Compte rendu du Lundi de la Cybersécurité du 14 septembre 2026

Les enjeux de la médecine du futur autour de la data

Présenté par Cédric CARTAU

Organisé par Pr. Gérard Peliks, Béatrice Laurent et Pr. Ahmed Mehaoua
Rédigé par Rayan Al Mohaize, consultant en Cybersécurité

Table des matières

I Introduction

L'événement « Lundi de la Cybersécurité » est une série mensuelle de conférences en ligne organisée de manière indépendante par Gérard Peliks, Béatrice Laurent et Pr. Ahmed Mehaoua. Elle a pour vocation d'explorer chaque mois une thématique différente liée aux enjeux contemporains de la sécurité numérique et de la société.

1 Les intervenants

Pour animer ce Lundi de la Cybersécurité, **Cédric CARTAU**, responsable de la sécurité des systèmes d'information et délégué à la protection des données du CHU de Nantes et du GHT44, nous a fait l'honneur de partager avec nous son expérience au sein du domaine médical pour nous en présenter les grands enjeux de cybersécurité.

Par la suite, **Claire ALBERIO**, membre du CA de l'ARCSI, et par ailleurs Directrice Cybersécurité chez ORANGE Ile de France, nous a présenté le Groupe Jeunes de l'ARCSI, pour le quart d'heure des associations.

2 Le thème de la sécurité des données dans le secteur de la santé

Le Lundi de la Cybersécurité du 14 septembre 2026 portait sur les enjeux de la médecine du futur autour de la data. Lors de ce webinaire, Cédric Cartau a défendu une idée centrale : la donnée est devenue la matière première de la médecine, au point que soigner revient de plus en plus à traiter de l'information. Cette dépendance ouvre des perspectives considérables, mais elle fait aussi de la donnée de santé une cible de choix et un enjeu de souveraineté, de conformité et d'éthique.

II Les enjeux de la médecine du futur autour de la data (par Cédric CARTAU)

La médecine du futur repose sur l'agrégation de données toujours plus massives et plus hétérogènes. La donnée est devenue la matière première de la pratique médicale, ce qui crée une dépendance croissante à son égard. Cette évolution soulève plusieurs préoccupations majeures, qui correspondent aux grands principes de la sécurité de l'information : la disponibilité, l'accessibilité, l'intégrité et la confidentialité des données. Ces exigences entrent d'ailleurs en tension les unes avec les autres, car plus une donnée est accessible, moins elle est confidentielle, et inversement, plus elle est protégée, moins elle est facile d'accès. Tout l'enjeu consiste donc à trouver le bon équilibre entre ces deux impératifs.

1 Les évolutions de paradigme en santé

Pendant longtemps, la médecine a reposé sur la relation entre les hommes et les dieux, la maladie comme la guérison étant attribuées à des décisions divines. Jusqu'en 1895, date de la découverte des rayons X par Wilhelm Röntgen, l'imagerie médicale relevait de la science-fiction : observer l'intérieur du corps sans l'ouvrir paraissait tout simplement inconcevable. Dans les années 1950, l'apparition des centres hospitaliers universitaires a

favorisé le développement de la pluridisciplinarité, et l'on a pris conscience de l'importance de la donnée.

Est ensuite venue l'ère du big data, grande révolution qui a précédé celle de l'intelligence artificielle. L'exploitation de volumes massifs de données a permis des analyses médicales plus poussées, et la donnée s'est progressivement imposée au cœur de la prise en charge des patients. L'IA a pris le relais et occupe désormais une place importante dans de nombreux domaines de la médecine. Ses modèles étant entraînés sur des quantités de données toujours plus grandes, certains considèrent aujourd'hui que la prise en charge médicale se résume à du traitement de données.

2 Cadre & contexte : pourquoi la data devient le cœur de la médecine

La donnée constitue une véritable matière première, et la médecine de demain reposera sur son agrégation massive. Or la donnée de santé figure parmi les plus sensibles qui soient : le RGPD la range d'ailleurs dans les catégories particulières de données, dont le traitement est en principe interdit sauf exceptions strictement encadrées.

Toute la difficulté réside donc dans l'arbitrage entre la valorisation de ces données et l'impératif de confidentialité. Pour entraîner un algorithme d'IA, il est nécessaire d'y injecter des données de santé qui peuvent être pseudonymisées, c'est-à-dire dont les identifiants directs comme le nom ont été remplacés, mais jamais véritablement anonymisées. Contrairement à l'anonymisation, qui rend toute réidentification impossible, la pseudonymisation laisse subsister un lien possible avec la personne concernée, et les données restent donc soumises au RGPD.

3 Les grands usages de la médecine du futur

3.1 IA et aide au diagnostic

Parmi les usages dits tactiques, on retrouve tout ce qui relève de la prise en charge directe du patient, et en premier lieu le diagnostic. C'est dans ce domaine que se développent les outils d'aide au diagnostic fondés sur l'IA, capables notamment de lire des images médicales ou d'analyser des examens de scanner et d'IRM. Ces outils restent toutefois entièrement dépendants de la qualité des données qui les alimentent : dès lors qu'une donnée n'est pas fiable, les capacités de l'outil et les usages qu'on peut en faire s'en trouvent limités. Un algorithme entraîné ou alimenté avec des données erronées ou incomplètes produira en effet des résultats eux-mêmes peu fiables.

3.2 Médecine personnalisée, prédictive et génomique

Le séquençage à grande échelle d'un très grand nombre de génomes permet de détecter, à l'échelle d'une population, l'apparition de certaines pathologies. Il ouvre la voie à une médecine de précision, capable de prédire la réponse d'un patient à un traitement.

Cette approche comporte cependant un risque majeur : la discrimination génétique. Si une information génétique révèle une prédisposition à une pathologie future, elle pourrait

conduire à priver une personne de certains droits, comme l'accès à une assurance ou à un emploi. Le film Bienvenue à Gattaca illustre bien ce danger, en dépeignant une société où les individus sont classés selon leur patrimoine génétique.

3.3 Jumeau numérique du patient

Le principe du jumeau numérique consiste à numériser un individu, en injectant dans un modèle l'ensemble de ses caractéristiques physiologiques. Il devient alors possible de simuler des traitements ou des protocoles sur cette réplique virtuelle, sans avoir à les tester directement sur le patient. Ce concept ne se limite pas à la santé et se développe dans de nombreux domaines, mais il repose partout sur la même condition : sans données, rien n'est possible.

3.4 Santé connectée & objets médicaux connectés (IoMT)

Des capteurs sont déjà intégrés dans de nombreux objets du quotidien, comme les montres, les écouteurs ou les balances. Pourtant, l'Internet des objets médicaux (IoMT, pour Internet of Medical Things) est encore loin d'avoir atteint son plein potentiel, et cette technologie est appelée à se développer considérablement. Cette expansion s'accompagne néanmoins de risques importants : 75% des pompes à insuline présenteraient des vulnérabilités exploitables, ce qui ouvre notamment la possibilité d'une prise de contrôle à distance de ces dispositifs.

3.5 Télémédecine et parcours de soins numérique

La télémédecine recouvre déjà de nombreux outils : l'application Mon espace santé, qui intègre le Dossier Médical Partagé (DMP), les consultations en visioconférence, ou encore les cabines de téléconsultation installées dans certaines gares SNCF. Selon l'intervenant, la manière dont se déroulent les consultations devrait profondément évoluer d'ici une dizaine d'années. La télémédecine représente également un levier important pour lutter contre les déserts médicaux, en permettant aux patients éloignés des professionnels de santé d'accéder plus facilement à des soins.

3.6 Autres usages de la médecine du futur

Certains usages se situent à la frontière de la réglementation. L'intervenant a pris l'exemple d'une personne chez qui l'on détecte une maladie génétique incurable. Sa fille a 70% de risque de développer à son tour cette maladie, mais le médecin ne peut pas la prévenir, car cela reviendrait à lui communiquer des informations issues du génome de son parent.

Au-delà du diagnostic, la donnée intervient aussi dans le champ tactique, c'est-à-dire dans tout ce qui entoure la prise en charge du patient. Le CHU de Nantes a ainsi mis en place une « clinique des données » : les données du patient y sont analysées afin d'éclairer les décisions médicales, par exemple sur les médicaments à prescrire ou à éviter. Cet outil constitue un véritable support pour les consultations.

Le champ stratégique concerne quant à lui l'organisation des filières de soins. La filière mère-enfant, par exemple, accompagne la mère et l'enfant pendant la grossesse, lors de

l'accouchement et après la naissance. L'analyse des données issues de cette filière permet d'adapter l'offre de soins à l'échelle d'un département ou d'une région. Enfin, les données de santé sont également exploitées dans les études épidémiologiques, notamment pour détecter l'apparition d'épidémies.

4 Sécurité de la donnée de santé

4.1 État de la menace

Selon l'ANSSI, la santé est le troisième secteur le plus touché par les cyberattaques. Sur les 1 366 incidents traités par l'agence en 2025, les principales menaces qui pèsent sur ce secteur sont :

- les fuites de données ;
- les rançongiciels ;
- la compromission de comptes ;
- l'exploitation d'accès à distance mal sécurisés ;
- les attaques par la chaîne d'approvisionnement (supply chain), qui visent un prestataire pour atteindre sa cible.

Ce dernier mode opératoire a été illustré de façon concrète fin mars 2026 : une cyberattaque menée via le serveur d'un prestataire externe a permis de dérober des données particulièrement sensibles, notamment des états civils, des identifiants de connexion, des comptes rendus d'analyses médicales et des numéros de sécurité sociale.

4.2 Pourquoi le secteur est vulnérable

Plusieurs facteurs expliquent la vulnérabilité particulière du secteur de la santé. Le premier tient à son parc informatique, extrêmement hétérogène, parfois très ancien voire obsolète, et donc difficile à maintenir à jour et à corriger.

Le deuxième réside dans la complexité de la chaîne de sous-traitance : chaque prestataire constitue un maillon supplémentaire, et il suffit qu'un seul soit faible pour fragiliser l'ensemble.

Enfin, la surface d'attaque est démultipliée par la nature même de l'activité hospitalière. Un hôpital doit nécessairement s'ouvrir sur l'extérieur et sur Internet pour échanger avec les patients, les professionnels et les partenaires, faute de quoi il ne peut pas assurer correctement les soins. Cette ouverture indispensable l'expose d'autant plus aux menaces.

4.3 Les enjeux de confidentialité

Déterminer qui peut accéder aux données de santé constitue une problématique particulièrement complexe. En réalité, de nombreuses personnes y ont accès dans le cadre de la prise en charge d'un patient : pharmaciens, infirmiers, professionnels paramédicaux ou encore juristes. À cela s'ajoute le domaine de la recherche, où les chercheurs exploitent également ces données. Celles-ci sont alors pseudonymisées, mais jamais anonymisées, ce qui laisse subsister un risque de réidentification.

Pour faire face à ces enjeux, plusieurs leviers réglementaires existent ou se mettent en place.

— La directive européenne NIS2 sera appliquée au secteur de la santé, en imposant aux établissements des obligations renforcées en matière de cybersécurité.
— Le Cyber Resilience Act, autre texte européen, va quant à lui responsabiliser les fournisseurs et les prestataires en exigeant un niveau de sécurité minimal pour les produits numériques qu'ils mettent sur le marché.
— Enfin, les organismes qui hébergent des données de santé doivent obtenir la certification HDS (Hébergeur de Données de Santé), qui garantit le respect d'exigences strictes de sécurité.

5 Souveraineté & hébergement des données

La souveraineté en matière d'hébergement des données représente aujourd'hui l'un des enjeux les plus importants, en France comme en Europe. Une grande partie des infrastructures numériques, et notamment des services de cloud, est détenue par des acteurs étrangers, principalement américains. Cette situation crée une forte dépendance technologique et expose les données à des législations qui ne relèvent pas du droit européen.

L'affaire de l'hébergement du Health Data Hub en est une illustration très interessante. Créée en 2019, cette plateforme a pour mission de centraliser les données de santé des Français afin de faciliter la recherche. Son hébergement a été confié à Microsoft sans véritable mise en concurrence, ce qui a suscité de vives critiques, notamment de la part de la CNIL et de plusieurs acteurs du numérique. En 2020, l'invalidation par la justice européenne de l'accord encadrant les transferts de données vers les États-Unis (le Privacy Shield) a renforcé ces inquiétudes, et le gouvernement s'est engagé à migrer la plateforme vers une solution souveraine, une transition qui s'est révélée longue et difficile à mettre en œuvre.

Dès lors que des données sont confiées à un hébergeur américain, elles peuvent tomber sous le coup de lois extraterritoriales comme le Cloud Act, qui permet aux autorités des États-Unis d'exiger d'une entreprise américaine l'accès aux données qu'elle héberge, y compris lorsque celles-ci sont stockées en Europe.

6 Cadre réglementaire & gouvernance

L'AI Act, le règlement européen sur l'intelligence artificielle, va s'appliquer aux systèmes d'IA considérés comme « à haut risque », une catégorie dans laquelle entrent les dispositifs médicaux intégrant de l'IA.

De son côté, l'EHDS (Espace européen des données de santé) vise à simplifier la recherche en facilitant l'agrégation et le partage des données de santé des citoyens européens, mais cette mise en commun accroît mécaniquement les risques.

Les établissements de santé font ainsi face à un véritable empilement réglementaire :

— RGPD
— NIS2
— AI Act

— Cyber Resilience Act
— règlements européens sur les dispositifs médicaux (MDR) et sur les dispositifs de diagnostic in vitro (IVDR)
— EHDS

Se conformer à l'ensemble de ces textes représente un enjeu majeur et une charge considérable pour les établissements.

7 Impacts éthiques & sociétaux

La question du consentement est au cœur des enjeux éthiques. Celui-ci doit être éclairé, mais aussi dynamique, c'est-à-dire pouvoir évoluer dans le temps et être retiré à tout moment. Il doit également couvrir la réutilisation secondaire des données, notamment à des fins de recherche. Reste à savoir comment rendre ce consentement réellement effectif lorsque les patients ne comprennent pas précisément quelles données sont collectées ni comment elles seront utilisées.

Les biais algorithmiques posent un autre problème majeur, avec le risque d'aggraver les inégalités de santé. Certains algorithmes ont en effet été entraînés sur des jeux de données composés essentiellement de patients occidentaux, ce qui biaise leur apprentissage et peut conduire à des discriminations envers les populations moins représentées, par exemple des diagnostics moins fiables.

Enfin, se pose la question de la responsabilité : lorsqu'un médecin suit l'avis d'une IA et que celui-ci se révèle erroné, qui doit être tenu pour responsable ?

8 Approche systémique : la vision au prisme de la 27001

La norme internationale ISO 27001 définit les exigences d'un système de management de la sécurité de l'information (SMSI), c'est-à-dire un cadre permettant à une organisation de piloter et d'améliorer en continu la protection de ses informations. L'une de ses premières étapes consiste à identifier les parties intéressées, comme les patients, les soignants, les prestataires ou les autorités, puis à déterminer leurs attentes et leurs enjeux. Appliquée au secteur de la santé, cette approche conduit toutefois à parler plutôt d'un système de management des données de santé, afin de placer la donnée elle-même au centre de la démarche.

9 Conclusion

À qui appartient la donnée de santé ? La question paraît simple, mais la réponse l'est beaucoup moins.

On pourrait d'abord penser qu'elle appartient au patient. Pourtant, si celui-ci demande à un établissement de supprimer ses données de santé, l'établissement ne le fera pas. Or, si nous ne disposons d'aucun moyen d'action sur nos données, c'est bien qu'elles ne nous appartiennent pas.

Faut-il alors considérer qu'elles appartiennent à l'établissement de santé ? Pas davantage, puisque celui-ci ne peut les supprimer qu'avec l'accord de l'État.

On pourrait donc en conclure qu'elles appartiennent à l'État, seul habilité à décider de leur sort à l'issue du délai légal de conservation. Mais là encore, la réponse ne tient pas. Chacun d'entre nous bénéficie aujourd'hui des données médicales de nos ancêtres et des connaissances acquises, parfois au prix d'expérimentations, sur les patients des générations passées.

Nos données de santé n'appartiennent ainsi ni à nous-mêmes, ni aux établissements de santé, ni à l'État : elles appartiennent aux générations futures.

Reste alors une question ouverte : les médecins de demain vont-ils devenir des « fermiers de la donnée », réduits à exécuter ce qu'une super-IA leur dictera de faire ?

III Présentation du Groupe Jeunes de l'ARCSI (par Claire ALBERIO)

Le Groupe Jeunes de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information) a pour vocation de sensibiliser les jeunes générations au chiffrement en les attirant par le jeu. L'idée est de capitaliser les connaissances et de les transmettre au plus grand nombre, en montrant aux jeunes que les mathématiques peuvent être amusantes et qu'ils ont toute leur place dans ce domaine. À leur tour, ils pourront ensuite sensibiliser les générations suivantes.

Pour cela, le groupe a conçu des ateliers pédagogiques regroupés dans La Boîte à Crypto, accessible sur le site de l'ARCSI : `https://www.arcsi.fr/la-boite-a-crypto.php`

Claire Alberio en a présenté plusieurs exemples, comme l'alphabet Herbin ou le cadran d'Alberti, qui proposent des exercices de cryptographie ludiques et pédagogiques adaptés à tous les âges, des plus jeunes enfants jusqu'aux lycéens. Ces ateliers sont libres d'utilisation pour toute personne souhaitant animer des séances dans des écoles, lors de forums ou d'autres événements.

IV Questions / Réponses

Est ce que la transposition NIS2 pourra aider les CHU à se mettre à niveau et à avoir plus de budget ? Et est ce que le retard de cette transposition est un risque ?

Selon Cédric Cartau, la directive NIS2 ne sera d'aucune utilité tant qu'elle ne s'accompagnera pas de financements permettant de résorber la dette technique des établissements, dans un contexte où cette dette ne cesse de croître.

REMARQUE : L'ANSSI n'a pas les compétences requises en cybersécurité.

Cédric Cartau s'est dit en désaccord avec cette remarque : selon lui, l'ANSSI dispose au contraire de très bonnes compétences en cybersécurité, et le problème tient plutôt à la marge de manœuvre qu'on lui laisse. Il cite l'exemple de la faille IDOR de l'ANTS, qui était parfaitement connue de l'ANSSI. La difficulté venait des prises de décision : l'attaque de l'ANTS relève donc moins d'un sujet technique que d'un sujet managérial. Cédric Cartau ajoute qu'il en va peut-être de même pour le cas de la DGFiP.

Comment endiguer la surface d'attaque que l'État creuse lui même en créant des plateformes sans savoir les sécuriser ?

D'après Cédric Cartau, l'État français sait très bien valoriser l'innovation et lancer de nouveaux projets en y consacrant des moyens considérables, alors que la plupart d'entre eux finiront par être abandonnés. Il estime que ces ressources seraient mieux employées à renforcer la sécurité.