Cour des comptes

SIXIEME CHAMBRE

TROISIEME SECTION

S2024-1456

OBSERVATIONS DÉFINITIVES

(Article R. 143-11 du code des juridictions financières)

LA SÉCURITÉ INFORMATIQUE DES ÉTABLISSEMENTS DE SANTÉ

Un renforcement récent et à poursuivre, face à la multiplication des cyberattaques

Exercices 2019 à 2023

Le présent document, qui a fait l'objet d'une contradiction avec les destinataires concernés, a été délibéré par la Cour des comptes, le 14 octobre 2024.

13, rue Cambon ▪ 75100 PARIS CEDEX 01 ▪ T +33 1 42 98 95 00 ▪ www.ccomptes.fr

TABLE DES MATIÈRES

SYNTHÈSE

Selon le panorama dressé en 2023 par l'Agence nationale de la sécurité des systèmes d'information (Anssi), la cybermenace, définie comme *« tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes »,* est en constante augmentation, dans un contexte de fortes tensions géopolitiques.

Le secteur de la santé, et les hôpitaux en particulier, sont affectés par ces attaques qui peuvent entraîner des conséquences graves sur le fonctionnement des établissements de santé et sur la continuité et la qualité des soins.

Une forte exposition des hôpitaux aux attaques informatiques

En 2023, selon les données de l'Agence nationale de la sécurité des systèmes d'information (Anssi), sur le territoire français, 10 % des victimes d'attaques par des rançongiciels[1] étaient des hôpitaux, qu'ils soient publics ou privés.

La première attaque informatique d'envergure a concerné le CHU de Rouen en novembre 2019. En 2023, neuf attaques majeures ont été identifiées et la plus récente a touché le CH de Cannes en avril 2024.

Les menaces qui affectent les hôpitaux prennent principalement la forme de « compromissions » du système d'information, c'est-à-dire de violations de bases de données et de codes confidentiels, de messages électroniques malveillants et de rançongiciels, ces derniers étant les plus destructeurs.

La vulnérabilité des systèmes d'information des hôpitaux et leur interconnexion accrue avec des systèmes d'information extérieurs les placent au troisième rang des secteurs les plus touchés, après les collectivités territoriales et les entreprises, des plus petites d'entre elles à celles de taille intermédiaire.

La fragilité des systèmes d'information hospitaliers tient à leur complexité croissante, mesurée en nombre d'applications, sans équivalent dans d'autres secteurs d'activité (jusqu'à 1 000 applications pour les CHU les plus importants) et au sous-investissement chronique dans le numérique (1,7 % du budget d'exploitation en moyenne contre 9 % dans la banque et 2 % dans l'industrie des biens de consommation), auxquels s'ajoutent l'obsolescence de plus de 20 % des équipements (postes de travail et serveurs ayant un système d'exploitation ne faisant plus l'objet de maintenance, équipements de réseaux et applicatifs « métiers » ne pouvant plus être réparés ou mis à jour) et la prise en compte insuffisante des enjeux de cybersécurité par le personnel hospitalier.

[1] Logiciel malveillant qui empêche l'accès aux données stockées sur un ordinateur et propose leur récupération contre le paiement d'une rançon. En général, un logiciel rançonneur crypte les données de l'ordinateur cible et indique les instructions de paiement.

Malgré l'obligation à laquelle sont astreints les établissements de santé en la matière, les incidents de cybersécurité qui les affectent ne sont pas tous déclarés, faute de compétence interne suffisante en matière de cybersécurité mais, aussi sans doute, par crainte de retombées médiatiques et réputationnelles.

Les conséquences graves des cyberattaques

Les cyberattaques ont des effets directs sur le fonctionnement des établissements de santé et sur la prise en charge des patients tels que des interruptions de service pouvant durer plusieurs mois et le vol de données médicales et personnelles. Ces effets peuvent se cumuler. En outre, de nombreux dysfonctionnements opérationnels, logistiques ou encore financiers affectent les structures confrontées à de telles attaques.

Selon les évaluations réalisées par des hôpitaux victimes de cyberattaques, le coût pour un hôpital peut atteindre 10 M€ pour la gestion de la crise et la remédiation et 20 M€ pour la perte de recettes d'exploitation. Ces coûts n'intègrent pas les potentielles conséquences financières du vol et de la publication de masses de données, médicales et non médicales, de patients et de professionnels de santé.

L'arrêt du fonctionnement de services médicaux peut en outre entraîner la déprogrammation de prises en charge et, dans certains cas, le transfert de patients vers d'autres hôpitaux avec, nécessairement, des risques à court et à moyen terme sur la continuité et sur la qualité des soins (séquelles, perte de chances…), risques ou conséquences effectives non mesurés aujourd'hui.

A titre d'illustration, un délai de 18 mois a été nécessaire à un centre hospitalier disposant de 800 lits et places et accueillant 35 500 séjours en hospitalisation complète dans le champ « médecine, chirurgie et obstétrique » (MCO) pour reconstruire son système d'information ; l'activité d'hospitalisation MCO de cet établissement, qui a chuté de plus de 20 % après l'attaque, n'avait pas encore retrouvé son niveau de novembre 2022 à la fin du mois de février 2024.

Les pertes d'exploitation et les coûts de remise en état des systèmes d'information des établissements de santé attaqués sont supportés par les établissements de santé ; ceux-ci bénéficient souvent d'aides financières attribuées par les agences régionales de santé mais de manière non systématique et d'une ampleur variable selon les régions.

Une réponse tardive mais résolue des pouvoirs publics nationaux

Le ministère chargé de la santé a clarifié la gouvernance nationale du numérique en santé en en confiant la responsabilité à la délégation au numérique en santé (DNS), érigée en direction d'administration centrale en mai 2023. Face à l'émergence des premières cyberattaques, un financement destiné à la sécurité informatique a été institué et la certification des hôpitaux par la Haute Autorité de santé comprend désormais un volet relatif à la sécurité informatique.

La DNS pilote la « feuille de route du numérique en santé 2023-2027 » dont le volet cybersécurité, mis en œuvre par l'agence du numérique en santé (ANS), prévoit un programme de financement sur cinq ans ayant pour objectif de rattraper le sous-investissement numérique des hôpitaux.

Le programme « Cyberaccélération et résilience des établissements » (CaRE) prévoit un financement de 750 M€ en faveur de la sécurité des systèmes d'information sur cinq ans (de 2023 à 2027). Toutefois, cet engagement financier n'est assuré que jusqu'à la fin de l'année 2024. Il est indispensable qu'il soit poursuivi jusqu'au terme du programme. Au-delà de 2027, échéance de l'actuelle feuille de route du numérique en santé, le financement par les établissements de santé de l'élévation de leur cyberprotection devra être poursuivi, d'autant plus que les exigences s'élèvent.

Pour faire face au développement de la cybermenace à l'échelle européenne, un nouveau cadre juridique visant à assurer un niveau commun sensiblement plus élevé de cybersécurité dans l'ensemble de l'Union a été défini. Ainsi, la directive européenne NIS 2 (Network and Information Security), adoptée le 14 décembre 2022, élargit le champ des établissements soumis à régulation et relève le niveau d'exigence de leur protection. Cette directive n'était pas encore transposée en droit français le 17 octobre 2024, échéance du délai laissé aux Etats membres pour y procéder.

La Haute Autorité de santé (HAS) a complété son référentiel de certification en renforçant les critères de cybersécurité et en recrutant des experts visiteurs numériques à partir de 2024, contribuant ainsi à renforcer les actions en faveur de la sécurité informatique dans les établissements. Les hôpitaux s'inscrivent en parallèle dans une dynamique d'amélioration continue en faisant réaliser des audits thématiques encouragés par les programmes de financement ministériels. Une unification de cette démarche d'audit à l'échelle nationale, en lui conférant un caractère obligatoire et périodique, pourrait apporter une assurance externe sur la sécurisation des systèmes d'information et enrichir la certification par la HAS sur le volet technique.

Des actions à prolonger pour mieux préparer les hôpitaux

La création en 2016 des groupements hospitaliers de territoire (GHT) avait pour objectif de renforcer la coopération entre les établissements publics de santé afin d'améliorer l'efficacité et la qualité des soins tout en rationalisant la consommation des ressources.

Huit ans plus tard, la convergence qui était attendue des 136 GHT, notamment, en matière de systèmes d'information, demeure très inégale par manque d'impulsion locale et nationale. La construction d'un environnement numérique unifié et sécurisé, favorable à la coopération entre établissements publics, à l'amélioration de la qualité des soins et à l'optimisation des ressources financières et humaines doit donc être poursuivie et accélérée au vu des menaces auxquelles les hôpitaux sont confrontés. Doter les groupements hospitaliers de territoire de la personnalité morale serait un facteur déterminant pour atteindre cet objectif.

La meilleure prise en compte par les professionnels de santé du cyber-risque passe, certes, par la formation continue mais aussi et surtout par la formation initiale dans laquelle le numérique est jusqu'à présent absent. Sur l'initiative de la DNS qui pilote les actions de formation au numérique en santé des professionnels de santé, en relation avec le ministère de l'enseignement supérieur, des modules obligatoires de formation au numérique sont intégrés, à compter de la rentrée 2024, dans le premier cycle des formations initiales médicales et paramédicales.

RECOMMANDATIONS

Recommandation n° 1 : (DGOS, Cnam) *Mettre en place un groupe national d'expertise chargé, en cas de cyberattaques d'ampleur exceptionnelle, d'évaluer les pertes de recettes à compenser et, pour les établissements les plus gravement affectés, de proposer une dispense de codification a posteriori de leur activité hospitalière.*

Recommandation n° 2 : *(SGMAS) Mettre fin à l'utilisation d'un fonds de concours pour le financement de la Délégation au numérique en santé.*

Recommandation n° 3 : *(SGMAS, DNS, ANS) Conduire à son terme le programme CaRE.*

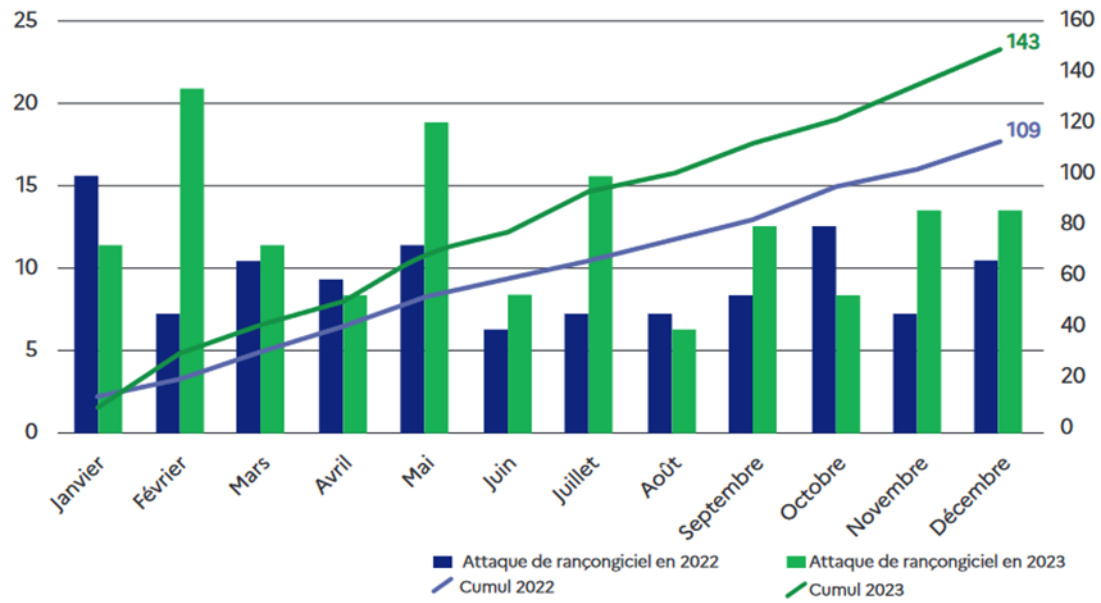
Recommandation n° 4 : *(DNS, ANS, DGOS, HAS, Anssi) Mettre en place un audit périodique obligatoire pour tous les établissements de santé, qui pourrait être pris en compte dans le dispositif d'incitation à la qualité et dans la certification par la HAS.*

Recommandation n° 5 : *(DGOS, DNS, ANS) Doter les groupements hospitaliers de territoire de la personnalité morale.*

INTRODUCTION

Selon le panorama dressé en 2023 par l'Agence nationale de la sécurité des systèmes d'information (Anssi), la cybermenace, définie comme *« tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes »*[2], est en constante augmentation, dans un contexte de fortes tensions géopolitiques.

Graphique n° 1 : Comparaison des signalements à l'Anssi d'attaques par rançongiciel[3], tous secteurs confondus, en 2022 et 2023



Source : Agence nationale de la sécurité des systèmes d'information (Anssi)

Le secteur de la santé, et les hôpitaux en particulier, sont affectés par ces attaques qui peuvent entraîner des conséquences graves sur le fonctionnement des établissements de santé et sur la continuité et la qualité des soins.

La Cour des comptes a produit, en 2016, un rapport sur la modernisation des systèmes d'information hospitaliers (Ralfss) et, en 2020, un rapport sur les groupements hospitaliers de territoire contenant une analyse de leurs systèmes d'information (communication à la commission des affaires sociales du Sénat). Compte tenu de l'évolution de la menace, la Cour actualise cette analyse afin d'apprécier la manière dont le ministère chargé de la santé a pris en

[2] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications.

[3] Un rançongiciel est un logiciel malveillant ou virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

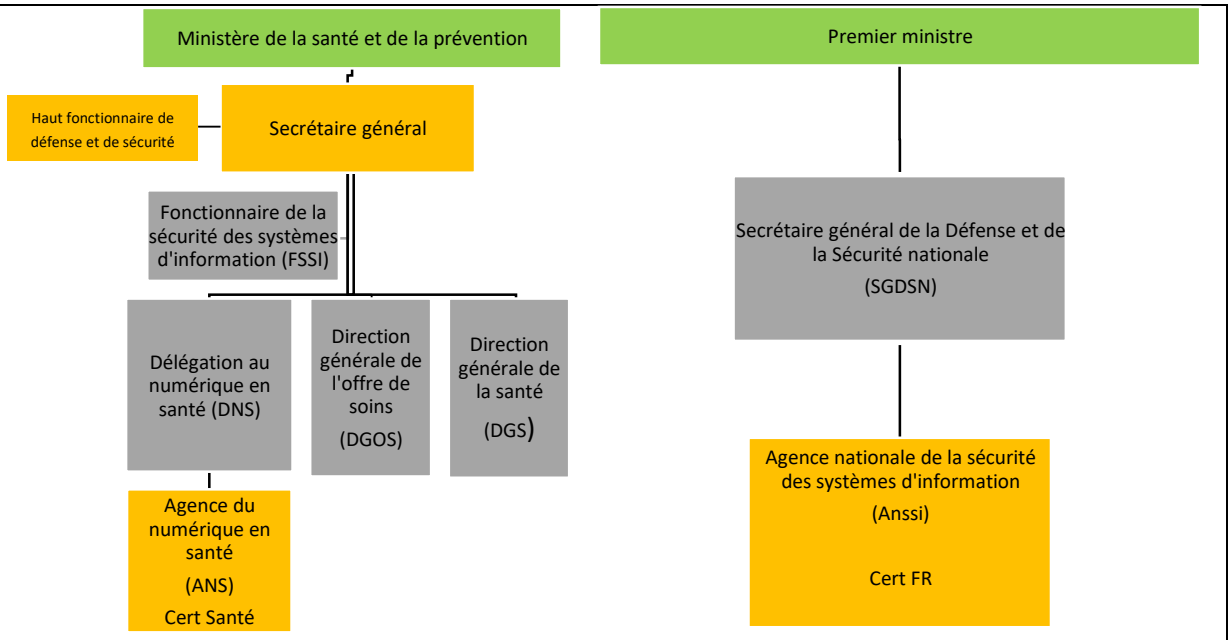
compte cette cybermenace, et d'examiner les actions engagées pour inciter les établissements de santé à se protéger.

Le rapport présente dans une première partie l'état de la menace à laquelle les 2 400 hôpitaux publics et privés sont confrontés, expose les raisons de la vulnérabilité des systèmes d'information hospitaliers et évalue les conséquences des cyberattaques sur les hôpitaux en termes de fonctionnement et de coût.

La seconde partie présente la réponse qui a commencé à être apportée au travers de la « feuille de route du numérique en santé » qui prévoit une évolution de la gouvernance et un financement d'actions destinées à accroître le niveau de préparation et de résilience des hôpitaux, et le renforcement des critères numériques et de cybersécurité dans la certification par la Haute Autorité de santé des établissements de santé.

La troisième partie s'attache à identifier les leviers permettant aux hôpitaux d'être mieux armés, qu'il s'agisse d'une plus grande homogénéité des actions conduites par les ARS ou d'un pilotage plus affirmé des groupements régionaux d'appui au développement électronique de la santé (GRADeS), de l'accélération de la convergence en matière de sécurité des systèmes d'information au sein des groupements hospitaliers de territoire ou de mesures liées au recrutement et à la formation.

Organigramme n° 1 : Gouvernance nationale du numérique et de la sécurité des systèmes d'information des hôpitaux



L'Anssi est responsable de la politique nationale de cybersécurité et en assure la coordination à l'échelle interministérielle.

Au niveau ministériel, jusqu'en 2023, la DGOS et la DGS contribuaient conjointement à la définition des politiques numériques et de sécurité des systèmes d'information des hôpitaux.

Depuis le début de l'année 2024, afin de gagner en efficacité et en lisibilité, le ministère de la santé et de la prévention a décidé d'unifier la mise en œuvre de la politique de sécurité des systèmes d'information en santé en la confiant à la délégation au numérique en santé (DNS). Les équipes de la DGOS et de la DGS spécialisées dans ces domaines ont été transférées à la DNS.

La DNS assure le pilotage de la feuille de route du numérique en santé et de l'ensemble des chantiers de transformation du numérique dont celui relatif à la sécurité des systèmes d'informations des hôpitaux. Elle assure la tutelle de l'Agence du numérique en santé (ANS) qui met en œuvre cette politique.

L'organisation de la sécurité numérique des établissements de santé relève du champ de responsabilité du fonctionnaire de la sécurité des systèmes d'information (FSSI) qui s'appuie sur la DNS et sur l'ANS dans ce domaine.

Le Cert (acronyme de la dénomination anglophone *« Computer Emergency Response Team »*) Santé, animé par l'ANS, constitue le service de référence chargé de la gestion des menaces de cybersécurité envers les établissements de santé et les établissements et services médico-sociaux. Il est en relation fonctionnelle avec le centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (Cert FR, pour « Cert France »), animé par l'Anssi et visant plus spécifiquement les établissements de santé les plus critiques ou d'importance vitale.

Source : Cour des comptes à partir des informations du ministère de la santé et de la prévention.

La méthode d'enquête de la Cour

Les constats et conclusions reposent sur les réponses apportées à la Cour par les autorités ministérielles et interministérielles chargées de la sécurité informatique. Ils s'appuient également sur des entretiens réalisés avec plus d'une vingtaine d'établissements de santé, publics, privés à but lucratif et privés à but non lucratif, qu'ils aient ou non été victimes de cyber attaques et dans des implantations géographiques variées. Enfin, ils tiennent compte de l'exploitation d'un sondage national réalisé auprès des établissements de santé.

1 L'INTENSIFICATION DE LA CYBER-MENACE, REVELATRICE DE LA FRAGILITE DES SYSTEMES D'INFORMATION DES HOPITAUX

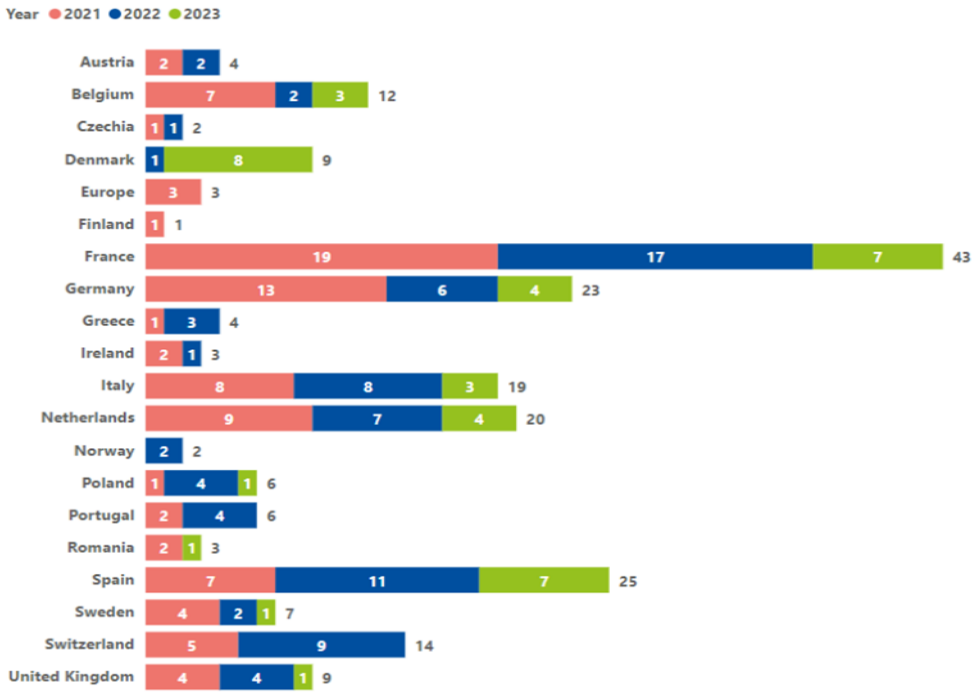
Les cyberattaques contre les hôpitaux, facilitées par des systèmes d'information vieillissants et mal sécurisés en raison d'un sous-investissement, peuvent occasionner de graves dommages en termes financiers et humains.

1.1 L'aggravation du risque en matière de sécurité informatique dans les établissements de santé

1.1.1 Une intensification des cyberattaques

Parmi les pays européens, la France est celui qui apparaît comme le plus touché par les cyberattaques dans le secteur de la santé (hôpitaux, laboratoires, mutuelles de santé, organismes publics de santé ou, encore, industries pharmaceutiques) selon le premier rapport de l'Agence européenne pour la cybersécurité (ENISA) sur la cybermenace, publié en 2023.

Graphique n° 2 : Panorama européen des menaces cyberattaques visant le secteur de la santé (janvier 2021 à mars 2023)[4]



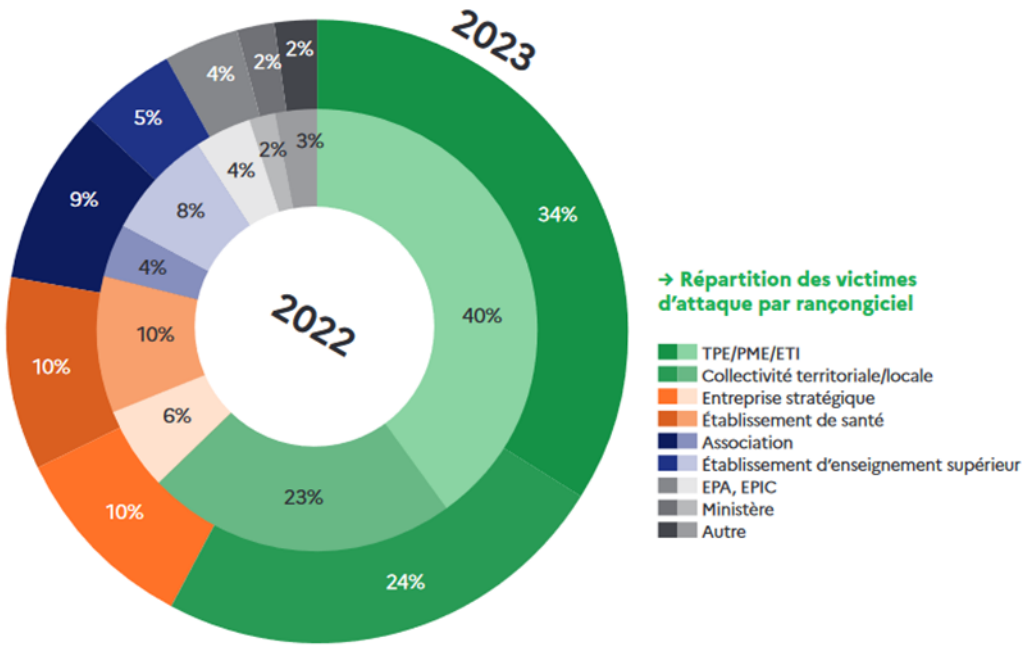
Source : Agence européenne pour la cybersécurité (ENISA) - Cyber threat landscape of the health sector in the EU (2023)

[4] Le rapport a été réalisé sur la base de 215 incidents identifiés par l'ENISA et ayant eu lieu entre janvier 2021 et mars 2023 sur le territoire européen dans diverses structures rattachées au secteur de la santé : hôpitaux, laboratoires, mutuelles de santé, organismes publics de santé et industries pharmaceutiques.

Il convient cependant d'interpréter avec prudence ce panorama dont l'ENISA reconnaît qu'il n'est pas complet : d'une part, la France apparaît relativement avancée en matière de déclaration d'incidents de sécurité des systèmes d'information, celle-ci étant obligatoire depuis plusieurs années au titre du code de la santé publique, et, d'autre part, notre pays compte davantage d'établissements sur son territoire que d'autres États comparables.

Même si, en France, les hôpitaux ne sont pas directement ciblés, l'augmentation de l'usage du numérique, la vulnérabilité de leurs systèmes d'information et leur exposition accrue les placent au troisième rang des secteurs les plus touchés, après les collectivités territoriales et les très petites, les petites et les moyennes entreprises ainsi que les entreprises de taille intermédiaire.

Schéma n° 1 : La répartition des victimes d'attaques par rançongiciel en France, en 2022 et en 2023



Source : Agence nationale de sécurité des systèmes d'information

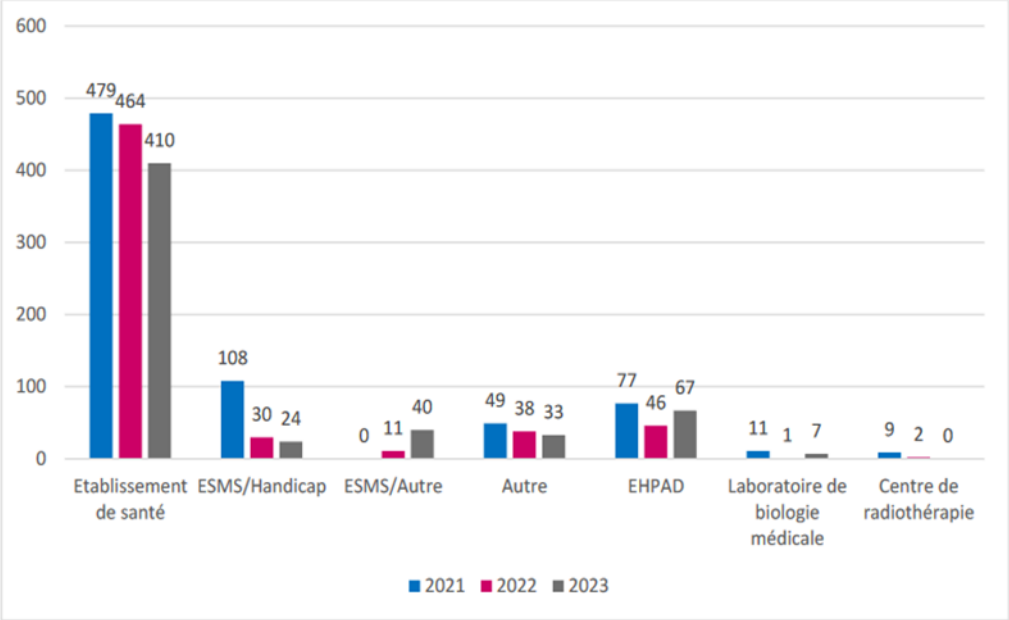
Les premières cyberattaques d'envergure ont concerné des établissements publics de santé : le CHU de Rouen, en 2019, puis l'hôpital de Dax-Côte d'Argent, en 2020. Depuis, les cyberattaques dont sont victimes, parmi d'autres, les hôpitaux français, quel que soit leur statut, se sont intensifiées et plusieurs incidents ont eu une résonance médiatique forte comme ce fut le cas en 2022 pour le Centre hospitalier Sud-francilien (CHSF) de Corbeil-Essonnes et pour l'hôpital André Mignot de Versailles.

En 2023, des cyberattaques ont affecté l'hôpital de Brest, le CHU de Rennes, le CHU de Rouen, le Centre hospitalier de l'Ouest-Vosgien, le groupe hospitalier Diaconesses-Croix Saint Simon, quatre établissements du groupe Ramsay ainsi que des cliniques du groupe Elsan.

Depuis le début de l'année 2024, d'autres cyberattaques ont été signalées par le centre hospitalier d'Armentières et le centre hospitalier de Cannes.

Parmi l'ensemble des attaques signalées dans le secteur de la santé, la grande majorité des incidents de sécurité est déclarée par les établissements de santé (71 %).

Graphique n° 3 : Répartition des signalements selon le type de structure victime



Source : Agence du numérique en santé - Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social (2023)

1.1.2 Une diversité de menaces pouvant affecter les établissements de santé

Sur le plan interministériel, l'Anssi, créée par décret en 2009[5], est un service à compétence nationale chargé de la politique de sécurité des systèmes d'information placé sous l'autorité du Premier ministre et rattaché au secrétaire général de la défense et de la sécurité nationale (SGDSN). Selon son directeur général, les hôpitaux ne seraient pas des victimes spécifiquement recherchées par les cyberagresseurs ; ceux-ci seraient plutôt victimes d'une *« pêche au chalut, dans laquelle les attaquants ne ciblent personne en particulier et tout le monde en général »*. Il s'agit d'attaques larges, à grande échelle, qui se démocratisent[6], notamment sous la forme de logiciels malveillants, communément qualifiés de rançongiciels, qui touchent, entre autres victimes, des hôpitaux.

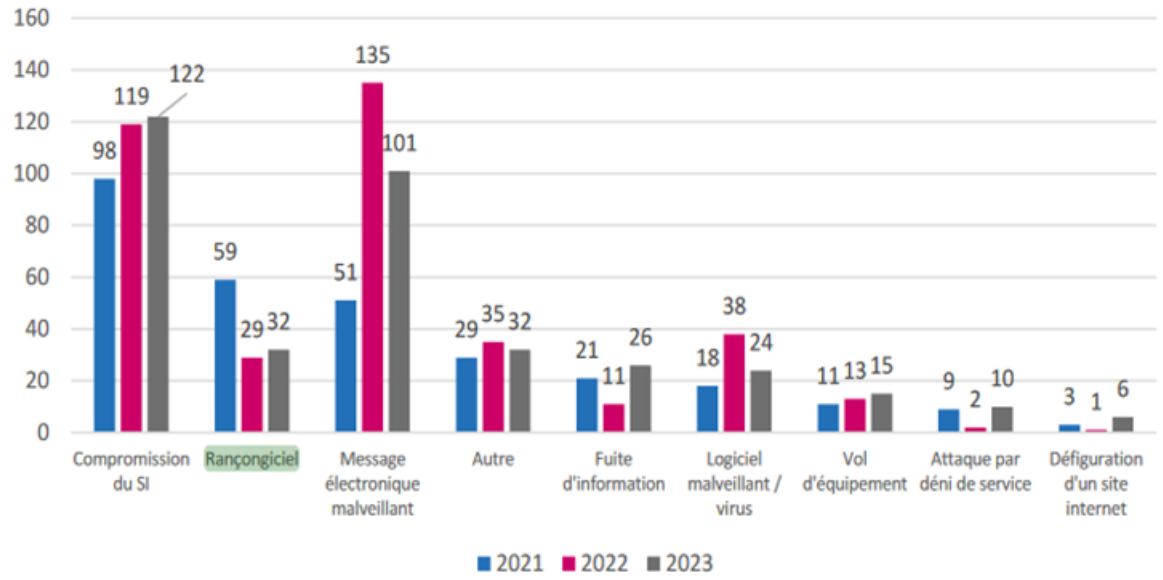
Les attaques les plus violentes dont sont victimes les hôpitaux sont le fait de ces rançongiciels qui, par le cryptage des données, conduisent à la paralysie du système d'information hospitalier et comportent la menace de divulgation des données de santé et de leur revente. Sur ce point, l'Anssi recommande aux établissements et organismes victimes de telles attaques de ne jamais payer la rançon demandée car le paiement ne garantit pas l'obtention d'un moyen de décryptage pour récupérer les données ni leur non-divulgation, incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux. En outre,

[5] Décret 2009-834 du 7 juillet 2009.

[6] Développement d'un nouveau type de rançongiciel à bas coût disponible sur différents forums de cybercriminalité, en particulier sur ceux fréquentés par les agresseurs les moins qualifiés. Ces rançongiciels ne constituent une menace significative mais ils permettent aux cybercriminels de s'engager dans ce type d'attaques à moindre coût - Enquête de Sophos, société de logiciels et de solutions de sécurité – 17 avril 2024.

le paiement d'une rançon n'empêche pas l'entité attaquée d'être à nouveau la cible de cybercriminels.

Graphique n° 4 : Typologie des incidents ayant affecté les établissements de santé en 2023



Source : Agence du numérique en santé - Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social (2023)

Les attaques pouvant affecter un système d'information

Compromission du système d'information : la compromission de données est un incident de sécurité à l'occasion duquel des informations sont dérobées, reproduites, consultées ou divulguées illégalement par une personne ou par un groupe non autorisé.

Rançongiciel : logiciel malveillant qui empêche l'accès aux données stockées sur un ordinateur et propose leur récupération contre le paiement d'une rançon. En général, un logiciel rançonneur crypte les données de l'ordinateur cible et indique les instructions de paiement.

Message électronique malveillant (hameçonnage ou *phishing*) : technique de fraude visant à obtenir des informations confidentielles telles que des mots de passe ou des numéros de cartes de crédit, au moyen de messages ou de sites usurpant l'identité d'institutions financières ou d'entreprises commerciales.

Attaque par déni de service : attaque visant à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer, ou par l'exploitation de failles de sécurité afin de provoquer une panne ou une forte dégradation du service.

Défiguration d'un site internet : signe visible qu'un site Internet a été attaqué et que l'attaquant a obtenu les droits lui permettant d'en modifier le contenu.

Qu'il soit victime d'un rançongiciel ou d'une compromission de son système d'information, dès lors qu'il est attaqué, un hôpital est contraint de fonctionner en mode dégradé pendant une période plus ou moins longue, de quelques heures à plusieurs mois.

Schéma n° 2 : Chronologie de cyberattaques marquantes en 2023, selon le type d'incident subi

Source : Agence du numérique en santé (Rapport annuel 2023)

1.1.3 Face aux attaques, un dispositif efficace d'alerte et d'appui en réponse aux incidents

Depuis 2016[7], les établissements de santé, organismes et services exerçant des activités de prévention, de diagnostic ou de soins sont soumis une obligation de signalement qui permet d'identifier les incidents graves de sécurité des systèmes d'information, c'est-à-dire les événements à l'origine d'une situation exceptionnelle au sein d'un établissement[8].

Ce dispositif de traitement des signalements des incidents de sécurité des systèmes d'information constitue un élément de la stratégie d'amélioration du niveau de sécurité numérique du secteur de la santé portée par le ministère chargé de la santé, en coordination étroite avec l'Anssi.

[7] Code de la santé publique, art. L. 1111-8-2, et décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information. Cette obligation de signalement a été étendue aux établissements médico-sociaux depuis 2022.

[8] Les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins, les incidents ayant des conséquences sur la confidentialité ou sur l'intégrité des données de santé et les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service.

Sa mise en œuvre opérationnelle relève de la responsabilité du Cert Santé[9], cellule d'assistance en cybersécurité des structures de santé hébergée au sein de l'Agence du numérique en santé depuis sa création, en 2017.

Le Cert Santé, qui fonctionne 24 heures sur 24 et sept jours sur sept, est à la fois un service d'alerte et un service de réponse à incident.

Les alertes sont des informations, communiquées heure par heure, signalant des vulnérabilités sur des applicatifs utilisés par des établissements de santé, afin de les prévenir d'un danger immédiat et de leur proposer des moyens pour s'en prémunir.

Exemple d'alerte diffusée le 20 juin 2024 par le Cert Santé

« Un défaut dans la fonction render_raw du plugin WordPress ElementsKit Pro permet à un attaquant ayant les privilèges contributor, de mener des attaques de type Server-Side Request Forgery (SSRF) ».

Risques :

- atteinte à la confidentialité des données
- atteinte à l'intégrité des données

Solutions ou recommandations :

- mettre à jour le plugin WordPress ElementsKit Pro vers la version 3.6.3 ou ultérieure

Source : site internet du Cert Santé

Par ailleurs, le Cert Santé porte assistance aux établissements confrontés à un incident majeur ayant déjà affecté un ou plusieurs services numériques et contraignant l'établissement à mettre en place un mode dégradé de fonctionnement.

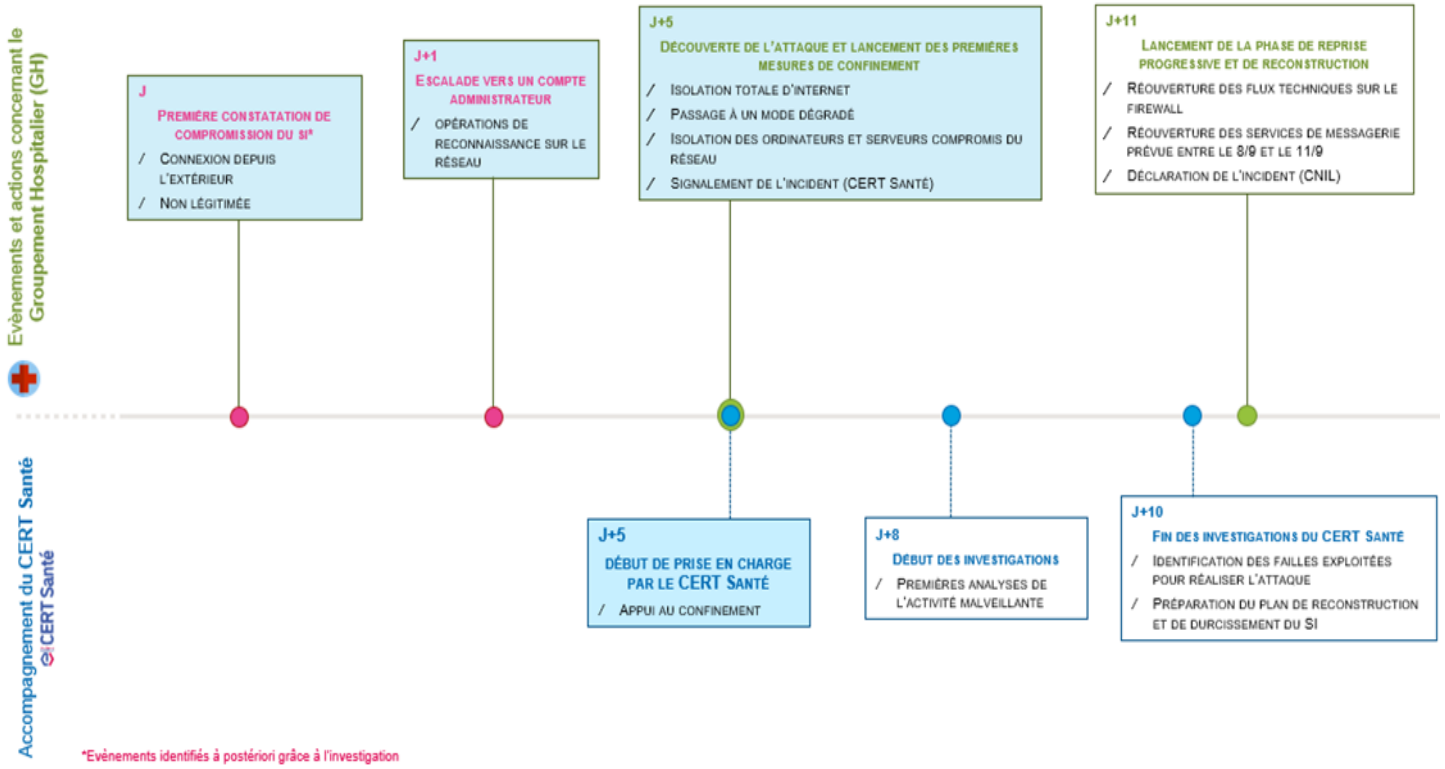
Le signalement est déclaré sur un portail opéré par l'Agence du numérique en santé en coordination avec le Service du haut fonctionnaire de défense et de sécurité (HFDS) des ministères chargés des affaires sociales.

À titre d'exemple, dans la situation décrite dans le graphique ci-dessous tirée d'une situation réelle, l'intervention du Cert Santé a permis une investigation approfondie et une identification de la faille utilisée par l'attaquant. L'infiltration dans le parc a eu lieu *via* la réutilisation d'un identifiant de compte de prestataire sur l'accès VPN[10].

[9] *"Computer Security information Response Team"* (Cert).

[10] « *Virtual Private Network* » : système de cryptage permettant de créer un lien direct entre des ordinateurs distants, connectés à des réseaux locaux différents, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

Schéma n° 3 : Chronologie de la cyberattaque d'un groupe hospitalier en 2023



Source : Agence du numérique en santé - Cert Santé

Plusieurs identifiants ont été exfiltrés au cours de l'incident. Au moins un compte d'administrateur de domaine ainsi qu'un compte d'utilisateur ont été compromis par accès depuis l'extérieur. Aucun effet n'a été constaté sur la prise en charge des patients. L'étape d'investigation a permis d'identifier les points de vulnérabilité du système d'information du groupe hospitalier exploités par l'attaquant, afin de renforcer sa sécurité.

À des fins d'information et de sensibilisation, le Cert Santé décrit et tient à jour sur son site internet l'expérience d'établissements de santé victimes d'attaques. Parmi les établissements publics interrogés[11], ceux qui ont signalé un incident expriment à plus de 80 % une opinion positive sur les prestations du Cert Santé.

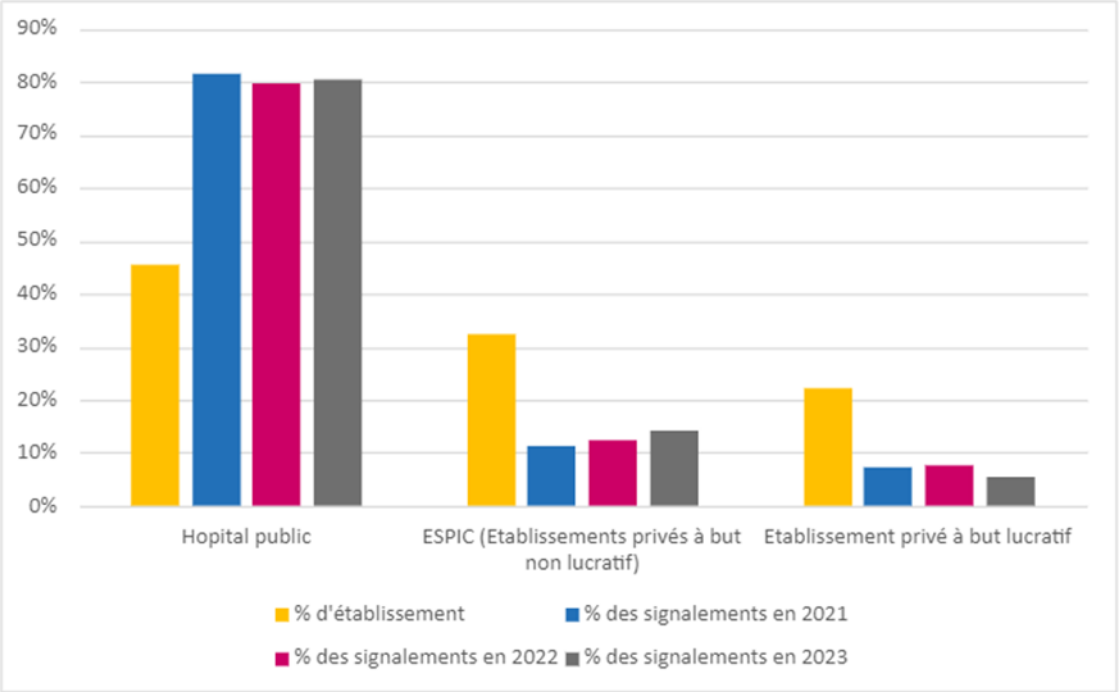
L'efficacité du Cert Santé repose sur la disponibilité et sur l'expertise de neuf agents. La dimension de l'équipe par rapport au volume d'activité auquel elle est confrontée ne lui permet pas d'assurer une permanence pendant les heures non ouvrées, ce qui ne facilite pas le suivi. L'ANS fait alors appel à des prestataires extérieurs qualifiés.

Enfin, il ressort des signalements reçus par le Cert Santé que près de 80 % des incidents sont déclarés par les établissements publics de santé alors qu'ils ne représentent que 45 % des établissements de santé. Selon l'ANS, ce constat pourrait s'expliquer par le fait que les établissements publics ont une plus grande diversité d'activités hospitalières avec un grand

[11] Enquête réalisée par les rapporteurs de la Cour des comptes en relation avec les fédérations hospitalières auprès de tous les hôpitaux, publics (97 % de répondants), privés à but lucratif (18 % de répondants) et privés à but non lucratif (41 %), en mars et avril 2024.

nombre d'interconnexions avec l'extérieur, offrant par conséquent une plus large surface d'exposition.

Graphique n° 5 : Part des signalements au Cert santé selon le statut des établissements



Source : Agence du numérique en santé - Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social (Rapport annuel 2023)

Selon l'ANS, aucun élément tangible ne permet d'affirmer que certains établissements seraient plus spécifiquement ciblés selon leur statut.

L'évaluation de l'ampleur de la menace reste incomplète en l'absence de certitude que tous les établissements déclarent bien les incidents. Or, ce signalement immédiat et systématique des incidents est vital pour que les organismes publics compétents puissent apporter un appui à la structure touchée, identifier une nouvelle cybermenace et proposer à l'ensemble des structures de santé des mesures de prévention et de réaction adaptées.

Il convient donc d'améliorer l'efficacité du système de signalement des incidents en rappelant à toutes les structures de santé l'obligation de déclaration des incidents de sécurité, en particulier aux établissements de santé privés et aux établissements implantés dans les régions où le nombre de signalements rapporté à l'activité hospitalière est faible.

1.2 Des attaques facilitées par la fragilité des systèmes d'information hospitaliers

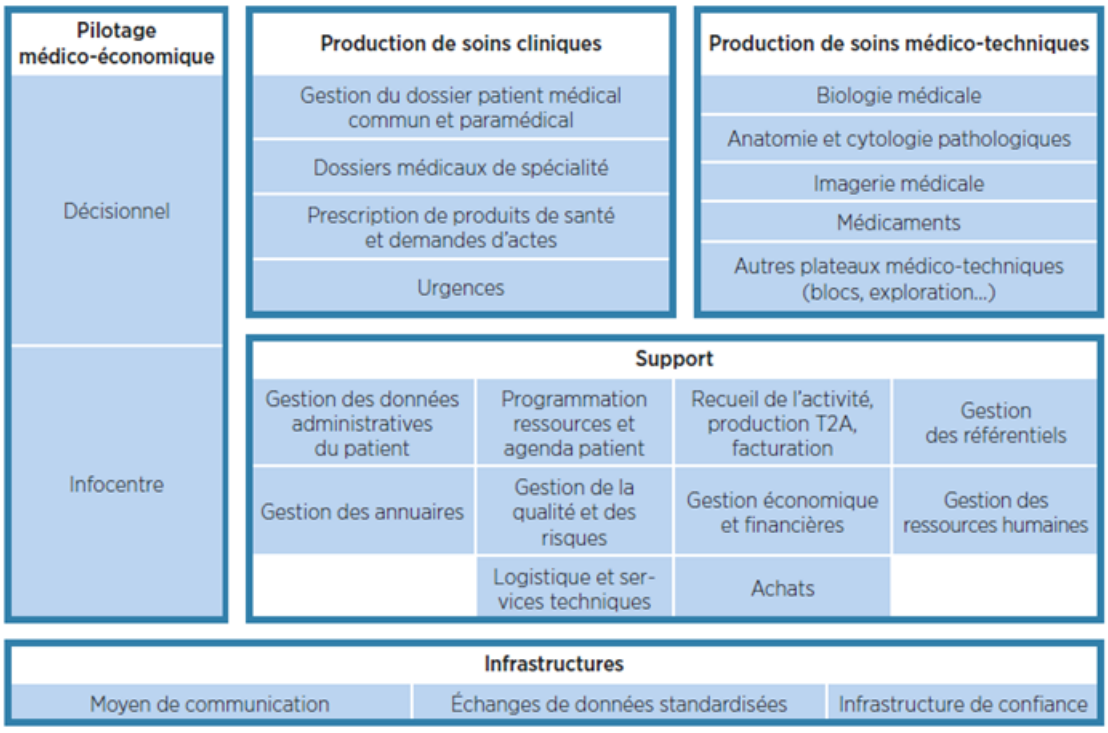
La fragilité des systèmes d'information hospitaliers tient à leur complexité, mesurée en nombre d'applications à exploiter, au sous-investissement chronique dans le numérique et à la prise en compte encore insuffisante des enjeux de cybersécurité par le personnel hospitalier.

1.2.1 Une complexité croissante et sans équivalent des systèmes d'information hospitaliers

Les systèmes d'information des hôpitaux (SIH) rassemblent de très nombreux applications et processus permettant de collecter, de stocker, de traiter et de partager les informations et les données liées aux missions et aux activités de l'établissement de santé telles que le soin, la recherche, l'enseignement et la gestion.

Parmi les systèmes d'information des organisations administratives civiles, ceux des hôpitaux se rangent dans les plus complexes, en raison de la diversité des acteurs, des sources, des outils, des techniques et des processus. Cette complexité peut entraîner des difficultés et des défis dans la conception, la mise en œuvre, la gestion, l'évolution d'un SIH et sa sécurisation.

Schéma n° 4 : Périmètre fonctionnel d'un système d'information hospitalier



Source : Agence du numérique en santé

1.2.1.1 Un système d'information complexe, riche en fonctionnalités

Les SIH se sont fortement développés ces dernières années. À l'origine centrés sur les fonctions administratives et financières, les premiers logiciels se limitaient à la comptabilité et à la facturation. Les informations concernant le suivi des patients étaient, quant à elles, enregistrées dans des dossiers de papier. Ces systèmes étaient souvent peu interconnectés, limitant ainsi leur capacité à échanger des informations.

Le développement des réseaux informatiques locaux[12] a ensuite facilité l'informatisation des activités médicales des établissements de santé. D'abord isolées les unes des autres, les applications composant un SIH ont été progressivement interconnectées dans le but d'échanger des informations. La démocratisation de l'accès à internet dans les années 90 a conduit les SIH à s'ouvrir vers l'extérieur. La dématérialisation de la feuille de soin, la facturation électronique et les premières tentatives de mise en place des messageries sécurisées de santé (MSS) ont constitué les prémices d'un système d'information de plus en plus ouvert sur l'environnement de l'hôpital.

L'informatisation des processus de soin a, de même, connu une accélération notable ces dernières années à la faveur de plusieurs plans numériques impulsés par le ministère. Le déploiement du dossier du patient informatisé (DPI), visant à remplacer le dossier en format papier, a largement contribué à la transformation du processus de soin.

Parallèlement, les équipements médico-techniques ont évolué au rythme des avancées techniques. Les trois principaux systèmes d'information relevant de ce champ (radiologie, laboratoire, pharmacie) ont connu des avancées majeures ces dernières années, telles que la robotisation et que l'interconnexion avec le dossier du patient informatisé.

Le SIH couvre aujourd'hui la quasi-totalité des métiers des établissements de santé. Fortement interconnectées, les applications échangent des informations, tant internes qu'externes. Le SIH compte, selon la taille des hôpitaux, entre 80 et 500 applications informatiques propres à des processus « métiers » (prescriptions pharmaceutiques, résultats d'examens de biologie) ou à des fonctions support (gestion économique et financière, gestion des ressources humaines, gestion administrative des patients, demande de transport interne…). Les Hospices civils de Lyon (HCL) comptent plus de 500 applications sur 14 sites différents et l'Assistance publique-Hôpitaux de Paris (AP-HP) utilise près d'un millier d'applications sur 40 sites. Les établissements de santé du secteur privé comptent moins d'applications, en raison d'un spectre d'activité moins large, mais présentent d'autres types de risques, liés notamment aux interactions entre les systèmes d'information utilisés par les médecins libéraux et ceux des établissements où ils exercent. Ces connexions des médecins libéraux au SIH peuvent présenter des failles de sécurité.

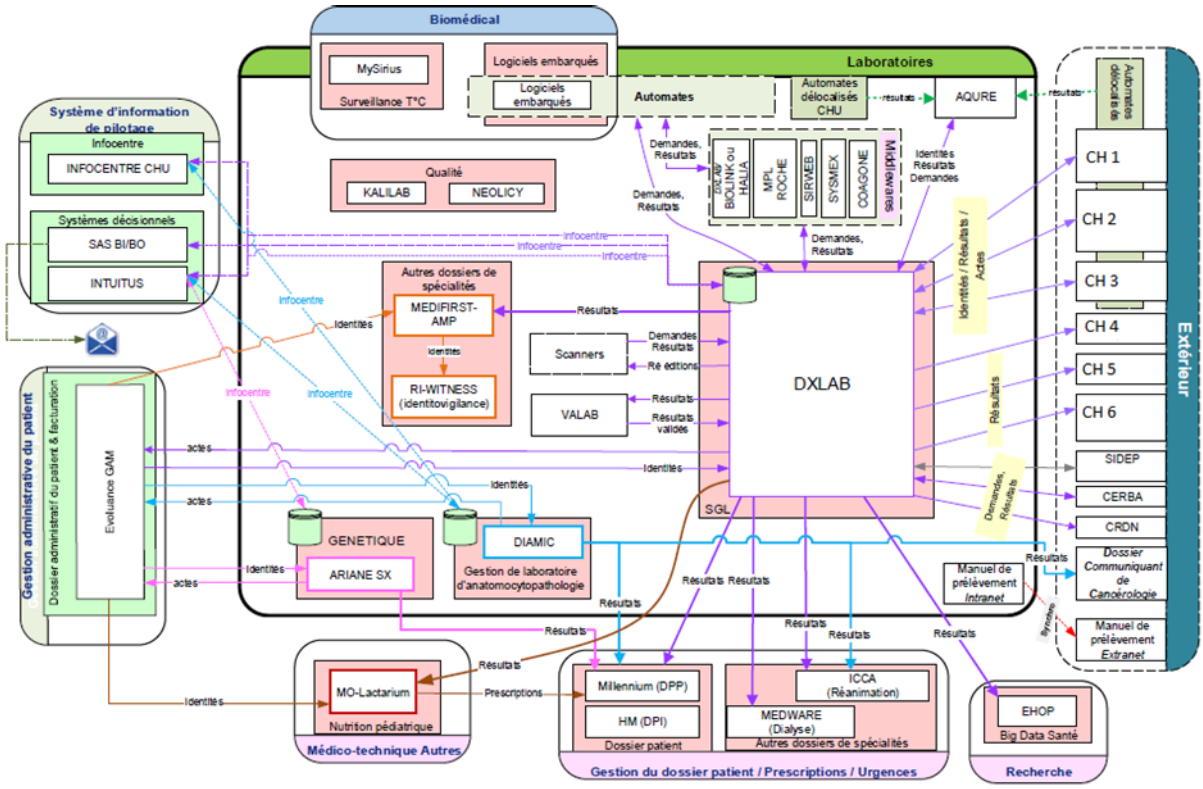
Les perspectives de développement des usages des objets connectés[13] pour la surveillance des patients, pour la gestion des médicaments ou la gestion logistique rendent les SIH encore plus complexes.

---

[12] Un réseau local est un réseau informatique dans lequel les équipements qui le composent s'échangent des informations sans utiliser l'accès internet.

[13] Les objets connectés, ou Internet des objets (IoT), désignent des dispositifs physiques équipés de capteurs, de logiciels et d'autres dispositifs techniques qui leur permettent de se connecter à internet et de communiquer entre eux ou avec d'autres systèmes. Ces objets peuvent collecter, échanger et analyser des données pour automatiser

Schéma n° 5 : Représentation schématique du système d'information du laboratoire d'un CHU



Source : CHU

1.2.1.2 Une ouverture du système d'information à de multiples parties prenantes

D'abord cantonné au personnel administratif pour l'accomplissement des tâches liées à la gestion de l'établissement, le SIH s'est progressivement ouvert aux partenaires et prestataires de l'hôpital tels que les laboratoires d'analyses pour des échanges d'information, les fournisseurs de matériel médical pour la supervision et la maintenance à distance de celui-ci, et les prestataires des services informatiques.

Les applications informatiques, hébergées à l'origine exclusivement au sein des centres de données des établissements, le sont désormais aussi bien en interne qu'en externe[14]. Le développement de l'informatique en nuage dit *cloud computing*[15] et de la location de logiciels

---

des tâches, améliorer l'efficacité et offrir de nouvelles fonctionnalités dans divers domaines tels que la santé, la domotique, l'industrie et la logistique.

[14] L'enquête réalisée par la Cour des comptes auprès des établissements de santé montre une prépondérance de ce type d'hébergement (55 % pour le secteur public, 58 % pour le secteur privé lucratif, 78 % pour le secteur privé non lucratif). Les trois questionnaires (un questionnaire par fédération) couvraient cinq thèmes : ressources humaines, gouvernance des systèmes d'information, infrastructure, budget et programmes de financement, cybersécurité. Ils ont été élaborés en concertation avec la FHF, la FHP et la FEHAP et les résultats ont fait l'objet d'une relecture par ces fédérations. Cette collaboration a permis d'affiner l'analyse des résultats et de vérifier la bonne interprétation de certaines atypies dans les réponses.

[15] L'informatique en nuage, ou « cloud-computing », est un modèle de prestation de services informatiques qui permet aux utilisateurs d'accéder à des ressources informatiques, telles que des serveurs, des applications et des services à la demande et via Internet, sans avoir à gérer et à maintenir ces ressources eux-mêmes.

en mode dit *SaaS*[16] permet aux établissements d'accélérer la modernisation de leurs infrastructures informatiques. Ce mode de gestion accroît encore la complexité du SIH en raison des nombreuses interconnexions de réseaux et des interfaces applicatives qu'il nécessite. Ces flux, nécessaires à la prise en charge des patients, augmentent d'autant la surface d'attaque[17] et requièrent des mécanismes de sécurisation spécifiques.

L'offre de services numériques aux patients et à leurs familles a, de même, considérablement évolué ces dernières années, notamment depuis la crise sanitaire de 2020. La prise de rendez-vous en ligne devient un outil essentiel de gestion de la relation avec les patients. Le développement de la télémédecine, avec ses différentes applications (la téléconsultation, la télé-expertise, la télésurveillance, la télé-assistance), vient enrichir les services numériques. Certains établissements ont développé un guichet numérique regroupant un ensemble de services[18], à l'image de l'application « ViaPatient » développée et diffusée par les HCL ou de « l'Espace Patient » de l'AP-HP.

L'accès à distance au SIH pour le personnel médical et paramédical s'est aussi développé, 75 %[19] des établissements l'ayant autorisé dès 2021.

1.2.2 Des budgets hospitaliers consacrés au numérique trop modestes

La fragilité des systèmes d'information résulte d'un sous-investissement chronique que les établissements consultés par la Cour ont confirmé.

Les établissements publics présentent une obsolescence de leurs matériels et logiciels plus élevée que les hôpitaux privés. Près de 20 % des postes de travail dans les hôpitaux publics ont plus de sept ans ou un système d'exploitation hors de maintenance ou obsolète. En outre, 23 % des équipements de réseaux ne peuvent plus être mis à jour ou réparés en cas de panne, comme le montre le tableau ci-dessous.

[16] Le mode SaaS, ou « Software as a Service », est un modèle de prestation de services informatiques qui permet aux utilisateurs d'accéder à des applications logicielles à la demande via Internet, sans avoir à les installer, à les gérer et à les maintenir eux-mêmes. Les applications sont hébergées et gérées par un fournisseur de services, qui les met à disposition des utilisateurs, moyennant un abonnement ou une redevance d'utilisation.

[17] La surface d'attaque correspond à l'ensemble des points d'entrée qu'un attaquant potentiel peut exploiter pour accéder à un système informatique. Elle comprend toutes les vulnérabilités, chemins et méthodes possibles par lesquels une attaque peut être lancée.

[18] Rendez-vous en ligne, échanges patients soignants, e-admissions, documents de prise en charge médicale, comptes-rendus, radios…

[19] Source : Atlas des SIH, ministère des solidarités et de la santé, novembre 2021.

Tableau n° 1 : Obsolescence des équipements numériques des établissements de santé (2024)

	Publics	Privés à but non lucratif	Privés à but lucratif
Postes de travail *(matériel de plus de 7 ans ou ayant un système d'exploitation hors maintenance ou obsolète)*	19 %	11 %	8 %
Serveurs *(matériel de plus de 5 ans ou ayant un système d'exploitation hors maintenance ou obsolète)*	28 %	29 %	19 %
Équipements réseaux *(équipement ne pouvant plus être mis à jour ou réparés en cas de panne)*	23 %	11 %	11 %
Applicatifs métiers *(part des applicatifs métiers obsolètes)*	22 %	18 %	5 %

Source : enquête réalisée par la Cour des comptes auprès de tous les hôpitaux, publics (97 % de répondants), privés à but lucratif (18 % de répondants) et privés à but non lucratif (51 %) entre mars et avril 2024

Pour mesurer l'effort financier que les hôpitaux consacrent à leur système d'information, la DGOS et l'ATIH procèdent annuellement, depuis 2012, à une enquête auprès des établissements de santé publics et privés à but non lucratif. Une instruction de la DGOS définit la liste limitative de comptes budgétaires et des règles d'imputation pour répondre à cette enquête[20]. La dernière édition de cette enquête date de 2022 et révèle que ces établissements consacrent 1,7 % de leur budget d'exploitation à leurs systèmes d'information.

Tableau n° 2 : Dépenses en informatique rapportées au budget total des établissements de santé publics et privés à but non lucratif (2022)

Catégorie d'établissements	Budget informatique/ budget total	Nombre d'établissements
Établissements de santé publics et privés non lucratif	***1,69 %***	***888***
CHU	*1,89 %*	*20*
CH de moins de 20 M€	*1,30 %*	*216*
CH de 20 à 70 M€	*1,54 %*	*159*
CH de 70 à 150 M€	*1,57 %*	*89*
CH de plus de 150 M€	*1,54 %*	*42*
Centres de lutte contre le cancer	*2,53 %*	*12*
Établissements privés à but non lucratif	*1,98 %*	*350*

Source : Observatoire des systèmes d'information de santé (OSIS)

Comparé avec les budgets alloués dans d'autres secteurs économiques, l'effort financier déployé par les établissements de santé apparaît très réduit.

[20] Instruction N°DGOS/MSIOS/2013/259 du 7 juin 2013 relative à la définition et au suivi des ressources et des charges des systèmes d'information hospitaliers.

Tableau n° 3 : Dépenses en informatique rapportées au chiffre d'affaires, par secteur économique

Secteur économique	Dépenses en informatique /chiffre d'affaires
Services financiers, banques	*9,0 %*
Télécom	*5,5 %*
Conseil et services, informatique	*4,5 %*
Électronique, santé, assurance, transport	*3,5 %*
Automobile, chimie, biens de consommation, énergie	*2,0 %*
Bâtiment, distribution	*1,0 %*

Source : The Computer Economics IT Spending and Staffing Benchmarks 2020-2021

La feuille de route du numérique en santé 2023-2027 du ministère de la santé et de la prévention fixe comme objectif que, *« au plus tard en 2027, les établissements sanitaires consacrent en moyenne au moins 2 % de leur budget au numérique, dont 10 % sur la cybersécurité et les infrastructures, avec la mise en place d'un forfait numérique pérenne dans la tarification »* [21].

Cet objectif de 2 % concerne tous les établissements de santé, quel que soit leur statut. La vérification de l'atteinte de cet objectif suppose que le mode de recueil des données financières en matière de numérique évolue pour intégrer les établissements privés, jusqu'ici non pris en compte, que la part de budget que chaque établissement consacre à la sécurité, aujourd'hui non connue, soit mesurable et que tous les établissements répondent à l'enquête annuelle[22].

En matière d'identification des dépenses de sécurité, les établissements devront être aidés pour appliquer une méthode identique car la définition du périmètre des ressources consacrées à la sécurité est complexe et son application est l'objet de grandes différences d'interprétation.

1.2.3 Une sensibilisation progressive mais encore insuffisante du personnel hospitalier au cyber-risque

Comme cela ressort du graphique sur la typologie des incidents affectant les établissements de santé en 2023, la première source d'incidents déclarés au Cert Santé en 2022, et la deuxième en 2023, est le message électronique malveillant, attaque lancée au hasard sur internet, sans cible définie, aussi qualifié d'hameçonnage ou *phishing*.

La vulnérabilité des SIH trouve donc essentiellement son origine dans le comportement des utilisateurs, quelles que soient les fonctions exercées et le niveau de leurs responsabilités. La compréhension des impératifs de cybersécurité et de la responsabilité individuelle pour sécuriser un réseau est encore insuffisante.

[21] Page 33 de la feuille de route du numérique en santé 2023-2027 - « Mettre le numérique au service de la santé », annoncée le 7 mai 2023.
[22] Lors de la dernière enquête annuelle, 16 % des établissements n'avaient pas répondu.

On peut émettre l'hypothèse que l'exigence élevée des soins conduirait le personnel médical à ne pas accorder la même priorité aux contraintes liées à la sécurité informatique[23] alors que celle-ci conditionne aussi la qualité des soins.

Par ailleurs, la sensibilisation du personnel de direction des établissements de santé a certes évolué mais, dans l'enquête en ligne lancée par la Cour auprès de tous les établissements de santé, une minorité de directeurs d'établissement a répondu[24], laissant le soin aux DSI ou RSSI d'y répondre.

L'une des expressions recueillies insiste sur le fait que « *la sensibilisation à la sécurité informatique est une composante vitale de notre stratégie de défense contre les menaces numériques. Cependant, le simple fait de dispenser des sessions de sensibilisation ne suffit pas. Il est également nécessaire de mettre en place des rappels réguliers et des mesures de suivi pour renforcer les messages et encourager une culture de sécurité durable. En investissant dans des programmes de sensibilisation plus interactifs et personnalisés, nous pouvons aider à garantir que les bonnes pratiques en matière de sécurité restent ancrées dans l'esprit de tous les membres de l'hôpital* ».

1.3 De lourdes conséquences pour les établissements de santé attaqués

Les cyberattaques au sein des établissements nécessitent la mise en place d'organisations de gestion spécifiques telles que des cellules de crise qui visent à garantir la réactivité des équipes et la mise en place de modes de communication adaptés aux différents publics (presse, médias, professionnels de santé, patients). Ainsi, au centre hospitalier d'Armentières, une cellule composée d'experts de la sécurité des systèmes d'information de l'établissement et du CHU de Lille, établissement support du groupement hospitalier de territoire (GHT), a été constituée, et des assemblées générales du personnel réunies pour informer les professionnels de l'établissement. Le centre hospitalier de Versailles a mis en place, durant la crise, une lettre d'information régulière à l'attention de l'ensemble du personnel.

1.3.1 Des conséquences majeures sur le fonctionnement de l'établissement et pour les patients

Les cyberattaques, en fonction des différents modes opératoires utilisés, ont des effets directs sur le fonctionnement des établissements de santé et sur la prise en charge de leurs patients, matérialisés principalement par des interruptions de service et par le vol de données médicales et personnelles. Ces deux types d'effets peuvent, ou non, se cumuler. En outre, de nombreux dysfonctionnements opérationnels, logistiques ou encore financiers affectent directement ou indirectement les structures confrontées à de telles attaques.

[23] Jean-Roch Letellier - Mémoire produit à l'Ecole des hautes études en santé publique, *Le rôle du directeur d'hôpital en matière de cybersécurité*, 2020.

[24] 13 % de réponses émanant de directeurs (DG ou DGA) pour les établissements publics et 34 % émanant des directeurs pour les établissements privés, les autres répondants étant les DSI ou RSSI.

1.3.1.1 La continuité de l'activité et la prise en charge des patients

Les cyberattaques engendrent une diversité de conséquences selon des temporalités et des gravités variables en fonction des cas. Les comptes rendus des établissements ayant subi de tels événements en décrivent les principaux effets.

- *Les activités et la continuité des soins sont affectées*

- certains services sont temporairement fermés (le plus souvent, les urgences[25]), certaines opérations planifiées sont reportées, les admissions de patients sont réduites, des fonctionnalités et activités clé sont mises à l'arrêt telles que la stérilisation, le stockage des données d'imagerie, la radiothérapie ;
- les professionnels de santé ne peuvent plus accéder au dossier du patient informatisé (DPI), aux plans de lits, au calendrier de rendez-vous des patients, ou aux données informatisées des fiches plateau[26] pour la restauration des patients.

- *Les fonctions support peuvent être mises à l'arrêt*

- c'est le cas du logiciel de gestion administrative des malades (GAM), de la régulation informatisée des transports sanitaires ou de la rupture des commandes et des approvisionnements, comme du paiement des fournisseurs ;
- les logiciels des ressources humaines et, en particulier, la paie du personnel ou, encore, le logiciel de gestion économique et financière (GEF) peuvent être totalement bloqués et le codage en vue de la valorisation et de la facturation des actes réalisés devenir inaccessible.

Des solutions dérogatoires mises en œuvre en cas de crise

Des solutions temporaires ont été imaginées par des établissements pour maintenir le paiement des fournisseurs et les approvisionnements, tel qu'un dispositif d'ordre de paiement en version papier, comme en a fait état le directeur des affaires financières du centre hospitalier sud-francilien de Corbeil-Essonnes. S'agissant de la paie du personnel, dans ces circonstances, la paie du mois N-1 est généralement mandatée à l'identique, avec un ajustement pour retirer manuellement les agents ayant quitté l'établissement, procéder à des acomptes pour les nouveaux venus et, le cas échéant, sans les éléments variables (gardes, astreintes, heures supplémentaires, temps additionnel…).

Le retour à l'utilisation « du papier et du crayon » (par exemple, afin de reconstituer le dossier du patient, de rédiger des ordonnances ou des demandes d'examen, d'assurer les commandes de restauration) et aux tâches manuelles en remplacement de celles habituellement automatisées et informatisées (cas de la pharmacie et de la préparation manuelle des piluliers), s'impose aux équipes des établissements confrontées à ces situations. Cette phase de retour au papier peut durer jusqu'à plusieurs semaines, voire plusieurs mois.

La prise en charge des patients et la fiabilité des traitements administrés sont alors potentiellement pénalisées par ces dysfonctionnements. Le rapport annuel 2023 de l'observatoire des signalements d'incidents de sécurité des systèmes d'information élaboré par

[25] A l'exemple du centre hospitalier d'Armentières pour lequel la décision a été prise de fermer les urgences (durant trois jours) pour garantir la sécurité des patients et pour permettre aux équipes de se concentrer sur le rétablissement des systèmes critiques.

[26] Y sont notamment consignées les informations sur les allergies ou intolérances alimentaires des patients.

l'ANS et le Cert Santé dresse un bilan des deux types de mises en danger de patients résultant des incidents de sécurité des systèmes d'information : les mises en danger dites « potentielles », d'une part, et les mises en danger dites « avérées », d'autre part :

- le Cert Santé a recensé 68 « mises en danger potentielles » en 2023 (contre 71 en 2022)[27], attribuées à diverses causes ; *« Il s'agit notamment d'attaques par rançongiciel, de coupures de courant ou de liens télécom, ainsi que de pannes d'équipement. Ces incidents ont eu un impact direct sur la disponibilité des services de santé, entraînant des interruptions prolongées de l'accès à des services hébergés, des perturbations du service téléphonique du SAMU et des dysfonctionnements des logiciels de prescription/aide à la dispensation. Ces situations ont engendré des risques plus ou moins accrus pour la sécurité des patients, mettant en évidence la nécessité de mesures préventives et d'une gestion proactive des incidents pour garantir la continuité des soins. En outre, les dysfonctionnements des logiciels de prescription/aide à la dispensation, attribués à des bugs logiciels, ont été identifiés comme une cause supplémentaire d'incidents de mise en danger patient ».*
- une « mise en danger avérée » a été identifiée en 2023 (contre cinq en 2022) ; si aucune définition précise de ce terme n'est communiquée, ce portail de déclaration des événements sanitaires indésirables contient quelques illustrations pour faciliter la démarche des établissements : *« séquelles, perte de chances, décès… »* ; de telles « mises en danger » qui se sont concrétisées par des dommages peuvent notamment être liées à une intervention dans un bloc nécessitant un transfert vers un autre hôpital et impliquant des pertes de chance ; le seul cas de décès rendu public à l'échelle européenne concerne une patiente qui est décédée lors de son transfert de l'hôpital de Düsseldorf, cyberattaqué, vers l'hôpital de Wuppertal en septembre 2020 ; à cet égard, les acteurs ministériels[28] ne disposent pas de données chiffrées ni de suivi en la matière, qu'il s'agisse de décès ou de dégradation de l'état de santé des patients concernés à plus ou moins long terme et aucune relation n'est établie avec le dispositif de déclaration des événements indésirables graves associés aux soins (EIGS)[29].

Les informations sur l'incident, enregistrées par l'établissement sur le portail de signalements et transmises dans ce cadre à l'ANS et au Cert Santé, sont analysées : si une conséquence sur le soin est constatée, le Centre opérationnel de régulation et de réponse aux urgences sanitaires et sociales du ministère de la santé (Corruss)[30] est alors mobilisé.

---

[27] Point d'attention concernant les données recensées dans le rapport du Cert Santé : les mises en danger résultent des « incidents de sécurité des systèmes d'information » de tout type et ne résultent donc pas nécessairement en totalité de cyberattaques. En outre, ces données devraient être analysées par la DGOS afin d'évaluer les conséquences des cyberattaques sur la prise en charge et sur la mise en danger des patients.

[28] La Haute autorité de santé, dans le cadre du volet numérique de la certification des établissements de santé (se référer à la partie 2.3 du présent rapport), ne procède pas à une mesure des impacts des cyberattaques sous l'angle de la mise en danger de patients. La DGOS, l'ANS ou la DNS n'effectuent pas de suivi chiffré ni d'analyse des impacts générés par des cyberattaques sur les patients.

[29] Un événement indésirable grave associé aux soins (EIGS) est un événement inattendu au regard de l'état de santé et de la pathologie de la personne et dont les conséquences sont le décès, la mise en jeu du pronostic vital, la survenue probable d'un déficit fonctionnel permanent, y compris une anomalie ou une malformation congénitale (décret n° 2016-1606 du 25 novembre 2016 ; CSP, art. R1413-67).

[30] Sa mission est d'assurer 24h/24 et 7j/7 la réponse opérationnelle aux urgences sanitaires ayant des conséquences sur le territoire national. L'équipe composée de médecins, pharmaciens, ingénieurs spécialisés en santé publique et gestionnaires de crise, bénéficie de l'appui de communicants de crise, de juristes et autres experts du ministère.

1.3.1.2 Les vols de données

Les activités malveillantes concernant les données sont les attaques par hameçonnage et les messages frauduleux destinés à récupérer des identifiants ou des données sensibles (identifiants bancaires ou données de santé à caractère personnel). Les attaques par rançongiciel sont, quant à elles, les plus dommageables car elles peuvent entraîner l'exfiltration de données des patients et la perte de confidentialité de ces dernières, qui peuvent se retrouver en vente sur le *darknet*[31]. Une autre conséquence indirecte possible pour les patients ou pour le personnel est l'usurpation d'identité.

Situations d'établissements ayant subi des vols de données (données publiques issues des comptes rendus des établissements)

Lors de la cyberattaque subie par le CHU de Rennes le 28 juillet 2023, 300 gigaoctets de données ont été publiées en ligne après le vol opéré en juin.

Lors de l'attaque du centre hospitalier d'Armentières, dans la nuit du samedi 10 au dimanche 11 février 2024, 10 gigaoctets de données concernant 230 000 patients ont été dérobées[32]. Une coordination avec les autorités judiciaires ainsi qu'avec la CNIL pour le dépôt de plainte auprès du commissariat d'Armentières et auprès du procureur de la République de de Paris, et la gestion des violations de données ont été nécessaires.

De même, lors de la cyberattaque du centre hospitalier de Cannes, le 16 avril 2024, 61 gigaoctets de données personnelles et médicales ont été exfiltrées (cartes d'identité, bilans médicaux, bulletins de salaires, RIB) aux fins de mise en vente sur le *darknet.*

Certains établissements tels que le CHSF de Corbeil-Essonnes ou le CHU de Rennes ont dû envoyer des lettres aux patients et au personnel ayant été victimes d'une violation de leurs données médicales et personnelles.

1.3.2 Des coûts élevés en matière de gestion de crise et de pertes de recettes

1.3.2.1 Les coûts directs et indirects provoqués par les cyberattaques

Les coûts liés à la gestion de la crise et à la reconstruction du système d'information peuvent atteindre un montant très important.

Ils définissent ensemble et coordonnent la réponse aux urgences sanitaires identifiées à partir des signalements et des informations transmises par un vaste réseau de partenaires tels que notamment les ARS, l'ANS-Cert Santé, Santé publique France, de nombreuses agences, les ministères contribuant à la sécurité sanitaire des Français sur le territoire ou à l'étranger, les institutions internationales. Trente à quarante incidents par an seraient signalés au Corruss en relation avec des incidents affectant la sécurité des systèmes d'information des établissements de santé.

[31] Le darknet, ou internet clandestin, est un ensemble caché de sites internet accessibles uniquement par des outils spécialement conçus à cet effet. Il est utilisé pour préserver la confidentialité et l'anonymat d'activité, le plus souvent illicites, sur internet.

[32] Dans les jours ayant suivis la cyberattaque, l'établissement avait indiqué que les pirates informatiques à l'origine de la cyberattaque avaient rendu accessibles des fichiers informatiques.

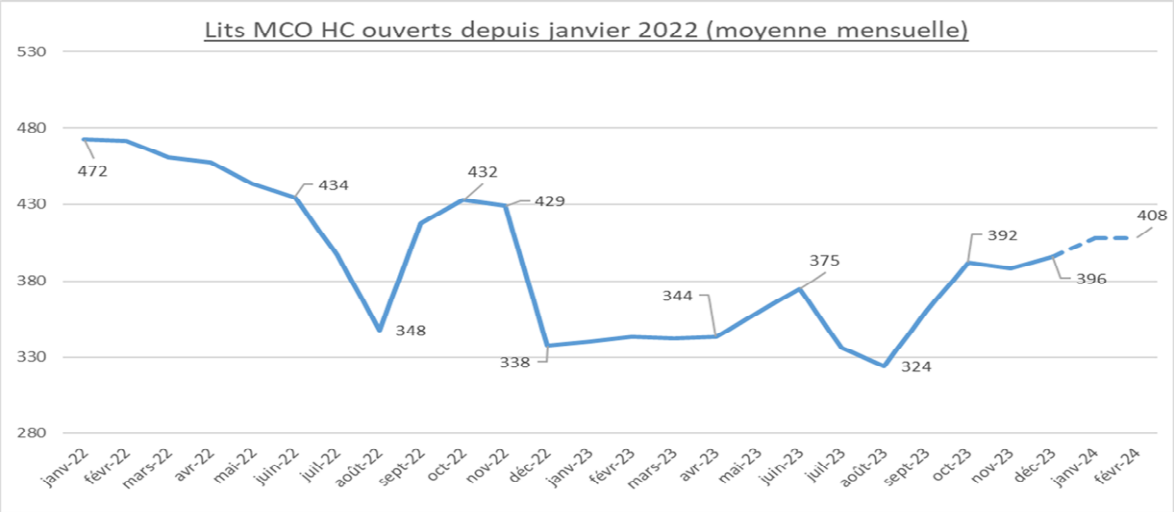
Ces coûts recouvrent les principaux éléments suivants :

- les coûts de personnel, au titre des heures supplémentaires pour toute la période de continuité d'activité et de travail en mode dégradé et du recrutement de personnel temporaire en renfort (par exemple technicien informatique en contrat à durée déterminée) ;
- les coûts d'identification des failles exploitées lors de l'attaque et de préparation du plan de remédiation (reconstruction et durcissement du SI), le plus souvent assuré par des prestataires extérieurs dits « de réponse à incidents de sécurité » (PRIS)[33] ;
- les coûts de reconstruction et de remise en service ; il s'agit de dépenses pour permettre la reconstruction du réseau, la remise en service de l'ensemble des éditeurs et logiciels associés ou, encore, des coûts de sous-traitance pour certaines activités à l'arrêt (par exemple, laboratoires de biologie) ;
- d'autres coûts interviennent, qu'ils concernent la communication de crise et d'information (communiqués de presse, envoi de courriers au personnel et aux patients…), le transfert de patients ou le paiement d'intérêts moratoires découlant des difficultés à assurer le paiement des fournisseurs.

En outre, une majeure partie des dommages financiers peut provenir de la perte des recettes, engendrée par la déprogrammation d'activités ou la fermeture temporaire de certains services de l'hôpital, surtout dans les cas où la crise est durable. Le graphique ci-dessous illustre la difficulté pour un établissement attaqué de retrouver le niveau d'activité observé avant la crise.

[33] Le Prestataire de Réponse aux incidents de Sécurité (PRIS) est chargé de vérifier et d'attester d'un savoir-faire et de compétences conformes au référentiel établi par l'Anssi en matière de réponse aux incidents de sécurité. Le PRIS est soumis à un contrat et n'intervient que sur les aspects techniques de la réponse à incident. Comme le note l'Anssi, ce sont ces prestataires externes qui assurent la plus grande partie de la charge d'assistance ; l'offre commerciale s'est structurée et certains qui ont développé une spécialité dans le domaine de la santé, sont suivis dans leurs actions par le Cert Santé.

Graphique n° 6 : Évolution du nombre de lits d'hospitalisation complète ouverts en Médecine-Chirurgie-Obstétrique après une cyberattaque
Exemple d'un centre hospitalier victime d'une cyberattaque en décembre 2022



Source : données recueillies par la Cour des comptes, d'après le compte rendu transmis par un centre hospitalier

Les éventuels transferts d'activité d'un établissement cyberattaqué vers un autre établissement (non quantifiés à ce jour par le ministère) ne compensent pas les pertes d'activité à l'échelle de l'ensemble des hôpitaux, dans la mesure où les activités de consultation ou d'intervention programmée ne sont pas systématiquement prises en charge par une structure voisine (notamment dans les petites villes ou les établissements implantés dans des territoires ruraux).

Tableau n° 4 : Estimation des coûts et des pertes de recettes provoqués par cinq cyberattaques intervenues entre 2021 et 2024 selon les informations rendues publiques par les hôpitaux

Établissement	Année	Fuites ou vol de données	Coûts de la gestion de crise et de la remédiation	Pertes de recettes	Source
CH de Dax-Côte d'Argent	2021	*Pas de vol de données selon les informations disponibles*	2,3 M€	2,3M€	*Compte rendu produit par l'établissement, un an après la crise*
CH Sud-Francilien (Corbeil-Essonnes)	2022	11 gigaoctets de données dérobées (mises en ligne vendredi sur le site du groupe cybercriminel Lockbit	9 à 10 M€ de coût total estimé Dont 1 M€ au titre de l'envoi des lettres aux patients et au personnel dont les données ont été volées	Information non disponible	*Témoignage du directeur des affaires financières lors du séminaire des directeurs achats et logistique hospitaliers en octobre 2023*
CH de Versailles	2022	*Pas de vol de données selon les informations disponibles*	Plusieurs millions d'euros de dépenses de rémunération	20 M€	*Compte rendu du 18 décembre 2023, un an après l'attaque*
CH d'Arles	2022	*Pas de vol de données selon les informations disponibles*	750 000 €	2 M€	*Compte rendu du directeur-adjoint, en date du 7 juin 2022 (Forum cybersécurité en santé des Hauts de France)*

CH d'Armentières	2024	10 gigaoctets de vol de données concernant 230 000 patients	2 M€ au total	*Compte rendu du responsable de la sécurité des systèmes d'information et du Cert Santé le 22 mai 2024 lors du salon Santexpo*

Source : Cour des comptes, d'après les retours d'expérience des établissements et le site internet de l'ANS

Dans certains cas, comme celui du centre hospitalier de Dax, les coûts de la cyberattaque ont été partiellement ou totalement couverts par l'ARS *via* le fonds d'intervention régional[34]. Il n'existe cependant pas de doctrine en matière de soutien financier des établissements ayant subi des attaques. Cette situation engendre un traitement différencié des conséquences des cyberattaques selon les régions et les établissements.

1.3.2.2 Les conséquences d'une cyber-crise sur la facturation de l'activité et sur les recettes

L'établissement qui subit une cyberattaque peut connaître une paralysie de son système d'enregistrement des actes médicaux réalisés. En ce cas, les données sont enregistrées sans support numérique et l'établissement n'est pas en mesure de transmettre à l'assurance maladie les données servant de fondement à sa facturation.

Pour surmonter ces difficultés, des dispositifs spécifiques sont proposés à l'établissement par la Cnam, notamment le paiement d'avances remboursables, avec mise en place d'un échéancier différé, conditionné par la reprise de la facturation et par son rattrapage (recodification) sur la période du sinistre[35]. Par ailleurs, la LFSS pour 2024 a modifié l'article L. 162-25 du code de la sécurité sociale qui permet désormais, au directeur général de l'agence régionale de santé, de prolonger le délai de prescription des actes remboursés par l'assurance maladie aux établissements de santé, proportionnellement à la durée et aux dommages subis, dans la limite d'un an supplémentaire (ces derniers ayant normalement un an pour transmettre à l'assurance maladie les prestations réalisées), en visant notamment les événements *« qui l'empêchent d'accomplir de manière durable les obligations de transmission des informations relatives à son activité prévues aux articles L. 6113-7 et L. 6113-8 du code de la santé publique »*.

Dans les cas de cyberattaques d'ampleur exceptionnelle, il pourrait être justifié d'envisager de supprimer cette obligation d'enregistrement de l'activité hospitalière *a posteriori*. En outre, se pose la question d'une compensation des éventuelles pertes de recettes d'activité liées à l'attaque informatique, aujourd'hui difficiles à évaluer.

[34] Le fonds d'intervention régional (FIR) a été créé le 1er mars 2012, en application de l'article 65 de la loi de financement de la sécurité sociale (LFSS) pour 2012. La gestion du FIR est confiée aux ARS. Le FIR s'inscrit dans le cadre de l'objectif national des dépenses d'assurance maladie (Ondam) et de la stratégie nationale de santé (SNS).

[35] À titre d'exemple, il a été demandé à un centre hospitalierd'enregistrer *a posteriori* plus de six mois d'activité.

Recommandation n° 1 :	(DGOS, Cnam) : Mettre en place un groupe national d'expertise chargé, en cas de cyberattaques d'ampleur exceptionnelle, d'évaluer les pertes de recettes à compenser et, pour les établissements les plus gravement affectés, d'accorder une dispense de codification *a posteriori* de leur activité hospitalière.

2 CLARIFIER ET CONSOLIDER LA REPONSE NATIONALE

En cohérence avec l'accroissement des exigences de la réglementation européenne, la réponse nationale a commencé à s'organiser sous la forme d'un programme quinquennal de financement de rattrapage et d'une inscription de la sécurité des systèmes d'information dans la politique de qualité et de sécurité des soins.

2.1 Un environnement juridique et institutionnel en évolution

2.1.1 Un cadre juridique européen aux exigences croissantes

Avant 2016, les textes européens qui réglementaient les systèmes d'information s'intéressaient surtout à la protection des individus et, en particulier, au traitement des données à caractère personnel et à leur libre circulation[36].

La directive « Sécurité des réseaux et de l'information » (dite « directive NIS », de son nom anglais Network and Information System Security) a été adoptée le 6 juillet 2016[37]. Son objectif est d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes de l'Union européenne. Comme l'indique son deuxième considérant, « *l'ampleur, la fréquence et l'impact des incidents de sécurité ne cessent de croître et représentent une menace considérable pour le fonctionnement des réseaux et des systèmes d'information. Ces systèmes peuvent également devenir des cibles pour des actions intentionnelles malveillantes qui visent à la détérioration ou à l'interruption de leur fonctionnement. Ces incidents peuvent nuire à l'exercice d'activités économiques, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et porter un grand préjudice à l'économie de l'Union*. »

2.1.1.1 Une première directive, tardivement étendue au secteur hospitalier

La directive européenne communément appelée NIS 1 a demandé aux États membres de se doter d'une gouvernance comprenant, notamment, une autorité nationale de cybersécurité et de cyberdéfense et un centre de réponse aux incidents (CSIRT[38] ou Cert[39]). En France, cette double mission a été dévolue à l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Les exigences de NIS 1 visent une catégorie d'opérateurs qualifiés d'« opérateur de service essentiel » (OSE), intervenant sur un certain nombre de secteurs d'activité. Si la

[36] Par exemple, avec la directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données , ou encore règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

[37] Directive n° 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

[38] *Computer Security Incident Response Team (CSIRT).*

[39] *Computer Emergency Response Team (Cert).*

directive précise les secteurs (et éventuels sous-secteurs) qu'elle couvre, elle laisse en revanche aux États-membres le choix de désigner les entités qui seront qualifiées d'OSE au sein de ces secteurs et sous-secteurs et qui devront répondre aux exigences de la directive. La directive NIS 1 se révèle, par ailleurs, assez peu prescriptive en termes d'exigences de sécurité et d'obligations auxquelles doivent se conformer les OSE[40].

La directive NIS 1 a été transposée dans le droit français, dans les délais requis, par la loi 2018-133 du 26 février 2018 et par plusieurs textes règlementaires d'application[41]. La désignation des OSE est intervenue progressivement entre 2019 et 2021. Les OSE, 142 au total, sont principalement les établissements supports de GHT. Ce délai explique sans doute la montée en charge progressive de la politique de cyberdéfense des hôpitaux, même si quelques progrès ont été réalisés durant cette période.

La loi n° 2013-1168 du 18 décembre 2013 de programmation militaire pour les années 2014 à 2019[42], complétée par un décret[43], a créé la notion d'opérateurs d'importance vitale (OIV). Une vingtaine d'hôpitaux environ sont considérés OIV[44]. Depuis la directive NIS 1, et en tant qu'autorité nationale sur la cybersécurité, l'Anssi, *via* son Cert-FR, porte assistance aux établissements de santé les plus critiques subissant ou ayant subi une cyberattaque (établissements OIV et hôpitaux classés OSE).

2.1.1.2 La deuxième directive, des conséquences majeures non anticipées

La deuxième directive européenne relative à la cybersécurité, dite NIS 2, répond à la nécessité de renforcement du cadre juridique européen au regard de la progression de la menace dont les dommages deviennent très marquants dans les secteurs les moins protégés (PME, collectivités locales et hôpitaux). Adoptée le 14 décembre 2022[45], elle devait être transposée au plus tard le 17 octobre 2024, ce qui n'est pas encore le cas en France. La directive NIS 2 contient deux changements majeurs pour les établissements de santé :

- un élargissement massif du périmètre des établissements concernés par les obligations européennes en termes de cybersécurité ;
- un objectif de mise en conformité des établissements beaucoup plus ambitieux que précédemment, avec un grand nombre de règles à respecter, entraînant un risque accru de pénalité pour les entités qui ne respecteraient pas ces règles.

NIS 2 est sensiblement plus prescriptive que NIS 1 ; par ailleurs et contrairement à NIS 1, elle laisse peu de latitude aux États-membres pour décider des organisations qui seront concernées par le texte.

---

[40] Les OSE doivent prendre les *« mesures techniques et organisationnelles nécessaires et proportionnées »* pour gérer les risques sur la sécurité de leurs réseaux et systèmes d'informations. Il s'agit de garantir « un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances ».

[41] Dont les deux principaux sont le décret 2018-384 du 23 mai 2018 et l'arrêté du 14 septembre 2018 (qui précise les règles de sécurité de l'article 10 du décret du 23 mai 2018).

[42] Cf. Chapitre IV *« Dispositions relatives à la protection des infrastructures vitales contre la cybermenace »*.

[43] Décret 2015-351 du 17 mars 2015.

[44] La liste des OIV étant secrète, ni leur nombre ni les hôpitaux concernés ne sont publiés.

[45] Directive UE n° 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement UE n° 910/2014 et la directive UE n° 2018/1972, et abrogeant la directive UE n° 2016/1148.

- *Une très forte hausse du nombre d'établissements relevant des obligations de la nouvelle directive*

La directive NIS 2 encadre désormais des entités considérées, soit, comme essentielles, soit comme importantes. La ligne de partage est inspirée de la recommandation de la Commission sur la définition des petites et moyennes entreprises[46]. Seront « entités essentielles » toutes celles dont le nombre d'employés et le chiffre d'affaires excèdent les seuils définissant les PME, c'est-à-dire 250 employés et 50 M€ de chiffre d'affaires (ou 43 M€ de bilan). Pour les « entités importantes », les seuils sont de 50 salariés et de 10 M€ de chiffres d'affaires (ou de 10 M€ de bilan).

Sans préjudice de la transposition du texte de la directive et de l'interprétation en droit français de ces seuils[47], l'ANS et la DNS confirment la hausse massive du nombre d'établissements de santé appelés à être classés comme entités essentielles, sans donner de chiffre à ce stade[48]. La Cour évalue leur nombre entre 750 et 800[49] à partir des données issues de la Statistique annuelle des établissements de santé[50] (SAE). Par ailleurs, près de 1 300 établissements seraient classés en entités importantes. Même si ces chiffres doivent être considérés avec prudence[51], ils donnent une mesure du changement, au regard du nombre actuel d'OSE.

- *Des exigences de mise en conformité avec la directive NIS 2 induisant des coûts pour les établissements de santé*

L'article 21 de la directive recense les mesures de gestion des cyber-risques qui devront être prises, tandis que les articles 32 et 33 fixent les mesures de supervision et d'exécution concernant les entités essentielles et les entités importantes[52].

Selon la DNS, l'extension du champ et les exigences de la directive devraient se traduire par des charges nouvelles pour nombre d'établissements de santé dès 2025, charges qui ne sont pas couvertes par le programme 2023-2027 d'aide au financement de la cybersécurité (CaRE). Il en est ainsi des contrôles d'accès des personnes physiques dans les établissements ou de l'analyse des risques de sécurité des systèmes d'information.

---

[46] Recommandation n° 2003/361/CE, annexe, art. 2, paragraphe 1.

[47] Par exemple, selon que le calcul est effectué sur des ETP, des ETP rémunérés ou sur des effectifs physiques ; ou encore, dans le cas des établissements privés lucratifs, selon que l'on intègre ou non dans le total les médecins qui y travaillent sans en être salariés.

[48] L'ANS et la DNS considèrent en outre que des établissements médico-sociaux pourraient être concernés (non éligibles au programme CaRE).

[49] Ce nombre intègre les établissements qui sont actuellement OSE.

[50] Drees, SAE 2000-2022 publiée en octobre 2023. La statistique annuelle des établissements porte uniquement sur les établissements sanitaires.

[51] En effet, les effectifs dans la SAE sont comptés en équivalents-temps plein rémunérés ou ETPR (hormis pour les médecins libéraux dans les cliniques privées qui sont comptés en personnes physiques). Si la référence pour le classement des établissements en entités essentielles ou importantes devait se mesurer en personnes physiques et non en ETP, le nombre d'établissements passants en entités essentielles ou en entités importantes serait supérieur.

[52] Les États membres doivent s'assurer que les mesures de supervision ou d'exécution imposées aux entités sont effectives, proportionnées et dissuasives. Ils s'assurent que les autorités compétentes sont en mesure d'effectuer des contrôles et des inspections, soit, sur place, soit à distance, de soumettre les entités à des audits de sécurité réguliers, de demander des preuves de la mise en œuvre de politiques de cybersécurité.

L'Anssi fait observer que l'atteinte des objectifs fixés dans le cadre de NIS 2 suppose des moyens supplémentaires pour le ministère de la santé et pour les établissements de santé[53]. Cependant, l'étude d'impact du projet de loi de transposition ne contient aucun élément spécifique à ces derniers.

Par ailleurs, l'extension du champ des secteurs couverts par la directive NIS 2 devrait accroître l'activité de l'Anssi. Cet accroîssement paraît encore plus marqué pour le Cert Santé. Enfin, et même s'ils ne relèvent pas du champ de cette enquête, un certain nombre d'établissements médico-sociaux pourraient être concernés.

Un autre facteur de charges potentielles supplémentaires pour les établissements de santé tient au fait que les fabricants de dispositifs médicaux doivent aussi répondre aux exigences de NIS 2. Cette intégration dans la réglementation européenne pourrait amener ce secteur à devoir rehausser sa sécurité et à chercher à retraduire les coûts de conformité dans ses facturations aux établissements de santé.

2.1.1.3 Le marquage « CE » ne garantit pas complètement la sécurité des dispositifs médicaux connectés

Les dispositifs médicaux connectés[54] constituent une composante sensible du parcours de soin. Les établissements de santé en utilisent une grande variété provenant de différents fabricants, chacun ayant ses propres protocoles de communication, systèmes d'exploitation et niveaux de sécurité. Cette diversité complique la mise en place de mesures de sécurité uniformes et cohérentes. Pour fonctionner, les dispositifs médicaux doivent souvent être interconnectés avec d'autres composantes du SIH (dossier du patient informatisé ou gestion administrative des malades), interconnexion créant de multiples points d'entrée pour les cyberattaques. En outre, les dispositifs médicaux ont souvent une durée de vie plus longue que les équipements informatiques moins spécialisés. Dès lors, de nombreux appareils en service peuvent devenir obsolètes sur le plan technologique et ne plus recevoir de mise à jour de sécurité pour les protéger des attaques. Ces dernières années, plusieurs intrusions et cyberattaques ont pu utiliser la vulnérabilité de dispositifs médicaux.

Les exigences en matière de cybersécurité figurant dans le cahier des charges du marquage CE[55] ne vont pas au-delà de quelques mesures de protection des données personnelles et de gestion des accès au dispositifs médicaux. Cela a conduit les acteurs de la cybersécurité des SIH à tenter d'introduire des clauses spécifiques[56] lors de la conclusion de marchés avec les fabricants. Les fabricants ont comme seule obligation, en effet, de maintenir les dispositifs

[53] S'y ajoute le risque de se voir infliger des amendes pour les établissements qui ne répondent pas aux conformités exigées par la Directive NIS 2.

[54] Tout instrument, appareil, équipement, matière, produit, à l'exception des produits d'origine humaine, ou autre article utilisé seul ou en association, y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques, ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Constitue de même un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques.

[55] Lorsqu'ils veulent commercialiser leurs produits, les fabricants font appel à des organismes de contrôle habilités pour en évaluer la conformité à la législation européenne.

[56] Clausier « sécurité » publié en mai 2024 par le club des RSSI santé ; « Trousse à outils » proposée par le groupe de travail de l'association des ingénieurs biomédicaux en 2023, recommandations de l'ANSM.

médicaux dans un état de fonctionnement conforme au marquage CE alors que leur maintien en conditions de sécurité supposerait une mise à jour régulière de leur niveau de protection.

Le problème ne devrait pas être résolu par le « *Cyber Resilience Act* », proposition de règlement de l'Union européenne en cours de négociation, visant à renforcer la cybersécurité des produits connectés et à améliorer leur résilience globale face aux cybermenaces, car les dispositifs médicaux seraient exclus de son champ d'application au motif que ces derniers répondent à une réglementation spécifique[57].

La loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, impose aux fabricants d'informer les utilisateurs des éventuelles vulnérabilités de leurs logiciels. Cependant, selon l'Anssi, les éditeurs d'applications destinées aux établissements de santé prennent insuffisamment en compte les exigences de cybersécurité.

2.1.2 Une réorganisation récente de la gouvernance nationale, à parachever

2.1.2.1 Une montée en charge progressive de la gouvernance nationale

La construction de la gouvernance du numérique en santé et de la réponse aux défis de la cyber-malveillance a été tout aussi progressive que sa prise en compte dans les programmes successifs en faveur du numérique en santé.

Depuis 2017, les établissements de santé sont tenus d'informer sans délai l'ARS[58] de tout incident grave sur leur système d'information, En 2019, le programme HOP'EN, pour « Hôpital numérique ouvert sur son environnement », a été instauré[59] et la même année, l'Agence du numérique en santé (ANS) [60] et la Délégation au numérique en santé ont été créées, complétant ainsi une première gouvernance unifiant le numérique en santé et les sujets de cybersécurité[61]. Dans cette organisation, la DNS pilotait la feuille de route du numérique en santé que l'ANS mettait en œuvre. Sur la cybersécurité, l'ANS agissait en relation avec le HFDS. Toutefois, la multitude des administrations intervenantes (DNS, ANS, DGOS, DGS, fonctionnaire de sécurité des systèmes d'information placé auprès du haut-fonctionnaire de défense et de sécurité du ministère du travail, de la santé et des solidarités) brouillait cette organisation.

---

[57] Règlement (UE) n° 2017/745 en date du 5 avril 2017 relatif aux dispositifs médicaux.

[58] Article L. 1111-8-2 du code de la santé publique.

[59] Détaillés par l'instruction n° DGOS/PF5/2019/32 du 12 février 2019, les indicateurs sur le prérequis « sécurité » du programme HOP'EN étaient les suivants : un plan de continuité d'activité (existence de procédures assurant un fonctionnement en mode dégradé du système d'information, ainsi qu'un plan de reprise d'activité formalisé et testé) ; un taux de disponibilité des applicatifs ; la présence dans les établissements d'une politique de sécurité, d'une analyse des risques détaillée et d'un plan d'action associé et l'existence d'un responsable sécurité des systèmes d'information (RSSI) placé hors de la direction des systèmes d'information ; plus spécifiquement sur la cybermenace, la réalisation régulière d'un audit externe (par exemple, *via* des tests d'intrusion, des audits de vulnérabilité...).

[60] L'ANS a été précédée par l'ASIP Santé (Agence nationale des systèmes d'informations partagés de santé) avec, en son sein, une cellule d'accompagnement de cybersécurité des structures de santé (ACSS) qui débouchera ensuite sur le Cert Santé.

[61] Communiqué de presse du 22 avril 2024 du ministère chargé de la santé et de la prévention *: « Évolution du numérique en santé au sein du ministère pour plus d'impact et de lisibilité ».*

En mai 2023, la DNS a été érigée en direction d'administration centrale du ministère du travail de la santé et des solidarités[62]. Elle exerce la tutelle ministérielle de l'ANS[63]. Par ailleurs, la mutualisation des équipes numériques, préconisée par l'Igas[64], s'est traduite par le transfert à la DNS des équipes « numérique » provenant de la DGS et de la DGOS.

Cette réorganisation, associée à la mutualisation d'équipes jusqu'alors séparées, répond à une recommandation qu'avait formulée la Cour en 2016 sur la nécessité pour le ministère de se doter d'une « *instance de coordination commune à l'ensemble des projets concernant les systèmes d'information* ».

Toutefois, hormis la réponse immédiate aux incidents de cybersécurité, la répartition des rôles du niveau central demeure floue pour les établissements de santé, en particulier en matière d'actions de remédiation après une attaque.

2.1.2.2 Des difficultés à surmonter pour conforter la gouvernance nationale

La gouvernance de la sécurité des systèmes d'information et de la cybersécurité en santé s'appuie désormais, au niveau national, sur trois instances principales : la Délégation du numérique en santé (DNS), l'Agence du numérique en santé (ANS) et le fonctionnaire de sécurité des systèmes d'informations (FSSI) placé auprès du haut fonctionnaire de défense et de sécurité (HFDS), qui s'appuie largement sur la DNS et sur l'ANS.

Quelques difficultés réelles ou potentielles subsistent toutefois et doivent être résolues pour ancrer et affirmer au mieux cette gouvernance récente :

- l'effectif réduit du Cert Santé (neuf personnes, dont seulement cinq ETP affectés à l'activité de vérification de la menace et à la réponse à incident) pour faire face à l'augmentation massive du nombre d'établissements de santé qui vont entrer dans le champ de la directive NIS 2. Le Cert Santé constituant un des rares Cert sectoriels à même de décharger le Cert-FR de l'Anssi[65], la répartition des interventions entre ces derniers devra être reprécisée ;
- le caractère non pérenne des moyens de l'ANS[66] en matière de cybersécurité (160 M€ dont 150 M€ de crédits d'intervention) car en grande partie issus du « Ségur du numérique »[67] ;

[62] Par le décret n° 2023-373 du 15 mai 2023 ; cette évolution résulte des conclusions d'une mission de l'Inspection générale des affaires sociales.

[63] L'ANS est constituée sous la forme d'un GIP qui regroupe notamment le ministère de la santé (DNS), la Cnam, la CNSA, un représentant des ARS, un représentant des GRADeS.

[64] Rapport de l'Igas de septembre 2022 sur le positionnement et le modèle d'action de la DNS – lettre de mission du ministre de la santé du 21 avril 2022.

[65] L'Anssi indique dans sa réponse à la Cour que *« la montée en maturité du Cert Santé ces dernières années lui a permis de prendre en compte de plus en plus de cas et d'un niveau de gravité de plus en plus significatif »,* et que les deux instances se coordonnent très régulièrement pour échanger, notamment *« en cas d'incident ou de vulnérabilités »*.

[66] Le budget initial de l'ANS en 2024 est de 625 M€ de crédits de paiements, dont près de 420 M€ de crédits d'intervention.

[67] Le programme du « Ségur du numérique » vise à soutenir le développement massif et cohérent du numérique en santé en France. Il est mis en œuvre par l'Etat à partir des fonds européens issus du plan de relance et de résilience européen.

- le caractère non conforme aux règles budgétaires applicables à une administration centrale du budget de la DNS (11 M€).

Le financement de la DNS par fonds de concours : un processus inadapté pour une administration centrale, qui doit être corrigé

Lors de la création du poste de délégué ministériel au numérique en santé, le ministère de la santé a jugé qu'un financement par fonds de concours constituait une solution pragmatique, afin de permettre la constitution de l'équipe initiale de la DNS.

Or, ce fonds de concours se traduit par un circuit inutilement complexe. Il est alimenté par un versement provenant de l'ANS, quand elle-même est financée par une dotation de l'assurance maladie dans le cadre d'un complément de budget issu du « Ségur du numérique ». Pour 2024, le montant du fonds de concours sur le programme 124 « Conduite et soutien des politiques sanitaires et sociales » est de 11 M€. La convention qui le régit précise que cette somme se partage en 2,5 M€ pour financer, sur le titre 2, 19 emplois de la DNS, et 8,5 M€ pour les dépenses de la DNS hors titre 2. Le fonds de concours ne finance donc pas, en 2024, l'ensemble du personnel de la DNS. Sur les 54,5 ETP, 19 ETP sont rémunérés par le fonds de concours, 19 ETP le sont sur le programme 124, avant les transferts de personnel de la DGOS et de la DGS, et, depuis ces transferts, 16,5 ETP sont financés par leur administration d'origine sur le programme 124 (10,5 ETP en provenance de la DGOS et 6 ETP de la DGS).

Au-delà de sa complexité, ce financement n'est pas sécurisé puisqu'il émane du complément budgétaire issu du « Ségur du numérique » dont les crédits s'éteindront à la fin de 2025. Le financement de la DNS devrait être assuré à partir de crédits budgétaires, à l'instar de toutes les directions centrales de ce ministère.

La Cour a déjà, dans le passé, critiqué l'usage de fonds de concours alimentant des programmes budgétaires. Dans les observations définitives sur les achats liés à la crise sanitaire financés par les dotations exceptionnelles de l'Assurance maladie à Santé publique-France, la Cour a rappelé que les « *fonds de concours sont définis par l'article 17 de la LOLF comme une procédure budgétaire permettant d'affecter au sein du budget de l'État, notamment, des fonds à caractère non fiscal versés par des personnes morales pour concourir à des dépenses d'intérêt public* ». Notant que les fonds de concours provenaient de dotations exceptionnelles versées à Santé publique-France et alimentaient plusieurs programmes du budget de l'État, elle a relevé que ces enveloppes étaient décidées sans autorisation parlementaire, et recommandé leur extinction.

Aucune justification ne permet aujourd'hui de faire échapper le financement de la DNS à la discussion budgétaire. Il convient donc qu'il soit mis fin à ce dispositif irrégulier.

Recommandation n° 2 : (SGMAS) Mettre fin à l'utilisation d'un fonds de concours pour le financement de la Délégation au numérique en santé.

2.2 Un financement national à garantir puis à pérenniser

2.2.1 CaRE, un programme de rattrapage

2.2.1.1 La traduction financière de la priorité « cybersécurité » inscrite dans la feuille de route numérique en santé 2023-2027

La feuille de route du numérique en santé pour les années 2023 à 2027, présentée le 17 mai 2023, inscrit dans ses priorités *« la cybersécurité dans les établissements, la souveraineté sur l'hébergement et la résilience face aux futures crises sanitaires »*[68].

Six objectifs sont fixés au regard de cette priorité :

- un renforcement de la gouvernance sur la cybersécurité ;
- la sensibilisation de tous les acteurs à la problématique de la sécurité des systèmes d'information face au danger de la cybercriminalité ;
- la pérennisation des ressources du numérique en santé et de la cyberdéfense en établissement ;
- le renforcement de la souveraineté dans l'hébergement des données de santé, avec une nouvelle certification « hébergement de données de santé » (HDS)[69] ;
- la préparation aux crises futures en termes de systèmes d'information, *via* la construction d'un schéma directeur des systèmes d'information spécifique pour les crises sanitaires ;
- le programme « Cyber accélération et résilience des établissements » (CaRE), objectif majeur de la feuille de route et seul muni de financements pluriannuels.

2.2.1.2 Un programme d'allocation de financement sur appels à candidatures ouverts à l'ensemble des hôpitaux

C'est à la suite des cyberattaques du centre hospitalier du Sud-Francilien de Corbeil-Essonnes, en août 2022, et du centre hospitalier de Versailles, début décembre 2022, que le gouvernement a confié à la DNS la mission de piloter un groupe de travail[70] pour rédiger le programme « Cyber accélération et résilience des établissements » ou CaRE, présenté le 18 décembre 2023 au centre hospitalier de Versailles par le ministre de la santé et de la prévention et par le ministre délégué chargé du numérique.

---

[68] Priorité n°15 de la feuille de route ministérielle du numérique en santé (qui en compte vingt).

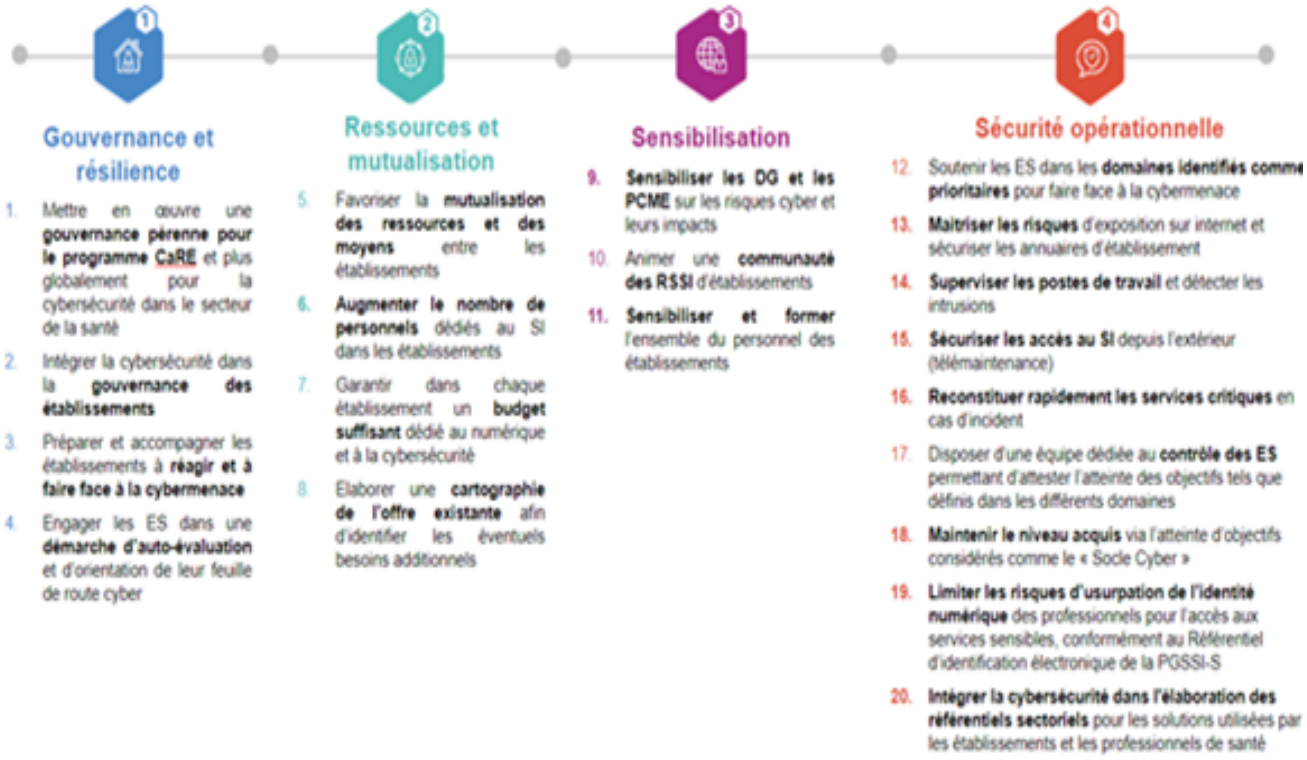
[69] L'objectif est d'intégrer un hébergement systématique des données de santé dans l'Espace économique européen avec des mesures juridiques ou techniques de réduction du risque de transfert extraterritorial des données.

[70] Ce groupe de travail a notamment associé, au-delà de la DNS, de l'ANS, de l'Anssi et de la DGOS, le haut fonctionnaire de défense des ministères sociaux et son fonctionnaire de sécurité des systèmes d'informations (FSSI), des représentants des ARS et de leurs GRADeS (pour le développement au niveau territorial). Elle a aussi sollicité les fédérations hospitalières, comme celles du secteur médico-social, des représentants des établissements de santé et des industriels.

Il reflète le besoin de combler, au moins pour partie, le retard accumulé dans les investissements et les ressources affectées à l'organisation des systèmes d'information hospitaliers. Il prend acte de l'urgence avec laquelle il convient de mettre à disposition des hôpitaux un certain nombre de protections techniques, face à un accroissement quantitatif et qualitatif de la cyber-malveillance, en particulier des rançongiciels.

Les financements prévus par le programme CaRE de 2023 à 2027 s'élèvent à 750 M€. Ils sont répartis entre les quatre axes décrits dans le schéma ci-dessous :

Schéma n° 6 : Les quatre axes du programme CaRE



Source : Agence du numérique en santé

Certains axes sont détaillés par domaine (exposition internet, annuaires techniques[71], postes de travail, accès extérieurs...).

Les établissements de santé candidatent sur ces différents domaines du programme pour obtenir des financements en présentant des dossiers examinés et contrôlés par les instances nationales. À titre d'exemple, pour le domaine « accès internet et annuaires techniques », un appel à demandes de financement a été lancé par arrêté ministériel de la DNS en mars 2024.

[71] L'annuaire technique est un service de gestion des identités et des accès. Il permet la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information. L'obtention de privilèges élevés sur l'annuaire technique entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI. Le service ADS permet à la fois de quantifier le niveau de sécurité de l'annuaire et d'accompagner progressivement les bénéficiaires.

L'octroi des aides est assujetti à l'atteinte d'une série d'objectifs[72] qui sera vérifiée à titre principal par l'ANS. Contrairement aux programmes précédents, les ARS ne sont mobilisées que pour la phase de recueil des candidatures et de vérification de leur éligibilité[73].

Le programme CaRE s'adresse à tous les établissements de santé, quel que soit leur statut, et couvre une partie des exigences contenues dans la directive NIS 2 telles que l'obligation de continuité et de reprise des activités (PCRA) ou la gestion des sauvegardes. Il en est de même des exercices de crise ou du chiffrement des connexions *via* internet. En matière d'exercice de crise, l'objectif convenu entre la délégation du numérique en santé (DNS) et les ARS, inscrit dans les dialogues de gestion, est que 80 % des établissements devront avoir réalisé un exercice de crise avant la fin du premier semestre, démarche qui doit ensuite devenir annuelle. Plus de 350 exercices ont déjà été planifiés entre mars et juin 2024[74]. Un bilan est prévu à la fin du premier semestre. Les comptes rendus des hôpitaux attaqués, notamment des centres hospitaliers d'Armentières et de Cannes, ont montré que la pratique des exercices de crise permet de mieux réagir et, *in fine,* de diminuer les conséquences des cyberattaques.

Un plan de continuité d'activité (PCA) permet à une entité de préparer l'organisation de son activité en cas de crise. Il peut s'agir de crises internes (incendie, grève, panne informatique) ou de crises externes (crise financière, sanitaire, mouvement social, covid-19). En l'anticipant, l'entité augmente son niveau de résilience et peut ainsi en limiter les conséquences. Ces plans concernent de manière distincte l'activité informatique (rétablissement des dysfonctionnements techniques) et l'activité sanitaire (continuité des soins)[75].

2.2.2 Un programme à améliorer et à poursuivre jusqu'au terme prévu

2.2.2.1 Des axes de progrès

Les modalités de recueil des candidatures et les réponses aux appels à demande de financement devraient évoluer pour mieux répondre aux attentes et contraintes des établissements :

- des délais de candidatures trop courts pour les appels à financement, d'autant plus qu'ils sont centrés sur un seul domaine d'action à la fois[76] ; il conviendrait donc de revoir les délais lors des futurs appels à financement ;

[72] Par exemple, atteindre un niveau minimal de sécurisation des annuaires techniques en justifiant d'un score d'au moins deux sur plusieurs audits des Active Directory (AD ou annuaires techniques), ou encore avoir réalisé des audits d'exposition réguliers, et en apporter la preuve.

[73] Pour être éligibles, les établissements doivent montrer qu'ils ont atteint un certain nombre de prérequis en termes de maturité de leurs systèmes d'informations, qui sont souvent la reconduite des résultats de programme précédents comme HOP'EN par exemple.

[74] À la date du dépôt du présent rapport, en juin 2024, entre 60 et 70 % des établissement avaient réalisé un exercice de crise, ce qui correspond à 2 000 exercices comptabilisés depuis début 2023, selon la DNS et l'ANS.

[75] Les acteurs ministériels, de même que la HAS (cf. partie 2.3 du présent rapport), notent le caractère inabouti à ce jour des PCA-PRA dans la majorité des établissements, en particulier dans leur dimension métier, ce que les rapporteurs ont pu également constater au cours de leur enquête.

[76] En effet, le premier appel à demandes de financement sur les expositions internet et les annuaires, annoncé depuis l'automne 2023, n'a été ouvert par arrêté qu'en mars 2024, avec un délai d'un mois seulement pour candidater (entre le 18 mars et le 19 avril 2024).

- des règles de calcul des aides qui diffèrent selon le statut des établissements au détriment des établissements privés, du fait d'une moindre rémunération de l'activité, et qui sont contestées par la Fédération de l'hospitalisation privée[77] ;
- un manque d'information des établissements sur leur éligibilité à certains financements ; par exemple, certains établissements avaient déjà effectué, sur leur propre fonds, les travaux de sécurisation des annuaires techniques avant le lancement de l'appel à projets « exposition sur internet et annuaires techniques » ; aussi, s'interrogent-ils sur l'éligibilité, *a posteriori,* de cette dépense à l'aide[78].

Pour autant, ce premier appel à projets sur les annuaires techniques et l'exposition internet a trouvé un large public.

Le premier appel à projets sur l'exposition internet et les annuaires techniques, plébiscité par les établissements de santé

À la fermeture du guichet de candidatures, le 19 avril 2024, l'Agence du numérique en santé (ANS) a dressé un bilan qui montre que 84 % des établissements éligibles ont déposé une candidature :

- 1 207 demandes été reçues dont une pour chacun des GHT ; près de 2 000 établissements sont donc concernés, dont 898 établissements publics appartenant à un GHT ;

- la quasi-totalité (99 %) des établissements publics éligibles a déposé une candidature ;

- l'ensemble des GHT et, par suite, tous leurs établissements sont représentés, ainsi que 18 établissements hors GHT (sur 24 potentiels) ;

- les établissements privés à but lucratif ont aussi très majoritairement candidaté ; la proportion des établissements privés sans but lucratif ayant candidaté est un peu moins élevée : 763 établissements privés à but lucratif, soit 89 % des établissements éligibles dans cette catégorie ; 292 établissements à but non lucratif (soit 72 % des éligibles) ont déposé une candidature.

2.2.2.2 Des financements non assurés au-delà de 2024

La réalisation du programme CaRE, qui court de 2023 à 2027, prévoit une dotation de 750 M€ au sein de l'objectif national de dépense d'assurance maladie (Ondam)[79].

Sur les années 2023 et 2024, les actions du programme ont pu être financées à partir de crédits exceptionnels, issus du « Ségur du numérique », initialement prévus pour d'autres

[77] Les montants plafonds qui sont alloués aux établissements pour l'appel à demandes de financement « exposition sur internet et annuaires techniques » dépendent de deux paramètres : le nombre d'implantations dépendant d'un même établissement, d'une part, et « l'activité combinée », c'est-à-dire l'activité mesurée en nombre de journées et de séances selon un barème d'équivalent-journée « Médecine, chirurgie, obstétrique ». Or, les forfaits « activité combinée » diffèrent entre hôpitaux publics (environ 17 400 € pour 100 000 unités « activité combinée ») et hôpitaux privés (environ 12 900 €). La Fédération de l'hospitalisation privée a introduit un recours gracieux sur ce point.

[78] À cet égard, l'arrêté relatif à cet appel à financement n'est pas suffisamment clair car ce n'est qu'en annexe qu'il précise que des travaux de sécurisation peuvent être éligibles aux financements même s'ils ont été effectués avant la date d'ouverture du guichet de dépôt des demandes de financement. À titre d'exemple, un établissement ayant réalisé, entre juin et octobre 2023, des audits de son annuaire technique lui permettant d'atteindre un score supérieur ou égal à 2 (ce qui correspond à un niveau minimal de sécurisation, dont l'atteinte est demandée à ce stade par CaRE), pourra recevoir l'aide financière correspondant aux coûts qu'il a engagés à ce titre.

[79] Communiqué de presse du ministère de la santé en date du 19 décembre 2023.

finalités et réorientés vers la cybersécurité des établissements de santé[80]. Ces crédits exceptionnels ne sont par nature pas pérennes. Le « Ségur du numérique » s'éteindra en 2026 et les crédits restant en 2025 sont destinés à d'autres objectifs[81].

Les modalités de financement du programme CaRE entre 2025 et 2027 devront donc être précisées.[82]

Selon l'ANS, le financement du programme est couvert jusqu'en 2025 à hauteur de 233 M€ alors que la cible d'engagement atteint près de 380 M€. À ce jour, seuls 45 M€ sont prévus en 2025 pour l'extension à l'ensemble des établissements l'appel à projet Hospiconnect[83].

Tableau n° 5 : Financements du programme CaRE sécurisés assurés sur crédits « Ségur du numérique » ou sur crédits de l'Ondam (FIR)

En M€	2023	2024	2025	2023-2025
Financements hors « Ségur du numérique » (subvention Ondam et FIR)	**3,8**	**32,7**	**0,0**	**36,5**
HAS certification	3,8			3,8
Sécurisation des accès distants		32,7		32,7
Financements sur « Ségur du numérique »	**10,0**	**142,0**	**45,0**	**197,0**
Exercices de crises	10,0			10,0
Exposition internet et annuaires		65,0		65,0
Continuité et reprise d'activité		45,0		45,0
Hospiconnect		6,0	45,0	51,0
Financement des CRRC (*)		26,0		26,0
Coûts de pilotage et de contrôle assuré par l'ANS				
Total	**13,8**	**174,7**	**45,0**	**233,5**

(*) Centre de ressources régionaux cyber ; sur les 26 M€, 8 M€ sont affectés aux établissements du secteur médico-social.

[80] Cette réorientation a été rendue possible du fait d'une sous-consommation de crédits prévus pour le développement des usages numériques en santé par les médecins de ville.

[81] L'année 2025 est la dernière année du « Ségur du numérique ». Les arrêtés relatifs à la « vague 2 » du « Ségur du numérique » à l'hôpital ont été publiés le 19 mai 2024, l'un relatif au dossier du patient informatisé (DPI), l'autre relatif aux plates-formes d'intermédiation (PFI) qui permettront de transmettre, par messagerie de santé sécurisée et vers le dossier médical partagé, les documents engendrés par le dossier du patient informatisé et par les solutions logicielles du système d'information hospitalier. Selon l'annexe 2 du projet de loi de financement de la sécurité sociale pour 2024, le montant mobilisé pour ces projets serait de 302 M€.

[82] Seuls les financements pour la certification HAS et la dotation de 35,2 M€ assurant pour l'essentiel le financement du domaine « sécurisation des accès de maintenance » relèvent de l'Ondam.

[83] L'appel à projets Hospiconnect vise à sécuriser et simplifier l'identification électronique des professionnels dans les établissements sanitaires et médico-sociaux. Il se rattache à l'axe 4 « sécurité opérationnelle » du programme CaRE.

Nota : ce tableau n'intègre pas les coûts de pilotage et de contrôle des objectifs atteints par les établissements de santé, coûts qui sont supportés par l'ANS. Ils s'élèvent à 0,8 M€ en 2023 et à 6 M€ en 2024. Pour 2025, ils sont prévus à 9 M€ et ne sont, à ce stade, pas sécurisés.
Source : données ANS – Calculs Cour des comptes.

Pour construire une réponse préventive durable à la cybercriminalité et à la cybermalveillance, il est nécessaire de sécuriser la poursuite du programme CaRE à l'horizon 2027. La feuille de route du numérique en santé 2023-2027 prévoit l'élaboration et la mise en œuvre d'un forfait numérique pérenne dans la tarification de l'activité des établissements. Or, les travaux sur ce projet n'ont pas été engagés[84]. À défaut, il faudrait sanctuariser dès 2025 et jusqu'en 2027, une ligne de financement destinée à CaRE. Elle pourrait être introduite dans le sous-objectif « fonds d'intervention régional et soutien à l'investissement » de l'Ondam.

Recommandation n° 3 : (DNS, ANS) Conduire à son terme le programme CaRE.

2.2.3 Poursuivre les objectifs du programme après son extinction en 2027

La fin du programme CaRE ne marquera pas la fin des besoins de sécurisation des systèmes d'information des établissements hospitaliers.

Les SIH doivent être régulièrement révisés en termes de sécurité, par exemple parce que de nouveaux logiciels sont implantés ou rendus interopérables entre eux, ou parce que les systèmes d'exploitation doivent être régulièrement mis à jour. La menace évolue elle-même continuellement pour s'adapter aux défenses mises en place.

Dès lors, il est nécessaire de trouver un moyen pour pérenniser une part de dépenses hospitalières strictement affectées à cet objectif. La logique de « maintien des capacités de défense » existe déjà dans CaRE avec une enveloppe strictement affectée à un « socle cyber » (réalisation de nouveaux tests pour vérifier l'exposition sur internet, ou poursuite de l'entraînement des équipes à la gestion de crise *via* de nouveaux exercices de crise).

À titre d'exemple, le niveau de sécurité des annuaires techniques est codé de 1 (niveau le plus bas) à 5 (niveau maximal). Or, le programme CaRE relatif aux annuaires techniques a pour objectif que le score soit, dans tous les établissements, d'au moins 2 en 2024.

Dans ce contexte, un financement au-delà de 2027 pourrait être conditionné par la progression de la sécurité des SIH, mesurée par une hausse de ces scores. Par ailleurs, d'autres objectifs tels qu'une augmentation régulière de la part des ressources propres de l'hôpital consacrée à la sécurité informatique ou, encore, le renforcement de la mutualisation des moyens techniques et humains à l'échelle d'un GHT, pourraient être pris en compte.

[84] Selon la DGOS, ce dispositif ne garantirait en aucune manière la non-fongibilité des sommes issues de ce forfait au sein des ressources des établissements de santé.

Les dépenses de sécurité informatique aux Pays-Bas, en Allemagne et au Royaume-Uni

Aux Pays-Bas, aucun plan budgétaire spécifique n'aide les hôpitaux à accroître la sécurité de leur système d'information. Cependant, le gouvernement soutient la politique de cybersécurité en aidant financièrement le Cert sectoriel du secteur de la santé.

En Allemagne, ce sont les Länder qui sont compétents en matière d'investissements hospitaliers. Toutefois, leur contribution spécifique à la cybersécurité est extrêmement limitée, voire nulle. Aussi, une loi sur l'avenir des hôpitaux d'octobre 2020 a-t-elle créé un fonds de 4,3 Md€ (dont 3 Md€ sur le budget fédéral et 1,3 Md€ sur ceux des Länder) pour soutenir financièrement la numérisation des hôpitaux. Cette loi indique qu'au moins 15 % des crédits doivent être affectés à l'amélioration de la sécurité informatique (soit au moins 645 M€). Début 2024, seuls 45 % des hôpitaux auraient sollicité un financement au titre de la cybersécurité, pour un montant qui pourrait approcher 450 M€.

Au niveau national, le Royaume-Uni s'est doté d'un National Cyber Security Center, équivalent de l'Anssi. La santé est un sujet dévolu à chaque nation qui dispose de sa propre organisation et de sa propre stratégie numérique. Le gouvernement britannique a consacré, sur la période 2015-2020, 4,2 Md£ aux programmes budgétaires numériques dont 338 M£ pour améliorer la cybersécurité du système de santé.

Source : réponse du réseau des conseillers aux affaires sociales des ambassades à la sollicitation de la direction des relations internationales, de l'audit externe et de la francophonie de la Cour des comptes

2.3 Une stratégie d'audit et de certification à renforcer et à harmoniser

2.3.1 La montée en puissance d'un volet numérique dans la certification des établissements de santé

2.3.1.1 Une étape marquante franchie en 2024

La certification des établissements de santé, dont le pilotage est assuré par la Haute autorité de santé (HAS), est un dispositif obligatoire[85] destiné à assurer la connaissance, l'amélioration et la régulation de la qualité et la sécurité des soins, à l'attention tant des usagers que des professionnels de santé et des autorités de tutelle. Tout établissement de santé, quel que soit son statut (public, privé à but lucratif, privé à but non lucratif), est soumis à cette évaluation externe effectuée environ tous les quatre ans par des professionnels (des pairs) mandatés par la HAS, désignés sous le terme d'« experts-visiteurs ». Le référentiel de certification[86] fixe les attendus de ce dispositif et en détaille le contenu, les méthodes et le processus de décision[87]. Les résultats de la certification sont publiés sur le site internet de la HAS.

[85] Depuis 1996. Cette démarche est réalisée selon des standards internationaux *via* l'accréditation par l'iSQua (*International Society for Quality in Health Care*).

[86] *Certification des établissements de santé pour la qualité des soins*, HAS, Manuel, Mesurer et améliorer la qualité (version 2024 en vigueur).

[87] La certification des établissements de santé est visée aux articles L. 6133-7, L. 6321-1, L. 6147-7 et L. 6322-1 du code de la santé publique. La procédure de certification fixant les grands principes du dispositif est publiée au Journal Officiel et renvoie pour la mise en œuvre opérationnelle aux supports utilisés par la HAS.

Avec le développement des programmes et des financements consacrés au numérique en santé, certaines priorités ont été traduites et intégrées par la HAS dans la certification des établissements de santé à partir de 2021, *via* l'inclusion de premiers critères numériques au sein du référentiel de certification.

En 2024, une évolution est intervenue avec la diffusion d'un nouveau référentiel de certification issu d'un travail d'actualisation achevé fin 2023, renforçant la thématique du numérique en santé, sur le fondement d'un travail commun entre la DNS, l'ANS et la HAS. Un guide public de la HAS[88] expose ces objectifs. En outre, en vue d'auditer spécifiquement ces domaines lors des visites de certification des hôpitaux, la HAS a procédé, pour la première fois au second semestre 2023, au recrutement d'« experts-visiteurs numériques », professionnels des SIH (directeur, responsable ou ingénieur des systèmes d'information, ou encore professionnel paramédical ou médical qualifié dans les projets du numérique en santé, en exercice ou ayant exercé depuis moins de trois ans en établissement de santé de tout statut). Formés aux méthodes de la HAS, ils participent depuis janvier 2024 aux visites de certification aux côtés des experts-visiteurs.

2.3.1.2 Un dispositif fondé sur la coopération entre la HAS et l'ANS

Un contrat de coopération[89] a été conclu le 29 juin 2023 entre l'ANS et la HAS pour une durée de quatre ans, dans le cadre de la feuille de route du numérique en santé 2023-2027 et du programme CaRE. Son objectif est de *« sécuriser l'investissement pérenne des établissements de santé dans le développement et la sécurisation des systèmes d'information hospitaliers, en s'assurant que la gouvernance et l'organisation des établissements répondent aux prérequis objets de la certification ».*

Le financement de cette coopération est pris en charge par l'ANS qui verse à la HAS, pour la période 2023 à 2026, une somme correspondant au remboursement des dépenses réalisées par cette dernière, à hauteur d'un montant prévisionnel maximal de 3,9 M€[90].

[88] Guide disponible sur le site internet : *Évaluation de la gestion des risques numériques dans les pratiques de soins selon le référentiel de certification*, date de validation du Collège le 7 septembre 2023, HAS, Mesurer et améliorer la qualité.

[89] Le contrat est conclu en application des dispositions de l'article L. 2511-6 du code de la commande publique relatif aux coopérations entre pouvoirs adjudicateurs, permettant de collaborer en dehors de toute obligation de publicité et de mise en concurrence dès lors que la coopération n'obéit qu'à des considérations d'intérêt général, ne place pas des opérateurs privés dans une situation privilégiée par rapport à leurs concurrents et suppose la réalisation de moins de 20 % des activités sur le marché concurrentiel. En l'espèce, l'objet du contrat concourt à un objectif d'intérêt général, la continuité d'activité des établissements répondant à une mission de service public. La certification réalisée par la HAS n'intervient pas sur le marché concurrentiel, étant réalisée dans le cadre d'une mission légale exclusive, et l'appui de l'ANS à la certification n'intervient pas dans le domaine concurrentiel.

[90] 3 878 422 € mentionnés dans le contrat de coopération, montant pouvant être ajusté à la marge au vu d'un compte-rendu financier établi annuellement par la HAS.

La coopération entre la HAS et l'ANS pour le développement et la sécurisation des systèmes d'information hospitaliers : une démarche efficace au profit de la qualité

Les principales missions suivantes sont assurées par l'ANS au titre du contrat de coopération :

- proposition des critères d'évaluation à intégrer dans le référentiel de certification ;
- définition du profil de compétences des experts-visiteurs numériques, communication et sensibilisation des réseaux professionnels, webinaires d'information et participation à l'analyse des candidatures ;
- contribution aux supports de communication pédagogiques à destination des experts-visiteurs numériques (moyens pratiques de mener l'évaluation des critères) ;
- élaboration d'une fiche pédagogique de présentation du dispositif aux établissements de santé et accompagnement des établissements pour la préparation des visites sur le volet numérique.

La HAS assure, quant à elle, la réalisation des principaux travaux suivants :

- discussion des critères proposés par l'ANS avec l'animation de groupes de travail avec des experts puis approbation pour intégration dans le référentiel de certification ;
- mise en œuvre du processus de recrutement et de formation des experts-visiteurs numériques et de leur gestion administrative ;
- réalisation des visites dans les établissements incluant le volet de sécurisation des systèmes d'information et rédaction d'une partie de rapport consacrée à ce sujet pour chaque établissement visité.

Source : contrat de coopération entre l'ANS et la HAS.

2.3.1.3 Un levier déterminant de diffusion de la culture de la sécurité informatique dans les établissements

À la fin du mois de mai 2024, grâce à 174 experts-visiteurs numériques recrutés et formés[91], 308 visites incluant le volet numérique et sécurité informatique ont été effectuées[92].

Le temps consacré à l'évaluation de la gestion des risques numériques par les experts-visiteurs numériques est d'une journée par visite, quel que soit l'établissement. Les documents tels que le schéma directeur des systèmes d'information, les plans de continuité et de reprise d'activité ou le volet numérique du plan blanc[93] sont examinés préalablement à la visite.

Des documents complémentaires dont la nature est considérée comme plus sensible sont analysés sur place, tels que la liste des déclarations d'incidents auprès des autorités compétentes

[91] Comme prévu dans la convention entre la HAS et l'ANS, la formation *ad hoc* des experts-visiteurs numériques s'est concrétisée par un webinaire en septembre 2023, à la suite de l'ajustement du référentiel de certification, incluant la participation d'établissements attaqués « témoins », dont le centre hospitalier de Versailles. Les experts-visiteurs du numérique ont également accès au module de formation générale à l'attention de l'ensemble des experts-visiteurs.

[92] Sur une prévision de 680 visites annuelles.

[93] Autres documents transmispréalablement : rapport d'activité de la commission des usagers (informations relatives à « mon espace santé ») ; plan d'amélioration qualité et sécurité des soins (PAQSS) intégrant les actions relatives aux usages du numérique en santé ; cartographie du système d'information applicatif ; charte d'utilisation des ressources informatiques, incluant la charte de la connexion par les partenaires.

(Anssi, ARS, Cert Santé), le bilan des cyber-exercices ou, encore, le bilan des audits de sécurité numérique et plan d'actions[94].

Lors des visites, les experts-visiteurs numériques rencontrent, d'une part, les membres de la direction et les services concernés par les enjeux du numériques et de la sécurité informatique (la direction générale, la présidence de CME[95], la direction des soins, le département d'information médicale, le DSI, le RSSI, le DPO responsable de la gestion administrative des patients), d'autre part, les professionnels de santé et les équipes de soins, et les représentants des usagers désignés par la commission des usagers (CDU)[96].

Le travail des experts-visiteurs numériques se concentre sur deux thèmes reposant sur sept critères d'analyse, pour lesquels des grilles d'évaluation doivent être remplies. En 2024, cinq critères, pré-existants, ont vu leur contenu renforcé. Deux critères ont été créés :

- *Gestion des risques numériques* : maîtrise par l'établissement du risque de sécurité numérique ; sécurisation de l'identification des professionnels (nouveau critère créé en 2024) ;
- *Promotion des bons usages du numérique* : usage du SI pour l'accès au dossier du patient ; sécurisation des usages des communications informatiques d'informations médicales ; accès du patient à son dossier ; information du patient (nouveau critère créé en 2024) ; respect des bonnes pratiques d'identification du patient.

Les principaux constats formulés sur le volet numérique du référentiel de certification[97] n'apparaissent dans le rapport synthétique de certification de l'établissement, publié sur le site de la HAS, que s'ils n'ont pas pour effet indirect une surexposition de l'établissement à des risques de cyberattaque. Par ailleurs, comme pour les autres critères, les conclusions sur chacun des critères numériques sont transmises au sein d'un rapport détaillé à l'établissement lui-même et à sa tutelle.

Fin 2024[98], un premier bilan des évaluations des risques numériques pourra être dressé. D'ores et déjà, la HAS a rendu ses premières décisions de certification résultant de cette nouvelle procédure : si les constats relatifs au volet numérique ne revêtent pas à ce jour de caractère bloquant pour l'octroi de la certification, ils peuvent entraîner un refus d'attribution de la mention la plus élevée « haute qualité des soins ». La HAS a donné l'exemple d'un hôpital,

---

[94] Autres documents consultés sur place : politique générale de sécurité des systèmes d'information ; plan de formation et sensibilisation sur la sécurité informatique ; matrice d'habilitation ; procédures de gestion et listes d'habilitation des accès et comptes aux différents logiciels métiers prestataires compris ; procédure de gestion des identités pour les patients (INS) et de mise en œuvre des bonnes pratiques en matière d'identitovigilance ; attestation des audits sécurité des systèmes d'information si l'établissement est éligible.

[95] La commission médicale d'établissement (CME) contribue à l'élaboration de la politique d'amélioration continue de la qualité et de la sécurité des soins et à l'élaboration des projets relatifs aux conditions d'accueil et de prise en charge des patients.

[96] La commission des usagers (CDU) a pour mission principale de veiller au respect des droits des usagers et de faciliter leurs démarches pour qu'ils puissent exprimer leurs difficultés. Elle contribue aussi, par ses avis et propositions, à l'amélioration de l'accueil et de la prise en charge des personnes concernées et de leurs proches.

[97] Dès lors qu'une visite a eu lieu, le coordinateur des experts-visiteurs dispose de quinze jours pour rédiger son rapport et recueillir des commentaires de la part de l'établissement ; le contenu est validé trois mois environ après la visite. En résulte deux productions : un rapport de synthèse comprenant des données quantitatives (scores) et des données qualitatives (analyse et appréciation), ainsi qu'un rapport plus détaillé à destination de l'établissement, allant jusqu'au niveau du critère et qui conserve un caractère confidentiel.

[98] La DNS a néanmoins d'ores et déjà effectué un premier bilan d'expérience avec la HAS fin mars 2024, conduisant à des mises à jour sur les fiches pédagogiques à destination des experts-visiteurs.

visité au premier semestre 2024, atteignant un score global lui permettant de prétendre à la mention « haute qualité des soins » mais auquel elle n'a pas été attribuée en raison de garanties insuffisantes sur les mesures techniques les plus simples et élémentaires, qualifiées aussi d'hygiène informatique, sur la politique de fiabilisation de l'identification de l'usager et sur les règles d'habilitation[99].

La HAS pourra transmettre de manière régulière à l'ANS des informations anonymisées sur la situation des établissements visités. Par exemple, un premier point d'attention relevé par la HAS lors de ses visites porte sur le faible niveau de déploiement des plans de continuité et de reprise d'activité (PCA-PRA), en particulier de ceux orientés « métier ».

Les représentants des usagers sont informés ou associés à cette démarche d'évaluation des risques numériques dans le cadre d'un comité de concertation sur le référentiel de certification. Trois membres-usagers siègent en outre au sein de la commission de certification des établissements de santé (CCES) qui approuve les ajustements du référentiel.

Le recours à des experts visiteurs numériques professionnalisés renforce la crédibilité de la démarche, même si le niveau d'exigence devait être rehaussé à l'avenir, comme l'ont noté certains hôpitaux ayant eux-mêmes subi des cyberattaques. Ce dispositif constitue en outre un levier très important de prise de conscience, notamment de la part des directeurs.

2.3.2 Des démarches d'audit à coordonner

2.3.2.1 De multiples démarches d'audit proposées par les acteurs nationaux

Indépendamment du processus de certification périodique, les établissements de santé s'inscrivent d'eux-mêmes, peu à peu, dans une dynamique d'amélioration continue. Encouragés par les différents plans consacrés au numérique en santé ou par les financements France Relance portés par l'Anssi et l'ANS, des audits sont réalisés par des prestataires spécialisés en cybersécurité. Ces audits, au moyen de tentatives d'intrusion (tests d'intrusion), mettent en lumière les vulnérabilités présentes dans le SIH et préconisent des actions correctrices priorisées.

Les établissements recourent à différents types d'audit techniques de leur sécurité informatique.

[99] Extrait de la décision de la HAS, non rendu publique : « *Bien que la DSI maîtrise le risque numérique, certains professionnels de la clinique sont en retrait des attendus : méconnaissance des bonnes pratiques en matière d'hygiène informatique, méconnaissance des bonnes pratiques d'identification des patients (identification primaire), méconnaissance des outils sécurisés autorisant l'échange et le partage de données de santé (MES, DMP, MSS, Messagerie sécurisée citoyenne). Le livret d'accueil de l'établissement est le seul point d'information structuré à cet égard. La politique d'identitovigilance n'est pas à jour, les modes opératoires sont partiellement conformes au référentiel national d'identitovigilance, la gestion des risques ne couvre pas l'ensemble des risques. Les règles d'habilitation selon les rôles de chacun ne sont pas suffisamment fines, la politique et la gouvernance des habilitations doit être décrite (revue régulière des habilitations). L'accès des professionnels administratifs au SI parait insuffisamment sécurisé et ne répond pas entièrement aux attendus : existence de comptes génériques, absence de renouvellement des mots de passe* ».

- *Les audits automatisés mis à disposition par l'Anssi : le service Silene pour l'exposition internet et le service ADS pour les annuaires techniques*

L'Anssi met à disposition des opérateurs réglementés et de la sphère publique une capacité d'analyse de leur surface d'exposition au cyber-risque sur internet au travers du service Silene. Elle les assiste ensuite pour définir et appliquer les mesures pour le réduire. Silene s'appuie sur l'expérience et l'expertise acquises par l'Anssi lors des audits et s'enrichit, au fil du temps, de l'observation des modes opératoires utilisés par les attaquants.

L'Anssi met par ailleurs à disposition des mêmes opérateurs[100] une capacité d'audit des annuaires techniques (Active Directory et Samba-AD) au travers du service ADS (Active Directory Security) pour en évaluer le niveau de sécurité et aider à élever le plus possible celui-ci.

À cet égard, le domaine relatif aux accès internet et aux annuaires techniques du programme CaRE exige l'atteinte d'un niveau minimal de sécurisation de ceux-ci (en atteignant un score d'au moins 2 sur une échelle à 5 niveaux, sur plusieurs audits des annuaires techniques) et d'avoir réalisé des audits d'exposition réguliers

Le nombre d'établissements ayant recours à ces services est en forte croissance en 2024 (760 entités en mars et mai, contre 34 sur la même période en 2023 pour le service ADS ; 667 sur les cinq premiers mois contre 77 sur la même période 2023 pour le service Silene).

- *L'audit de cybersurveillance de l'ANS via le Cert Santé*

Initialement pour des besoins de protection de ses propres systèmes, l'ANS a développé un service de cybersurveillance. Ce service recherche et détecte de façon préventive les points de vulnérabilité dans les domaines exposés à l'internet. Ce service est proposé prioritairement aux GHT avec une convention entre le Cert Santé et les établissements.

Par ailleurs, dans le cadre de France Relance, l'Anssi a financé un « cyber-parcours »[101] pour les bénéficiaires (tous secteurs confondus) ; 25 M€ ont été réservés à la santé sur 136 M€. La méthode personnalise le suivi et les objectifs en fonction du diagnostic et un cyber-score (de D- à A+) est calculé au début et en fin de parcours pour l'établissement audité[102].

En complément de ces audits, certains établissements ont recours à des prestataires de confiance spécialisés dans les tests d'intrusion visant à éprouver la robustesse de leur SIH.

Les tests d'intrusion (*« red teaming »*, en anglais)

L'approche dite « d'équipe rouge » (attaquants) contre l'« équipe bleue » (défenseurs) consiste pour le prestataire à effectuer des tentatives d'intrusion physique et numérique, à l'image de ce que feraient des attaquants à la recherche d'une aubaine (« opportunistes ») ou cherchant à atteindre une cible particulière (menace d'origine souvent étatique), par tout moyen

[100] L'Anssi envisage d'étendre ces outils d'audit automatisés aux établissements privés à but lucratif.

[101] Un parcours de cybersécurité se déroule en trois temps successifs : un pré-diagnostic permet de s'orienter vers le parcours de cybersécurité le plus adapté au contexte et aux enjeux de sa structure ; un temps d'accompagnement d'une durée d'environ trois mois consiste en une série de prestations standardisées s'achevant par l'élaboration d'un plan de sécurisation et de l'obtention d'un indice de cybersécurité ; enfin, la mise en œuvre opérationnelle des mesures de sécurisation.

[102] 133 établissements de santé accompagnés, selon le bilan d'activité 2023 de l'Anssi.

qui lui semble adéquat, sous réserve de ne pas perturber les opérations de l'hôpital, de ne pas endommager le système d'information et de supprimer les données obtenues à l'issue du test.

Ces actions sont peu, ou pas, coordonnées avec l'établissement, avec très peu de personnes dans la confidence. Aucune information privilégiée n'est mise à disposition des prestataires. L'objectif est d'arriver par tout moyen à récupérer certains trophées définis à l'avance (ex : compromission d'un compte d'utilisateur, prises de contrôle d'applications ou de serveurs de fichiers, extraction de données médicales, désactivation d'une protection antivirale, capacité à établir un lien distant permanent, etc.). Ces éventuelles réalisations, obtenues avec plus ou moins de difficultés, servent ensuite à la sensibilisation interne et permettent d'identifier et de de prioriser les actions de remédiation (ex : renforcement de la sécurité physique, serveurs exposés sur internet, application vulnérable, etc.).

2.3.2.2 L'institution nécessaire d'un audit technique périodique et obligatoire

La multiplicité de ces audits thématiques appelle à une réflexion sur la stratégie globale des audits numériques et amène à envisager l'intérêt d'un audit global intégrant l'ensemble de ces items par souci d'efficacité. Parallèlement, l'évaluation de la gestion des risques numériques dans le cadre de la certification des établissements de santé est, comme le souligne elle-même la HAS, un levier de développement des usages du numérique au bénéfice de la continuité et de la sécurité des soins mais ne constitue pas pour autant un audit technique ni une inspection de la sécurité des systèmes d'information.

Un regroupement des divers audits partiels sous la forme d'un audit technique plus global, périodique et obligatoire, réalisé par des auditeurs externes[103] pourrait être une solution pertinente. Les résultats seraient confidentiels et communiqués à l'établissement, à l'ARS et à l'ANS.

L'ajout d'un indicateur portant sur la sécurité des systèmes d'information dans le dispositif d'incitation financière à l'amélioration de la qualité et de la sécurité des soins des établissements de santé[104] pourrait aussi constituer une incitation utile à l'amélioration de cette sécurité.

Recommandation n° 4 :	*(DNS, ANS, DGOS, HAS, Anssi)* Mettre en place un audit périodique obligatoire pour tous les établissements de santé, qui pourrait être pris en compte dans le dispositif d'incitation à la qualité et dans la certification par la HAS.

[103] Incluant des tests d'intrusion ou « *pentests* ». Cette proposition d'audit technique externe est distincte de la mission menée par les commissaires aux comptes (CAC), qui analysent d'une part la gestion des comptes utilisateurs des applications générant de la dépense ou des recettes, et d'autre part la maîtrise des interfaces des logiciels pour assurer l'exhaustivité du chiffre d'affaires.

[104] Le dispositif d'incitation financière à la qualité (IFAQ) a été généralisé à partir de 2016 et évolue régulièrement depuis 2019 pour accompagner son extension financière, avec pour objectif d'utiliser un levier de financement pour améliorer la qualité des soins et de la prise en charge. Le chapitre du Ralfss de 2016 précité notait déjà : *« D'autres dispositifs, tels que le programme d'incitation financière à l'amélioration de la qualité et de la sécurité des soins, généralisable en 2016, prennent en compte les indicateurs d'« Hôpital numérique », ce qui ouvre la voie à des modulations financières selon le niveau de service informatique rendu par les hôpitaux ».*

3 FAIRE EVOLUER L'ORGANISATION ET LES PRATIQUES DES ETABLISSEMENTS DE SANTE EN MATIERE DE CYBERSECURITE

Au-delà des financements, des évolutions au niveau régional et local sont nécessaires pour améliorer la cybersécurité des établissements de santé : harmoniser les réponses des agences régionales de santé (ARS) et des groupement régionaux d'appui au développement de l'électronique en santé (GRADeS), inciter les établissements à développer des actions de mutualisation et des bonnes pratiques, et accélérer la convergence des systèmes d'information au sein des groupements hospitaliers de territoire (GHT).

Ces changements doivent s'opérer en tenant compte de la rareté des ressources humaines disposant des compétences requises en informatique.

3.1 Harmoniser les réponses apportées par les ARS et les GRADeS

3.1.1 Une capacité d'intervention auprès des établissements de santé très variable selon les ARS

Les ARS relaient le pilotage national et la promotion de la cybersécurité auprès des établissements de santé. Elles les sensibilisent aux cyber-risques, favorisent le partage des bonnes pratiques et préparent la réponse sur le versant « offre de santé » dans l'hypothèse d'un incident de sécurité informatique. Elles suivent l'octroi des financements aux établissements[105].

En situation de crise, leur action est nettement moins affirmée. Sur ce segment, leur éventuel soutien semble conditionné par les compétences et ressources qu'elles sont en mesure de mobiliser en interne. Certaines agences, comme celles de La Réunion ou de la Bretagne dont l'appétence est forte pour le numérique et la cybersécurité, ont développé des compétences plus affirmées, ou depuis plus longtemps, que leurs homologues d'autres régions.

Cette assistance demeure conditionnée par les moyens humains affectés à ces questions au sein même des ARS ; le nombre moyen d'ETP consacrés à la sécurité est de 1,1 (de 0,3 ETP à l'ARS Pays-de-la-Loire à 2,7 ETP en Auvergne-Rhône-Alpes). Généralement, les ARS disposent de peu de compétences internes sur la question de la cybersécurité.

Les initiatives prises dans les domaines suivants peuvent être portées en exemple :

[105] Les sondages réalisés par la Cour auprès des adhérents des fédérations hospitalières FHF, FHP et FEHAP montrent que, si les ARS bénéficient d'une évaluation positive, leur rôle auprès des établissements de santé est quasi exclusivement centré sur les questions de financement (77 % pour la FHP, 86 % pour la FHF et la FEHAP) et de contrôle de financement (42 % FHP, 47 % FHF, 30 % FEHAP), et peu sur l'appui technique (31 %, 35 %, 30 %) ou la mise à disposition d'expertise (18 %, 19 %, 16 %).

- *Prévention et audit*

Dès 2019, l'ARS de La Réunion a financé à hauteur de 297 000 € un audit d'évaluation et d'appui à la sécurisation des systèmes d'information du GHT, ayant abouti à un plan d'actions. Pour la période 2021 à 2025, le soutien financier de l'ARS représente 50 % des dépenses d'investissement résultant de ce plan, soit 3,8 M€.

- *Réponse à la crise*

Face à une menace accrue, l'Ile-de-France se démarque par des compétences et des moyens opérationnels développés avec l'appui de l'AP-HP et par le projet d'inscription d'un volet cybersécurité dans le plan ORSAN.

- *Apport en ressources humaines*

L'ARS Occitanie propose un programme de renfort en ressources humaines[106] dans un objectif de mutualisation entre établissements. Cette mesure concerne l'ensemble des établissements de santé de la région, quel que soit leur statut. L'agence mobilise une enveloppe devant permettre le recrutement de 55 postes sur trois ans. En Bretagne, le financement d'un poste d'ingénieur en cybersécurité pour chacun des huit GHT que compte la région, et éventuellement d'autres ressources humaines opérationnelles, est garanti sur trois ans[107]. Cependant, peu d'ARS mettent des ressources à disposition des établissements, y compris par l'intermédiaire des GRADeS.

- *Actions de sensibilisation*

Une démarche a été engagée en 2024 par la DNS afin qu'une première trame d'objectifs consacrés à la cybersécurité soit mise à disposition des ARS, permettant à ces dernières de les intégrer dans les contrats pluriannuels d'objectifs et de moyens (CPOM) conclus avec les établissements de leur ressort. Les ARS ont vocation à transmettre à terme, dans le cadre des dialogues de gestion entre ces dernières et la DNS, le nombre de CPOM signés sous ce format. Ce « dialogue de gestion numérique » permet d'aligner l'action régionale sur les priorités nationales issues de la feuille de route « Numérique en santé » adoptée en mai 2023. Des priorités annuelles décomposées en objectifs, indicateurs et cibles sont transmises aux ARS et passées en revue lors de dialogues de gestion régionaux, chaque semestre. La cybersécurité est identifiée comme une priorité pour 2024 dans ce cadre.

Outre la création d'un item sur la cybersécurité dans les comptes rendus d'entretiens d'évaluation professionnelle des directeurs d'établissements, l'ARS Bretagne a constitué, en fin d'année 2023, un groupe de travail réunissant autour d'elle les RSSI de GHT et d'établissements privés (à but non lucratif comme lucratif). A ainsi été défini de manière collégiale un ensemble d'objectifs à inclure au sein d'une annexe « cybersécurité » des CPOM (qui seront signés à la fin de 2024 pour les premiers contrats arrivant à échéance), contenant 16 actions à réaliser par les établissements d'ici à la fin de 2025. L'un des objectifs porte sur la *« sensibilisation et la formation aux enjeux de la cybersécurité »*, reposant sur deux actions : intégrer la sécurité des systèmes d'information, la cybersécurité et la protection des données

[106] Le 4e axe du programme CaRE de pérennisation des ressources humaines.
[107] 1,2 M€ sur trois ans, soit 150 000 € par GHT.

dans les plans de formation et réaliser des actions de formation sur ces thèmes, à destination de tous les professionnels.

Le ministère devrait faire connaître ces initiatives et inciter toutes les ARS à en engager de similaires.

L'organisation de la cyberrésilience en Ile-de-France

L'action de l'ARS Ile-de-France, accélérée par l'organisation des Jeux Olympiques, vise à associer toutes les ressources disponibles sur la question de la cybersécurité et à concevoir un protocole de résilience en cas de cyberattaque. Plusieurs briques sont prévues :

Introduction d'un volet « cybersécurité » dans le plan Orsan[108]:

- organiser la réponse dans les établissements avec des objectifs précis et des méthodes régionales commese préparer à réorganiser l'offre de soins ; au sein de l'établissement, être capable de réduire, de déprogrammer, d'interrompre les soins non programmés ; réorganiser les flux des patients au sein de la région par l'ARS ;
- mise à disposition de matériel en cas de crise pour refaire les capacités bureautiques dans un premier temps par l'AP-HP ;
- appui méthodologique et envoi d'experts par l'ARS, le GRADeS d'Ile-de-France (Sesan) et l'AP-HP.

Structuration des chaînes d'alerte pour bâtir une réponse commune et aider les établissements : Cert Santé, ministère, systèmes de veille en continu de l'ARS pour mobiliser des ressources, notamment celles de Sesan, les Samu pour organiser les flux et les établissements.

Conception d'une offre de services par l'AP-HP en relation avec Sesan, dans le contexte d'une activité forte à l'approche des Jeux Olympiques qui constitue aussi une occasion pour des évolutions indispensables en matière d'assistance aux établissements en cas de cyberattaque sur le volet matériel. L'AP-HP a déjà éprouvé l'utilité de l'assistance portée à plusieurs hôpitaux ayant connu une cyberattaque avec une offre bureautique de base livrée dans un temps très court : téléphonie, Internet, imprimante fournie après une cyberattaque. Cette offre d'assistance, officialisée dans le cadre d'une convention, est financée par l'ARS à hauteur de 500 000 €/an et organisée de la manière suivante :

- une procédure de déclenchement auprès de l'ARS qui transmet l'information à la direction des services numériques de l'AP-HP située à l'hôpital Rothschild, campus Picpus, qui livre les postes et assure les premiers services d'installation (24h/24, 7j/7) pour la reprise des activités les plus critiques ;
- les services d'urgence ou critiques et les activités de médecine, chirurgie, obstétrique sont prioritaires ;

[108] Orsan cyber : plan devant être opérationnel à la fin du premier semestre 2024.

- la livraison de 500 postes informatiques en trois tranches déterminées par les capacités de stockage, de transport et d'organisation d'astreinte (deux personnes, les jours fériés et de fin de semaine) : première tranche : 50 postes livrés en deux heures avec installation Windows, imprimantes, routeurs 4G+ et cartes SIM incluses ; deuxième tranche : 150 postes ; troisième tranche : 300 postes ;
- les structures publiques comme privées peuvent faire appel à cette offre ; les adhérents du Sesan bénéficient dans tous les cas de ses services.

L'AP-HP développe son propre plan de résilience en cas de cyberattaque d'un de ses hôpitaux. Ce plan inclut toutes les prestations techniques et logistiques et l'organisation des flux hors région en cas d'attaque majeure.

3.1.2 Des GRADeS engagés à des degrés divers dans la cybersécurité

Les groupements régionaux d'appui au développement de l'électronique en santé (GRADeS) sont des structures de soutien et de conseil pour faciliter l'intégration et l'utilisation des outils numériques dans le secteur de la santé au niveau régional. D'après le texte constitutif[109], le GRADeS est l'opérateur préférentiel de l'ARS pour l'élaboration et la mise en œuvre de la stratégie régionale de l'électronique en santé.

Les résultats des enquêtes réalisées par la Cour auprès des adhérents des fédérations hospitalières permettent de constater que les GRADeS sont des structures connues davantage des établissement publics et associatifs que des établissements privés à but lucratif[110]. Leur rôle est apprécié[111] malgré l'hétérogénéité des prestations proposées et le degré variable du soutien technique qu'ils apportent aux établissements dans les différentes régions.

Certains développent une réponse large avec la proposition de marchés de prestations communs pour les exercices de crise ou l'assistance à la remédiation *via* les prestataires de réponse aux incidents de sécurité (PRIS)[112], de solutions concurrentes de celles proposées par les éditeurs de logiciels, de mise à disposition de matériel de secours en cas de cyberattaque ou de centres ressources répondant aux besoins des établissements en matière de cybersécurité. D'autres assurent seulement des missions de sensibilisation et d'information.

À ce jour, moins de la moitié des GRADeS ont passé un marché régional de prestation de réponse aux incidents de sécurité (PRIS)[113].

[109] Instruction no SG/DSSIS/2017/8 du 10 janvier 2017 relative à l'organisation à déployer pour la mise en œuvre de la stratégie d'e-santé en région.
[110] 84 % des établissements publics et 80% des établissements privés non lucratifs connaissent le GRADeS de leur région, versus 65 % des établissements privés lucratifs.
[111] 94 % des établissements privés non lucratifs répondant au sondage le trouve utile.
[112] Les marchés PRIS se sont principalement mis en place dans les régions concernées par les Jeux olympiques de Paris ou dans certaines régions ayant connu des incidents massifs de cybersécurité, sans que leur financement soit garanti dans la durée.
[113] 11 sur les 17 ARS ayant répondu au questionnaire de la Cour.

Exemples d'initiatives prises par des GRADeS

En Nouvelle-Aquitaine comme en Normandie, le GRADeS expérimente une contractualisation de PRIS mutualisé associant plus de dix établissements. Le prestataire sélectionné couvre la période allant d'avril à fin septembre 2024[114].

En Centre-Val de Loire, le GRADeS propose une solution de cyber-protection de type EDR/SOC[115] en lieu et place des éditeurs, avec une refacturation aux hôpitaux.

En Bretagne, le GRADeS et l'ARS ont défini une feuille de route régionale. En sus des actions de sensibilisation *via* des campagnes régionales (par exemple, campagne de lutte contre l'hameçonnage par questionnaire), il propose une animation des exercices de crises, la mise à disposition d'un kit PCA-PRA (plans de continuité et de reprise de l'activité) et du guide du plan blanc numérique, et met à disposition un marché de PRIS régional.

Les GRADeS sont aussi chargés par le ministère d'organiser les « centres régionaux de cyber-ressources » (CRRC) qui visent à assister les structures sanitaires et médico-sociales dans le renforcement de leur cybersécurité. Ce rôle a été précisé par l'instruction n° DNS/2024/54 du 2 juillet 2024.

Les établissements privés à but lucratif qui appartiennent à des groupes transrégionaux ou nationaux ne font pas appel aux GRADeS, de même que les établissements privés à but non lucratif appartenant à de grandes structures associatives nationales. Ce sont plutôt les plus petites structures hospitalières et médico-sociales, tous secteurs confondus, qui sont les bénéficiaires de l'action des GRADeS, avec un taux d'adhésion variable d'une région à l'autre.

Malgré un socle commun de besoins identifiés, quel que soit le statut et le territoire des établissements, les réponses apportées par les GRADeS dépendent en grande partie des moyens dont ils disposent et du niveau d'engagement de l'ARS dans cette coopération. À cet égard, la DNS précise que des travaux d'harmonisation des missions des GRADeS sont en cours.

Une animation nationale renforcée des GRADeS par l'ANS est en effet souhaitable, afin d'harmoniser leur gouvernance et leur pilotage et que leur action au soutien des établissements soit plus homogène.

3.2 Renforcer l'attractivité des métiers du numérique et développer la formation en direction des professionnels de l'hôpital

Une étude de 2022 relative aux métiers en 2030 réalisée par France Stratégie et la Dares[116] montre que le métier d'ingénieur dans l'informatique est celui qui connaîtra la plus

[114] La prolongation du dispositif n'est pas assurée au-delà de cette période ni sa possible ouverture à tous les établissements, la principale réserve consistant à trouver des prestataires en mesure de répondre aux besoins de l'ensemble des établissements.

[115] EDR : *endpoint detection and response*, technologie logicielle de détection des menaces de sécurité (évolution des anti-virus et pare-feu), associée à une surveillance dite SOC *security operations center*, c'est-à-dire une tâche de surveillance continue, 24h/24 et 7j/7, de la sécurité informatique d'une entité, confiée à des professionnels, équipe interne ou prestataire externe, en mesure de détecter et de faire face aux événements de cybersécurité.

[116] Les métiers en 2030 | France Stratégie (strategie.gouv.fr)

forte expansion, avec une croissance de 26 %, soit une création nette de 115 000 postes. Cette étude annonce une augmentation des difficultés de recrutement, le nombre de diplômés ne suivant pas la dynamique des besoins du marché de l'emploi en raison, notamment, des délais et des capacités de formation.

Le taux moyen de vacance de poste dans les équipes informatiques des hôpitaux, publics comme privés, déterminé par l'enquête réalisée par la Cour, était de 5 % pour les années 2022 et 2023. Tous secteurs confondus en France, il était de 2,1 % au quatrième trimestre 2023[117]. Cette situation n'est pas spécifiquement française. Selon une étude de l'Institut hospitalier allemand[118] datant de 2024, 76 % des hôpitaux interrogés déclarent connaître des difficultés pour pourvoir les postes vacants de spécialistes en informatique.

Les établissements déclarent que leurs besoins prioritaires, quel que soit le statut de l'établissement, sont en premier lieu le recrutement de spécialistes en cybersécurité, puis la formation, qui viennent devant l'achat de matériel[119].

3.2.1 Un déficit de compétences appelant à davantage de mutualisations

3.2.1.1 Des ressources spécialisées en cybersécurité difficiles à attirer

Les établissements de santé sont en concurrence avec les secteurs d'activité hors santé (industrie, banque, etc.) qui offrent des rémunérations et des évolutions de carrière plus intéressantes pour ces profils limités en nombre et très recherchés. La rémunération des RSSI dans les hôpitaux publics[120] peut être deux fois moins élevée que dans les entreprises privées.

Confronté à la même difficulté, l'Etat, par la circulaire n° 6434/SG du 3 janvier 2024 relative à la politique salariale interministérielle des métiers de la filière numérique, a revu la grille de rémunération du personnel numérique contractuel afin de réduire l'écart avec l'offre privée et de répondre aux difficultés de recrutement. Cette nouvelle grille, qui n'a pas de caractère obligatoire, offre des souplesses de recrutement, telles que la première embauche en CDI, et n'a pas d'équivalent dans la fonction publique hospitalière. Quelques hôpitaux s'y réfèrent mais cette situation crée un déséquilibre salarial avec les agents titulaires (ingénieur hospitalier et technicien supérieur hospitalier) et suscite des tensions internes. La grille des ingénieurs titulaires a certes été revue à la hausse[121] mais le salaire d'un titulaire reste plus faible que celui d'un RSSI contractuel[122]. Même dans le cas où la grille de rémunération a été

[117] Dares, Données provisoires sur les emplois vacants 4e trimestre 2023, publiées le 19 février 2024. Les données excluent l'agriculture, l'intérim, les particuliers employeurs et les emplois publics.
[118] L'Institut hospitalier allemand est un organisme de recherche dans le domaine de la santé publique et est soutenu par des associations telles que la Fédération allemande des hôpitaux (Deutsche Krankenhausgesellschaft).
[119] Données issues de l'exploitation des résultats des sondages adressés par la Cour aux adhérents des fédérations hospitalières dans le cadre de la présente enquête. Valeurs FHF : recrutement de spécialistes : 22 %, formation : 19 %, achat de matériel : 17 %. Valeurs FHP : le recrutement de spécialistes : 27 %, la formation : 18 %, l'achat de matériel : 17 %. Plus de la moitié des hôpitaux publics (55 %) et des établissements privés (57 %) ont réalisé des estimations de leurs besoins en matière de cybersécurité.
[120] Grille indiciaire hospitalière : ingénieur hospitalier.
[121] Par décret du 30 janvier 2024 relatif à l'échelonnement indiciaire du corps des ingénieurs hospitaliers.
[122] Le traitement indiciaire de la grille des ingénieurs hospitaliers au dernier échelon est de 3 337 € alors que la rémunération la plus basse proposée par la grille interministérielle pour les nouveaux contractuels de l'État est de 4 600 €. La rémunération la plus basse dans le secteur privé, toutes activités confondues, est de 4 750 €.

améliorée, comme à l'AP-HP, le recrutement sur les postes d'expert en cybersécurité reste difficile.

3.2.1.2 Des compétences à mutualiser

Le financement du support numérique s'est construit principalement par des opérations ponctuelles d'investissement, sans appréhension des coûts de maintenance et de fonctionnement, y compris de personnel, inévitablement associés et indispensables à l'utilisation et à la pérennité des équipements et applications. L'inscription dans les CPOM des établissements de santé de ces recrutements et d'une offre salariale attractive traduit toutefois une logique de pérennisation.

Selon une estimation de la DGOS, 4 000 postes de cyber-spécialistes sont à pourvoir. Les ingénieurs hospitaliers en poste (fonctionnaires) n'ont pas toujours les compétences nécessaires pour traiter les questions de cybersécurité, même si certains d'entre eux parviennent à accomplir des parcours intéressants grâce à la formation au cours de leur carrière, selon l'AP- HP. Des experts peuvent aussi être formés parmi les agents hospitaliers chargés de la mise en œuvre de la politique de qualité et de gestion des risques car ils maîtrisent une démarche utile aux fonctions liées à la cybersécurité. Des viviers de compétences peuvent être constitués par le repérage des formations pertinentes en cybersécurité et le développement de l'alternance.

Dans ce contexte, la mutualisation des compétences entre plusieurs établissements se révèle encore plus indispensable. Les GHT ont naturellement vocation à la permettre.

Exemples de difficultés rencontrées par les établissements en matière de recrutement

Dans l'un des établissements visités, les équipes chargées du numérique et de la sécurité des systèmes d'information sont constituées principalement d'ingénieurs avec peu de techniciens. Le coût de la prestation d'un cabinet de recrutement mandaté pour rechercher ces profils est ressenti comme particulièrement élevé par les établissements. L'établissement a dû, dans certains cas, consentir à satisfaire à des exigences posées par des candidats parfois peu adaptées au contexte de travail, comme la possibilité de télétravailler en continu.

Dans un autre centre hospitalier, le poste de responsable d'infrastructure est vacant depuis trois ans en raison des grandes difficultés de recrutement dues à la faible attractivité du territoire et de l'hôpital, et au rapport défavorable entre la complexité du travail et la rémunération proposée.

3.2.2 La sensibilisation et la formation du personnel, une condition de la sécurité des systèmes d'information

Les programmes de formation initiale du personnel médical et paramédical ne comprennent pas de module consacré au numérique et à la cybersécurité.

La nouvelle feuille de route du numérique en santé prévoit pour 2027 l'intégration de modules de formation dans toutes les formations initiales médicales et paramédicales. Un référentiel de compétences concernant toutes les branches du secteur médical, élaboré par la DNS en relation avec la DGOS et avec le ministère de la recherche, regroupe les compétences

socles sur le numérique. Les modules ainsi conçus, financés sur crédits interministériels, ont été rendus obligatoires pour 14 professions en formation initiale par un décret de 2022 et par deux arrêtés interministériels pris, l'un en 2022, l'autre en 2023[123].

En outre, la direction générale de l'enseignement supérieur et de l'insertion professionnelle (DGESIP)[124], chargée de l'appel national à manifestation d'intérêt « Compétences et métiers d'avenir », a associé la DNS à l'élaboration d'un volet « santé numérique[125] ». Il concerne l'ensemble des universités du secteur de la santé et des instituts de formation paramédicale[126].

Pour le personnel de direction, dans le cadre de la tutelle de l'école des hautes études en santé publique (EHESP), le secrétaire général des ministères sociaux a associé la DNS pour introduire dans le nouveau contrat d'objectif et de performance (COP) 2024-2027 la composante numérique dans la majorité des objectifs de formation de l'établissement d'enseignement.

Il ne s'agit pas d'une spécificité française : le gouvernement du Royaume-Uni a lancé en décembre 2022 une stratégie visant à atteindre la cyber-résilience dans l'ensemble du secteur anglais de la santé d'ici à 2030. Son lancement est intervenu après plusieurs retards et une cyberattaque massive du National Health Service (NHS) en août 2022. Elle repose notamment sur la formation du personnel soignant aux méthodes de la cyber-protection[127].

En matière de formation continue, l'ensemble des professionnels de santé hospitaliers, salariés et libéraux de France sont soumis à l'obligation triennale de développement professionnel continu (DPC). Chaque professionnel de santé doit, par période de trois ans, suivre un parcours combinant de la formation, de l'évaluation de pratiques professionnelles ou de la gestion des risques. Un minimum de deux actions de deux types différents est requis. Les inscriptions se font sur le site de l'Agence nationale du DPC. La DNS travaille avec les opérateurs de compétences (Opco) et avec les autres organismes financeurs et régulateurs de la formation continue pour intégrer des modules de formation numérique en santé, dont la cybersécurité pour les professionnels en activité. Ainsi, la DNS a fait intégrer une orientation prioritaire numérique en santé au DPC pour la période triennale 2023-2025[128].

---

[123] Décret n°2022-1419 du 10 novembre 2022 relatif à la formation socle au numérique en santé dans les formations d'audioprothésiste et d'orthophoniste ; arrêté du 10 novembre 2022 relatif à la formation socle au numérique en santé des étudiants en santé ; arrêté du 9 juin 2023 portant diverses modifications relatives aux modalités de fonctionnement des instituts de formation paramédicaux et aux formations conduisant aux diplômes d'État d'aide-soignant et d'auxiliaire de puériculture.

[124] La DGESIP a pour mission d'élaborer et de mettre en œuvre la politique relative aux formations supérieures, initiales et continues relevant du ministre chargé de l'enseignement supérieur et de la recherche.

[125] Les cinq objectifs du volet de formation numérique : mettre en place des modules de santé numérique dans les formations initiales aux métiers du secteur sanitaire et médico-social, accroître la proportion de spécialistes en numérique ayant une culture santé, former des directeurs d'établissements sanitaires et médico-sociaux, juristes et chargés d'affaires réglementaires aux questions du numérique.

[126] Actuellement ,21 des 34 universités ainsi que leurs organismes de formation paramédicaux conventionnés, sont lauréates et 12 des 13 universités restantes sont candidates.

[127] Données issues de la consultation du réseau des conseillers aux affaires sociales des ambassades par la direction des relations internationales, de l'audit externe et de la francophonie de la Cour des comptes.

[128] Introduit dans le code de la santé publique par la loi dite HPST (Hôpital, patient, santé et territoires) de 2009, puis réformé en 2016 par la loi de modernisation de notre système de santé, le DPC a pour finalité l'amélioration de la qualité, de la sécurité et de la pertinence des soins.

Par ailleurs, l'Anssi dispose d'un centre de formation qui s'investit dans les missions de sensibilisation aux questions de sécurité informatique et la CNIL s'investit dans la sensibilisation et la formation au règlement général sur la protection des données (RGPD) et à la loi « informatique et liberté »[129].

De son côté, l'Anap préconise la sensibilisation de l'ensemble des professionnels aux bonnes pratiques clés « d'hygiène informatique » au sein d'une démarche de promotion de la qualité pilotée par le RSSI.

Malgré la richesse et la diversité de l'offre de formation, les besoins en formation continue des hôpitaux sont importants et spécifiques, et nécessitent des formules sur mesure, souples et adaptées aux profils divers des professionnels, aux mouvements de personnel et aux contraintes de calendrier de certains métiers.

La création de centres de formation, sur le modèle du « Campus du numérique » que propose la Dinum pour les agents de l'État, pourrait répondre à ce besoin. Le campus propose des formations sur mesure en partant de bilans de l'existant et s'adresse à tout type de profil, spécialiste comme novice. Le contenu des formations est adapté aux groupes constitués, dans un format souple, en présence physique, en visioconférence ou selon une formule hybride proposant les deux options.

Enfin, pour les établissements privés à but lucratif ou non lucratif, l'opérateur de compétences du secteur privé de la santé (Opco Santé) peut de même proposer, outre les formations en ligne d'initiation et de sensibilisation, des modules de formation sur mesure en cybersécurité[130].

3.3 Accélérer la convergence en matière de sécurité des systèmes d'information dans le secteur public

Une convergence informatique aboutie suppose un système d'information hospitalier (SIH) mutualisé, englobant l'ensemble des ressources matérielles et logicielles, des données et des ressources humaines.

Le code de la santé publique, art. L. 6132-3-I., prévoit que « *l'établissement support désigné par la convention constitutive assure pour le compte des établissements parties au groupement [...] la stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent, en particulier la mise en place d'un dossier patient permettant une prise en charge coordonnée des patients au sein des établissements parties au groupement* ».

La note méthodologique de la DGOS de juillet 2016[131], adressée aux établissements de santé, définit le contenu d'un SIH convergent : des applications identiques pour chacun des domaines fonctionnels, principalement avec la mise en place du dossier du patient informatisé. En conclusion, l'ambition de convergence prévue par le code de la santé publique s'est limitée, au mieux, à l'interopérabilité des applications. Seul un système d'information unique est de nature à permettre réellement la convergence.

---

[129] Une journée « RGPD santé » a été organisée à Rennes en juin 2023 et une journée à Bordeaux en 2022 avec une partie consacrée à la SSI et à plusieurs webinaires « santé ».
[130] L'Opco Santé est implanté dans toutes les régions de la métropole et d'outre-mer, et compte 25 sites régionaux.
[131] dgos_guide_systeme_information_convergent.pdf (sante.gouv.fr)

3.3.1 Partager les bonnes pratiques

Bien que la sécurité des SIH ne soit pas explicitement visée dans les différents programmes nationaux antérieurs pour le numérique en santé, cette préoccupation est constante et considérée comme un prérequis à tout financement. De nombreuses préconisations en la matière sont régulièrement diffusées par l'Anssi, le Cert Santé, des associations ou clubs professionnels. Les bonnes pratiques ci-dessous n'ont pas vocation à être exhaustives ; elles s'inspirent des différents contrôles réalisés par les judications financières et des visites de terrain effectuées dans le cadre de la présente enquête. Il s'agit, le plus souvent de pratiques déterminantes pour l'amélioration du niveau de sécurité du SIH.

3.3.1.1 L'organisation de la sécurité du SIH à renforcer

Les établissements de santé doivent mettre en place une organisation consacrée à la sécurité informatique, avec des rôles et des responsabilités clairement définis. Cette organisation doit s'appuyer sur une politique de sécurité du système d'information (PSSI) hospitalier qui définisse les objectifs, les principes et les mesures de sécurité à mettre en œuvre. La PSSI doit permettre d'identifier, d'évaluer et de hiérarchiser les risques liés à la sécurité informatique afin de mettre en place des mesures de protection adaptées et proportionnées dans chaque établissement.

Le suivi effectué par la plate-forme OSIS[132], publié dans l'Atlas du SIH en novembre 2021, montre que la quasi-totalité des établissements (95 %) sont dotés d'une PSSI, avec une part plus faible pour les petits établissements, de type centre hospitalier (77 %). Cependant, les équipements biomédicaux connectés au réseau tardent à être inclus dans le périmètre de la PSSI, seulement 47 % des établissements ayant réalisé cette intégration. S'agissant de la carte des risques, 62 % des établissements affirment disposer de celle-ci, mise à jour depuis moins d'un an. En revanche, l'analyse systématique de risques lors de l'introduction dans le système d'information d'une application ou d'un équipement biomédical n'est réalisée que dans 29 % des établissements.

L'organisation de la sécurité s'appuie aussi sur un responsable de la sécurité des systèmes d'information (RSSI)[133] dont la majorité des établissements se sont dotés. En revanche, la fonction n'est que très rarement exercée à temps complet (dans 7 % des établissements seulement).

Malgré des tendances globalement à la hausse de tous les indicateurs, l'Atlas ne présume pas de la qualité du pilotage de la sécurité des systèmes d'informations, notamment de son adéquation avec les risques propres à l'établissement. La conscience du risque au sein du personnel reste variable. La création d'un comité de sécurité au niveau stratégique, avec la participation de la commission médicale d'établissement, est impérative, afin d'intégrer le

[132] Un recueil composé de 41 questions est proposé depuis 2016 ; il cible principalement l'organisation de la sécurité du SI qui s'appuie sur les référentiels et les guides de politique générale des SI santé, produits par l'agence du numérique en santé (ANS).

[133] Cette fonction est généralement présente dans les CHU, dans les grands groupes privés et dans les établissements support de GHT. Dans les plus petits établissements, ce sont des référents sécurité qui sont désignés.

risque lié à la cybersécurité au niveau de la direction de l'établissement et d'associer la communauté soignante.

3.3.1.2 La connaissance du SIH comme préalable à toute sécurisation

Il est impossible de protéger correctement un système d'information sans en connaître précisément les composantes, les interactions et les dépendances. Tous les établissements répondant aux enquêtes OSIS déclarent disposer d'un inventaire des ressources informatiques (plus de 97 %), réputé à jour dans plus de 88 % des cas car il date de moins d'un an. Ces chiffres, fondés sur une démarche déclarative, sont optimistes. Les différents contrôles des systèmes d'information réalisés par les chambres régionales des comptes ne les confirment pas. Bien que ne contestant pas l'existence d'une démarche de capitalisation des connaissances du SIH, les chambres régionales des comptes relèvent la difficulté constante que rencontrent les établissements pour cartographier les risques et réunir une documentation complète. Le plus souvent, le matériel biomédical n'est pas repéré. Les visites effectuées dans trois régions, à l'occasion de la présente enquête, ont aussi fait apparaître la difficulté, notamment pour les petits établissements, de connaître précisément leurs systèmes d'information.

3.3.1.3 La gestion des accès au SIH, la segmentation du réseau informatique et la sauvegarde des données, des outils à généraliser

En restreignant l'accès aux données sensibles aux seuls agents autorisés, les établissements de santé peuvent réduire considérablement les risques de compromission. Cela empêche les cybercriminels de profiter des accès non sécurisés pour infiltrer les réseaux hospitaliers et lancer des attaques, telles que des rançongiciels. La centralisation de la gestion des identités et des accès (IAM, Identity and Access Management), automatisant les processus de création, de gestion et de suppression des comptes d'utilisateurs, est un moyen de limiter les risques. L'authentification multi-facteurs[134] renforce la sécurité en exigeant plusieurs formes de vérification, rendant ainsi plus difficile l'accès non autorisé, particulièrement en cas de vol des identifiants d'un utilisateur. La revue régulière, au moins une fois par an, des comptes d'utilisateurs est aussi une pratique à rendre plus systématique. Enregistrer et surveiller toutes les tentatives d'accès et les activités sur les systèmes permet de détecter rapidement les comportements anormaux ou les tentatives d'intrusion. Ce dispositif exige des ressources humaines et financières conséquentes mais peut être conçu à l'échelle d'un GHT, pour les établissements publics, ou de toute autre structure de mutualisation pour les autres établissements. L'enquête a montré une mise en œuvre inégale de ce type de dispositifs, essentiellement pour des raisons financières et de disponibilité des compétences.

La segmentation du réseau (aussi appelée cloisonnement) est une approche de sécurité informatique qui consiste à diviser un réseau informatique en sous-réseaux isolés les uns des autres, afin de limiter la propagation des cyberattaques. En cas d'attaque ou d'infection par un

[134] Méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN. Au lieu de se contenter d'un nom d'utilisateur et d'un mot de passe, l'authentification multi-facteur exige un ou plusieurs facteurs de vérification supplémentaires, ce qui réduit la probabilité de succès d'une cyberattaque. Le programme CaRE octroie des financements sur ce thème.

logiciel malveillant, la propagation de l'attaque est limitée au sous-réseau concerné, ce qui permet de réduire ses conséquences pour l'ensemble du SIH et de faciliter la remise en état du système. Cette mesure nécessite toutefois une approche rigoureuse afin de garantir l'efficacité du cloisonnement et de minimiser les risques de perturbation du fonctionnement du SIH. Il est ainsi nécessaire d'identifier les différentes composantes du système et les flux d'information entre elles. Ensuite, il convient de définir une doctrine de segmentation qui précise les règles d'accès entre les différents sous-réseaux et les mesures de sécurité à mettre en œuvre pour chaque sous-réseau (pare-feu, chiffrement, etc.). Bien que faisant partie des exigences de différents programmes nationaux de financement du numérique en santé[135], cette mesure n'est que rarement mise en place.

La sauvegarde des données est indispensable à la protection des systèmes d'information contre les cyberattaques car elle permet leur récupération en cas d'incident. Il existe plusieurs types de sauvegardes, chacun avec ses avantages spécifiques. Il est recommandé d'utiliser la règle « 3-2-1 » : utiliser trois copies des données sur deux types de supports différents, avec une copie externe. Si les établissements de santé sont conscients de l'importance des sauvegardes pour la sécurité des SIH, de nombreux hôpitaux ne disposent pas de sauvegarde hors site ou déconnectée du réseau informatique, ce qui les rend vulnérables aux attaques susceptibles de compromettre l'ensemble du réseau interne. Sans redondance suffisante, une cyberattaque réussie, telle que celle par rançongiciel, peut crypter ou détruire, à la fois, les données primaires et les sauvegardes sur site.

3.3.2 Des groupements hospitaliers de territoire (GHT) peu structurés et une convergence des systèmes d'information toujours attendue

3.3.2.1 La convergence des systèmes d'information confrontée à la diversité de l'existant et au développement des usages

La Cour, dans son rapport de 2020 sur les GHT[136], a fait état du faible niveau d'intégration des établissements membres des GHT et a recommandé que ceux-ci soient mis dans l'obligation d'unifier et de mutualiser les applications informatiques utilisées à cette échelle, et que les financements alloués soient accordés sous cette condition. Du fait de l'inégale maturité des SIH et des besoins importants en financements nécessaires à leur fusion, les stratégies de convergence adoptées par les établissements se caractérisent par une grande diversité de périmètre et de rythme de réalisation. Si la grande majorité des GHT a élaboré un schéma directeur unique du système d'information, la convergence reste inaboutie[137].

Le pilotage de la convergence est mesuré par la DGOS au regard de trois critères : la réalisation de l'état des lieux des systèmes d'information des établissements membres du GHT (réalisé par 95 % des établissements), la définition de la stratégie de convergence (83 %) et l'approbation du schéma directeur des systèmes d'information (80 %). L'évaluation de la

[135] Cf. instruction SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information, reprise dans le programme HOP'EN.

[136] Rapport sur les Groupements hospitaliers de territoire 2014-2019 (Communication à la commission des affaires sociales du Sénat) Les groupements hospitaliers de territoire (ccomptes.fr)

[137] Les groupements hospitaliers de territoires, Cour des comptes, 2020.
Bilan d'étape des groupements hospitaliers de territoires, IGAS, 2019.

convergence des processus SIH se fonde essentiellement sur des aspects organisationnels tels que la définition d'une doctrine commune de sécurité des systèmes d'information, la nomination d'un responsable de la sécurité des systèmes d'information de GHT et d'un délégué à la protection des données, et des marchés en cours pour les établissements membres du GHT.

Or, la traduction concrète d'une doctrine de sécurité des systèmes d'information commune à l'échelle du GHT est confrontée au nombre et à l'hétérogénéité des SIH, à la coexistence d'équipes informatiques non mutualisées et d'instances de direction dominées par l'établissement pivot du GHT. Les référents pour la sécurité des SI présents dans les établissements membres ne sont pas toujours affectés entièrement à cette fonction et peinent à traduire des orientations générales issues de la politique de sécurité des systèmes d'information du GHT.

La convergence du SIH est, quant à elle, appréciée en fonction de critères[138] centrés, d'une part, sur des indicateurs mesurant le nombre d'applications communes aux établissements et, d'autre part, sur les référentiels d'identité des patients, des séjours et des professionnels. Si l'incitation à l'augmentation des applications communes et à la mise en place de référentiels uniques au sein des GHT contribue à la convergence du SIH, ils ne contiennent aucun critère portant sur l'infrastructure elle-même du système d'information. Les programmes de financement sont aussi orientés quasi exclusivement vers le développement des usages. La convergence de l'infrastructure, très longue à mettre en place, reste donc embryonnaire.

Le besoin en ressources humaines, dont la mise en commun est effective dans les structures en direction commune, est encore difficile à évaluer. Ainsi, la majorité d'établissements publics et d'établissements privés à but non lucratif déclarent avoir amorcé leur convergence, principalement sur les applicatifs[139].

A contrario, les établissements privés à but lucratif[140] déclarent mutualiser en premier lieu leur DSI (71 %) puis les applicatifs (65 %), la contrainte financière, plus sévère depuis la fin des années 2000, ayant incité les établissements du secteur privé lucratif à se regrouper, sous diverses formes, pour partager le coût de leurs fonctions support.[141]

Illustrations de la convergence dans les régions

En Occitanie, la crise sanitaire a fortement ralenti les projets de convergence des systèmes d'information soutenus par l'ARS. Ainsi, sur les 14 GHT du territoire, 50 % d'entre eux ont mutualisé leurs équipes informatiques ; en revanche, le dossier informatisé du patient (DPI) n'est mutualisé que dans 17 % des cas. Un certain nombre ont mutualisé leur RSSI et leur référent RGPD. La mutualisation est mise en œuvre pour uniformiser les applications ou pour renforcer des infrastructures techniques et fonctionnelles comme l'annuaire technique. Ces

[138] Nombre total d'applications installées et utilisées dans les établissements parties au GHT, nombre d'applications communes installées et utilisées par l'ensemble des établissements, nombre d'interfaces exploitées, existence d'un référentiel unique d'identité des patients quel que soit le mode de prise en charge et l'établissement, existence d'une cellule d'identitovigilance du GHT opérationnelle, existence d'un référentiel unique de séjours et de mouvements quel que soit le mode de prise en charge et l'établissement, existence d'un annuaire des professionnels unique et partagé entre tous les établissements.

[139] 78 % des adhérents de la FHF et 58 % des adhérents de la FEHAP ayant répondu au sondage de la Cour.

[140] Dans le secteur privé, trois voies de mutualisation sont mises en œuvre : la création de groupes d'établissement avec des opérations de rachat ou d'entente entre associations, l'intégration dans des groupes privés, la mise en place de structures de coopération autour du SI *via* des groupements d'intérêts économiques.

[141] 30 % des répondant au sondage de la FHP font partie d'un groupe depuis moins de 10 ans.

démarches sont essentielles et prioritaires pour de petits établissements qui disposent de peu de moyens.

En Bourgogne-Franche Comté, le niveau de convergence est très variable. Le DPI commun tend à se développer mais les autres briques logicielles (gestion des achats mutualisés, gestion budgétaire et financière, gestion des ressources humaines...) et les briques techniques (annuaire, sauvegarde, supervision) ne sont que très peu mutualisées ou même rendues compatibles. Pour les établissements privés hors groupes, les compétences internes en informatique sont rares, voire absentes. Dans ces établissements, le recours à l'externalisation du SI associé à un appui sur des ressources externes spécialisées serait une solution.

Dans le Grand-Est, 90 % des 11 GHT ont déjà lancé ou sont en passe de lancer leur convergence. Le niveau actuel de convergence est variable selon la configuration du GHT (nombre d'établissements, présence ou non d'un CHU, hétérogénéité des CH selon la taille et selon les activités MCO, PS, SSR...), de la maturité et de l'hétérogénéité initiale des SI (en logiciels et infrastructures) et des moyens humains existants. La mutualisation des ressources humaines en informatique est prioritaire.

3.3.2.2 La convergence technique des SIH : des atouts et des précautions

En regroupant les infrastructures et les services informatiques, les GHT peuvent mutualiser les compétences et les outils, assurant ainsi une surveillance continue et une réponse rapide aux incidents de sécurité. Cette mutualisation facilite aussi l'application uniforme des protocoles de gestion des accès, réduisant ainsi les points de vulnérabilité.

Par ailleurs, l'harmonisation des protocoles garantit l'application des mêmes normes de sécurité par tous les établissements et minimise ainsi les risques liés à des pratiques disparates et incohérentes. Le regroupement facilite le partage des meilleures pratiques en matière de cybersécurité, permettant aux établissements de bénéficier des expériences réussies et des enseignements tirés des incidents de cybersécurité connus. Cette synergie améliore la capacité collective à prévenir, à détecter et à répondre efficacement aux cybermenaces.

Enfin, une gouvernance centralisée permet une meilleure coordination des efforts et une réponse plus efficace en cas de cyberattaque. Les décisions stratégiques peuvent être prises au niveau du GHT, offrant une vision globale du SIH qui permet de mettre en place des plans de reprise d'activité et des plans de continuité d'activité cohérents et interopérables, assurant ainsi une continuité des services de soin même en cas d'incident majeur.

Cependant, la mise en place du socle technique de la convergence est à conduire avec précaution : un dossier informatisé du patient commun pour tous les établissements d'un GHT suppose un référentiel commun mais pas nécessairement un même serveur car, même si la mutualisation des outils diminue le risque de sécurité physique, elle augmente le risque logique. De même, sans segmentation des réseaux, la convergence peut augmenter les conséquences d'une cyberattaque.

Certains aspects techniques peuvent être mutualisés sans risque : par exemple, les sondes informatiques pour détecter les comportements anormaux dans les établissements du GHT qui reviennent à une console centrale de surveillance. Il est en effet préférable de recourir à des pare-feux et à des outils de détection identiques au sein d'un même groupement.

L'interconnexion des réseaux accroît la surface exposée ; il est donc nécessaire de respecter des étapes préalables, notamment la convergence des annuaires qui exige un travail méticuleux de vérification du profil de chaque utilisateur. Le sujet des annuaires n'est par ailleurs pas qu'un sujet informatique. Il relie l'approche technique à une mission de gestion des ressources humaines. Un lien entre les deux est donc nécessaire, avec une clarification des responsabilités.

3.3.2.3 L'unification des directions des systèmes d'information (DSI) dans les établissements publics membres d'un GHT

Les GHT devraient travailler sur l'organisation de leur cybersécurité dans le cadre d'une DSI commune pour faire face à la raréfaction des ressources. Les rôles de responsable de la sécurité des systèmes d'information et de délégué à la protection des données devraient être mutualisés afin d'apporter des réponses plus efficaces en cas d'incident, d'uniformiser les procédures dégradées et les bonnes pratiques et d'être plus attractifs en matière de recrutement en diversifiant les missions et en développant les évolutions de carrière. Dans cette configuration, toutes les ressources liées au système d'information se trouveraient rattachées à la direction des systèmes d'information de l'établissement support.

Peu de temps avant la cyberattaque qu'il a subie, le centre hospitalier de Versailles avait mis en place une direction commune avec d'autres établissements ; celle-ci a permis la constitution d'un dossier informatisé du patient commun grâce auquel il a été possible de récupérer les dossiers des patients après l'attaque.

L'Atlas des SIH de 2020 de l'ATIH[142] fait état d'une augmentation significative de la mise en place de DSI communes : 87 % des 133 GHT ayant répondu à l'enquête (sur 136 GHT existants, à l'échelle nationale) déclarent une DSI déjà opérationnelle (60 GHT) ou en cours de mise en œuvre (56 GHT) soit une augmentation de six points par rapport à 2018. On constate une prévalence des DSI combinant des rattachements organiques et fonctionnels, pour 46 % des 115 GHT ayant répondu.

La création d'une DSI commune de GHT reste dépendante de la volonté des établissements, du niveau de développement du SIH de GHT et des incitations locales des ARS. L'organisation de la DSI commune est actuellement dominée par un modèle mixte entre un rattachement complet et un rattachement seulement fonctionnel à la DSI de l'établissement pivot de GHT. Faisant le constat de l'hétérogénéité et de la complexité des SIH, la DGOS estime cependant que leur maintenance par la DSI de l'établissement support est complexe et non viable. En outre, ce rôle constitue un frein pour évoluer vers des missions transversales et mutualiser les fonctions support du GHT, ce qui coïncide avec la faible intégration des équipes dans les DSI seulement mutualisées.

3.3.2.4 Des objectifs et des modalités de convergence à clarifier

Initialement, le législateur n'a pas doté les GHT de la personnalité morale, leur existence reposant sur une convention passée entre plusieurs établissements publics de santé. Cette disposition présentait pour les établissements la garantie de préserver leur autonomie et d'éviter

[142] 2021.11_DGOS_Etats lieux SI Hospitaliers.pdf (ccomptes.fr)

la multiplication des fusions dans cette nouvelle organisation. Cependant, l'absence de personnalité morale ne permet pas au GHT de disposer d'un budget autonome, de recruter et de gérer directement du personnel, d'acquérir et de gérer du patrimoine mobilier et immobilier en propre.

Alors que plusieurs réformes se sont succédé afin d'accélérer l'intégration des GHT, les établissements de santé ont eu des difficultés à les mettre en application. Conséquence de l'absence de personnalité morale du GHT, les obligations inhérentes aux GHT sont assumées par l'établissement support[143]. Le budget du GHT[144] est inscrit dans sa comptabilité pour suivre les opérations liées aux mutualisations dans le groupement. Les GHT n'ont pas encore tout à fait trouvé leur stabilité puisque des mouvements de sortie et de regroupement sont encore opérés dans le but de créer des liens de coopération plus adaptés aux besoins de la population et aux territoires.

Le modèle de financement peut être un autre vecteur important pour la convergence. La campagne d'appel à demandes de financement au titre du premier domaine du programme CaRE (exposition internet et annuaires techniques) conduit à un constat positif : tous les GHT ont candidaté. Le programme CaRE est aussi le premier à associer un financement à la convergence des infrastructures (annuaire). En dehors de ce développement récent, il n'existe aucun programme de financement spécifique conditionné par l'effectivité de la convergence alors que celle-ci incite à la réorganisation de l'offre de soins publique dans son ensemble.

La réponse à long terme pour une fonction informatique prête à répondre efficacement à l'état de la menace se construit selon le degré de maturité de la convergence qui permet de rationaliser les moyens en les mutualisant. Les besoins non objectivés des établissements de santé en matière de ressources humaines spécialisées en sécurité informatique ont un effet, à la fois, sur la soutenabilité financière et sur la capacité des établissements à accéder aux compétences rares. La prochaine transposition de la directive NIS 2, avec un socle de mesures de sécurité applicables aux établissements de santé, apparaît comme l'occasion d'objectiver ces besoins des établissements et de veiller à l'allocation des moyens financiers nécessaires.

Les principaux défis à relever pour permettre la convergence des SIH incluent donc les aspects techniques et organisationnels, les contraintes budgétaires, l'accès aux ressources rares. Pour surmonter ces obstacles, il est essentiel de renforcer le soutien aux établissements dans cette transition, de promouvoir la formation continue du personnel affecté à la cybersécurité et d'assurer un soutien financier adéquat. Il est aussi nécessaire de définir des objectifs de mutualisation organisationnelle et technique en fonction des risques identifiés[145].

La Cour avait déjà recommandé, dans son rapport sur les groupements hospitaliers de territoire d'octobre 2020[146], de doter les GHT de la personnalité morale. La DGOS, reconnaît la nécessité de compléter la loi (code de la santé publique, art. L 6132-3 I 1°) puis le règlement (code de la santé publique, art. R 6132-15) afin de doter les GHT de la personnalité morale.

---

[143] Le code de la santé publique,art. L 6132-3 I 1°, précise que l'établissement support du GHT assure pour le compte des établissements parties du groupement *« la stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent et interopérable »*. Cette disposition législative est complétée, sur le plan règlementaire, par l'article R 6132-15 du code de la santé publique.

[144] Ce budget est alimenté par les établissements qui sont membres du groupement hospitalier de territoire.

[145] La nouvelle organisation de la DGOS prévoit la création d'une « Mission gouvernance des établissements de santé » qui devrait permettre d'avancer sur la définition de ces objectifs en relation avec la DNS.

[146] Communication à la commission des affaires sociales du Sénat.

Recommandation n° 5 :	*(DGOS, DNS, ANS)* Doterl les groupements hospitaliers de territoire de la personnalité morale.

CONCLUSION

En raison de leur très grande complexité, de leurs connexions avec de nombreux utilisateurs extérieurs, de la vétusté de certaines applications et d'investissements insuffisants dans le domaine de la sécurité au cours des années passées, les systèmes d'information des hôpitaux sont vulnérables aux cyberattaques les plus courantes, comme l'ont démontré les sinistres récents subis par plusieurs établissements.

Les dommages engendrés par ces agressions informatiques peuvent pourtant être considérables, tant pour les établissements eux-mêmes et leur personnel que pour les patients et pour le système de santé. La gestion des sinistres et de leurs conséquences commence à s'organiser mais les mesures d'assistance aux établissements victimes et de rétablissement de leur fonctionnement ne sont pas encore harmonisées. Il convient de mettre en place un groupe national d'expertise chargé, en cas de cyberattaques d'ampleur exceptionnelle, d'évaluer les pertes de recettes à compenser et, pour les établissements les plus gravement affectés, de proposer une dispense de codification *a posteriori* de leur activité hospitalière.

Pour limiter les conséquences des cyberattaques sur le fonctionnement des hôpitaux et sur la continuité des soins, le ministère de la santé a élaboré un programme de rattrapage (CaRE) pour les années 2023-2027 qui vise à renforcer la sécurité des hôpitaux en modernisant leurs systèmes d'information et en mettant en place des mesures pour protéger les données sensibles et les infrastructures critiques. Ce programme au contenu cohérent dont la mise en œuvre commence à porter des fruits, n'est financé que jusqu'à 2024 ; il est indispensable qu'il soit conduit à son terme. En outre, à partir de 2028, compte tenu de l'évolution de la cybermenace, le besoin de financement perdurera, d'autant plus que la directive européenne NIS2 renforcera les exigences en matière de cybersécurité, et s'appliquera à un périmètre d'établissements de santé beaucoup plus large qu'aujourd'hui. .

Parallèlement à ces efforts financiers, dans une logique d'utilisation plus efficace et plus efficiente des ressources informatiques et humaines, il est impératif de doter les groupements hospitaliers de territoire de la personnalité morale pour rendre effective la convergence technique des systèmes d'information des établissements publics de santé.

ANNEXES

Annexe n° 1. Liste des sigles

ACSS : cellule d'accompagnement cybersécurité des structures de santé ; remplacée en 2019 par le Cert Santé

AD : *active directory* (annuaire technique)

AMOA : assistance à maîtrise d'ouvrage

Anap : Agence nationale de la performance sanitaire et médico-sociale

ANS : Agence du numérique en santé

ANSM : Agence nationale de sécurité du médicament et des produits de santé

Anssi : Agence nationale de la sécurité des systèmes d'information

AP-HP : Assistance publique-Hôpitaux de Paris

ARS : agence régionale de santé

ASIP-Santé : Agence nationale des systèmes d'informations partagés de santé (remplacée en 2019 par l'ANS)

ATIH : Agence technique de l'information sur l'hospitalisation

CHU : centre hospitalier universitaire

CH : centre hospitalier

CHSF : Centre hospitalier du Sud francilien (Corbeil-Essonnes)

CLCC : centres de lutte contre le cancer

Cloud Computing : informatique en nuage, modèle de prestation de services informatique qui permet aux utilisateurs d'accéder à des ressources (serveurs, applications), à la demande ou *via* internet sans avoir à gérer ces ressources sur des centres de données propres

CaRE : cybersécurité accélération et Résilience des Établissements (programme de financement cybersécurité)

Cert : *computer emergency response team* (centre de réponse aux urgences informatiques)

CME : commission médicale d'établissement

CNIL : Commission nationale de l'informatique et des libertés

CPom : contrats pluriannuels d'objectifs et de moyens

CSIRT : *computer security incident response team* (centre de réponse aux incidents de sécurité informatique)

CRRC : centre de ressources régional cyber

DGOS : Direction générale de l'organisation des soins

DGS : Direction générale de la santé

DM : dispositifs médicaux (connectés)

DNS : Délégation au numérique en santé

DPI : dossier du patient informatisé

DPO : délégué à la protection des données

DSI : directeur (ou direction) des systèmes d'information

EDR : *endpoint detection and response*, technologie logicielle de détection des menaces de sécurité (évolution des anti-virus et pare-feu), associée à une surveillance dite SOC

EE : entités essentielles

EI : entités importantes

ETP : équivalent temps plein

ETPR : équivalent temps plein rémunérés

ENISA : european union agency for cybersecurity (agence européenne pour la cybersécurité)

FEHAP : fédération des établissements hospitaliers et d'aides à la personne

FHF : Fédération hospitalière de France

FHP : Fédération de l'hospitalisation privée

FIR : fonds d'intervention régional ; relève d'un sous-objectif spécifique de l'Ondam

FSSI : fonctionnaire de sécurité des systèmes d'information

GAM : gestion administrative des malades

GEF : gestion économique et financière

GCS : groupement de coopération sanitaire

GHT : groupement hospitalier de territoire

GIP : groupement d'intérêt public

GRADeS : groupement régional d'appui au développement de la santé électronique

HAS : Haute Autorité de santé

HCL : Hospices civils de Lyon

HDS : hébergeur de données de santé

HFDS : haut-fonctionnaire de défense et de sécurité

Hop'EN : hôpital numérique ouvert sur son environnement (programme de financement)

Igas : Inspection générale des affaires sociales

INS : identifiant national de santé

ISQUA : international society for quality in heath care : organe accréditeur des processus de certifications des hôpitaux selon des standards internationaux

LOLF : loi organique relative aux lois de finances

MSS : messageries sécurisées de santé

NIS : *network and information security* (sécurité des réseaux et systèmes de l'information) : nom communément donné aux deux directives européennes de 2016 et 2022, relatives à la cybersécurité, dites NIS1 et NIS 2

OIV : opérateur d'importance vitale

ONDAM : objectif national de dépenses d'assurance maladie

ORSAN : organisation de la réponse du système de santé en situations sanitaires exceptionnelles

OSE : opérateur de services essentiels

PASSI : prestataire d'audit de sécurité des systèmes d'information

PCRA (ou PCA-PRA) : plans de continuité et de reprise de l'activité

PMSI : programme de médicalisation des systèmes d'information

PRIS : prestataire de réponse aux incidents de sécurité

RSSI : responsable de la sécurité des systèmes d'information

SaaS : *software as a service* (mode d'hébergement dans lequel les applications sont hébergées, moyennant un abonnement, chez un fournisseur de service, à l'extérieur de l'hôpital)

SAE : statistique annuelle des établissements de santé

SI : système d'information

SIH : système d'information hospitalier

SOC : *security operations center* (équipe interne ou externalisée de professionnels de la sécurité informatique qui surveille l'ensemble de l'infrastructure informatique d'une entité, 24h/24 et 7j/7, afin de détecter et faire face aux événements de cybersécurité)

SPF : Santé publique-France

SUN-ES : Ségur usage du numérique – volet établissements de santé

Annexe n° 2. Personnes auditionnées

Administration centrale :

- **Ministère en charge de la santé**

Secrétariat général des ministères chargés des affaires sociales (SGMCAS) et haut fonctionnaire de défense et de sécurité (HFDS)

Pierre Pribile, secrétaire général
Yann Debos, chef de service Pôle santé ARS
Patrice Bigeard, fonctionnaire de sécurité des systèmes d'information

Direction générale de l'offre de soins (DGOS)

Cécile Lambert, cheffe de service, adjointe à la directrice générale
Clotilde Durand, cheffe de service, adjointe à la directrice générale
Marion Fages, adjointe à la sous-directrice PF (pilotage de la performance des acteurs de soins)
Judicaël Thévenard, chef du bureau PF5 chargé des SI de l'offre de soins
Nicolas Voss, adjoint au chef du bureau PF5

Délégation ministérielle au numérique de santé (DNS)

Héla Ghariani, directrice
David Sainati, co-directeur
Christophe Mattler, directeur de projets, chargé du pilotage du programme national Care (Cybersécurité accélération et résilience des établissements)

Agence du numérique en santé (ANS)

Annie Prévot, directrice générale
Jean-Baptiste Lapeyrie, directeur Expertise, innovation et international
Elodie Chaudron, directrice du programme CaRE

Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP)

Tim Brienen, directeur du pôle finances, IA et data
Anaelle Valdois, experte numérique et finances

Agence technique de l'information sur l'hospitalisation *(*ATIH)

Housseyni Holla, directeur général
Max Bensadon, directeur-adjoint
Delphine Leroux, cheffe de service-adjoint, Financement et analyse économique
Isabelle Hernando, statisticienne

- **Services du Premier ministre**

  Direction interministérielle du numérique (Dinum)

  Stéphanie Schaer, directrice
  Frédéric Culie, conseiller à la sécurité numérique pour les produits interministériels
  Perica Suvecic, cheffe de service

  Agence nationale de la sécurité des systèmes d'information *(*Anssi)

  Vincent Strubel, directeur général
  Stéphane Deharvengt, chef de la division Coordination sectorielle
  Silvère Ruellan, chef du bureau santé et affaires sociales, division coordination sectorielle, sous-direction stratégie

- **Caisse nationale d'assurance maladie (Cnam)**

  Marc Scholler, directeur délégué de l'audit, des finances et de la lutte contre les fraudes
  Catherine Mark, cheffe du service facturation des établissements de santé

- **Haute Autorité de Santé (HAS)**

  Anne Chevrier, cheffe du service de certification des établissements de santé

- ***Commission nationale de l'informatique et des libertés*** **(Cnil)**

  Bertrand Pailhès, directeur des technologies de l'innovation
  Aurore Gaignon, juriste
  Florent Della Valle, responsable de l'expertise technologique au sein de la direction des technologies de l'innovation
  Belaïd Aït Hamouda, en charge du traitement des contentieux

- **Cour des comptes**

  Francis Autran, Conseiller maître, quatrième chambre

- **Chambre régionale des comptes Bretagne**

  Stéphane Guillet, président de section
  Frédéric Chanliau, premier conseiller
  Xavier Boschet, vérificateur

- **Chambre régionale des comptes Centre-Val de Loire**

  Matthieu Waysman, premier conseiller

- **Fédération hospitalière de France (FHF)**

  Laurent Pierre, conseiller numérique en santé

- **Fédération de l'hospitalisation privée (FHP)**

  Bertrand Sommier, secrétaire général, chargé du numérique en santé
  Marie-Claire Viez, directrice de la stratégie

- **Fédération des établissements hospitaliers et d'aide à la personne privés solidaires (FEHAP)**
  Blandine Vachon, directrice de l'observation et des études
  Arnaud Joan-Grangé, directeur de l'offre de soins et des parcours de santé,

- **France Assos Santé**
  Arthur Dauphin, chargé de mission numérique en santé

- **Club RSSI Santé**
  Béatrice Bérard, officier de sécurité des systèmes d'information du GHT Val Rhône Centre, présidente du club RSSI Santé

- **Association pour la sécurité des systèmes d'information de santé (APSSIS)**
  Vincent Trély, président

- **Syndicat National de l'Industrie des Technologies Médicales SNITEM**
  Armelle Graciet, directrice des affaires industrielles
  William Rolland, directeur délégué au numérique en santé
  Arnaud Augris, responsable affaires règlementaires
  Alice Languille, stagiaire numérique en santé

- **Assureur Relyens**
  Dominique Godet, directeur général
  Pierre-Yves Antier, directeur général-adjoint

- **Cédric Carteau, RSSI CHU Nantes et GHT 44**

- **Jonathan LOTZ,** directeur du GRADeS Pulsy

Ile-de-France

- **ARS**
  Julien Marchal, directeur de la DIRNO
  Christian Lemaire, chargé de mission DIRNOV sécurité
  Jéromine Lemaire, responsable-adjointe Département défense et sécurité
  Damien Mathey, directeur-adjoint Veille et sécurité sanitaire

- **GradeS Sesam**
  Naïma Mezaour, directrice
  Rémi Tilly, directeur du département Sécurité des systèmes d'information

- **AP-HP**

Professeur Catherine Paugam, directrice générale-adjointe
Raphaël Beaufret, directeur des services numériques
Jean-Baptiste Hagenmüller, directeur délégué
Didier Perret, responsable de la sécurité des systèmes d'information

- **Hôpital privé d'Antony (Groupe Ramsay)**
  François Papart, directeur délégué
  Sandrine Eldin, responsable des systèmes d'information
  David Bardin, responsable informatique du Pôle Ile-de-France-Sud
  Arnaud Vandesmet, directeur de la sécurité des systèmes d'information et de la protection des données au siège de Ramsay Santé pour l'ensemble des établissements
  Vincent Lorette, responsable de la sécurité des systèmes d'information au sein de la DSI siège

- **Groupe hospitalier Diaconesses-Croix Saint Simon**
  Anne Fabrègue, directrice générale
  Guillaume Chesnel, directeur général-adjoint
  Dr Laurence Marsal, directrice Qualité-hygiène-gestion des risques

- **Hôpital André Mignot-Centre Hospitalier de Versailles, établissement support du groupement hospitalier de territoire Yvelines Sud**
  Pascal Bellon, directeur général
  Valérie Gaillard, directrice générale-adjointe

- **CH Corbeil-Essonne Sud Francilien, établissement support du groupement hospitalier de territoire Île-de-France Sud**
  Gilles Calmes, directeur général
  Bénédicte Dragne-Ebrardt, directrice générale-adjointe
  Patrice Garcia, directeur des systèmes d'information
  Thierry Pasquelin, adjoint au directeur chargé des systèmes d'information
  Nicolas Campuiz Ruz, responsable SSI

Bretagne

- **ARS**
  Elise Noguera, directrice générale
  Anne-Briac Bili, directrice de cabinet
  Hélène Delaveau, responsable du département Innovation en santé
  Lionel Lecomte, expert référent cybersécurité

- **GRADeS eSanté**
  Romain Lemoine, directeur général
  Pierre-Alain Laforêt, responsable administratif et financier
  Gilles Laroche, chef de projet cybersécurité

- **Préfecture de région, préfecture de la zone de défense et de sécurité Ouest**
  Philippe Gustin, préfet d'Ille-et-Vilaine

- **CHU de Rennes, établissement support du Groupement hospitalier de territoire Haute-Bretagne**
  Véronique Anatole-Touzet, directrice générale
  Frédéric Rimattei, directeur général-adjoint
  Christine Pichon-Abarnou, directrice des systèmes d'information du CHU et du GHT

- **CH de Redon (Groupement hospitalier de territoire Haute-Bretagne)**
  Jean Belet, directeur général adjoint en charge des ressources et directeur des systèmes d'information
  Bérengère Rouxel-Madec, responsable qualité et responsable de la sécurité des systèmes d'information
  François le Nalio, chef de service informatique

- **CH Saint-Malo (Groupement hospitalier de territoire Rance-Emeraude)**
  Guilhem Bonenfant, directeur des systèmes d'information du groupement hospitalier de territoire Rance-Emeraude
  Johann Thomas, responsable infrastructures des systèmes d'information du groupement hospitalier de territoire Rance-Emeraude

- **Clinique La Sagesse (Groupe Hospi Grand Ouest)**
  Gwenaël Bodin, directeur
  Gwenaëlle Herrault, responsable service numérique
  Philippe Dupont, responsable de la sécurité des systèmes d'information du groupe Vyv 3
  Florence Jubault, responsable qualité
  Mathieu Moulègues, responsable projet sécurité santé du groupe
  John Charriat, directeur des affaires financières

- **Hôpital Saint-Grégoire (Groupe Vivalto Santé)**
  Artus de Saint-Pern, directeur
  Olivier Boixière, directeur du digital et des systèmes d'information groupe
  Thomas Jouvin, responsable des systèmes d'information, territoire Bretagne-Est

Centre-Val de Loire

- **ARS**
  Clara de Bort, directrice générale
  Cédric Maréchal, directeur-adjoint
  Dominique Pierre, chargé de mission SI Santé
  Ali Troudi, chef de projet Ségur Santé

- **GradeS**

Armelle Quanty, directrice générale
Amandine Ore, Référente Cybersécurité de centre de ressources régional
Hubert Fabri, Délégué à la protection des donnés
Christelle Pinto, Responsable formation

- **CHU de Tours, établissement support du groupement hospitalier de Touraine-Val de Loire**
  Floriane Rivière, directrice générale du CHU
  Julien Berthel, DSI du CHU
  Eliane Boutin, responsable du système d'information

- **CH du Chinonais (Groupement hospitalier de Touraine-Val de Loire)**
  Dominique Osu, directrice du CH

- **CH d'Amboise (Groupement hospitalier de Touraine-Val de Loire)**
  Frédéric Mazurier, directeur général
  Bruno Rebouillau, directeur des systèmes d'information

- **CH Jacques Cœur de Bourges, établissement support du groupement hospitalier de territoire du Cher**
  Rémi Fauquembergue, directeur général
  Noelle Périer, directrice des systèmes d'information
  Frank Moussé, responsable de la sécurité des systèmes d'information

- **CH de Vierzon (Groupement hospitalier de territoire du Cher)**
  Barbara Fouet, directrice des ressources physiques et économiques
  Charles Berthias, technicien supérieur hospitalier

- **CH George Sand Bourges (Groupement hospitalier de territoire du Cher)**
  Marie Roulx-Laty, directrice générale
  Aurélien Hyppolite, directeur-adjoint affaires financières et systèmes d'informations
  Frank Moussé, responsable de la sécurité des systèmes d'information
  Eric Faure, responsable du service informatique

- **Clinique Alliance Saint-Gatien (Groupe Saint-Gatien)**
  Sylvie Lefebvre, directrice générale
  Didier Baty, directeur des systèmes d'information

- **Clinique associative Bel-Air (Groupe Croix Rouge)**
  Valérie Pelletier, directrice
  Guillaume Bruel, directeur régional des systèmes d'information
  Priscilla Laignel, responsable siège du support technique

- **Pôle de santé Léonard de Vinci (Groupe Vivalto Santé)**
  Aurélien Frot, directeur général-adjoint

- **Clinique de l'Archette (Groupe Elsan)**
  Eric Bordeaux-Montrieux, directeur général

Pierre Bedel, responsable des systèmes d'information du groupe
Aurélien Petitjean, responsable des systèmes d'information, région Centre
Renaud Fortin, responsable des systèmes d'information de la clinique de l'Archette