins ou encore dans le contrôle technique des bâtiments.

C'est dire combien la sécurisation des données numériques est devenue l'affaire de tous. Un des grands enjeux actuels est l'intégration de l'ensemble des systèmes numériques, notamment ceux du secteur biomédical, dans le champ de la politique de sécurité des systèmes d'information de l'établissement.

Tout autour du patient apparait un environnement numérique. Il se construit par couches successives qui concernent autant sa prise en charge médicale et soignante que son environnement matériel immédiat.

Source pour le schéma : https://www.securityevaluators.com/hospitalhack/securing_hospitals.pdf

2 Les systèmes d'information vous font-ils prendre des risques inconsidérés ?

Vulnérabilité

Les systèmes d'information sont des outils de partage et d'échanges incontournables, au bénéfice des patients, des professionnels et du système de santé. Il est donc crucial de garantir leur sécurité pour maintenir la confiance des patients dans le système de santé et celle des professionnels dans les outils qu'ils utilisent chaque jour.

La progression réelle du Dossier Patient Informatisé (DPI) dans les établissements de santé montre que les soins s'appuient de plus en plus sur le système d'information (SI).

La standardisation des technologies fait que la barrière séparant les équipements biomédicaux du reste du réseau informatique tend à disparaître. Le pilotage de ces équipements et les données traitées se trouvent donc dépendants de la sécurité globale du Système d'Information (SI).

L'utilisation des technologies de l'information améliore la qualité des soins, les conditions de travail… mais elle est aussi porteuse de nouveaux risques et de nouvelles contraintes.

Ainsi, la mise en place du DPI doit être accompagnée d'une garantie de disponibilité adaptée aux exigences fixées par l'établissement lui-même et la réglementation.

Un dysfonctionnement du SI entraînant un mélange de résultats de biologie peut avoir un impact fort sur une prise en charge d'un patient.

Qu'est-ce qu'un risque ?

C'est un scénario qui combine :

- Un **événement redouté** et
- Une ou plusieurs **menaces**.

On estime son niveau par :

- Sa **gravité** (hauteur des impacts)
- Sa **vraisemblance** (possibilité qu'il se réalise)

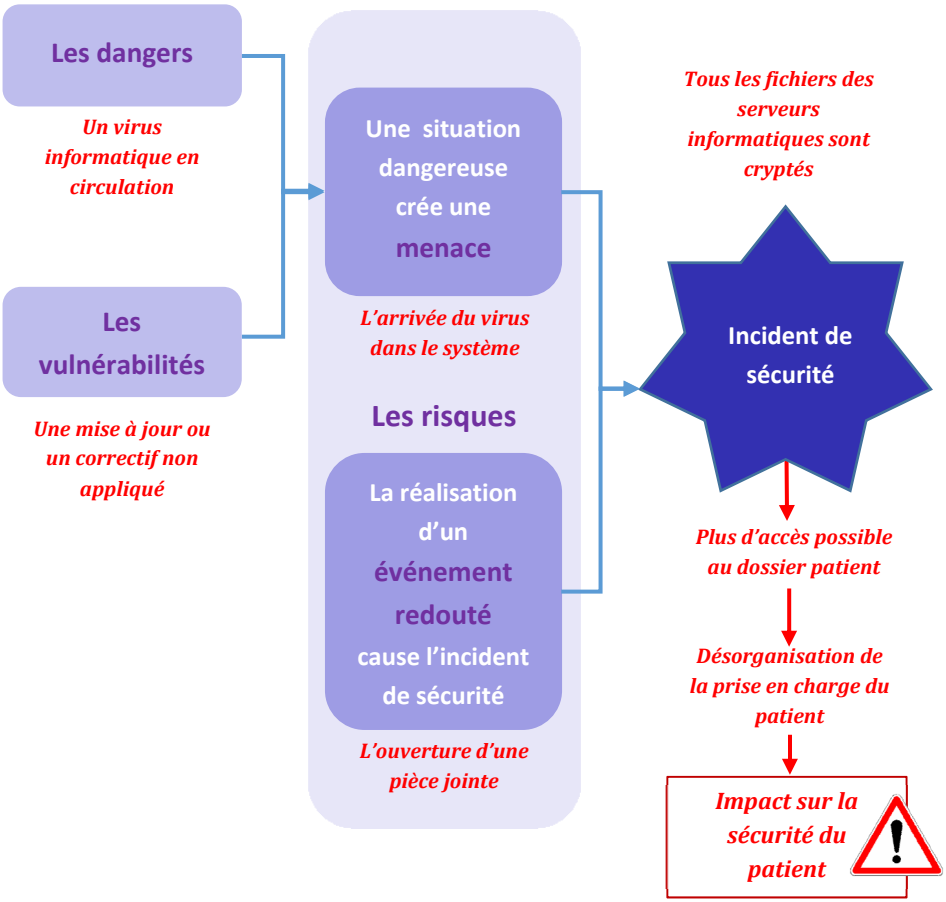
Quatre grandes parties, dans ce guide, pour vous permettre :

- de mieux comprendre les sources de vulnérabilités,
- d'identifier les risques et enjeux autour de la protection des données,
- d'installer une gouvernance tournée vers la gestion du risque,
- et de mettre en place les outils de pilotage et de contrôle nécessaires.

■ L'informatisation croissante de la prise en charge du patient rend celle-ci vulnérable à tout incident impactant le système d'information.

Prenons un exemple tiré de faits réels : lorsqu'un virus paralyse les applications utilisées dans la gestion des urgences, l'incident qui en résulte peut engendrer une désorganisation des interventions et des accès à l'information relative à l'état de santé du patient.

Ce n'est pas l'utilisation des systèmes d'information au sein des établissements de santé qui est en cause ici, mais les liens possibles entre un incident informatique et son impact sur la sécurité du patient et la qualité de sa prise en charge.



Vulnérabilité

3

L'engagement dans une démarche de gestion des risques numériques est une réelle opportunité de mieux accompagner l'évolution de son établissement

« L'importance de la culture de sécurité pour la sécurité des soins réside dans ce qu'elle participe à l'élaboration d'un ensemble cohérent et intégré de comportements des professionnels, et donc aux performances des organisations de santé. Au travers de l'évaluation et du développement d'une culture de sécurité des soins, il s'agit de faire de la sécurité une priorité de tous, des professionnels de terrain comme des managers »[1]

Témoignage

« Dans un établissement d'un groupe de cliniques : Suite au licenciement difficile d'un infirmier, ce dernier, via sa connaissance des identifiants et mots de passe de médecins, a procédé à de nombreuses prescriptions sans fondement obligeant le corps médical à vérifier chaque prescription faite au cours des dernières semaines »

■ Soutenir la politique de sécurité du système d'information devient aussi une exigence

La politique de sécurité ne se limite pas à la protection contre la perte, l'indisponibilité ou la divulgation de données personnelles médicales ou administratives, elle permet de créer un espace de confiance entre les professionnels et les patients et elle est un levier essentiel de l'amélioration de la qualité des soins. Il est donc de la responsabilité du management des établissements de santé (directeur, directeur des soins, directeur des ressources humaines, présidents des commissions médicales d'établissements) de la promouvoir

LA NOTION D'AQSSI - Pour les établissements de santé publics, la responsabilité de **la sécurité du SI est assurée par le directeur en tant qu'Autorité Qualifiée pour la Sécurité des Systèmes d'Information** (AQSSI) - cf. Arrêté du 13 décembre 2016

Art. 2. de l'arrêté – L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) est la personne responsable, pour sa structure, de la sécurité des systèmes d'information. C'est l'autorité juridiquement responsable, sa responsabilité ne peut être déléguée.

[1] Source : https://www.has-sante.fr

L'analyse des situations à risques est indispensable pour évaluer les impacts potentiels

Le système d'information se caractérise par l'usage des technologies numériques au service de l'organisation de la prise en charge du patient. Il devient, de ce fait, porteur de risques nouveaux. Une analyse de ces risques permet de construire les solutions visant à en réduire le plus possible les impacts. Les impacts des incidents de sécurité doivent être mesurés dans toutes leurs composantes.

Stratégique	Le risque stratégique est lié à l'incapacité de l'établissement à s'adapter aux évolutions des environnements et des exigences des patients.	
Opérationnel	Le risque opérationnel met en jeu toutes les défaillances internes ou externes pouvant avoir de graves conséquences sur le bon fonctionnement de l'établissement.	
Facteur Humain	Le risque lié au facteur humain est sans doute le plus important dans un établissement de santé. Il peut toucher aussi bien les patients que les professionnels de santé.	
Juridique	Le risque juridique est lié à la non application d'une disposition législative ou règlementaire. Il impacte directement le représentant légal. La gestion de ce risque est essentielle car elle peut éviter la mise en jeu de la responsabilité pénale.	
Financier	Le risque financier est associé à la perte de revenus, aux indemnités pouvant être mise en jeu, aux conséquences en matière d'investissements, aux amendes, etc.	
Image	Le risque d'image est directement associé à la perte de confiance envers l'établissement de santé et envers toutes ses équipes. Il porte atteinte à la réputation de l'établissement.	

4

L'incident de sécurité : l'éviter, c'est avant tout connaître et réduire ses vulnérabilités, identifier les situations dangereuses et apprendre à réagir face à elles

Vulnérabilité

Tout l'enjeu d'une démarche de gestion des risques est de les traiter, c'est-à-dire, de les réduire, les éviter, les partager ou les accepter. Pour cela il convient d'agir simultanément sur 4 niveaux :

1. Connaître les dangers auxquels on est exposé
2. Comprendre ses principales vulnérabilités et chercher à les réduire
3. Essayer de détecter au plus tôt toute situation dangereuse
4. S'organiser pour gérer l'incident de sécurité

La **cartographie des risques** est la pierre angulaire de tout **plan d'action sécurité** du système d'information. Elle vise à définir toutes les actions nécessaires pour parvenir à un **niveau de risque résiduel qui puisse être accepté** en toute connaissance de cause, au bon niveau de décision.

Elle s'applique toujours sur un périmètre d'activité parfaitement défini.

Tout établissement de santé doit disposer d'une cartographie des risques liés à son système d'information (cf. les prérequis du programme Hôpital Numérique)

Vu dans la presse[1]

5 février 2017 - Les pirates informatiques attaquent le Presbyterian Medical Center de Hollywood

L'établissement médical, qui compte 434 lits et œuvre à la fois dans le domaine de l'obstétrique, de la pédiatrie, de la cardiologie, mais aussi de la cancérologie..., a publié le 17 février un communiqué dans lequel son président, apporte quelques précisions sur cette attaque. "Dans la soirée du 5 février, écrit-il, nos équipes nous ont rapporté des problèmes d'accès au réseau informatique de l'hôpital. Notre service informatique a immédiatement identifié qu'un logiciel malfaisant était à l'origine de ces dysfonctionnements. Ce malware avait crypté l'accès à certains des serveurs et nous empêchait de partager nos dossiers numériques. La police a été saisie. Des experts informatiques ont été diligentés pour déterminer l'origine du problème et remettre notre système en fonctionnement."

[1] Source : http://www.lepoint.fr/sante/les-hopitaux-cible-de-choix-des-hackers-22-02-2016-2020253_40.php#

Le plan d'action sur la sécurité des systèmes d'information dans les établissements de santé : un calendrier à 6, 12 et 18 mois

Selon les éditeurs et bureaux d'étude spécialisés, la France serait entrée en 2015 dans le top 10 des pays les plus touchés par le piratage informatique. Le nombre de cyber-attaques recensées aurait progressé de 38% dans le monde en 2015, et 51% en France.

Tous les secteurs d'activités sont concernés. La sphère santé et médico-sociale n'est pas épargnée : selon un article récent[1] , sur le deuxième trimestre 2016, les cybercriminels ont concentré leurs efforts sur le domaine particulièrement sensible et rentable de la santé. En effet, près de 90% des attaques par rançongiciel (ransomware) sur cette période ont visé des établissements de santé dans le monde. Dans ce secteur, les incidents liés à la sécurité des systèmes d'information peuvent avoir un impact direct sur la sécurité des soins. Ils peuvent également avoir, comme ailleurs, un impact économique. Leur traitement est donc une priorité pour les pouvoirs publics et pour tous les producteurs de soins

Quelques conséquences de cyber-attaques

À titre d'exemples, une intrusion avec mise hors service des systèmes d'information d'une ARS pendant 24h a engendré des coûts d'intervention par un prestataire de l'ordre de 10 000 €, la perte de productivité est estimée à près de 40 000 €, soit un total de 50 000 € ;

Un cryptovirus en EHPAD a coûté 50 000 € en coûts directs d'intervention et coûts indirects ;

Le piratage du standard d'un centre hospitalier a généré une surfacturation de téléphonie de l'ordre de 40 000 €.

■ Mener les actions les plus urgentes en trois étapes 6, 12 et 18 mois

Le **plan d'action sur la sécurité des systèmes d'information** qui a été introduit par **l'instruction N°SG/DSSIS/2016/309 du 14 octobre 2016** vise à opérer une mise à niveau minimale de la sécurité des systèmes d'information dans toutes les structures concernées, au sein desquelles la défaillance des outils numériques représente un haut niveau de criticité (probabilité/impact). Il propose un **calendrier à 6, 12 et 18 mois de réalisation de mesures prioritaires** en termes d'efficacité par rapport, notamment, au risque de piratage informatique. Le premier niveau de priorité à 6 mois permet de diminuer le risque de manière significative, avec des mesures dont la mise en œuvre ne doit pas poser de difficulté majeure, pour des gains importants en matière de sécurité. Le plan d'action concerne les directions des établissements de santé, laboratoires de biologie médicale, centres de radiothérapie, centres d'imagerie et de radiologie publics et privés.

☑ **Évaluez votre situation grâce au MEMO-QUIZZ de la page 34**

[1] Source : https://www.lexsi.com/securityhub/ransomware-a-bonne-sante/

5

Le nouveau règlement européen[1] donne une définition des données de santé et fixe le cadre de leur protection

Le nouveau règlement européen définit, dans son article 4, ce que sont les « données à caractère personnel concernant la santé » : il s'agit de "données à caractère personnel 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".

Il précise qu'elles devraient comprendre "toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro".

Il définit aussi les "données génétiques", "relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé", et les données biométriques, "résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique".

■ Les données de santé sont, par essence, des données dites « sensibles »

Et pour les protéger la réforme de la protection des données poursuit 3 objectifs :

- **Renforcer les droits des personnes**, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
- **Responsabiliser les acteurs traitant des données** (responsables de traitement et sous-traitants) ;
- **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données.

le 25 mai 2018, le règlement général européen sur la protection des données personnelles (RGPD) entre en vigueur

[1] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

Source : CNIL

Du Correspondant informatique et liberté (CIL) au Délégué à la protection des données personnelles (DPDP) appelé aussi Data Protection Officer (DPO)

■ Pour piloter la gouvernance des données personnelles et protéger les droits fondamentaux des personnes physiques que sont les patients et les personnels de votre établissement, vous aurez besoin d'un véritable chef d'orchestre : le Délégué à la protection des données personnelles

Egalement appelé DPO, pour Data Protection Officer, ce délégué exerce une mission d'information, de conseil et de contrôle en interne.

La désignation d'un délégué à la protection des données personnelles est obligatoire dès 2018 pour tout établissement de santé.

Référent
sur les questions de protection des données personnelles

Consultant
sur les nouvelles manières d'exploiter les données personnelles

Interlocuteur de confiance
pour les personnes extérieures à l'établissement (clients, partenaires, autorités de contrôle) et le personnel interne sur la collecte et le traitement responsable des données personnelles

- ✓ Plus de sécurité juridique
- ✓ Plus de sécurité numérique
- ✓ Plus de confiance
- ✓ Plus de valorisation des données
- ✓ Plus de services et d'informations de la part de l'autorité de régulation

6 La protection des données est fondée sur la responsabilisation des acteurs et le rôle donné au consentement des personnes.

Qu'il s'agisse de ses personnels, de ses patients ou de ses partenaires, les données personnelles en possession de l'établissement sont protégées par le droit français et européen qui garantit la protection de la vie privée.

■ Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

Alors que la règlementation nationale reposait jusqu'alors, en grande partie, sur la notion de « formalités préalables » (déclaration, autorisations), **le règlement européen repose lui sur une logique de conformité, dont les acteurs sont responsables**, sous le contrôle et avec l'accompagnement du régulateur**.**

Les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou doivent pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. Il est primordial pour les établissements de garantir leur confidentialité, une perte de donnée pouvant représenter des risques majeurs tant au niveau de l'image de l'établissement qu'au niveau du préjudice pour la victime du vol de donnée.

La conséquence de la responsabilisation accrue des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes**. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée**.

Une fuite de données impacte 1300 patients

La société RiverMend Health en Géorgie a découvert qu'une personne non autorisée avait accédé au compte de messagerie d'un de ses employés. La société fournit des services spécialisés de santé et d'aide à la personne, y compris des services d'aide contre la toxicomanie et à l'alcoolisme. L'accès non autorisé a été détecté le 10 août 2017, lorsque des courriels suspects ont été envoyés depuis le compte de l'employé. Ces courriels ont alors fait l'objet d'une enquête et le compte a été bloqué le 11 août 2017. Les patients ont été informés de la fuite de données par courrier postal et ont été informés que les informations suivantes étaient potentiellement accessibles: noms, âges, adresses, traitements, diagnostics ainsi que les informations relatives aux assurances et à la facturation.

Source : https://www.cyberveille-sante.gouv.fr

Source : CNIL

La donnée de santé numérique est par nature destinée à être stockée, échangée puis archivée, ce qui impose un cadre strict de sécurité

■ L'obligation de sécurité et de notification des violations de données personnelles pour tous les responsables de traitements

Les données personnelles doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées.

Lorsqu'il constate une violation de données à caractère personnel, le responsable de traitement doit notifier à l'autorité de protection des données (en France, la CNIL) la violation dans les 72 heures. L'information des personnes concernées est requise si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne.


CNIL.

NOTIFICATION DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

1 Identification du responsable de traitement

1.1 Identité du responsable de traitement

Raison sociale* _____

Service _____

N° SIRET* _____

Adresse* _____

Code postal* _____ Ville* _____

Téléphone* _____ Fax _____

1.2 Personne à contacter pour obtenir des informations complémentaires

Nom et prénom* _____

Service _____

Fonction _____

Adresse* _____

Code postal* _____ Ville* _____

Adresse électronique* _____

■ Les « études d'impact sur la vie privée » (EIVP ou DPIA ou EIPD)

Si l'analyse des risques des systèmes d'information s'attache à étudier les risques pour l'établissement, l'étude d'impact sur la vie privée (EIVP) étudie, quant à elle, les risques pour le patient ou l'agent. Pour tous les traitements à risque, le responsable de traitement doit conduire une étude d'impact complète, faisant apparaître les caractéristiques du traitement, les risques et les mesures adoptées. Concrètement, il s'agit notamment des traitements de données sensibles (données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, mais aussi, fait nouveau, les données génétiques ou biométriques), et de traitements reposant sur « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », c'est-à-dire notamment de profilage.

En cas de risque élevé, il devra consulter l'autorité de protection des données avant de mettre en œuvre ce traitement. Celle-ci pourra s'opposer au traitement à la lumière de ses caractéristiques et conséquences.

☑ **Évaluez votre situation grâce au MEMO-QUIZZ de la page 37**

7 L'hébergement de données de santé s'inscrit dans un cadre règlementaire spécifique

Les modalités d'hébergement de données de santé à caractère personnel sont encadrées par l'article L.1111-8 du code de la santé publique :

■ Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social pour le compte d'un tiers, doit être agréée à cet effet.

■ L'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.

L'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel a modifié l'article L.1111-8 du code de la santé publique en distinguant explicitement trois grandes catégories de services d'hébergement de données de santé :

■ **l'hébergement de données de santé sur support papier**, qui doit être réalisé par un hébergeur agréé par le Ministre de la Culture (procédure déjà existante – cf. décret 2011-246) ;

■ **l'hébergement de données de santé sur support numérique dans le cadre d'un service d'archivage électronique**, qui doit être réalisé par un hébergeur agréé par le Ministre de la Culture dans des conditions définies par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés (CNIL) et des conseils des ordres des professions de santé ;

■ **l'hébergement de données de santé sur support numérique (hors cas d'un service d'archivage électronique)** qui doit être réalisé par un hébergeur certifié dans des conditions définies par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés (CNIL) et des conseils des ordres des professions de santé.

Jusqu'à fin 2017, la qualité d'hébergeur de données de santé est obtenue selon les modalités antérieures (procédure d'agrément).

À partir de 2018, tout nouvel hébergeur de données de santé devra suivre une procédure de certification

Dès 2018 : La certification « Hébergeur de données de santé »

■ Le nouveau dispositif pour l'hébergement de données de santé sur support numérique est défini par la DSSIS et l'ASIP Santé. Il est validé par un comité de pilotage qui réunit des représentants institutionnels (Ministère de la Santé, ANSSI, CNIL, Fédérations hospitalières, Ordres, etc.) et des représentants d'industriels.

A partir de 2018, pour toute nouvelle demande, la qualité d'hébergeur de données de santé reposera sur une évaluation de conformité à un référentiel de certification, délivrée par un organisme certificateur accrédité par le COFRAC et choisi par l'hébergeur. Deux types de certificats seront délivrés aux hébergeurs :

■ Un certificat « hébergeur d'infrastructure physique » pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;

■ Un certificat « hébergeur infogéreur » pour les activités de mise à disposition d'infrastructure virtuelle, de mise à disposition de plateforme logicielle, d'infogérance et de sauvegarde externalisée.

Si tous vos systèmes informatiques stockent des données concernant uniquement des patients placés sous la responsabilité de votre entité juridique, la certification hébergeur de données de santé n'est pas, pour vous, une obligation règlementaire. Mais cela ne signifie pas que vous ne devez pas avoir la même exigence en matière de sécurité des systèmes d'information.

Le référentiel de certification Hébergeur de données de santé : les bonnes pratiques à l'état de l'art

Les normes de référence du dispositif de certification HDS sont principalement les normes ISO 27001:2013 et ISO 27018 :2014. Quelques compléments proviennent des normes ISO 27017 :2015 et ISO 20000-1 :2011.

La procédure de certification se fonde, quant à elle, sur le processus standard de type système de management décrit dans la norme ISO 17021 et précisé dans la norme ISO 27006. L'hébergeur choisit un organisme certificateur accrédité par le COFRAC et la certification se fait en deux étapes : un audit documentaire et un audit sur site.

Ce référentiel sera publié fin 2017

8 Disponibilité, intégrité, confidentialité et preuve

Une donnée ne devient une véritable information que si l'on y accède facilement, en permanence, de façon maîtrisée, si on la comprend et si on est en mesure de lui faire confiance. Quatre caractéristiques sont indispensables pour cela :

■ Disponibilité : un niveau contextualisé selon les finalités d'usage des données

La disponibilité des systèmes numériques permet à l'information d'être accessible et utilisable par la personne autorisée à l'endroit et à l'instant où elle en a besoin.

■ Intégrité : une fiabilité maximale des données de santé

Les données ne doivent pouvoir être modifiées que suivant des processus clairement définis et par des personnes clairement identifiées. Plus la fiabilité de l'information est critique, plus ces critères sont à prendre en compte.

■ Confidentialité : un accès modulable aux données de santé

L'information ne doit être accessible qu'aux personnes autorisées. En amont, la réflexion sur la gestion des droits et des accès est essentielle. Seules les personnes ayant besoin de l'information doivent pouvoir y accéder. Plus cette information est « sensible » plus le nombre de personnes doit être réduit.

■ Preuve : une conservation de traces à valeur de preuve

La preuve permet l'investigation en cas de dysfonctionnement et d'incidents. Il s'agit clairement de conserver les traces de l'état et des mouvements de l'information. La réforme de la protection des données rend cette preuve particulièrement importante car elle peut permettre de prouver qu'un contrôle sur l'utilisation des données est en place.

Témoignage d'un Responsable Sécurité du Système d'Information

« La principale source d'inquiétude, c'est l'intégrité des données »

Si je constate une erreur en consultant mon compte bancaire, il s'agit d'une erreur d'intégrité qui n'a pas de conséquence dramatique et qui peut être corrigée. Si je ne peux pas retirer d'argent à cause d'une panne informatique, c'est un souci de disponibilité et c'est déjà plus contrariant. Enfin, si la totalité de ma situation financière se retrouve dans Google, c'est un problème de confidentialité et c'est potentiellement très grave.

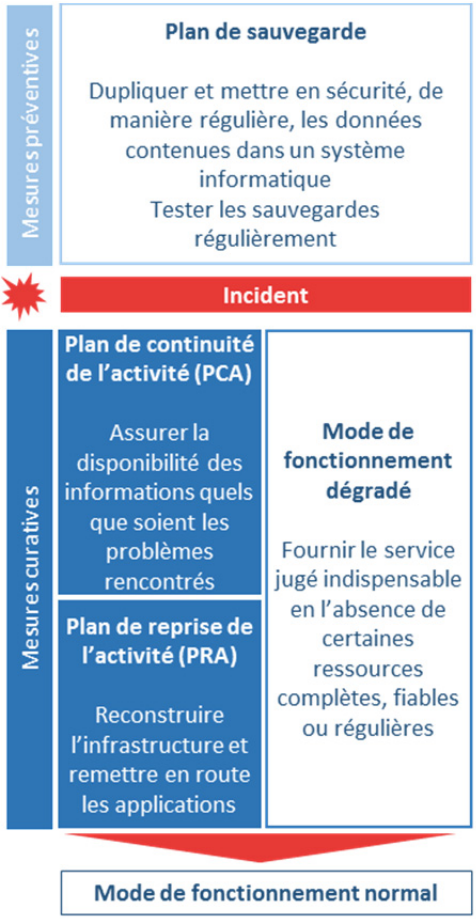
Il y a un ordre de priorité dans le secteur bancaire, qui n'est pas le même dans celui de la santé. Dans les établissements de santé, contrairement à ce que laissent penser certains articles, ce n'est pas la confidentialité des données qui est la principale source d'inquiétude, mais leur intégrité.

Source : https://www.digitalforallnow.com/securite-donnees-sante-cedric-cartau/

En cas d'incident, garantir un retour à un fonctionnement normal, dès que possible, est vital

■ Assurer la sécurité du système d'information permet de créer un espace numérique de confiance

Cet espace est favorable à la dématérialisation, au partage et à l'échange de données de santé, et doit permettre d'offrir une sécurité juridique lors de l'utilisation du système d'information. Pour y parvenir il est nécessaire d'adopter des mesures préventives, il faut donc mettre en place tous les dispositifs techniques, organisationnels et humains qui garantissent le maintien des activités vitales de l'établissement en cas d'incident temporaire perturbant ou arrêtant la production informatique.



9 Hôpital Numérique : poser un socle de sécurité incontournable

Le programme Hôpital numérique, lancé en 2011 et piloté par la Direction générale de l'offre de soins (DGOS), a pour ambition d'amener l'ensemble des établissements de santé à un palier de maturité de leur système d'information permettant :

■ le partage et l'échange d'informations au sein des établissements

■ l'amélioration significative de la qualité, de la sécurité des soins, et la performance dans des domaines fonctionnels prioritaires autour de la production de soins.

Trois grands objectifs sont poursuivis, en matière de sécurité, par le programme Hôpital Numérique, chacun correspond à un domaine de prérequis, chaque domaine possédant des indicateurs cibles à atteindre.

1. Pouvoir rattacher la bonne information, au bon patient, au bon endroit (prérequis P1 – Identité / mouvement)

   - Utiliser des **référentiels uniques d'identité patient, de séjours et de mouvements** pour la majorité des applications
   - Mettre en œuvre une **identitovigilance opérationnelle** pour assurer la sécurité du patient liée au soins
   - Décrire la **structure d'organisation de l'établissement** et l'actualiser

2. En toutes circonstances (prérequis P2 – Fiabilité, disponibilité)

   - Disposer d'un **plan de reprise d'activité** formalisé pour assurer la continuité de service
   - **S'engager sur la disponibilité** des applications
   - Savoir gérer les situations de pannes au moyen de **procédures dégradées**

3. Et en toute confiance (prérequis P3 – Confidentialité, preuve)

   - Évaluer les situations à risques et **définir une politique de sécurité** pour les prévenir et les maitriser
   - **Définir les bonnes pratiques** dans l'utilisation du SI afin de garantir la confidentialité auprès du patient et demander un engagement à les respecter
   - **Définir qui accède à quoi** et être en mesure de le vérifier

RSSI : Référent ou Responsable Sécurité du Système d'Information, il faut un maitre d'œuvre de la sécurité du SI

Comme l'exige le prérequis P3.1. du programme Hôpital numérique, l'organisation de la sécurité doit s'appuyer sur un référent sécurité. S'il est quasiment toujours désigné, il est, en revanche, très rarement affecté à temps complet sur la sécurité des systèmes d'information. Un peu plus de la moitié des référents sont affectés à temps partiel.

■ Dans un environnement qui se numérise de plus en plus, la fonction de Responsable des Systèmes d'information devient incontournable

Il doit, en particulier, au sein d'une organisation dédiée :

- Définir et mettre en œuvre de la politique de sécurité des systèmes d'information
- Mener les analyses des risques de la sécurité des systèmes d'information
- Effectuer les choix des mesures de sécurité et élaborer les plans de mise en œuvre
- Sensibiliser, former et conseiller sur les enjeux de la sécurité des systèmes d'information
- Mener des audits et contrôles de l'application des règles de la politique de sécurité des systèmes d'information
- Assurer une veille règlementaire, technologique et prospective
- Evaluer les coûts liés à la sécurité des systèmes d'information

■ Vers le RSSI de Groupement Hospitalier de Territoire

La mise en œuvre, dans le cadre d'un GHT, d'un projet commun de convergence des systèmes d'information vers un système d'information homogène entraîne une réflexion incontournable sur la gestion de la sécurité des systèmes d'information.

C'est dans ce nouveau contexte des GHT que l'exercice de la fonction de responsable de la sécurité des systèmes d'information (RSSI) doit désormais être envisagé.

Le référent sécurité dans les établissements de santé

Le référent sécurité interne à l'établissement est très rarement affecté à temps complet, à la sécurité des systèmes d'information : dans 9% des cas seulement.

Un peu plus de la moitié des référents sont affectés à temps partiel. Seuls se distinguent les CHU/R où un responsable sécurité SI est entièrement affecté à cette fonction dans 46% des cas.

Avec une externalisation dans 12% des cas ou un partage entre plusieurs établissements dans 27% des cas, la mutualisation de cette fonction est une réalité (pour 40% des établissements répondants).

Source : ATLAS des SIH 2017

http://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/article/atlas-des-systemes-d-information-hospitaliers

10

L'organisation collective : premier pas vers la réduction des risques

Gouvernance

Le soutien de la Direction est le principal facteur clé de succès. La Direction doit promouvoir, soutenir la démarche et en rappeler, si nécessaire, les enjeux. Il faut transformer l'image de la sécurité vue comme une contrainte sans apport sur la qualité et la sécurité des soins. Seule la Direction peut soutenir ce message de la sécurité créatrice de confiance sur le système d'information.

■ La gestion des risques liés au numérique ne passe pas uniquement par la mise en place de solutions techniques. C'est surtout une organisation prenant en compte les éléments de risque qui est la clef d'un pilotage réussi.

Cybersécurité : Gouverner la sécurité numérique

Le mot « cybersécurité » est construit à partir de la racine grecque *kubernao*, qui signifie « gouverner » et qui a produit de préfixe « cyber ». Avec l'avènement des ordinateurs et des réseaux de télécommunication le préfixe « Cyber » a été associé aux technologies de l'information et de la communication : la cybersécurité peut donc être comprise comme l'art de gourverner la sécurité liée à l'introduction des technologies numériques dans nos organisations

Et la responsabilité de gouverner revient aux dirigeants…

Cela est renforcé par la normalisation des obligations règlementaires poussant les directions à mettre en place une gouvernance clairement définie et des objectifs stratégiques et opérationnels associés.

La sécurité est l'affaire de tous les utilisateurs. Ceux-ci doivent respecter les règles d'usage du Système d'Information, même si bien souvent ces règles sont vues comme une contrainte sans intérêt opérationnel. Pour accepter cette contrainte, il faut communiquer vers les utilisateurs et les convaincre des enjeux sous-jacents.

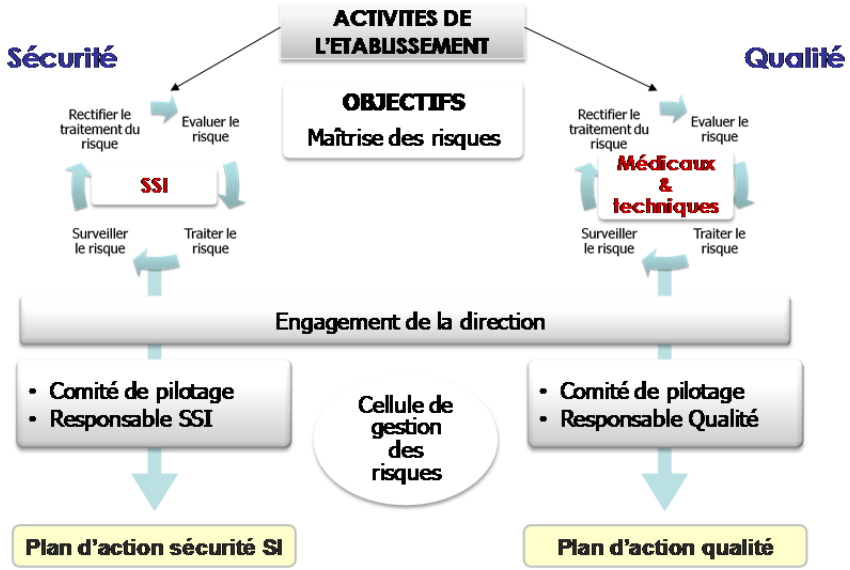
Le soutien de la Direction est alors d'autant plus important et précieux que les chantiers les plus complexes ont un impact sur l'organisation de l'établissement et les aspects opérationnels des services. C'est le cas, par exemple, de la gestion des identités et des accès des utilisateurs au système d'information ou de la mise en place d'un plan de continuité d'activité (en cas de panne grave du système d'information).

Lorsque l'on analyse les démarches adoptées par les établissements les plus avancés dans l'atteinte des prérequis du programme Hôpital Numérique, on constate que la démarche qualité et sécurité des soins et la démarche sécurité du SI présentent un grand nombre de ressemblances (Cf. la figure ci-dessous)

En effet, les circuits d'identification des risques métiers impliquent les mêmes acteurs dans l'établissement.

Tout semble indiquer qu'une gouvernance unique de gestion des risques est réalisable. Il est donc important que le responsable sécurité du système d'information travaille en étroite collaboration avec le responsable des risques et/ou de la qualité.

Les établissements pourront voir, au travers de cette organisation unique, des avantages en matière d'efficacité, de pilotage et de coût.



Par ailleurs, La HAS a repris, pour l'évaluation de la sécurité des systèmes d'information, dans le cadre de la procédure de certification des établissements de santé, la totalité des indicateurs de prérequis du programme Hôpital Numérique.

11 Les référentiels de sécurité comme moyen d'avancer en réduisant les risques

De nombreuses exigences réglementaires sont produites pour accompagner l'évolution numérique des établissements de santé. Les obligations légales, doivent être utilisées pour accompagner l'hôpital vers une amélioration de sa gestion des risques.

■ Il faut transformer la contrainte règlementaire en opportunité

Les exigences règlementaires sont nombreuses et variées à l'hôpital. Elles sont induites tant par l'évolution des métiers et des organisations, qui sollicitent de plus en plus les systèmes d'information, que par l'élévation des exigences de sécurité dues à l'évolution constante des technologies du numérique.

Citons, par exemple, la démarche de certification des comptes financiers des établissements de santé qui conduit à ce qu'une attention et un effort particuliers soit portés sur les processus de gestion des accès aux systèmes d'information (identification et authentification), sur ceux liés au changements du système d'information (mise à jour d'applications informatiques), ainsi que sur ceux concernant les sauvegardes et restaurations des données.

■ Les référentiels sont porteurs des bonnes pratiques à respecter afin de minimiser les risques

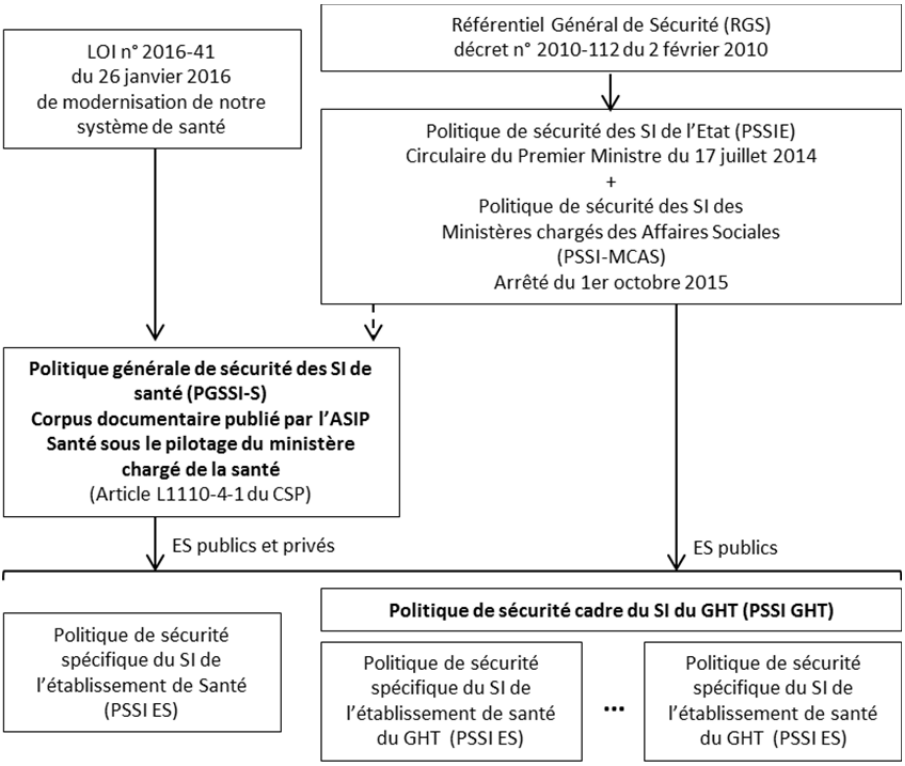
Un référentiel résulte en général d'une démarche d'élaboration longue, itérative et documentée auprès des spécialistes d'un domaine de compétence. Il fixe un cadre qui apparaît comme représentatif de l'état de l'art, et en ce sens il a vocation à fournir les meilleures garanties tant pour la sécurité que pour la qualité des systèmes d'informations.

La notion de référentiel opposable : Article L1110-4-1 du Code de la santé publique

Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, **les établissements et services de santé**, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social **utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 (l'ASIP Santé)**. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés

La mise en application des référentiels de sécurité doit trouver sa traduction, au niveau local d'un établissement de santé, dans le document de politique de sécurité des systèmes d'information à usage interne

■ Le cadre règlementaire se décline dans un ensemble de textes allant du général au particulier, en gagnant à chaque fois en précision. Pour le domaine de la santé, la hiérarchie peut être décrite de la façon suivante, dans le sens de son applicabilité :



Certains référentiels de la PGSSI-S seront rendus opposables dès 2018

Les certifications : de l'incitation au contrôle

La bonne application des référentiels, et donc des bonnes pratiques, doit être soutenue par des actions de sensibilisation, encouragée par des mesures d'incitation et doit pouvoir être vérifiée par des procédures de contrôle.

■ Sensibiliser les directions d'établissement : premier pas de l'action en matière de sécurité des systèmes d'information :

Citons à titre d'exemple :

- **Les prérequis du programme Hopital Numérique** : ils définissent un socle de sécurité de base et permettent d'établir un langage commun autour de la sécurité des systèmes d'information. Les 12 indicateurs qui y sont présentés sont les repères incontournables de toute action en matière de sécurité des SI.
- **Les guides de sensibilisation et d'évaluation**, comme le présent mémento : ils essaient de souligner les enjeux et perpectives liés à la sécurité des systèmes d'information tout en fournissant des repères pratiques pour encourager l'action au sein des établissements de santé
- **Le Colloque annuel** organisé, à l'automne par la DSSIS, le SHFDS la DGOS et l'ASIP Santé, marque un temps privilégié de synthèse et d'échange autour de la sécurité des systèmes d'information. Des actions ciblées en ARS peuvent égalements être réalisées.

■ Inciter les établissements par des mesures d'exigences règlementaires et/ou d'accompagnement financier :

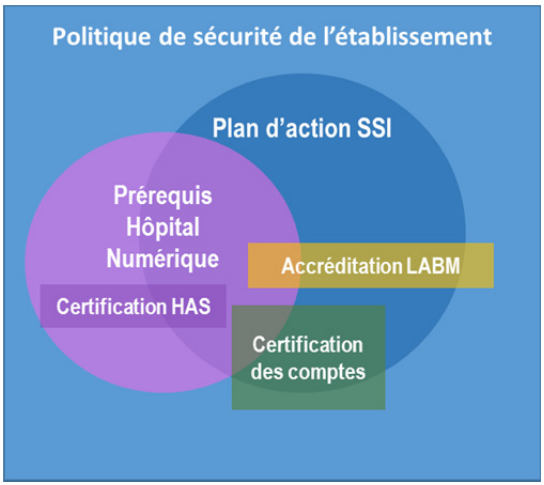
- **Le financement d'un domaine d'usage**, dans le cadre du programme Hôpital Numérique, n'est possible que si les indicateurs cibles fixées pour les prérequis ont été atteints.
- **La certification HAS intègre désormais les indicateurs de prérequis Hôpital Numérique** dans sa procédure de certification. il contribuent de façon opérationnelle à l'évaluation de plusieurs thématiques de la V2014 : management de la qualité et des risques, droit des patients, parcours du patient, identification du patient à toutes les étapes de sa prise en charge, gestion du système d'information.
- **L'incitation financière à l'amélioration de la qualité (programme IFAQ)** utilise également les indicateurs du programme Hôpital Numérique : il faut les avoir renseignés sur la plateforme OSIS pour pouvoir accéder au financement IFAQ
- **Le plan d'action SSI** lancé par l'instruction du 14 octobre 2016 constitue également une incitation forte au développement de la sécurité des systèmes d'information (cf. page 13)

Les contrôles in-situ accompagnent la prise de conscience des enjeux liés à la sécurité des systèmes d'information

Des procédures de contrôle sont généralement associées aux démarches de certification, elles permettent d'accompagner le travail déclaratif fait par l'établissement et de mieux percevoir les éventuelles difficultés d'application des règles.

■ Il revient à la politique de sécurité interne à l'établissement de fixer un cadre favorable au respect de l'ensemble des règles de sécurité que les procédures de certification décrivent.

En réalité, la tâche n'est pas aussi ardue qu'il y paraît, en effet chaque fois qu'une procédure de certification fixe des exigences de sécurité, elle le fait par référence aux règles de l'art qui sont portées par les référentiels de sécurité dont doit s'alimenter la politique de sécurité interne à l'établissement. **En réalisant le plan d'action SSI et en respectant les prérequis Hôpital Numérique, un cadre de conformité solide est posé.**



Quelques procédures de contrôle règlementaire portant sur la sécurité des systèmes d'information

Dans ces procédures de contrôle, le volet sécurité du système d'information peut jouer un rôle majeur quant aux conclusions apportées par les évaluateurs

- **Audit du volet système d'information dans le cadre de la certification des comptes**
- **Missions de contrôle des ARS dans le cadre du programme Hôpital numérique**
- **Audit des experts visiteurs de la HAS dans le cadre de la certification des établissements de santé**
- **Audit du Cofrac dans le cadre de l'accréditation des laboratoires d'analyse de biologie médicale**

La démarche de signalement des incidents de sécurité des systèmes d'information de santé

A partir du 1er octobre 2017, les signalements des incidents de sécurité sur les systèmes d'information sont obligatoires[1].

■ Le décret n° 2016-1214 du 12 septembre 2016 précise que les établissements des santé doivent signaler les incidents graves de sécurité ayant des conséquences potentielles ou avérées sur la sécurité des soins, sur la disponibilité, l'intégrité ou la confidentialité des données de santé, sur le fonctionnement normal de l'établissement.

Afin **d'apporter un appui et un accompagnement** aux structures de santé concernées par la déclaration de ces incidents, le ministère chargé de la santé met en place un dispositif pour traiter leur signalement, **en lien avec les ARS, l'ASIP Santé et le HFDS/FSSI**.

Les objectifs visés par ce dispositif sont de :

■ **Renforcer le suivi des incidents** pour le secteur santé ;

■ **Alerter et informer l'ensemble des acteurs** de la sphère santé dans le cas d'une menace pouvant avoir un impact sur le secteur ;

■ **Partager des bonnes pratiques** sur les actions de prévention ainsi que sur les réponses à apporter suite aux incidents, afin de réduire les impacts et de mieux protéger les systèmes.

Pour effectuer un signalement : https://signalement.social-sante.gouv.fr

[1] Cette obligation a été introduite par l'article 110 de la loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé. Elle s'applique aux établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie.

Un dispositif pour aider les établissements confrontés à des incidents graves de sécurité : la cellule ACSS

Dans le cadre du dispositif de traitement des signalements des incidents de sécurité des systèmes d'information numériques de santé, la cellule ACSS (Accompagnement Cybersécurité des Structures de Santé) développe un service dédié à l'accompagnement et l'appui au traitement ainsi qu'un service de veille et information

■ L'accompagnement et l'appui au traitement des signalements des incidents de sécurité des systèmes d'information comprend :

- La récupération du signalement et notification au déclarant de sa prise en compte ;
- l'analyse et la qualification du signalement pour le compte de l'ARS compétente ;
- l'apport si besoin d'un accompagnement dans le traitement de l'incident de sécurité des systèmes d'information ;
- la diffusion d'une alerte à la DGS dans le cas d'un incident ayant un impact sanitaire potentiel.

Le traitement de l'incident reste toutefois de la responsabilité de la structure de santé déclarante.

■ L'animation d'un portail de veille et d'échanges

Dans le cadre des actions de sensibilisation et d'accompagnement des structures, la cellule ACSS met en place un portail dédié d'information sur l'actualité de la sécurité des systèmes d'information de santé, les menaces sectorielles et les bonnes pratiques. Il présente des bulletins de veille sur certaines vulnérabilités logicielles critiques, des fiches réflexes et des guides pour répondre à différents types d'incidents.Ce portail met aussi à disposition de la communauté SSI du secteur un espace accessible uniquement par authentification, sur lequel d'autres services sont disponibles : forum de discussion, possibilité de commenter des documents mis en ligne sur l'espace public.

Source : ASIP Santé

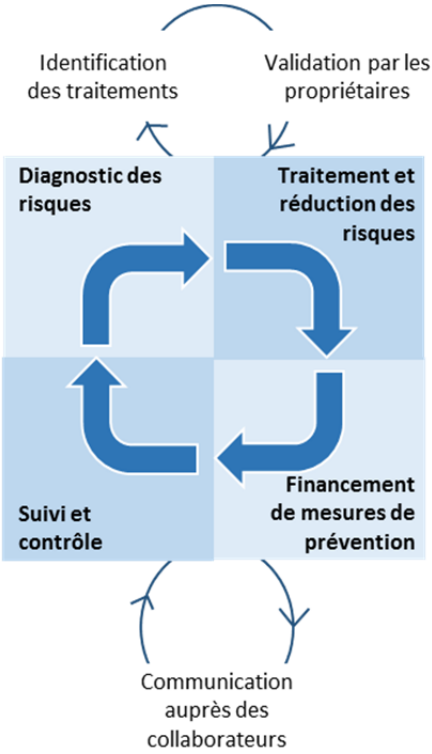
14

La gestion des risques comme moteur de l'amélioration continue

La gestion des risques liés aux soins fait partie de la culture de l'établissement de santé. Cependant elle ignore, trop souvent encore, les risques liés aux technologies numériques alors que celles-ci envahissent le secteur de la santé. Face à cela, l'engagement de la direction est essentiel, aussi bien en matière d'image véhiculée au sein de l'établissement qu'en matière de prise de décisions

■ La gestion des risques se concentre très souvent autour d'arbitrages tendant à adapter ses efforts uniquement pour faire face à des risques majeurs.

Il s'agit en réalité d'une démarche complète et continue d'analyse des risques, d'indentification des traitements possibles en vue de leur réduction et de validation des choix par le « propriétaire » du risque. Si cette approche doit, bien sûr, avoir lieu à l'échelle globale, **il faut également la conduire à l'échelle des différents projets, et cela dès la conception du projet**.



Les coûts liés à la sécurité des outils numériques sont trop souvent comparés aux économies qui pourraient être réalisées sans ces investissements. Pourtant, c'est bien par comparaison aux coûts de gestion des incidents et de leurs impacts qu'il faut faire l'exercice.

Pour qu'elle puisse être mise en œuvre et évoluer dans le temps, la trajectoire définie pour améliorer la sécurité du système d'information doit rester réaliste pour ne pas décourager les différentes parties prenantes.

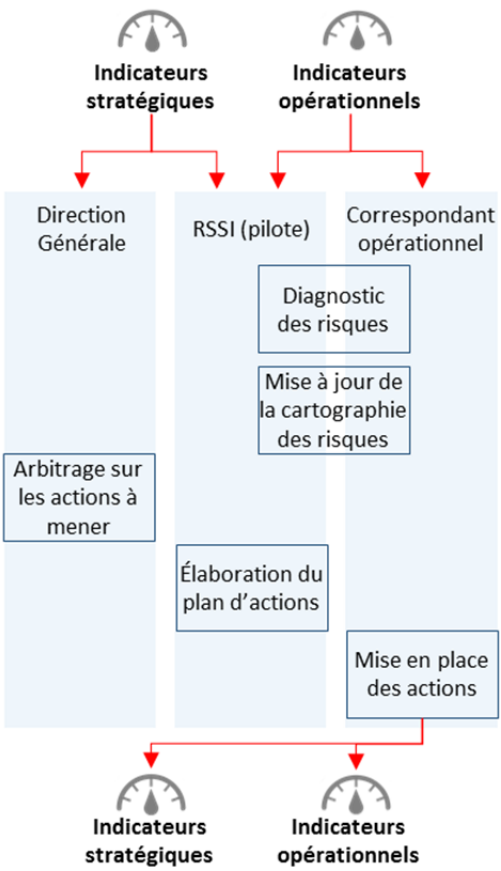
■ Le plan d'action sécurité, fruit du diagnostic et de l'analyse du risque, doit être actualisé régulièrement sur la base d'informations collectées par les équipes, les systèmes eux-mêmes, et rassemblées dans des tableaux de bord

Les indicateurs définis, permettant la démarche d'amélioration continue, sont de deux types :

- Stratégiques, permettant des retours réguliers vers la direction générale
- Opérationnels, permettant un pilotage de la sécurité au quotidien

Dans tous les cas**, ces démarches doivent s'appuyer sur des audits réguliers** permettant la mise à jour de la cartographie des risques et si besoin du plan d'action. **Il est donc essentiel d'avoir une ligne budgétaire dédiée à ce processus d'amélioration continue**.

De l'importance des indicateurs …



Le principe du mémo-quizz est très simple : il vous suffit de cocher les exigences qui vous semblent remplies. Tout ce qui n'est pas coché doit donner lieu, sans tarder, à une action.

■ Mesures de **priorité 1** à mettre en place **dans les 6 mois**

Gestion des ressources humaines [RH]

☐ La fonction sécurité des systèmes d'information est bien identifiée et prise en charge par la direction. Cette fonction est éventuellement mutualisée entre plusieurs entités, notamment dans le cadre d'un GHT.

Si oui : ☐ vous avez désigné un RSSI (Responsable Sécurité du Système d'Information)

☐ vous connaissez son nom (à indiquer) : _____

☐ Votre établissement a mis en place une charte utilisateur annexée à son règlement intérieur

Organisation [ORG]

☐ vous disposez d'une cartographie tenue à jour / d'un inventaire des ressources informatiques placées sous la responsabilité de votre établissement (postes de travail, serveurs,équipements réseaux, équipements biomédicaux…)

☐ Votre établissement a défini une procédure de signalement et de traitement des incidents de sécurité SI en vue de la mise en œuvre de l'obligation de signalement des incidents graves de sécurité des systèmes d'information en application de l'article L. 1111-8-2 du code de la santé publique

Gestion du poste de travail [PC]

☐ Vous vous êtes fait confirmer par vos responsables informatiques que tous les postes de travail sont protégés par un antivirus, les postes nomades étant, en plus, équipés d'un pare-feu local

Gestion des comptes utilisateurs [USER]

☐ vous savez que les mots de passe utilisés sont robustes (ils respectent les recommandation de la CNIL) et sont renouvelés périodiquement

Gestion des sauvegardes [SAUV]

☐ Vous avez la garantie de la mise en œuvre de sauvegardes régulièrement testées

■ Mesures de **priorité 2** à mettre en place **dans les 12 mois**

Organisation [ORG]

☐ Vous avez formellement délégué l'application d'une procédure d'appréciation du risque avant toute mise en production d'une application informatique (procédure dite d'homologation)

Gestion du poste de travail [PC]

☐ Vous avez la garantie qu'il existe un plan de mise à jour des postes de travail dans leur dernière version de système d'exploitation

☐ L'organisation du maintien en conditions de sécurité de l'ensemble des systèmes numériques est prise en charge par votre RSSI et votre DSI (postes de travail, serveurs, équipements actifs, équipements biomédicaux…) notamment en appliquant les mises à jour proposées par les éditeurs et constructeurs

Gestion des réseaux [RES]

☐ vous disposez d'un RSSI pouvant vous grantir l'identification et la protection de tous les accès à internet et de télémaintenance

☐ vous disposez d'un spécialiste réseaux pouvant assurer la sécurisation du wifi et la séparation des réseaux professionnels et des réseaux invités

Gestion des comptes utilisateurs [USER]

☐ la mise en œuvre d'une gestion des comptes utilisateurs avec profils et droits différentiés selon le principe du moindre privilège (utilisateur, prestataire, administrateur…) est assurée pas vos collaborateurs

Gestion des ressources humaines [RH]

☐ des actions de formation SSI et l'inscription d'au moins une action de sensibilisation à la SSI sont bien inscrite dans le plan de formation annuel des personnels de votre établissement

■ Mesures de **priorité 3** à mettre en place **dans les 18 mois**

Gestion des réseaux [RES]

☐ Vous disposez d'un spécialiste réseaux chargé de mattre en œuvre un cloisonnement du réseau de la structure par grandes familles d'usage (administration, paie, plateau technique…) et par niveaux de sécurité homogènes

☐ Votre RSSI a défini et vous a informé des modalités d'enregistrement et d'analyse des traces d'accès au système d'information

Gestion des contrats de sous-traitance SI [PRESTA]

☐ Vous avez validé avec vos collaborateurs concernés, l'encadrement contractuel de tous les accès par des prestataires, au réseau de votre établissement et la vérification des clauses de réversibilité

Organisation [ORG]

☐ Vous avez chargé votre RSSI et vos collaborateurs concernés :

- ☐ de réaliser et tenir à jour une analyse des risques SI de votre établissement ;
- ☐ de définir et mettre en œuvre un plan d'action associé,
- ☐ vous les avez fait validés par les instances de gouvernance de votre établissement

☐ Vous vous engagez, chaque année, sur la réduction d'un nombre limité de risques

☑ POUR AGIR : mémo-quizz « **Règlement Européen** »

Le principe du mémo-quizz est très simple : il vous suffit de cocher les exigences qui vous semblent remplies. Tout ce qui n'est pas coché doit donner lieu, sans tarder, à une action.

Pour piloter la gouvernance des données personnelles de votre établissement, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données.

☐ Vous disposer déjà au sein de votre établissement d'un correspondant informatique et liberté (CIL)

Si oui :

☐ vous avez prévu qu'il devienne votre délégué à la protection des données

Si non :

☐ vous avez prévu le recrutement ou la désignation d'un délégué à la protection des données (il peut être mutualisé , ou prestataire extérieur)

☐ votre délégué à la protection des données a organisé le recensement précis de vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point.

☐ Sur la base de ce registre, il a identifié et vous a présenté les actions à mener pour vous conformer aux obligations actuelles et à venir. Il a priorisé ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes

☐ Si il a identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, il doit avoir mené, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA)

☐ Pour assurer un haut niveau de protection des données personnelles, votre délégué à la protection des données doit mettre en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire).

☐ Pour prouver votre conformité au règlement, Votre délégué à la protection des données doit constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

sigle	*désignation*	*Voir page*
ACSS	Accompagnement cybersécurité des structures de santé	31
AQSSI	Autorité qualifiée pour la sécurité des systèmes d'information.	10
CIL	Correpondant Informatique et Liberté	15
DPDP	Délégué à la protection des données personnelles	15
DPI	Dossier patient informatisé	8
DPO	Data protection officer (idem DPDP)	15
EIPD	Etude d'impact sur la protection des données (idem EIVP)	17
EIVP	Etude d'impact sur la vie privée	17
GHT	Groupement Hospitalier de Territoire	23
HDS	Hébergeur de données de santé	18
PGSSI-S	Politique générale de sécurité du système d'information de santé	27
DPIA	Data protection impact assesment (idem EIVP)	17
RGPD	Règlement général européen sur la protection des données personnelles	14
RSSI	Responsable sécurité du système d'information	23
SI / SIH	Système d'information / Système d'Information Hospitalier	8

Les sites institutionnels de référence :

ANSSI	Agence Nationale de la sécurité des systèmes d'information	www.ssi.gouv.fr
ASIP Santé	Agence française de la santé numérique	esante.gouv.fr
CNIL	Commission nationale Informatique et Liberté	www.cnil.fr
DGOS	Direction générale de l'offre de soins	solidarites-sante.gouv.fr - lien DGOS
DSSIS	Délégation à la stratégie des systèmes d'information de santé	solidarites-sante.gouv.fr - lien DSSIS
HAS	Haute autorité de santé	has-sante.fr
FSSI	Fonctionnaire de sécurité des systèmes d'information	solidarites-sante.gouv.fr - lien FSSI

Remerciements

Ce « Mémento » a été élaboré en s'appuyant sur un groupe de correspondants ayant accepté de participer à un entretien téléphonique et/ou d'effectuer une relecture critique du mémento :

- M. Nasser Amani, DSIO du CH de Villefranche sur Saône/Tarare/Trévoux/Grandris
- M. Monsieur Karim Amri, Directeur du CH de L'Aigle
- Mme Béatrice Bérard, Officier de sécurité du SI, Hospices Civils de Lyon
- M. Cédric Cartau, RSSI et DPO du CHU de Nantes, RSSI du GHT44
- M. Jean-Christophe Dayet, Chargé de mission, DSSIS, Ministère des solidarités et de la Santé
- M. Michel Dubois, Officier de sécurité du SI, Service de Santé des Armées
- Mme Anne-Marie Fabretti, Directrice des activité de réseaux et de la qualité, CH Annecy Genevois
- M. Pascal Forcioli, Directeur du CH de Bastia
- M. Gérard Gautier, Directeur du Foyer d'accueil médicalisé APAJH (Gentioux)
- M. Christophe Jodry, Chargé de mission, expert sécurité des SI à l'ASIP Santé
- M. Jean-Michel Kermarrec, Délégué à la protection des données au CHU de Montpellier
- M. Philippe Loudenot, Fonctionnaire de sécurité des SI des ministères sociaux
- M. Bertrand Martin, Directeur du CH Victor Dupouy d'Argenteuil
- M. Stéphane Pasquier, Fonctionnaire de sécurité des SI des ministères sociaux adjoint
- Mme Frédérique Pothier, Chargée de mission, DSSIS, Ministère des solidarités et de la Santé
- M. Michel Raux, Chargé de mission, DGOS, Ministère des solidarités et de la Santé
- M. Pascal Sabatier, Responsable de la sécurité des SI du CH du Pays d'Aix
- M. Emmanuel Sohier, Chargé de mission, expert sécurité des SI à l'ASIP Santé
- M. Rémi Tilly, Responsable de la sécurité du SI du GCS Sesan
- M. Philippe Tourron, Responsable de la sécurité des SI de l'Assitance Publique – Hôpitaux de Marseille

Il a également bénéficié des nombreux échanges informels qui animent le « Club des RSSI Santé » dont les réunions régulières favorisent les partages d'expériences et permettent d'assurer une véritable veille technologique.

Pour toute remarque ou commentaire concernant ce mémento,
merci d'adresser un courriel à DGOS-PF5@sante.gouv.fr

solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/e-sante/sih/

DIRECTION GÉNÉRALE DE L'OFFRE DE SOINS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE CHARGÉ DE LA SANTÉ

HÔPITAL NUMÉRIQUE