

Lettre des "Lundi de la cybersécurité" n° 94

Les enjeux de la médecine du futur autour de la data

Les enjeux de la médecine du futur autour de la data

Lundi 14 septembre
18h00 - 20h00

Organisateurs

Pr Ahmed Mehaoua
Université Paris Cité
CENTRE BORELLI

Cédric CARTAU
RSSI du CHI de Nantes

Caire ALBERIO
Groupe jeunes De l'ARCSI

Bêatrice Laurent

Gérard Peliks

La médecine du futur, une matière première sensible et menacée

Le secteur de la Santé repose de plus en plus sur des données médicales dont le nombre est en très forte augmentation. La médecine en bénéficie bien sûr, car, en particulier avec l'Intelligence Artificielle, avec également le partage des données qui est facilité, les diagnostics sont plus détaillés et le personnel médical peut partager les informations trouvées dans le cyberspace, pour mieux assurer l'aide qu'il apporte aux patients.

Mais ces données médicales intéressent fortement les cybercriminels, qui les volent pour les revendre dans les marchés noirs de la cybercriminalité, qui les chiffrent pour réclamer une rançon, ou qui les suppriment pour semer la confusion dans les Centres Hospitaliers.

Pour le Lundi de la Cybersécurité du mois de septembre 2026, nous faisons appel à un grand expert de la sécurité des data, Cédric Cartau, qui nous expliquera le côté lumineux et le côté sombre de la médecine du futur basée sur les données médicales.

Je donne la plume à Cédric CARTAU

La médecine de demain sera prédictive, personnalisée et participative, mais à une condition : la donnée. Imagerie, génomique, biologie, objets connectés et jumeaux numériques reposent désormais sur l'agrégation de volumes massifs et hétérogènes de données de santé, la matière première la plus sensible qui soit : intemporelle, non révoquée et à très forte valeur sur les marchés criminels.

Cette dépendance crée une tension structurante entre valoriser la donnée (recherche, IA, médecine de précision) et la protéger (vie privée, sécurité, souveraineté). Or le secteur santé est aujourd'hui le 3e plus visé en France, avec un parc hétérogène, une supply chain fragile et un IoMT qui élargit massivement la surface d'attaque, jusqu'à toucher l'intégrité physique du patient.

Face à cela, un empilement réglementaire (RGPD, NIS 2, AI Act, CRA, EHDS) tente d'organiser la confiance, pendant que l'affaire Health Data Hub rappelle l'enjeu de souveraineté. Fil rouge : plus la médecine devient prédictive, plus elle dépend de la donnée, donc plus la sécurité et la souveraineté de cette donnée deviennent des enjeux de santé publique.



Qui est Cédric CARTAU ?



Cédric Cartau est le responsable de la sécurité des systèmes d'information et le délégué à la protection des données du CHU de Nantes et du GHT44.

Cédric Cartau assure également des formations aux systèmes d'Information à l'EHESP (Ecole des hautes études en santé publique, au CNAM, au CNEH, à l'ESIEA, à l'Université de Nantes et à POLYTECH NANTES. Il est Chroniqueur dans DSIH Magazine et auteur de 6 ouvrages sur les systèmes d'information, aux éditions Presses de l'EHESP.

Membre de l'APSSIS, ARCSI, CESIN, AFCDP, il est co-fondateur du groupe RSSI NANTAIS et ISO 27001 Pays de la Loire.

Demande d'inscription au lundi 14 septembre, par visio-conférence à partir de 18 h 00.



Nos « Lundi de la cybersécurité » sont gratuits et veulent vous offrir une fête technologique. Demandez votre inscription, par courriel, nous vous enverrons, un peu avant le jour de l'événement, un hyperlien pour entrer dans la visioconférence Zoom.

Les demandes d'inscriptions sont à adresser à **Béatrice Laurent** co-organisatrice de nos événements :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux

intervenants. Si vous voulez être ajoutés à ma liste de distribution des lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le-moi par mail (gerard.peliks@noos.fr).

Si vous vous inscrivez pour assister à notre évènement, soyez connectés le **lundi 14 septembre dès 18 h 00 ou mieux, un peu avant**. La salle d'attente Zoom sera ouverte aux alentours de **17 h 00** pour des conversations informelles entre intervenants et participants. Ce sont toujours d'agréables échanges qui se font avant 18 h 00.

Quelques minutes avec une association : Groupe Jeunes de l'ARCSI

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, qui commence autour de 19 h 30, nous donnons pour une quinzaine de minutes la parole à une organisation qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Dans la séquence des **quelques minutes avec une association**, **Claire ALBERIO**, membre du CA de l'ARCSI, et par ailleurs Directeur Cybersécurité chez ORANGE Ile de France, présentera le « **Groupe Jeunes de l'ARCSI** » - Association des Réservistes du Chiffre et de la Sécurité de l'Information.



Créé par **Claire ALBERIO**, le groupe « Jeunes de l'ARCSI » a pour ambition d'évangéliser les jeunes aux pratiques de la cryptologie, en leur fournissant des outils de cryptologie. Il propose un ensemble de ressources pédagogiques (notices textes et vidéos) et peut assurer des interventions, en particulier dans les collèges et les lycées, pour montrer les divers outils. Une page du site web de l'ARCSI explique ce qui existe aujourd'hui dans la « **Boîte à Crypto** ».

Voir en : <https://www.arcsi.fr/la-boite-a-crypto.php>

Le coin-coin de l'IA Générative

Allons-nous obtenir une « hallucination » ou une réponse qui décrit une situation bien réelle ?



Prompt posé à Gemini :

Quels sont les enjeux de la médecine du futur autour de la data ?

Réponse de Gemini :

La médecine du futur ne se fera pas au chevet du patient avec un simple stéthoscope ; elle se jouera en grande partie derrière des écrans, à analyser des milliards de téraoctets de données. L'intégration massive de la **data** (données de santé, génomique, objets connectés) est la clé de voûte de la médecine des "4P" : *Prédictive, Préventive, Personnalisée et Participative*.

Cependant, cette révolution numérique soulève des enjeux colossaux, que l'on peut diviser en trois grandes catégories : techniques, cliniques et éthiques.

1. Les enjeux techniques et scientifiques : Le défi du "Big Data"

Le principal obstacle actuel n'est pas le manque de données, mais notre capacité à les exploiter correctement.

- **L'interopérabilité des données** : Aujourd'hui, les données de santé sont silotées (parfois au sein d'un même hôpital). Le grand défi est de faire parler les différents systèmes entre eux (fiches patients, imagerie, résultats de laboratoires) en utilisant des standards universels.
- **La qualité et la structuration** : Une grande partie des données médicales est "non structurée" (comptes-rendus écrits à la main ou dictés). Il faut développer des IA capables de trier et de nettoyer ces données pour éviter le principe du *Garbage in, garbage out* (si les données d'entrée sont mauvaises, les résultats de l'IA le seront aussi).
- **Le traitement en temps réel** : Avec l'essor des objets connectés (montres intelligentes, capteurs de glucose en continu), la médecine du futur devra être capable d'analyser des flux de données constants pour alerter avant que la crise ne survienne.

2. Les enjeux cliniques : Transformer la data en soins

Pour le corps médical et les patients, la data doit apporter une réelle valeur ajoutée au quotidien.

- **La médecine de précision (personnalisée)** : L'enjeu est de croiser les données cliniques classiques avec les données génomiques (séquençage de l'ADN) et environnementales. Au lieu d'un traitement standard pour le cancer, la data permettra de concevoir un traitement sur-mesure pour *un* patient donné.
- **Les jumeaux numériques** : L'un des projets les plus fascinants est la création d'un "double virtuel" du patient. En simulant des traitements ou des chirurgies sur ce jumeau numérique nourri de toutes vos données, les médecins pourront tester l'efficacité d'une thérapie sans aucun risque pour vous.
- **L'évolution du rôle du médecin** : Le médecin ne sera plus celui qui cherche l'information, mais celui qui interprète les suggestions de l'IA. L'enjeu est d'éviter une perte de compétences cliniques et de veiller à ce que l'algorithme reste une aide à la décision, et non le décideur final.

3. Les enjeux éthiques, juridiques et sociétaux : Protéger le patient

C'est sans doute le volet le plus sensible. La donnée médicale est la plus intime et la plus convoitée qui soit.

<u>Type d'enjeu</u>	<u>Description et Risques</u>
<u>Sécurité et Souveraineté</u>	Les hôpitaux sont des cibles massives de ransomwares. Garantir la cybersécurité des serveurs et stocker les données sur des clouds souverains (et non dépendants de géants étrangers) est une priorité absolue.
<u>Confidentialité et Propriété</u>	À qui appartiennent vos données de santé ? Comment garantir un consentement éclairé du patient lorsque ses données sont utilisées pour la recherche ou pour entraîner des IA ?
<u>Discrimination et Assurances</u>	Si les algorithmes peuvent prédire vos maladies futures avec précision, le risque est grand de voir les compagnies d'assurance ou les employeurs ajuster leurs tarifs ou refuser des contrats basés sur votre "profil de risque" génétique.

<u>Type d'enjeu</u>	<u>Description et Risques</u>
<u>Biais algorithmiques</u>	Si une IA est entraînée majoritairement sur les données de populations de pays occidentaux et aisés, ses diagnostics risquent d'être biaisés ou inefficaces pour d'autres ethnies ou classes sociales.

💡 **En résumé** : Le véritable enjeu de la médecine du futur est de réussir à **humaniser la data**. La technologie doit libérer du temps médical pour que le médecin se concentre sur l'écoute et l'empathie, plutôt que de le transformer en simple gestionnaire de base de données.

Nous écouterons ce que **Cédric Cartau** en pense.

Inscrivez-vous (mail à beatricelaurent.cde@gmail.com) ou cliquez ici :

JE M'INSCRIS

Gérard



Selfie que j'ai pris lors des 5èmes Rencontres SSI Santé de l'APSSIS