

PÔLE D'EXCELLENCE CYBER

CYBER & IA EN SANTÉ

Comprendre les usages, garder la maîtrise, construire la confiance

LIVRE BLANC

Novembre 2026

Région Bretagne

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité

SOMMAIRE

PRÉFACE PAR ARNAUD COUSTILLIÈRE 4

LE MOTS LA DGRINES ET DE L'ANS 6

01. CONTEXTE 8

Pourquoi ce livre blanc ? 10

02. ETAT DES LIEUX 12

Connaître les actifs d'IA avant de pouvoir les maitriser 14

La cybersécurité & les structures médico-sociales : ce que le terrain nous apprend 21

Des établissements préparés à la crise… mais pas toujours à l'indisponibilité. 23

03. RÉGLEMENTATION DES DISPOSITIFS 26

Cybersécurité des logiciels en santé et des dispositifs médicaux numériques pouvant intégrer de l'IA : comprendre les exigences réglementaires 28

04. UNE RÉPONSE À NOS ENJEUX COMMUNS 32

Projet <BALISE> une avancée collective pour lutter contre les fuites de données de santé 34

05. CONCLUSION 40

Garder la maîtrise, sans perdre l'élan 42

PRÉFACE

par Arnaud Coustillière

Il y a quelques années à peine, la question pouvait être posée ainsi : quelle place l'intelligence artificielle prendra-t-elle demain dans notre système de santé ?

Aujourd'hui, cette question est en partie derrière nous. L'intelligence artificielle est déjà là. Dans les outils d'aide au diagnostic, dans l'imagerie médicale, dans les logiciels métiers ou encore dans les environnements collaboratifs. Elle est parfois même présente dans des fonctionnalités dont les utilisateurs ne perçoivent pas immédiatement qu'elles reposent sur des systèmes d'intelligence artificielle.

Cette évolution ouvre des perspectives considérables. Elle peut contribuer à améliorer les pratiques, faciliter le travail des professionnels, accélérer la recherche et soutenir la qualité des soins. Mais dans un domaine aussi essentiel que la santé, l'innovation ne peut être durable que si elle s'accompagne de confiance.

Et la confiance ne se décrète pas.

Elle suppose de savoir quelles technologies nous utilisons, quelles données elles mobilisent, de quels acteurs et de quelles infrastructures elles dépendent. Elle implique également de pouvoir comprendre, contrôler et sécuriser ces outils lorsque cela est nécessaire, mais aussi de conserver notre capacité à agir lorsqu'un outil n'est plus disponible.

C'est précisément à ce carrefour que se rencontrent les enjeux de cybersécurité, d'intelligence artificielle et de santé.

Le sujet dépasse largement la seule question technologique. Il concerne la capacité des établissements à conserver la maîtrise de leurs systèmes et de leurs données. Il interroge les relations avec les éditeurs et les prestataires, la continuité des activités, les responsabilités de chacun, la capacité à anticiper les crises et, au bout de cette chaîne, la protection des patients et des professionnels.

C'est aussi ce qui fait la valeur du travail présenté dans cet ouvrage. Il ne propose pas une vision uniquement théorique de l'intelligence artificielle appliquée à la santé. Il part des usages, des difficultés rencontrées sur le terrain et des questions concrètes auxquelles sont confrontés les établissements, les professionnels, les industriels et les acteurs publics.

Cette approche reflète la manière dont nous travaillons au **Pôle d'Excellence Cyber** : décloisonner les expertises, favoriser le dialogue entre des compétences et des expériences différentes et construire ensemble des réponses concrètes, collectives et directement mobilisables.

Ce livre blanc est ainsi le résultat d'un travail mené par des acteurs issus d'horizons complémentaires. Il croise les réalités des établissements de santé et du secteur médico-social avec celles des industriels, des spécialistes de la cybersécurité, du droit, de la continuité d'activité et des politiques publiques.

Cette diversité n'est pas accessoire. Elle est indispensable face à des transformations qui ne peuvent plus être appréhendées en silos.

Les constats présentés dans ces pages montrent qu'il reste beaucoup à faire. Mais ils montrent également que

les leviers existent : cartographier les systèmes d'intelligence artificielle présents dans les organisations, mieux connaître les données et les flux, encadrer les usages, renforcer le dialogue avec les fournisseurs et étendre à l'IA les mécanismes de gouvernance et de résilience déjà développés en cybersécurité.

L'enjeu n'est donc pas de choisir entre innovation et sécurité, ni d'opposer performance technologique et souveraineté. Notre ambition doit être de concilier le meilleur de la performance et le meilleur de la souveraineté, en créant les conditions d'une innovation durable, maîtrisée et responsable, sans renoncer à notre capacité de comprendre, de décider et d'agir.

Dans le domaine de la santé, plus encore qu'ailleurs, cette maîtrise est une responsabilité collective.

Je tiens enfin à remercier l'ensemble des contributeurs de cet ouvrage pour leur engagement, la richesse de leurs expertises et la qualité du travail accompli. Leurs contributions nous donnent des clés essentielles pour mieux appréhender les transformations en cours et les accompagner avec exigence, discernement et confiance.

LE MOTS DE LA DGRINES ET DE L'ANS

Cyber et IA, des leviers essentiels pour la santé de demain

La transformation numérique du système de santé français progresse depuis plusieurs années, et va encore accélérer avec le déploiement de l'intelligence artificielle (IA). Cette technologie, au cœur de la Stratégie nationale IA et données de santé 2025-2028, représente une opportunité historique pour améliorer la qualité des soins, optimiser les parcours patients et renforcer l'efficience de notre système de santé. Mais son déploiement exige une approche rigoureuse, sécurisée, éthique et inclusive, afin de garantir la confiance des professionnels comme des citoyens. La question de la cybersécurité est devenue particulièrement aigüe depuis quelques mois, avec une suite d'évènement qui ont démontré la place cruciale que vont tenir les IA dans ce domaine.

Des enjeux majeurs pour la santé publique

L'IA offre des perspectives inédites : détection précoce de pathologies (comme le cancer du sein ou le sepsis), personnalisation des traitements, automatisation des tâches administratives pour libérer du temps médical, ou encore optimisation de la logistique hospitalière. Les cas d'usage concrets se multiplient, avec des gains mesurables en termes de productivité et de qualité des soins.

Pourtant, ces avancées soulèvent des défis complexes :

- Les données de santé doivent être protégées avec la plus grande rigueur, sans nuire à leur interopérabilité et leur accessibilité.
- Les outils intégrant de l'IA doivent répondre à des exigences réglementaires renforcées, notamment avec l'entrée en vigueur du Règlement européen sur l'IA (RIA ou AI Act) en août 2026. Il s'agit d'assurer leur sécurité d'emploi, leur transparence et leur conformité éthique.
- La stratégie nationale prévoit la formation des soignants à l'IA avec un objectif clair, accélérer le déploiement des cas d'usage à fort impact et accompagner les professionnels dans leur montée en compétence pour permettre un usage effectif et sécurisé des outils.

Cybersécurité : un impératif pour l'IA en santé

L'IA et la cybersécurité sont indissociables. L'intégration croissante de solutions d'IA dans les systèmes d'information de santé accroît la surface d'attaque, à la fois par l'introduction de nouvelles zones exposées, mais également par le fait que les systèmes intégrés peuvent jouer un rôle d'ennemi intérieur. Les établissements de santé doivent adapter leurs infrastructures à ces nouveaux enjeux, former leurs équipes et adopter des standards de sécurité adaptés à ces nouveaux risques :

- Garantir intégrité, confidentialité et disponibilité des données, notamment via des environnements certifiés Hébergement de Données de Santé (HDS).
- Anticiper les risques liés à l'IA (biais algorithmiques, erreurs de prédiction, dépendance aux systèmes propriétaires, dérive des performances) et mettre en place des mécanismes de surveillance et de correction en temps réel.
- Associer tous les acteurs (professionnels, patients, industriels, chercheurs) à la définition des bonnes pratiques et des cadres éthiques, via des instances comme les Tiers-Lieux d'Expérimentation en santé numérique.

Le développement de l'IA en santé exige donc des fondations numériques solides : gouvernance des systèmes

d'information, protection des données, gestion des accès, continuité et reprise d'activité, sensibilisation des professionnels, prérequis relevant pleinement de la cybersécurité.

Les investissements engagés ces dernières années notamment dans le cadre du programme CaRE constituent un socle essentiel pour le déploiement maîtrisé et durable de l'intelligence artificielle au bénéfice des patients et des professionnels.

Vers une santé augmentée par l'IA et sécurisée par le cyber

L'IA et la cybersécurité ne sont pas des options, mais des nécessités pour répondre aux défis démographiques, économiques et sanitaires de notre époque. Le ministère de la Santé s'engage à structurer cette transformation avec rigueur, en plaçant l'humain au centre, les citoyens comme les professionnels.

Ce livre blanc, initiative du GT Cyber & IA en Santé , se veut un outil pour éclairer les décisions, orienter les actions et fédérer les énergies autour d'une ambition commune : une santé plus performante, plus équitable et plus résiliente, grâce à une IA maîtrisée, sécurisée et au service de tous.

DGRINES (Direction Générale de la Recherche, de l'Innovation et du Numérique En Santé)



PAULINE CHONE
Directrice de Projet
Stratégie IA en santé



CHRISTOPHE MATTLER
Directeur de Projet Cyber

ANS (L'Agence du Numérique en Santé)



ESTELLE NICAUD
Directrice de programme CaRE

CONTEXTE

01

POURQUOI CE LIVRE BLANC ?

Rendre visible l'intelligence artificielle pour mieux en maîtriser les usages

L'intelligence artificielle s'installe progressivement dans l'environnement numérique de la santé. Elle ne se présente pas toujours comme un projet autonome, clairement identifié et gouverné. Elle peut aussi apparaître au détour d'une mise à jour, d'un module complémentaire ou d'une nouvelle fonction activée par un éditeur. Le premier enjeu est donc de la rendre visible.

Une transformation déjà à l'œuvre

L'intelligence artificielle occupe une place croissante dans le secteur de la santé. Elle contribue à l'aide au diagnostic, à l'analyse d'images, à la recherche, à l'organisation des parcours, à la gestion administrative ou encore à l'assistance des professionnels. Ces usages peuvent apporter une réelle valeur lorsqu'ils répondent à un besoin identifié, qu'ils sont évalués et qu'ils s'inscrivent dans un cadre de confiance.

La transformation en cours est toutefois plus large que le seul déploiement de solutions explicitement présentées comme des outils d'IA. Des fonctionnalités algorithmiques ou génératives sont désormais intégrées aux logiciels métiers, aux outils bureautiques, aux plateformes collaboratives, aux services de communication et aux solutions proposées en mode SaaS. Leur arrivée peut être progressive et peu perceptible pour l'organisation utilisatrice.

Derrière un nouveau bouton ou une évolution d'interface peuvent pourtant se trouver de nouveaux traitements de données, le recours à des services tiers, des transferts ou des conditions d'utilisation différentes. La fonction ajoutée peut également modifier un processus métier, influencer une décision, créer une nouvelle dépendance ou transformer la répartition des responsabilités entre l'établissement, l'éditeur, l'hébergeur et d'autres prestataires.

Passer d'une IA constatée à une IA gouvernée

Ce constat place les directions d'établissements, les DSI, les RSSI, les juristes, les acheteurs, les professionnels de santé et les acteurs de l'innovation devant une même difficulté : comment identifier ce qui relève de l'IA dans un système d'information déjà complexe, comprendre ce que ces fonctions réalisent et décider dans quelles conditions elles peuvent être utilisées ?
La réponse ne peut pas être exclusivement technique. Elle suppose de croiser la sécurité des systèmes d'information, la protection des données de santé, la conformité juridique, la contractualisation, la gouvernance des usages, la supervision humaine, la continuité d'activité et la capacité de réversibilité. Elle implique également un dialogue plus structuré avec les industriels, les éditeurs et les prestataires.

Un livre blanc pour donner des repères communs

L'ambition de ce document n'est ni de freiner l'adoption de l'intelligence artificielle, ni d'en présenter une vision uniquement fondée sur les risques. Elle consiste à fournir des repères permettant aux organisations de prendre des décisions éclairées, proportionnées à leurs usages, à la sensibilité des données et aux conséquences possibles sur les activités de santé.
Le livre blanc vise ainsi à aider ses lecteurs à :

- repérer les fonctionnalités d'IA déjà présentes ou susceptibles d'être introduites dans les outils numériques ;
- qualifier les usages, les données mobilisées, les services tiers et les dépendances associées ;
- identifier les responsabilités et les exigences applicables à chaque étape du cycle de vie ;

- intégrer la cybersécurité, la conformité, la résilience et la réversibilité dès l'expression du besoin et la contractualisation ;
- organiser une supervision humaine adaptée et maintenir la maîtrise dans le temps ;
- favoriser un dialogue concret entre pouvoirs publics, structures de santé, professionnels, juristes, chercheurs, industriels et acteurs de l'innovation.

Une réalisation collective issue des écosystèmes

Ce livre blanc est né des réflexions conduites au sein du GT Corridor Cyber des EDIH France. Des enquêtes menées auprès de leurs écosystèmes par CYBIA, l'EDIH d'Île-de-France et l'EDIH Bretagne ont contribué à objectiver la perception des acteurs de terrain. Une première restitution de ces travaux a été réalisée lors de l'European Cyber Week 2025. Elle a confirmé le besoin d'un état des lieux partagé et de ressources permettant d'accompagner concrètement les organisations.

Dans leur prolongement, le GT Cyber & IA en Santé a rassemblé des acteurs aux responsabilités et aux expériences complémentaires. Cette pluralité constitue la méthode même du livre blanc : confronter les orientations institutionnelles aux réalités des établissements, les exigences juridiques et cyber aux contraintes industrielles, et les principes de gouvernance aux retours d'expérience opérationnels.

L'Agence Régionale de santé Bretagne (ARS) apporte une lecture institutionnelle et territoriale. Le Pôle d'Excellence Cyber contribue au contexte, à l'état des lieux et aux enseignements tirés des accompagnements de terrain, notamment dans le secteur médico-social. Biotech Santé Bretagne et Kereval éclairent les enjeux industriels ainsi que la cybersécurité des logiciels de santé et des dispositifs médicaux numériques pouvant intégrer de l'IA. Sopra Steria apporte l'analyse juridique nécessaire à la compréhension des responsabilités et des cadres applicables.
Les EDIH d'Île-de-France et des Hauts-de-France traduisent ces enjeux dans le champ de l'acquisition et de la contractualisation, au travers d'un clausier et d'un guide opérationnel appelés à évoluer avec les usages et le droit. Le Groupement Régional e-Santé Bretagne partage des retours d'expérience sur la protection des données avec le projet <BALISE>, ainsi que sur la continuité et la reprise d'activité au sein des établissements.
Ces contributions ne sont pas juxtaposées. Elles décrivent les différentes dimensions d'un même sujet et ont vocation à former un parcours cohérent : comprendre la diffusion de l'IA, mesurer la réalité du terrain, identifier les cadres applicables, sécuriser les produits et les achats, protéger les données, préparer la continuité des activités et faire vivre une gouvernance durable.

Une démarche utile, exigeante et évolutive

Le livre blanc ne crée pas une nouvelle doctrine et ne se substitue ni aux textes, ni aux référentiels, ni aux autorités compétentes. Il rassemble des analyses professionnelles et des expériences de terrain afin de proposer une lecture transversale et mobilisable. Les exigences devront être adaptées à la nature des usages, au niveau de risque, à la taille des organisations et à leurs capacités opérationnelles, sans réduire le niveau de protection attendu pour les données et les activités sensibles.



Parce que les technologies, les pratiques et les cadres évoluent, cette réflexion ne peut être figée. Le livre blanc doit être compris comme un point d'appui pour instaurer une culture commune et poursuivre le dialogue entre les acteurs. Son objectif est de permettre une intégration de l'intelligence artificielle à la fois utile, maîtrisée, sécurisée et responsable, au bénéfice des professionnels, des structures de santé et des personnes accompagnées.

MICHAEL BENOIT
Directeur de projet Cybersécurité & RSSI
Pôle d'Excellence Cyber

ETAT DES LIEUX

CONNAÎTRE LES ACTIFS D'IA AVANT DE POUVOIR LES MAÎTRISER

L'origine et objectif de l'enquête

Une enquête a été initiée par le Pôle d'Excellence Cyber à partir d'un constat partagé : l'intelligence artificielle s'intègre progressivement dans les logiciels métiers et les outils numériques de santé, parfois sans que cette évolution soit clairement identifiée par les établissements utilisateurs.

La question à l'origine de la démarche était donc volontairement simple : les établissements ont-ils conscience de la montée en puissance de l'IA dans leur environnement numérique et disposent-ils des informations nécessaires pour en maîtriser les usages ? Il s'agissait notamment d'évaluer leur capacité à identifier les fonctionnalités concernées, leur provenance, les données auxquelles elles accèdent, les pratiques des professionnels ainsi que les premières mesures de gouvernance et de sécurité mises en place.

Le questionnaire a été élaboré et travaillé collectivement dans le cadre du GT Cyber & IA en Santé. Sa diffusion a bénéficié de la mobilisation de l'UNA Bretagne, de l'Agence Régionale de Santé Bretagne et du Groupement Régional e-Santé Bretagne. Ces relais ont permis de recueillir les réponses d'établissements sanitaires et, plus largement, de nombreuses structures du secteur médico-social.

Cette enquête n'avait pas vocation à établir un classement des établissements ni à produire une mesure représentative de la situation nationale. Elle devait avant tout faire émerger des tendances, identifier les angles morts et confronter le constat initial à la réalité du terrain. Les résultats constituent ainsi un point de départ pour comprendre le niveau de visibilité dont disposent les organisations et les accompagner vers une meilleure connaissance de leurs actifs d'IA.

Le constat et les enseignements de l'enquête conduite auprès des établissements

L'intégration de l'intelligence artificielle dans le système d'information ne commence pas toujours par un projet formel. Elle peut résulter d'une fonction ajoutée à un logiciel métier, d'un service accessible depuis une suite collaborative ou d'un usage individuel adopté par un professionnel. L'enquête présentée ici cherche donc à répondre à une question préalable à toute démarche de sécurité : les établissements savent-ils où se trouvent leurs actifs d'IA, comment ils sont utilisés et quelles données ils mobilisent ?

Ce que l'enquête permet d'observer

Le questionnaire explore plusieurs dimensions complémentaires : présence déclarée d'IA dans les logiciels métiers, connaissance de sa provenance, information fournie par les éditeurs, identification des données de santé concernées, recours à des solutions externes, connaissance des usages des collaborateurs, analyse de risques, sensibilisation, encadrement interne et préparation à la gestion des incidents.

Les résultats ne constituent pas un inventaire technique des solutions déployées. Ils décrivent la capacité déclarée des organisations à voir et à gouverner leurs usages d'IA. Une réponse négative peut ainsi signifier l'absence d'un usage, mais aussi son manque de visibilité. Cette distinction est centrale pour interpréter les données.

NOTE MÉTHODOLOGIQUE

Le fichier comprend 71 saisies. Deux réponses manifestement destinées à tester le questionnaire, identifiées par les mentions « x » et « test » dans les champs de profil, ont été écartées. L'analyse porte donc sur 69 réponses exploitables, collectées entre avril et juillet 2026. L'échantillon est composé de 51 structures médico-sociales, 11 structures sanitaires et 7 structures mixtes. 65 répondants sont rattachés à la Bretagne. Les résultats sont exploratoires et ne doivent pas être extrapolés à l'ensemble des établissements français.

Des répondants majoritairement positionnés sur la gouvernance et le numérique

Le profil des personnes interrogées est une clé de lecture importante. Sur les 69 réponses exploitables, 29 proviennent de fonctions de direction générale ou de direction, soit 42 % de l'échantillon. Les fonctions SI, numériques ou de cybersécurité représentent 24 répondants, soit 35 %. Les autres réponses se répartissent entre les fonctions de soins ou d'encadrement métier (6), l'administration et la conduite de projets (6), ainsi que la qualité, la gestion des risques et la conformité (4).

Profil des établissements répondants

Un échantillon principalement médico-social et breton
69 réponses exploitables



Médico-social
51 répondants • 74 %

Sanitaire
11 répondants • 16 %

Structures mixtes
7 répondants • 10 %

Concentration régionale

65 répondants sur 69 sont rattachés à la Bretagne.

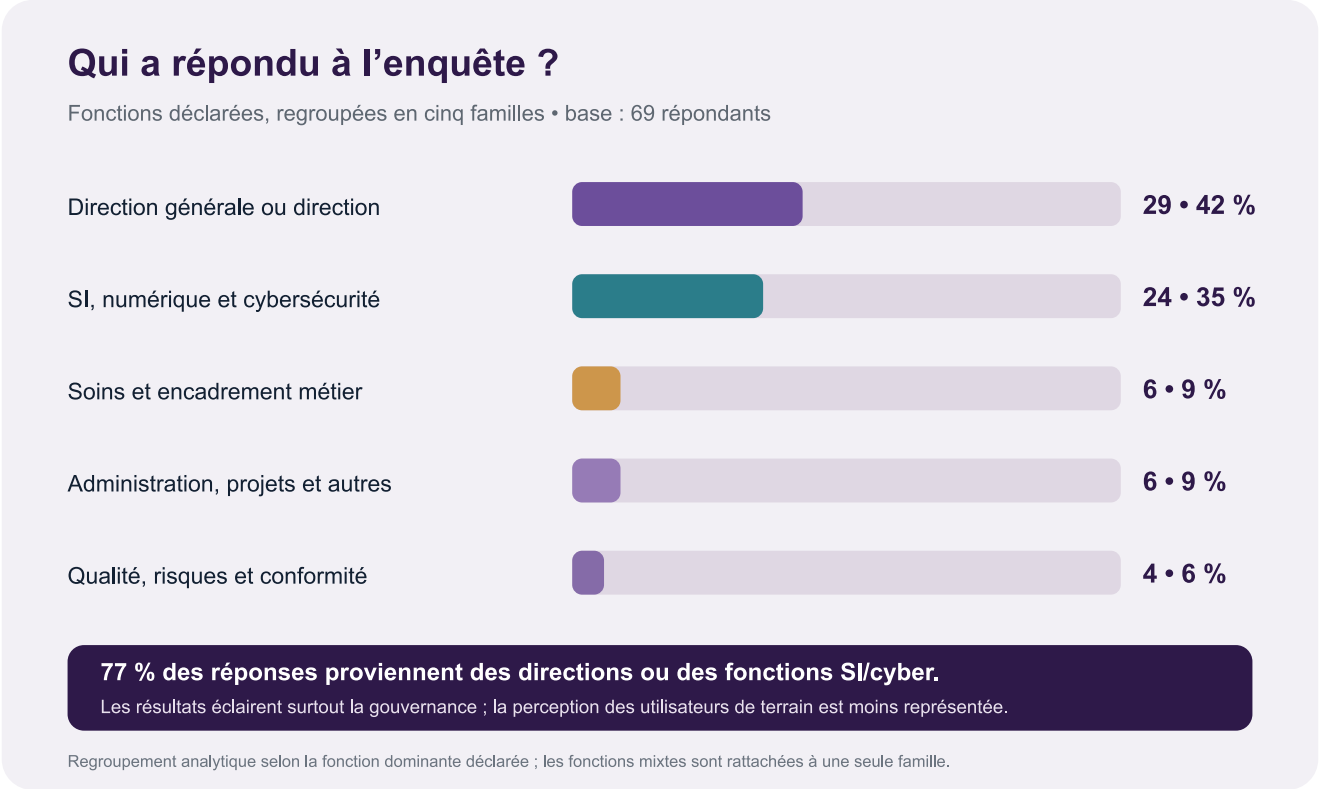
Précaution de lecture

Les comparaisons sectorielles sont indicatives et ne peuvent pas être généralisées à l'ensemble des établissements de santé français.

Source : enquête GT Cyber & IA en Santé, 2026. Deux saisies de test exclues.

Les directions et les fonctions SI/cyber représentent ainsi 77 % des répondants. L'enquête restitue donc principalement une perception de gouvernance, de pilotage et de maîtrise du système d'information. Cette composition est adaptée à l'objectif de connaissance des actifs, mais elle renseigne moins directement sur les pratiques quotidiennes des professionnels de terrain. L'absence ou la méconnaissance d'un usage déclaré par un responsable ne signifie pas nécessairement que cet usage n'existe pas dans les équipes.

Les réponses suggèrent par ailleurs un écart de visibilité entre fonctions. Parmi les répondants SI/cyber, 38 % identifient de l'IA dans les logiciels métiers, 54 % connaissent les usages des collaborateurs et 67 % déclarent une sensibilisation au moins ponctuelle. Parmi les répondants de direction, ces proportions sont respectivement de 21 %, 34 % et 28 %. Ces écarts ne permettent pas d'établir une causalité, mais ils montrent que la connaissance de l'IA demeure distribuée entre plusieurs niveaux de l'organisation. Un inventaire fiable doit donc croiser les informations des directions, des équipes SI et sécurité, des achats, des juristes et des métiers.



Constat n° 1 — L'IA est présente, mais sa cartographie demeure incertaine

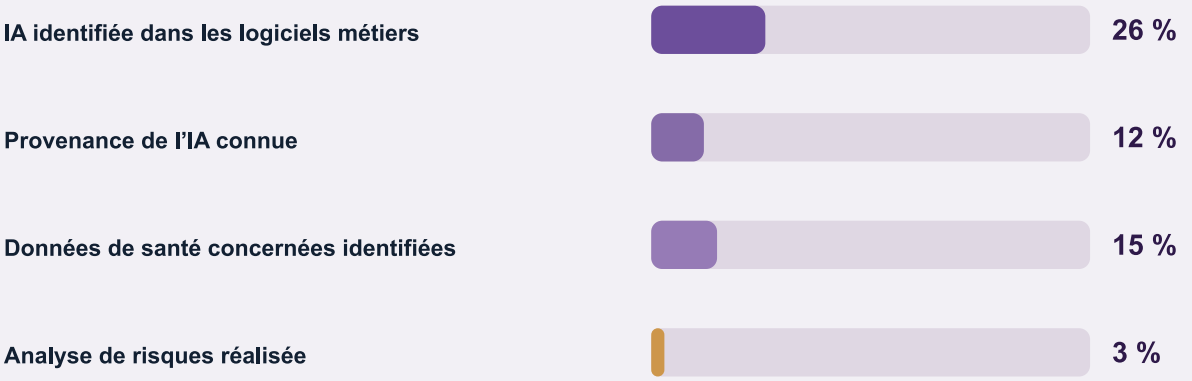
18 répondants sur 69, soit 26 %, déclarent utiliser des logiciels métiers intégrant de l'IA. 6 autres ne savent pas répondre à cette question. Cette proportion ne doit pas être lue comme une mesure de la diffusion réelle de l'IA : elle mesure d'abord ce que les répondants sont en capacité d'identifier.

Le niveau de connaissance diminue lorsque les questions deviennent plus précises. Seuls 8 répondants, soit 12 %, déclarent connaître la provenance de l'IA utilisée. 10 répondants, soit 15 %, indiquent avoir identifié les données de santé auxquelles les fonctions concernées accèdent. À l'inverse, 59 répondants, soit 86 %, répondent « non » ou « ne sait pas » sur ce dernier point.

Le principal enseignement n'est donc pas que les établissements utilisent peu l'IA. Il est qu'ils disposent rarement d'une vision consolidée leur permettant de relier une fonctionnalité à son fournisseur, à son modèle, à ses flux de données, à ses dépendances et à ses conditions d'exploitation.

Une connaissance encore incomplète des actifs d'IA

Part des répondants ayant répondu « oui » • base : 69 réponses exploitables



Identifier un usage ne suffit pas encore à garantir une maîtrise documentée.

Indicateurs complémentaires ; ils ne décrivent pas les étapes successives d'un même sous-échantillon.

Source : enquête GT Cyber & IA en Santé, collecte 2026.

Constat n° 2 — L'information fournie par les éditeurs ne permet pas encore de sécuriser la veille

La relation avec les fournisseurs apparaît comme un point de fragilité majeur. 38 répondants déclarent que leurs éditeurs ne les préviennent jamais de l'ajout de fonctions d'IA et 23 ne savent pas si une telle information est fournie. Au total, 61 répondants sur 69, soit 88 %, ne disposent donc pas d'une information identifiée et régulière. Une seule organisation déclare être informée systématiquement.

Ce résultat donne une portée concrète à la notion d'« IA peu visible ». Même lorsqu'un établissement organise une veille sur ses applications, il peut ne pas disposer d'un signal suffisamment clair pour déclencher une évaluation. Les notes de version, les conditions contractuelles, la documentation des sous-traitants et les mécanismes d'activation deviennent dès lors des sources essentielles de gouvernance.

Constat n° 3 — Les usages externes progressent plus vite que leur analyse

20 répondants, soit 29 %, déclarent utiliser des solutions d'IA externes. Les réponses libres citent notamment des assistants généralistes, des fonctions intégrées aux environnements collaboratifs et, plus ponctuellement, des usages liés à l'imagerie. Ces mentions décrivent des pratiques hétérogènes : elles ne permettent pas, à elles seules, de conclure que des données de santé sont effectivement transmises à ces services.

Le décalage avec l'analyse des risques est néanmoins marqué. Sur l'ensemble de l'échantillon, seuls 2 répondants déclarent avoir réalisé une analyse de risques liée à l'IA ; 66 répondent « non ». Parmi les 20 organisations déclarant utiliser une IA externe, 19 indiquent ne pas avoir réalisé cette analyse.

La connaissance des usages individuels reste elle aussi partielle : 26 répondants savent que leurs collaborateurs utilisent des outils d'IA, tandis que 25 ne savent pas se prononcer et 18 répondent par la négative. Or, parmi les 26 organisations qui connaissent ces usages, 19 déclarent ne disposer d'aucune charte ni mesure d'encadrement et 25 n'ont pas réalisé d'analyse de risques.

Usages et gouvernance : un décalage persistant

Part des 69 répondants • les réponses décrivent des niveaux de maturité distincts



IA externes : 19 utilisateurs sur 20 déclarent ne pas avoir réalisé d'analyse de risques.

Source : enquête GT Cyber & IA en Santé, collecte 2026.

Constat n° 4 — Des fondations cyber existent, mais elles sont encore peu transposées à l'IA

L'enquête ne décrit pas des organisations dépourvues de toute maîtrise numérique. 45 répondants déclarent avoir mis en place des mesures techniques de sécurité, 44 privilégier des solutions souveraines et 37 connaître les recommandations applicables. En matière de réponse aux incidents, 16 organisations disposent d'un plan et 25 indiquent qu'il est en cours d'élaboration, soit 59 % de l'échantillon.

Ces résultats contrastent avec les 3 % ayant réalisé une analyse de risques propre à l'IA. Le défi consiste donc moins à créer une gouvernance entièrement nouvelle qu'à étendre les mécanismes existants — inventaire, homologation, gestion des fournisseurs, analyse de risques, gestion des changements, journalisation, continuité et réponse aux incidents — aux particularités des systèmes d'IA.

Constat n° 5 — L'encadrement et la sensibilisation restent à structurer dans la durée

48 répondants, soit 70 %, déclarent ne disposer d'aucune charte ou mesure d'encadrement de l'IA. 21 signalent une charte dédiée, une disposition intégrée à la charte du système d'information, ou les deux. L'existence déclarée d'un document ne renseigne toutefois ni sur son périmètre, ni sur son appropriation, ni sur les contrôles associés.

La sensibilisation demeure majoritairement absente ou ponctuelle : 37 répondants n'ont jamais sensibilisé leurs équipes, 26 l'ont fait ponctuellement et seulement 3 indiquent une démarche systématique. Ce résultat appelle une approche continue, ciblée selon les métiers et reliée à des règles d'usage simples : données autorisées, outils approuvés, validation humaine, signalement des incidents et recours en cas de doute.

Une lecture différenciée selon les secteurs, à manier avec prudence

Les réponses sanitaires font apparaître une meilleure visibilité déclarée sur certains indicateurs : 7 structures sanitaires sur 11 identifient de l'IA dans leurs logiciels métiers et 6 sur 11 déclarent connaître les données de santé concernées. Dans le médico-social, ces proportions sont respectivement de 8 sur 51 et de 1 sur 51. La présence plus importante de fonctions d'IA dans certains environnements hospitaliers, mais aussi la disponibilité de compétences SI spécialisées, peuvent contribuer à cet écart.
Cette comparaison reste indicative. Les sous-échantillons sont de tailles très différentes et ne permettent pas d'isoler l'effet de la taille de l'organisation, de ses moyens, du rôle du répondant ou de la nature de ses activités. Elle conforte néanmoins le besoin d'un accompagnement proportionné, particulièrement pour les structures qui ne disposent pas d'une équipe SI ou cyber dédiée.

Ce que cet état des lieux invite à mettre en place

1. Rendre les actifs visibles
Créer un registre des fonctions d'IA, y compris celles ajoutées aux outils existants, et désigner un responsable de sa mise à jour.

2. Documenter les données et les flux
Identifier les catégories de données, les finalités, les destinataires, les lieux de traitement, les sous-traitants et les durées de conservation.

3. Organiser la relation éditeur
Exiger l'information préalable sur les nouvelles fonctions, les changements de modèle, les services tiers et les modifications contractuelles.

4. Encadrer les usages
Définir des outils autorisés, des règles accessibles, une supervision humaine et un processus simple de demande ou de signalement.

5. Étendre la gouvernance cyber à l'IA
Intégrer l'IA aux analyses de risques, à la gestion des changements, à la continuité d'activité, aux audits et aux exercices de crise.

CONSTAT

Les usages d'IA commencent à être perceptibles, mais ils ne sont pas encore systématiquement transformés en actifs gouvernés. L'enjeu prioritaire est de passer d'une connaissance fragmentaire, souvent dépendante des déclarations individuelles ou des informations éditeurs, à une capacité institutionnelle d'inventaire, d'évaluation et de décision.

Transition vers la suite du livre blanc

Cet état des lieux fournit le point de départ des contributions qui suivent. La visibilité des actifs conditionne en effet toutes les autres dimensions : application du droit, protection des données, sécurité des logiciels et dispositifs médicaux, rédaction des contrats, maîtrise de la chaîne de sous-traitance, continuité des activités et traitement des incidents. Sans inventaire ni responsabilité identifiée, l'organisation ne peut ni évaluer correctement les risques, ni dialoguer efficacement avec ses fournisseurs, ni démontrer la maîtrise de ses usages.



MICHAEL BENOIT
Directeur de Projet Cybersécurité & RSSI
Pôle d'Excellence Cyber.

LA CYBERSÉCURITÉ & LES STRUCTURES MÉDICO-SOCIALES : CE QUE L'EXPÉRIENCE NOUS APPREND

Si le GT « Cyber et IA en santé » est né d'un constat partagé entre partenaires du numérique en santé, il s'est aussi nourri, très concrètement, de la réalité du terrain. Dans le cadre du programme européen EDIH, le Pôle d'Excellence Cyber réalise des diagnostics de maturité cyber auprès d'organisations de la santé, notamment médico-sociales. Ces diagnostics ont pour objectif d'identifier les marges de progression des structures et de les accompagner pour se sécuriser. Derrière la maturité cyber du secteur médico-social se cache une disparité très marquée, corrélée à la taille de l'organisation et à l'existence, ou non, d'une équipe SI en interne. Les structures les moins matures peinent à s'emparer du sujet. Les exigences de sécurisation se multiplient et se durcissent, sans que les budgets ni les ressources internes ne suivent au même rythme. Surtout, la cybersécurité doit composer avec une autre priorité indiscutable dans le secteur médico-social : la qualité de la prise en charge et du soin des patients et des résidents. Face à des arbitrages permanents, les risques cyber sont parfois ignorés. Ce retour d'expérience « vue d'un auditeur » met en lumière les enjeux auxquels les structures médico-sociales sont confrontées.

Le premier constat, organisationnel, concerne la relation avec les prestataires d'infogérance. Une majorité des structures accompagnées n'a ni équipe SI interne, ni référent technique identifié. Le système d'information repose alors entièrement sur les prestations d'un infogérant, initiées par la direction ou collaborateurs sensibles au numérique mais sans compétence informatique. L'infogérance n'est pas en soi un problème : bien encadrée, c'est une réponse adaptée et légitime pour des organisations de cette taille. Ce qui interroge, en revanche, c'est la nature de cette relation. Dans la plupart des cas observés, il ne s'agit pas d'une délégation bien cadrée, mais d'une confiance totale et non questionnée. Les structures ne savent, la plupart du temps, ni ce que leur prestataire met réellement en œuvre en matière de sécurité, ni quels sont les engagements contractuels associés, ni comment vérifier que ce qui est annoncé est effectivement fait. Il n'y a pas de reprise en main possible du système d'information en cas de défaillance ou de rupture avec le prestataire, faute de contractualisation, de documentation, de cartographie ou même de compréhension basique de l'architecture en place. La structure a délégué la technique, mais elle a aussi, sans s'en rendre compte, délégué le pilotage. Elle ne garde plus la main sur son propre système d'information.

Cette situation se double d'un autre point faible : la sécurité n'est pas toujours perçue comme un axe prioritaire par les prestataires d'infogérance eux-mêmes. Ils ne sont pas toujours garant de la protection du système d'information. Les structures se reposent alors sur ce qui est mis en place « par défaut », qu'il s'agisse de l'absence de journalisation, de cloisonnement des réseaux, de veille des vulnérabilités, de sécurisation des accès ou encore de fiabilité des sauvegardes. Dans de nombreux contrats, les rôles et responsabilités en matière de cybersécurité restent insuffisamment définis entre la structure et le prestataire.

Le deuxième constat porte sur la gouvernance. Les actions engagées restent rarement formalisées, tracées ou pilotées dans la durée. Les procédures et politiques, lorsqu'elles existent, répondent souvent à des exigences de certification plus qu'à un usage réel, sans être nécessairement consultées au quotidien. Un exemple concret illustre bien cette absence de gouvernance : la gestion des entrées et sorties du personnel. Ce processus, pourtant élémentaire, n'est quasiment jamais formalisé dans les structures accompagnées. Lorsqu'un collaborateur quitte l'établissement, rien ne garantit systématiquement que ses accès soient révoqués, que ses droits sur les applications métier soient supprimés, ou que les actifs professionnels qui lui avaient été confiés (matériel, badges) aient été restitués. C'est un point d'entrée de risque, dans un secteur où le turn-over du personnel, notamment soignant, n'est pas négligeable.

Cette même logique de gouvernance défaillante se retrouve dans la sensibilisation. Un socle minimal a

généralement été mis en place. Le problème n'est donc pas l'absence totale d'action, mais son absence de suivi : pas de répétition dans la durée, pas de plan de sensibilisation à l'intégration d'un nouveau collaborateur, pas de mesure de son efficacité. Une session ponctuelle ne suffit pas à ancrer des réflexes durables face à des risques — phishing, ingénierie sociale, usurpation d'identité par email — qui restent, des menaces croissantes pour les structures.
La gestion des mots de passe illustre bien les limites de cette sensibilisation encore insuffisante. Les identifiants et mots de passe inscrits sur un post-it ou recensés dans un fichier en clair sont des pratiques dont les équipes ont généralement conscience du risque, mais qu'elles maintiennent faute d'alternative simple. Les gestionnaires de mots de passe suscitent un intérêt réel mais la conduite du changement auprès des collaborateurs aux mauvaises pratiques bien ancrées apparaît encore comme délicate.

Le troisième enjeu majeur concerne la gestion des incidents et la continuité d'activité. La plupart des structures disposent d'un plan bleu et ainsi d'une cellule de crise identifiée. Mais l'informatique n'y est, la plupart du temps, pas intégrée en tant que tel : un incident cyber majeur (rançongiciel, panne du SI) n'est pas anticipé comme le serait une crise sanitaire ou logistique.
Peu de structures connaissent l'existence du CERT Santé et la notion de PRIS (Prestataire de Réponse à Incident de Sécurité) reste, pour beaucoup, complètement inconnue. Des efforts significatifs restent à mener sur la rédaction de PCA et de PRA (plans de continuité et de reprise d'activité) pour mieux se préparer au risque cyber.

Enfin, la gestion des tiers constitue un angle mort quasi général dans l'approche cyber de ces structures. Le sujet est systématiquement sous-estimé : les structures affirment connaître leur écosystème de prestataires et de fournisseurs, mais aucune cartographie formelle n'existe, aucune évaluation des risques n'est menée sur ces points d'entrée pourtant potentiellement critiques. L'indisponibilité d'un prestataire doit également être anticipée dans le PCA/PRA.

Ce que nous recommandons :
1. Sensibilisation : de façon continue et planifiée, notamment à l'entrée d'un nouveau collaborateur;
2. Rédaction d'un PCA/PRA, en intégrant explicitement le risque cyber ;
3. Gestion des mots de passe robustes, notamment via un gestionnaire de mots de passe ;
4. Évaluation de la sécurité des fournisseurs, à commencer par le prestataire d'infogérance ;
5. Maitrise des droits d'accès, notamment dans le cadre des mouvements de personnel et de fin de contrat avec un prestataire.

Ce sont des mesures concrètes, accessibles, même à budget contraint qui s'appuient sur l'existant. C'est le message principal que porte ce retour de terrain : les petites structures médico-sociales ont besoin d'être accompagnées pour reprendre la main sur la sécurisation de leur système d'information et d'être soutenues — financièrement et méthodologiquement — dans une trajectoire de progression réaliste.
C'est aussi dans cette logique de progression, tournée vers un enjeu émergent, que s'inscrit l'analyse de l'article précédent : la sécurisation de l'usage de l'intelligence artificielle au sein des structures de santé.



CHLOÉ CHEMIN
Cheffe de projet Cybersécurité
Pôle d'excellence Cyber

DES ÉTABLISSEMENTS PRÉPARÉS À LA CRISE… MAIS PAS TOUJOURS À L'INDISPONIBILITÉ



En établissement de santé, la gestion des crises exogènes de type afflux massif de victime épidémie, canicule,… est ancrée depuis de nombreuses années. La réponse à une augmentation de la demande de soins est organisée : plan blanc, cellule de crise hospitalière, ré-organisation des services, exercices de crises, et dispositifs spécifiques (plan ORSAN, les ESR, les équipes zonales NRC…).

Les crises dites « endogènes » posent la problématique de l'indisponibilité de ressources. Elles se caractérisent par une diminution de la capacité de l'établissement à produire, à prendre en charge, à assurer son activité. Pénuries de médicaments, absentéisme, difficultés de recrutement, pannes majeures, défaillances techniques voire cyberattaques sont des situations régulières qui dégradent brutalement les capacités opérationnelles.
L'indisponibilité du système d'information ne touche pas uniquement l'informatique, elle vient perturber les processus métiers qui dépendent directement du numérique pour réaliser, tracer, coordonner ou sécuriser leurs activités. La question n'est donc pas seulement de savoir comment « remettre le SI en fonctionnement », mais bien « comment l'établissement continue à prendre en charge ses patients pendant cette indisponibilité », puis comment il organise le retour à la normale. C'est là tout l'enjeu du Plan de Continuité et de Reprise d'Activité (PCRA).

Un enjeu de pilotage avant d'être un enjeu méthodologique

Trop souvent, le sujet PCRA est confié à la direction des systèmes d'information, à la qualité, gestion des risques, sans que soient pleinement appréhendées par la gouvernance l'ampleur et la complexité du travail à conduire.
Construire un PCRA ne consiste pas à produire un document supplémentaire. La démarche nécessite d'identifier les activités critiques, de définir une stratégie d'établissement, de mobiliser les métiers, de décrire les solutions de continuité d'activité, de faire des arbitrages, de tester et de maintenir dans le temps. Elle demande donc du temps (méthodologique et métiers), des compétences, une coordination.

La question du « qui ? » est essentielle… qui pilote, qui coordonne, qui sollicite les métiers, qui arbitre les priorités, qui consolide les travaux et qui assure la mise à jour du PCRA ?

Le portage par la direction est donc déterminant pour donner à la démarche sa légitimité, dégager les ressources nécessaires et arbitrer les priorités. Le PCRA n'est pas un projet de la DSI : c'est un projet d'établissement, qui doit être porté comme tel.

D'une démarche documentaire, chronophage, à une démarche ludique et pragmatique

La construction d'un PCRA est souvent perçue comme une démarche complexe, chronophage et avant tout documentaire. Elle mobilise des professionnels déjà fortement sollicités et peut rapidement être vécue comme un exercice méthodologique supplémentaire, éloigné des préoccupations du quotidien et de surcroit abstrait.
La connaissance nécessaire à la construction du PCRA est avant tout détenue par les métiers. L'enjeu est donc de leur permettre de contribuer à la démarche sans les confronter directement à la complexité méthodologique. C'est avec ce prisme, et dans le cadre de ses missions d'accompagnement en cybersécurité, que le Groupement Régional e-Santé Bretagne a sollicité le prestataire Crisalyde, pour co-construire avec les établissements, une approche ludique, basée sur un jeu de cartes « contexte » et « activités ».

Pour réussir à consolider cette méthodologie pragmatique, le groupement a pu s'appuyer sur le concours de 13 établissements volontaires et représentatifs : public, privé, taille, activités cliniques …. Ainsi, à l'automne 2025 ce ne sont pas moins de 15 ateliers de travail (avec un atelier par processus métier : unité de soins, bloc opératoire, imagerie, laboratoire, RH, finances,…) et 180 professionnels qui ont contribué à la réalisation de 15 jeux de cartes.

Concrètement, le jeu permet de partir de situations concrètes, quotidiennes, métiers et de faire réfléchir collectivement les professionnels : que devons-nous continuer à faire ? Tout ou partie ? De quoi avons-nous besoin ? Avec qui ? Comment ? Pendant combien de temps ? L'enjeu ici est bien de répondre à la question : comment faire l'activité et non avec quel outil.

Les échanges permettent ainsi de faire émerger rapidement et naturellement les activités critiques, les ressources indispensables, les solutions de continuité et les interdépendances. La méthode reste présente, mais elle devient un support pour structurer les résultats plutôt qu'un préalable imposé aux métiers.

Le document n'est alors plus le point de départ de la démarche, mais le résultat d'une réflexion collective. Cette approche permet de rendre le PCRA plus accessible, plus concret et surtout davantage approprié par ceux qui auront à le mettre en œuvre. Par ailleurs, un document de synthèse pour la cellule de crise hospitalière est produit afin de faciliter le pilotage de la crise, notamment en projetant des difficultés de communication avec les services (absence de mail et de téléphone).

Et la prise en compte de l'IA ?

L'essor de l'intelligence artificielle invite à compléter la réflexion. Les systèmes d'IA deviennent progressivement des composants des processus métiers. Leur indisponibilité, comme celle d'une application « traditionnelle », doit être envisagée dans les dispositifs de continuité, d'autant qu'elle devient un élément grandissant des activités.
Il faut donc s'interroger sur les nouvelles dépendances créées par cette technologie, notamment sur la perte d'une capacité métier lorsque l'IA a pris en charge une partie de l'activité, par exemple pour l'interprétation de clichés en imagerie.

L'intelligence artificielle ne change donc pas le principe fondamental de la continuité d'activité. Elle élargit le périmètre des dépendances et solutions de continuité d'activités à prendre en compte.

Les enseignements

Préparer l'indisponibilité du système d'information ne consiste pas uniquement à prévoir des procédures papier ou à sauvegarder des données. La question essentielle est : *« Que sommes-nous capables de continuer à faire sans lui, comment et pendant combien de temps ? »*.

L'expérimentation conduite en Bretagne montre qu'une approche pragmatique, collaborative et ludique peut contribuer à rendre la démarche plus accessible aux métiers. En faisant des professionnels les acteurs de leur propre PCRA, elle permet de transformer progressivement un exercice documentaire abstrait en véritable démarche de résilience concrète et collective.

Le PCRA devient alors non plus seulement un plan que l'on possède, mais une capacité à continuer d'agir ensemble lorsque les outils habituels ne sont plus disponibles.



BÉRENGÈRE MADEC
Cheffe de projet cybersécurité
Groupement régional e-santé Bretagne

RÉGLEMENTATION DES DISPOSITIFS

03

CYBERSÉCURITÉ DES LOGICIELS EN SANTÉ ET DES DISPOSITIFS MÉDICAUX NUMÉRIQUES POUVANT INTÉGRER DE L'IA : COMPRENDRE LES EXIGENCES RÉGLEMENTAIRES

La transformation numérique du secteur de la santé s'accompagne d'une augmentation sans précédent des risques cyber. Les logiciels de santé, les dispositifs médicaux connectés, les applications mobiles et les plateformes d'échange de données constituent désormais des cibles privilégiées pour les cybercriminels. Cette évolution est d'autant plus préoccupante que les conséquences d'une attaque ne se limitent pas à une violation de données personnelles : elles peuvent affecter directement la continuité des soins, voire la sécurité des patients.

Face à cette menace, l'Union Européenne a profondément fait évoluer son approche réglementaire. La cybersécurité n'est plus considérée comme une fonctionnalité additionnelle mais comme une exigence intrinsèque à la conception, au développement et au maintien des produits numériques de santé. Les éditeurs de logiciels et les fabricants de dispositifs médicaux doivent désormais démontrer que leurs produits sont conçus selon des principes de « Security by Design » et qu'ils disposent de processus leur permettant de maintenir leur niveau de sécurité pendant toute leur durée de vie.

Cette évolution se traduit par un empilement de textes réglementaires qui poursuivent un objectif commun : renforcer la résilience numérique de l'écosystème de santé.

Une réglementation européenne qui se structure progressivement

L'Union Européenne a choisi de construire un cadre réglementaire cohérent dans lequel chaque texte répond à une problématique spécifique tout en venant compléter les autres.

La directive NIS2 constitue le socle de cette stratégie. Elle impose aux organisations considérées comme essentielles ou importantes de mettre en œuvre une gouvernance de la cybersécurité, de conduire des analyses de risques, de sécuriser leur chaîne d'approvisionnement et de notifier les incidents majeurs. De nombreux établissements de santé, laboratoires et industriels du secteur sont directement concernés par ces nouvelles obligations.

Le Cyber Resilience Act (CRA) poursuit une logique différente puisqu'il s'adresse non plus aux organisations mais aux produits comportant des éléments numériques. Son objectif est d'imposer des exigences minimales de cybersécurité dès la conception des produits, d'encadrer la gestion des vulnérabilités et de rendre obligatoire la fourniture de mises à jour de sécurité pendant une période adaptée au cycle de vie du produit.

À ces textes s'ajoute le règlement européen sur l'intelligence artificielle (AI Act). S'il s'agit avant tout d'un texte visant à encadrer les risques liés à l'intelligence artificielle, il comporte également, à travers son article 15, une exigence explicite de robustesse et de cybersécurité applicable à tout système d'IA à haut risque. Pour les logiciels de santé et les dispositifs médicaux intégrant des composants d'intelligence artificielle, cette exigence vient s'ajouter, sans s'y substituer, aux obligations cyber déjà imposées par le CRA et NIS2.

Parallèlement, l'Espace Européen des Données de Santé (EHDS) vise à favoriser le partage des données médicales

tout en garantissant leur confidentialité et leur intégrité. Cette initiative est complétée par eIDAS v2, qui renforce les mécanismes d'identification électronique et de signature qualifiée, devenus essentiels pour sécuriser les échanges entre professionnels de santé.
En France, l'Agence du Numérique en Santé (ANS) complète ce dispositif européen au travers de plusieurs référentiels structurants. Le référentiel d'interopérabilité et de sécurité définit les exigences applicables aux solutions numériques de santé, tandis que le référentiel HDS encadre l'hébergement des données de santé à caractère personnel. Le Référentiel d'Identification Électronique (RIE) précise quant à lui les mécanismes d'authentification devant être mis en œuvre au sein de l'écosystème numérique de santé.

Cette complémentarité entre réglementation européenne et référentiels nationaux conduit progressivement à l'émergence d'un cadre homogène dans lequel la cybersécurité devient un prérequis à la mise sur le marché.

Le cas particulier des dispositifs médicaux : une cybersécurité intégrée au marquage CE

Les dispositifs médicaux occupent une place particulière dans cet écosystème. Une vulnérabilité informatique peut en effet compromettre non seulement la confidentialité des données médicales mais également le fonctionnement du dispositif lui-même, avec un impact potentiel sur la sécurité du patient.

Le règlement européen relatif aux dispositifs médicaux (MDR 2017/745) impose déjà que les risques liés à la cybersécurité soient intégrés au processus global de gestion des risques. Les attentes des organismes notifiés sont principalement précisées au travers des guides publiés par le Medical Device Coordination Group (MDCG), et plus particulièrement du guide MDCG 2019-16, devenu la référence européenne en matière de cybersécurité des dispositifs médicaux.

Ce document introduit une approche fondée sur le cycle de vie du produit. Les fabricants doivent démontrer qu'ils identifient les menaces susceptibles d'affecter leur dispositif, qu'ils mettent en œuvre une architecture de sécurité adaptée, qu'ils assurent la protection des communications, qu'ils maîtrisent les mécanismes de mise à jour logicielle et qu'ils disposent d'un processus de surveillance post-commercialisation intégrant la gestion des vulnérabilités.

En pratique, la cybersécurité est désormais examinée au même titre que les performances cliniques lors de l'évaluation du dossier technique. Les organismes notifiés attendent une démonstration documentée des choix d'architecture, des analyses de risques, des tests de sécurité réalisés ainsi que des procédures permettant de maintenir le niveau de sécurité pendant toute la durée de vie du dispositif.
Cette évolution rapproche progressivement les exigences réglementaires européennes des meilleures pratiques déjà appliquées dans les secteurs de l'aéronautique ou de l'industrie critique.

Les éditeurs de logiciels en santé face à une nouvelle obligation de maturité

Pour les éditeurs de logiciels de santé, ces évolutions réglementaires modifient profondément les pratiques de développement. Il ne suffit plus de démontrer la conformité fonctionnelle d'une application ; il devient nécessaire d'apporter la preuve que la cybersécurité a été intégrée dès les premières étapes du projet.
Cette exigence se traduit par la mise en œuvre d'un cycle de développement sécurisé intégrant l'analyse des menaces, la définition d'exigences de sécurité, les revues de code, les tests d'intrusion, la gestion des dépendances logicielles et la surveillance continue des vulnérabilités après la mise sur le marché.

L'utilisation massive de composants open source renforce également les attentes des autorités. Les éditeurs doivent désormais être capables d'identifier précisément les bibliothèques intégrées à leurs logiciels au

travers d'un Software Bill of Materials (SBOM), devenu un élément central de la gestion des risques de la chaîne d'approvisionnement logicielle.

La cybersécurité n'est donc plus uniquement évaluée au moment de la livraison du logiciel ; elle s'inscrit désormais dans une démarche d'amélioration continue couvrant l'ensemble du cycle de vie du produit.

La FDA renforce les exigences des soumissions 510(k)

Les États-Unis ont engagé une évolution similaire avec la publication de la guidance Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. Cette guidance constitue désormais la référence pour les fabricants souhaitant obtenir une autorisation de mise sur le marché dans le cadre d'une procédure 510(k), De Novo ou PMA[1].

La FDA adopte une approche particulièrement exigeante. Les fabricants doivent démontrer que la cybersécurité est intégrée dans leur système qualité et fournir un dossier technique complet. L'autorité américaine accorde également une importance particulière à la capacité du fabricant à détecter, traiter et communiquer les vulnérabilités découvertes après la commercialisation. Les mécanismes de Coordinated Vulnerability Disclosure, longtemps considérés comme de simples bonnes pratiques, deviennent progressivement des exigences attendues lors de l'évaluation des dossiers.

Cette approche illustre une évolution majeure de la réglementation : la conformité ne s'arrête plus à la mise sur le marché, mais couvre désormais toute la durée de vie opérationnelle du dispositif.

Comment articuler réglementation, normes et bonnes pratiques ?

L'une des principales difficultés rencontrées par les éditeurs de logiciels en santé et les fabricants de dispositifs médicaux réside dans la coexistence de nombreux textes réglementaires et référentiels techniques. Le MDR, le Cyber Resilience Act, NIS2, l'AI Act, les guides du Medical Device Coordination Group (MDCG), les référentiels de l'ANS ou encore les exigences de la FDA poursuivent des objectifs complémentaires mais n'ont ni le même niveau juridique, ni le même périmètre d'application.

Il est essentiel de rappeler que les règlements définissent des objectifs de sécurité à atteindre, sans imposer les moyens techniques permettant d'y parvenir. Ce rôle est assuré par les normes harmonisées, les spécifications techniques et les guides de bonnes pratiques, qui constituent les référentiels sur lesquels les fabricants s'appuient pour démontrer la conformité de leurs produits.

Dans le cadre du marquage CE, le fabricant construit ainsi son dossier technique en démontrant que les exigences générales de sécurité et de performance du MDR sont satisfaites. Pour y parvenir, il s'appuie généralement sur l'ISO 14971 afin de structurer sa démarche de gestion des risques, sur l'IEC 62304 pour démontrer la maîtrise du cycle de développement logiciel et sur l'IEC 81001-5-1 pour apporter la preuve que la cybersécurité a été intégrée tout au long du processus de développement. Les recommandations du guide MDCG 2019-16 viennent ensuite préciser les attentes spécifiques relatives à la cybersécurité des dispositifs médicaux connectés, notamment en matière de modélisation des menaces, de défense en profondeur, de surveillance des vulnérabilités et de maintien en condition de sécurité après la mise sur le marché.

Pour les dispositifs médicaux intégrant des composants d'intelligence artificielle, cette logique s'enrichit encore avec l'AI Act, dont l'exigence de cybersécurité doit elle aussi s'appuyer sur des normes harmonisées, encore en cours d'élaboration par les organismes de normalisation européens (CEN/CENELEC). Les fabricants peuvent d'ores et déjà s'appuyer sur des référentiels internationaux existants tels que l'ISO 24971-2 (application de l'ISO 14971 aux dispositifs qui intègrent de l'IA), l'ISO/IEC 42001 (système de management de l'IA) ou l'ISO/IEC 23894 (gestion des risques liés à l'IA) pour structurer leur démarche, en complément des normes déjà mobilisées pour

la cybersécurité des dispositifs médicaux.

La logique est très proche dans le cadre d'une soumission 510(k) auprès de la FDA. La guidance Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions ne constitue pas une norme technique, mais un document décrivant les preuves attendues par l'autorité américaine. Le fabricant doit alors démontrer que son processus de développement sécurisé produit effectivement les éléments de preuve nécessaires à l'évaluation réglementaire. Ces éléments comprennent notamment une analyse des menaces, une architecture de sécurité documentée, les résultats des essais de cybersécurité, un plan de gestion des vulnérabilités ainsi qu'un Software Bill of Materials (SBOM). Les normes internationales servent alors de support méthodologique pour produire ces livrables de manière cohérente et reproductible.

Cette articulation entre réglementation et normes illustre une évolution majeure du secteur. Les autorités n'évaluent plus uniquement les caractéristiques techniques d'un produit, mais également la maturité des processus mis en œuvre par son fabricant. La capacité à démontrer l'existence d'un Secure Software Development Lifecycle (Secure SDLC), d'un processus de gestion des vulnérabilités, d'une gouvernance de la cybersécurité et d'une surveillance post-commercialisation devient ainsi un élément déterminant lors des évaluations réglementaires.

Dans ce contexte, les industriels les plus matures ne considèrent plus les normes comme une simple contrainte documentaire. Elles deviennent, au contraire, un véritable cadre méthodologique permettant de produire des preuves de conformité tout en améliorant durablement la sécurité des produits. Cette approche présente également un avantage stratégique : les mêmes livrables techniques peuvent être réutilisés pour répondre simultanément aux exigences du marquage CE, de la FDA, du Cyber Resilience Act ou encore des futurs référentiels européens relatifs aux produits numériques.

Conclusion

La cybersécurité est devenue un facteur structurant du développement des logiciels en santé et des dispositifs médicaux. Les exigences européennes, les attentes de la FDA et les normes internationales convergent désormais vers une même philosophie : intégrer la sécurité dès la conception, démontrer la maîtrise des risques tout au long du cycle de vie et maintenir un niveau de protection compatible avec l'évolution permanente des menaces.

Pour les éditeurs et les fabricants, cette évolution dépasse largement la simple conformité réglementaire. Elle impose une transformation des processus de développement, une collaboration étroite entre les équipes qualité, réglementaires et cybersécurité, ainsi qu'une capacité à produire des preuves techniques de plus en plus détaillées. Les industriels qui sauront intégrer ces exigences dès aujourd'hui disposeront non seulement d'un avantage compétitif lors des évaluations réglementaires, mais également d'un facteur de différenciation dans un marché où la confiance numérique devient indissociable de la sécurité des patients.



ALAIN RIBAULT
Directeur technique
Kereval en partenariat avec Biotech Santé Bretagne

UNE RÉPONSE À NOS ENJEUX COMMUNS



« PROJET <BALISE> UNE AVANCÉE COLLECTIVE POUR LUTTER CONTRE LES FUITES DE DONNÉES DE SANTÉ »

En 2025, plus de 2,6 milliards de données ont été compromises, plaçant la France parmi les pays européens les plus touchés[1]. Les établissements de santé sont en première ligne. L'enjeu dépasse aujourd'hui la seule détection des intrusions. Il s'agit d'assurer la protection des données de santé tout au long de leur cycle de vie et de leur parcours face à des menaces toujours plus nombreuses.
Face à ces enjeux, le projet <BALISE> apporte une réponse innovante et souveraine pour améliorer la détection et le repérage de fuites de données sensibles des structures de santé, via des dispositifs de marquage de la donnée.

Ce programme ambitieux, porté par le Groupement Régional e-Santé Bretagne et soutenu par de nombreux partenaires publics et industriels, avait été désigné lauréat d'un Appel à Manifestation d'Intérêt national (AMI) « sécuriser les territoires » opéré par la Banque des Territoires dans le cadre de France 2030[2].

Des données de santé toujours plus exposées : vers une approche globale de leur protection

Le secteur de la santé est régulièrement touché par des fuites de données d'ampleur nationale. Du fait de la nature sensible des données traitées, les structures de santé sont particulièrement vulnérables face à ces menaces. En effet, l'augmentation de la production de données de santé, la multiplication de leurs usages et leur circulation croissante, les exposent de plus en plus à ces risques.

Ce contexte, qui apparait anxiogène pour de nombreux patients, peut impacter la relation de confiance envers les acteurs de santé. Au-delà de cette perte de confiance, une fuite de données de santé peut exposer les patients à des risques de fraudes, de campagnes d'hameçonnage contextualisées, ou encore d'atteintes à leur vie privée liées à la divulgation d'informations médicales. Elle est également susceptible d'accroître la réticence des patients à consentir à la réutilisation secondaire de leurs données de santé à des fins de recherche, limitant ainsi le développement de projets de recherche médicale et d'innovation.

De par la variété de leurs natures, les fuites de données peuvent être complexes à détecter et repérer. La lutte contre les fuites de données peut s'effectuer en amont de la fuite (actions de prévention), en « temps réel » de la fuite (actions de blocage) ou en aval de la fuite (actions de repérage et d'analyse quant à son origine). Si les solutions de sécurité périmétriques actuellement déployées (EDR, NDR, etc.) constituent des dispositifs essentiels de protection, elles présentent néanmoins certaines limites. Leur capacité à détecter précocement les fuites de données demeure inégale. Elles offrent une visibilité parfois limitée sur l'identification des données ayant fuité et sur l'origine de ces fuites. Elles restent majoritairement centrées sur les systèmes et les infrastructures plutôt que sur les données elles-mêmes.

Face à ces constats, une approche de sécurité globale centrée sur la donnée s'impose. La prévention des fuites de données ne peut en effet se limiter à des mesures isolées. Elle exige d'agir sur l'ensemble du processus de

[1] Etat des lieux des fuites de données en 2025 [https://anozrway.com/fr/ressource/etat-des-lieux-des-fuites-de-donnees-en-2025/]
[2] Le projet <BALISE> a bénéficié d'un financement de l'État opéré par la Banque des Territoires dans le cadre du plan France 2030 [Logos]

gestion de ce risque : prévenir les situations à risque, détecter et bloquer les fuites dès leur survenue, repérer les données ayant fait l'objet d'une fuite et en retracer l'origine.

En renforçant la traçabilité des données de santé tout au long de leur cycle de vie et de leurs parcours entre acteurs de santé, le marquage des données constitue l'un des leviers innovants au service de cette approche.

Une mobilisation régionale des acteurs publics & privés



Pour concrétiser cette nouvelle approche, le Groupement Régional e-Santé Bretagne a fédéré plusieurs structures de santé bretonnes autour du projet <BALISE>, avec l'ambition de développer une réponse collective, innovante et souveraine aux enjeux de protection des données de santé.

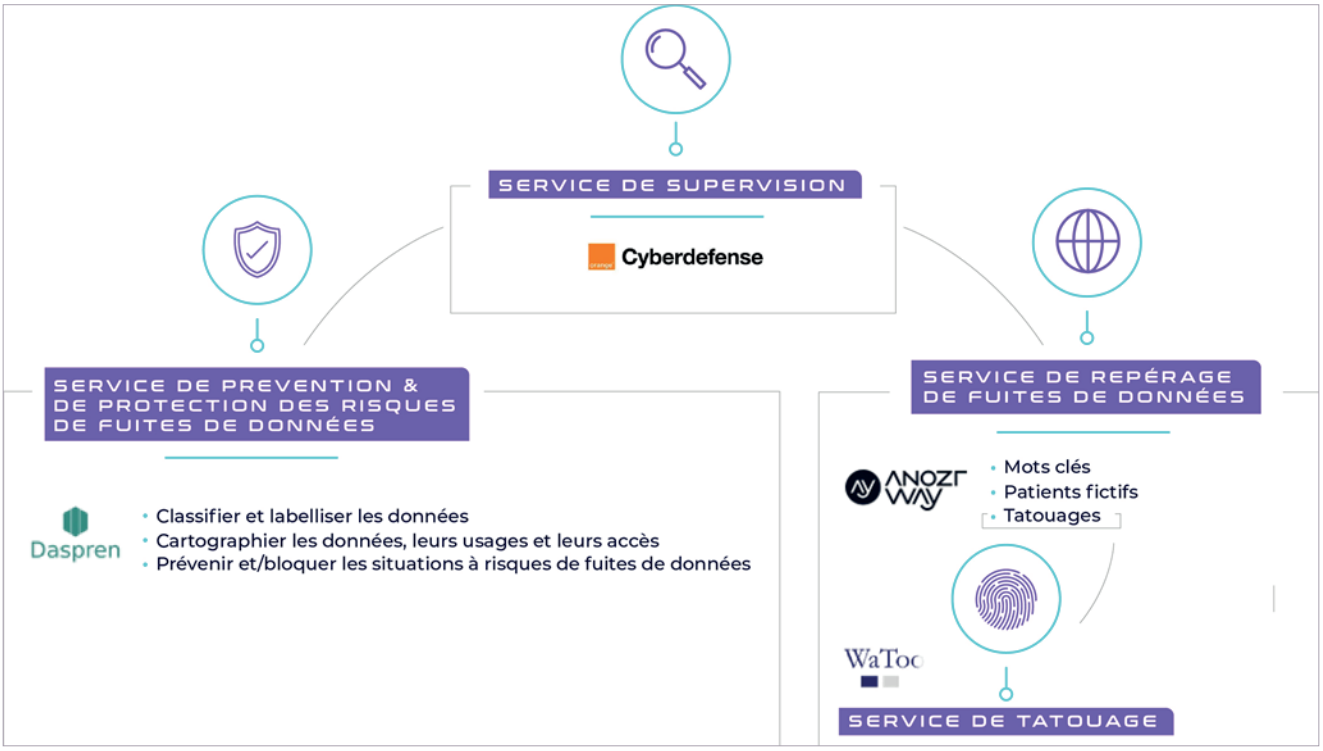
Soutenu par l'État dans le cadre de France 2030, ainsi que par l'Agence Régionale de Santé Bretagne, la Région Bretagne, Rennes Métropole et le Pôle d'Excellence Cyber, le projet s'appuie sur un écosystème réunissant établissements de santé, industriels et experts de la cybersécurité.

Sept établissements de santé bretons participent à l'expérimentation : le CHU de Brest, le CHU de Rennes, le Groupe Vivalto Santé, le Groupe Hospitalité Saint-Thomas de Villeneuve (HSTV), le GHT Armor, le GHT Brocéliande Atlantique et le GHT Rance Émeraude. Ils sont accompagnés par plusieurs partenaires technologiques : Orange Cyberdéfense, Anozr Way, Airbus Cybersecurity, Daspren et WaToo.

Un ensemble de services agissant sur l'ensemble du processus de gestion du risque de fuites de données

Le projet <BALISE> propose un ensemble de services agissant sur l'ensemble du processus de gestion du risque de fuites de données.

Schéma d'architecture <Balise>



Service de prévention & de protection des risques de fuites de données

Ce service repose sur quatre fonctionnalités complémentaires, mises en œuvre de manière continue pour renforcer la protection des données sensibles au sein des structures de santé :

- **Classifier et labelliser** : qualifier le niveau de sensibilité des données selon leur contexte d'utilisation et y apposer des <LABELS> afin d'adapter des mesures de protection ;
- **Découvrir et cartographier** : identifier les données sensibles, localiser leurs emplacements et analyser leurs usages, plus particulièrement les usages non maîtrisés[3] ;
- **Contrôler les accès** : vérifier que seules les personnes habilitées peuvent accéder aux données qui les concernent ;
- **Prévenir et protéger :** détecter en temps réel les situations à risque de fuites de données et y remédier, au moyen de messages de sensibilisation, de recommandations à destination des professionnels de santé ou, lorsque cela est nécessaire, de mécanismes de blocage avant qu'une fuite ne survienne.

Service de tatouage

En apposant des <TATOUAGES> numériques sur les documents de santé avant leur sortie des structures de santé, ce service garantit leur traçabilité tout au long de leurs échanges et partages. En cas de fuites de données

[3] **Transfert non autorisé de données de santé** vers un support de stockage personnel (clé USB, disque dur externe) ou un espace de partage cloud non sécurisé ;
Transmission de documents médicaux via une messagerie non sécurisée, par exemple l'envoi d'un compte rendu opératoire ou d'un dossier patient en pièce jointe ;
Utilisation d'une IA générative avec des données de santé, notamment l'intégration de comptes rendus médicaux ou d'autres informations sensibles dans un service d'IA non autorisé ;
Exfiltration de données sensibles par un acteur malveillant, à la suite d'une compromission de compte ou d'un accès non autorisé au système d'information ;
Copie ou extraction non maîtrisée de données par un prestataire ou un sous-traitant, en dehors du cadre contractuel ou des environnements sécurisés prévus à cet effet.

avérées, il permet de reconstituer le parcours de ces documents, d'en identifier rapidement l'origine et de faciliter les investigations nécessaires.
Dans le cadre du projet <BALISE>, le service de tatouage est intégré aux solutions d'interopérabilité des établissements de santé. À terme, ce service a vocation à être étendu à d'autres canaux de diffusion légitime de documents de santé, tels que les solutions de messageries ou de partages sécurisés de santé, ainsi que les applications de santé permettant le dépôt ou la mise à disposition de documents de santé.

Service de repérage de fuites de données

En complément de ces services, <BALISE> intègre un service dédié à la veille et à la surveillance continue du web. S'appuyant sur plusieurs moteurs d'analyse, ce service permet de repérer les fuites de données à travers le Darkweb et le Deepweb, d'identifier les informations sensibles exposées et de remonter les informations d'intérêts extraites de ces fuites.

Ce service mobilise trois mécanismes de détection complémentaires, conçus pour améliorer à la fois les capacités de repérage et d'identification de l'origine des fuites de données :

- **La surveillance par mots-clés** : détection automatisée dans les fuites de données de termes caractéristiques liés à l'établissement de santé (ex. nom, acronyme, domaine de messagerie, identifiants institutionnels FINESS, SIRET, etc.) ;
- **L'identification de <TATOUAGES> numériques** : tout document de santé préalablement tatoué numériquement et retrouvé dans des fuites de données est automatiquement identifié, permettant de retracer la chaîne de transmission et de disposer des métadonnées associées au document (ex. date d'envoi, producteur et destinataires du document, etc.) ;
- **Le repérage de <PATIENTS FICTIFS> :** des patients fictifs aux attributs uniques et ne pouvant être confondus avec des patients réels sont ajoutés dans les applications des structures de santé. Leur réapparition dans une fuite de donnée constitue un signal de compromission fiable, non ambigu et sans risque de faux positif.

Service de supervision

<BALISE> intègre un service de supervision (SOC) mutualisé, dédié au traitement continu des événements de sécurité et des fuites de données potentielles ou avérées. Intégré à l'ensemble des services du dispositif, le service de supervision remplit deux fonctions complémentaires.
D'une part, il centralise et corrèle les événements issus du service de prévention et de protection (par exemple un pic de volume de données extraites par un utilisateur ou un service sur une courte période, des tentatives de transferts non autorisés de données, etc.) afin de détecter des comportements suspects pouvant indiquer une fuite de données.

D'autre part, lorsqu'une fuite de données est détectée par le service de repérage, le service de supervision est automatiquement alerté afin d'en assurer l'analyse. Si la fuite contient des documents préalablement tatoués, il sollicite le service de tatouage pour récupérer les informations de traçabilité associées. Il dispose ainsi des éléments nécessaires pour qualifier l'incident, reconstituer le parcours des données ayant fuité, identifier les acteurs impliqués dans la chaine de transmission et formuler les recommandations de remédiation adaptées aux établissements de santé concernés.

Renforcer durablement la confiance dans le numérique en santé

La protection des données de santé n'a jamais été aussi complexe qu'aujourd'hui. La numérisation accélérée des parcours de soins, la multiplication des échanges de données entre acteurs impliqués dans la prise en charge des patients et l'ouverture croissante des systèmes d'information des structures de santé ont considérablement

élargi leur surface d'exposition aux risques de fuites de données. <BALISE> apporte une réponse collective, globale et mutualisée couvrant l'ensemble du processus de gestion des risques de fuites de données au service des acteurs de santé.

Mais cette complexité est appelée à s'accroître encore. L'irruption de l'intelligence artificielle dans les pratiques professionnelles du secteur de la santé introduit une nouvelle dimension de risques pour les données de santé. C'est précisément pour cette raison que l'approche centrée sur la donnée portée par <BALISE> (classification, cartographie, <TATOUAGE> numérique, <PATIENTS FICTIFS>, etc.) prend tout son sens dans un contexte de déploiement et d'utilisation de l'IA dans le secteur de la santé : elle s'applique à la donnée elle-même, indépendamment du canal ou de l'acteur — humain ou artificiel — par lequel elle est utilisée.

Au-delà de ces enjeux, <BALISE> contribue à l'émergence d'une offre française de cybersécurité dédiée à la protection des données de santé, en s'appuyant sur des solutions souveraines, intégrées et adaptées aux besoins des structures de santé. Le projet démontre également qu'une coopération étroite entre acteurs publics, établissements de santé et industriels constitue un levier essentiel pour renforcer durablement la confiance dans le numérique en santé.





BALISE

GILLES LARROCHE, Chef de projet Cybersécurité & DPO, Groupement Régional e-Santé Bretagne
YOHANN FOURCHON, RSSI & DPO, GHT d'Armor
EMERIC GUILLOU, RSSI, CHU de Rennes
ANTOINE HENNUY, RSSI, CHU de Brest & GHT Bretagne Occidentale
MARIE-LAURE KERVEGANT, DPO, GHT Brocéliande Atlantique
SÉBASTIEN LEBARBIER, RSSI, GHT Brocéliande Atlantique
Grégory LEMESTRE, RSSI Opérationnel, CHU de Brest
NICOLAS MILLEVILLE, RSSI & DPO, Groupe Hospitalité Saint-Thomas de Villeneuve
GILLES ROBERT, RSSI & DPO, GHT Rance Emeraude
Fabien VALLERIE, RSSI, Vivalto Santé

CONCLUSION

5

GARDER LA MAÎTRISE, SANS PERDRE L'ÉLAN

Faire de la confiance une construction collective

Au terme de ces travaux, une évidence s'impose : l'intelligence artificielle n'est plus une perspective lointaine pour le secteur de la santé. Elle est déjà présente, parfois clairement identifiée, parfois intégrée de manière plus discrète dans des outils utilisés chaque jour. La question n'est donc plus seulement de savoir si les organisations de santé auront recours à l'IA, mais de déterminer comment elles peuvent l'adopter sans perdre la maîtrise de leurs données, de leurs systèmes, de leurs décisions et, finalement, de leur mission.

Ce livre blanc est parti d'une interrogation très concrète : savons-nous réellement où se trouve l'IA dans nos organisations ? Les réponses recueillies montrent que cette connaissance reste encore fragmentaire. Des usages existent, des fonctions apparaissent, des professionnels expérimentent, mais l'inventaire, l'analyse des risques, l'information fournie par les éditeurs et l'encadrement ne progressent pas toujours au même rythme.

Ce décalage ne doit conduire ni au jugement ni à l'immobilisme. Les établissements de santé et les structures médico-sociales avancent dans un environnement particulièrement exigeant. Ils doivent assurer la continuité des soins et de l'accompagnement, répondre à des obligations croissantes, protéger des données parmi les plus sensibles et composer avec des moyens humains, techniques et financiers très différents. L'enjeu n'est pas de leur demander d'atteindre immédiatement un modèle théorique de perfection. Il est de leur permettre de reprendre la main, étape après étape, à partir de leur réalité.

La sécurité ne doit pas être ajoutée après coup

Les contributions réunies dans ce livre blanc convergent vers un même principe : la cybersécurité ne peut plus être considérée comme une vérification finale, menée une fois la solution choisie ou mise en service. Elle doit accompagner l'ensemble du cycle de vie, depuis l'expression du besoin jusqu'au retrait de la solution, en passant par la conception, l'achat, l'intégration, l'exploitation, les mises à jour et la gestion des incidents.

Pour les industriels et les éditeurs, cette exigence signifie concevoir des produits sûrs, maintenir leur niveau de sécurité dans le temps, documenter les choix réalisés et être en capacité de produire les preuves attendues. Pour les organisations utilisatrices, elle suppose de connaître leurs actifs, de comprendre les données et les flux concernés, de qualifier les dépendances et d'organiser une supervision adaptée. Entre les deux, le contrat doit devenir un véritable outil de maîtrise et de dialogue.

Le clausier et le guide opérationnel proposés dans le cadre de ces travaux donnent une traduction concrète à cette ambition. Ils ne constituent ni une réponse automatique ni une protection absolue. Ils fournissent un point de départ pour poser les bonnes questions, clarifier les responsabilités, définir les exigences essentielles et préparer la réversibilité. Leur valeur dépendra de leur appropriation par les acheteurs, les DSI, les RSSI, les juristes, les métiers et les fournisseurs, mais aussi de leur capacité à évoluer avec le droit, les technologies et les retours du terrain.

La confiance ne se décrète pas dans un document et ne s'obtient pas par une accumulation de clauses. Elle se construit par la connaissance, la transparence, la preuve, le dialogue et la capacité à agir lorsque la situation ne se déroule pas comme prévu.

Protéger la donnée, mais aussi la capacité à soigner

La protection des données de santé demeure au cœur de la démarche. Les travaux présentés autour de la détection et du repérage des fuites rappellent qu'une donnée doit pouvoir être protégée et suivie tout au long de son parcours, indépendamment de l'outil ou de l'acteur — humain ou artificiel — qui l'utilise. Cette approche centrée sur la donnée devient encore plus importante lorsque les chaînes de traitement se complexifient et font intervenir de nouveaux services ou sous-traitants.

Mais la maîtrise ne se limite pas à la confidentialité. Elle concerne également la disponibilité des outils et la capacité des professionnels à poursuivre leurs missions. À mesure que l'IA prend place dans les processus métiers, son indisponibilité, sa dégradation ou la perte d'une dépendance externe doivent être envisagées dans les plans de continuité et de reprise d'activité. La vraie question reste profondément opérationnelle : que sommes-nous encore capables de faire, ensemble, lorsque l'outil habituel n'est plus disponible ou ne peut plus être considéré comme fiable ?

Cette question remet les métiers au centre. La résilience ne se résume pas à un document technique. Elle repose sur une organisation connue, des arbitrages assumés, des solutions testées et des professionnels capables d'agir. Il en va de même pour l'intelligence artificielle : l'outil peut analyser, préparer, recommander ou structurer ; il ne doit pas effacer la compréhension du processus ni la capacité humaine à décider et à reprendre la main.

La responsabilité ne peut pas être déléguée avec la technologie
Une organisation peut externaliser une infrastructure, acquérir un logiciel, recourir à un hébergeur ou s'appuyer sur un prestataire spécialisé. Elle ne peut pas pour autant déléguer entièrement sa responsabilité. Celle-ci commence par la capacité à savoir ce qui est utilisé, pour quelle finalité, avec quelles données, selon quelles règles et sous le contrôle de qui.

C'est pourquoi le premier geste de gouvernance reste souvent le plus simple à formuler et le plus difficile à maintenir : établir un inventaire vivant. Non pas une photographie réalisée une seule fois, mais une démarche permettant de détecter les changements, d'interroger les mises à jour, de recueillir les usages des professionnels et de réévaluer les risques. Rendre visible ne signifie pas surveiller les équipes ou freiner leurs initiatives. Cela signifie créer un cadre dans lequel une expérimentation utile peut être discutée, accompagnée et sécurisée.

Une méthode collective avant d'être une réponse définitive
Ce livre blanc est aussi le résultat d'une méthode. Il a réuni des regards institutionnels, des acteurs de terrain, des spécialistes de la cybersécurité, des juristes, des industriels, des acteurs du numérique en santé et de l'innovation. Chacun a apporté une partie de la réalité. Aucun de ces regards, pris isolément, ne pouvait suffire.

Cette diversité explique la richesse des contributions : état des lieux des usages et de leur visibilité, retours du médico-social, exigences applicables aux logiciels et dispositifs médicaux, sécurisation des achats, protection et traçabilité des données, continuité d'activité et partage d'expériences. Elle rappelle surtout qu'une IA de confiance ne pourra pas être construite par une seule profession, une seule institution ou un seul fournisseur.

Le travail collectif ne consiste pas à effacer les contraintes ou les désaccords. Il consiste à les mettre autour de la même table, à distinguer ce qui est négociable de ce qui ne l'est pas, puis à construire des trajectoires réalistes. Les exigences doivent être suffisamment fortes pour protéger les personnes et les activités, mais également suffisamment comprises et opérationnelles pour pouvoir être appliquées. C'est dans cet équilibre que le dialogue entre établissements, pouvoirs publics, professionnels et offreurs de solutions prend tout son sens.

Faire vivre ce qui a été commencé

Ce document ne constitue pas un point d'arrivée. Les systèmes évoluent, les usages se transforment, les menaces changent et les cadres juridiques se précisent. Les outils proposés devront donc être confrontés à la pratique, enrichis par les établissements, discutés avec les fournisseurs et révisés lorsque cela sera nécessaire.

La suite se jouera moins dans la production de nouveaux principes que dans notre capacité à faire vivre ceux qui sont déjà posés : connaître, documenter, analyser, décider, contractualiser, tester, superviser, apprendre et partager. Cette progression peut commencer modestement. Un registre mis à jour, une question posée à un éditeur, une règle d'usage comprise par les équipes, une analyse de risques proportionnée ou un exercice de continuité constituent déjà des actes concrets de maîtrise.

La conviction qui demeure est profondément humaine

Dans la santé, la technologie n'a de valeur que si elle aide les professionnels à mieux exercer leur mission et si elle préserve la confiance des personnes soignées ou accompagnées. L'IA peut ouvrir des possibilités importantes. Elle ne doit ni rendre les responsabilités invisibles, ni éloigner les décisions de celles et ceux qui devront en assumer les conséquences.

Garder la maîtrise ne signifie donc pas renoncer à l'élan. Cela signifie choisir collectivement la direction, connaître les risques, préparer les réponses et rester capables d'agir. C'est à cette condition que l'intelligence artificielle pourra devenir non pas une transformation subie, mais une évolution comprise, sécurisée et réellement mise au service de la santé.



MICHAEL BENOIT
Directeur de Projet Cybersécurité & RSSI
Pôle d'Excellence Cyber.

MERCI À TOUS LES PARTENAIRES DU GT CYBER & IA EN SANTÉ

Partenaires du Corridor Cyber France

CYBIAH

EDiH GREEN POWER IT EUROPEAN DIGITAL INNOVATION HUB HAUTS-DE-FRANCE

EDIH EUROPEAN DIGITAL INNOVATION HUB BRETAGNE

Partenaires nationaux

HUB FRANCE IA

PÔLE D'EXCELLENCE CYBER

CITC DIGITAL INNOVATION HUB HAUTS-DE-FRANCE

Partenaires régionaux

Biotech Santé BRETAGNE

KEREVAL

ars Agence Régionale de Santé Bretagne

GROUPEMENT RÉGIONAL e-santé BRETAGNE

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org
02 23 06 10 30 | contact@pole-excellence-cyber.org