Femnov

bref, on propose un projet.

Le Secteur de la Santé face aux Cybermenaces Croissantes

Défis de l'IA

Problèmes de cybersécurité et de conformité liés à l'intégration de l'IA.

Augmentation des cyberattaques

Hausse des incidents de cybersécurité ciblant les infrastructures de santé.

Valeur des données médicales

Très haute valeur des données de santé sur le marché noir (50 fois plus cher qu'un numéro de CB).

Vulnérabilités de la digitalisation

Risques accrus en raison de la dépendance croissante aux systèmes numériques.

Renforcement de la sécurité d'une IA de détection sur imagerie médicale

Sécurité des échanges de données

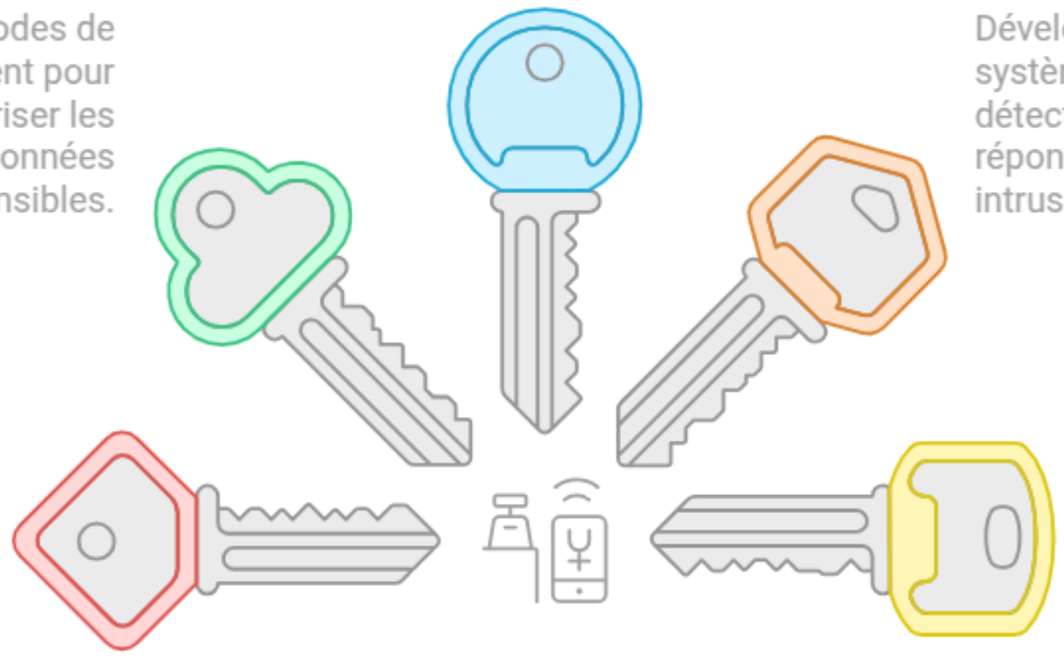
Assurer des transferts de données sécurisés entre les composants du système.

Mécanismes de chiffrement

Mettre en œuvre des méthodes de chiffrement pour sécuriser les données sensibles.

Mécanismes de détection des intrusions

Développer des systèmes pour détecter et répondre aux intrusions.



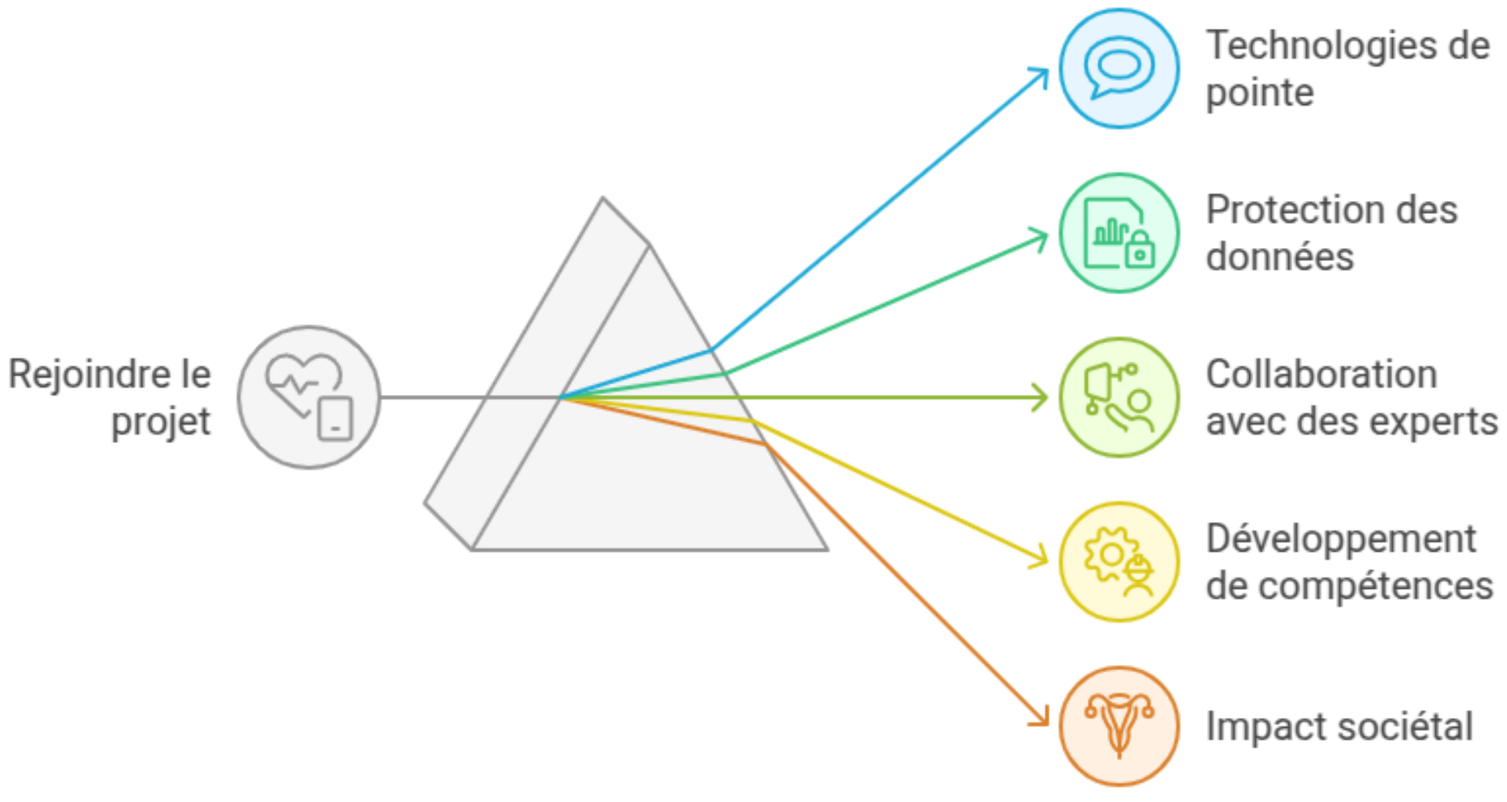
Identifier les vulnérabilités

Évaluer et identifier les points faibles potentiels dans le système.

Conformité aux normes

Se familiariser avec les normes/réglementations de sécurité des logiciels médicaux.

Rejoindre le projet



Femnov

Sécurisation du déploiement d'une IA pour l'analyse d’images médicales

Contexte et Problématique

Le secteur de la santé en France est de plus en plus ciblé par des cyberattaques, avec plus de 400 incidents recensés en 2023 par l'ANSSI. Les méthodes courantes incluent les rançongiciels et le phishing. La digitalisation croissante, notamment avec le développement de logiciels médicaux, accroît les vulnérabilités. **Les données médicales, très sensibles et précieuses, sont une cible de choix pour les cybercriminels**. Un rapport de l’ANSSI indique que ces informations peuvent se vendre jusqu’à 50 fois plus cher qu’un numéro de carte bancaire sur le dark web. L'intelligence artificielle révolutionne le domaine médical en offrant des outils puissants pour l'analyse des données médicales, le diagnostic précoce et la personnalisation des traitements. Cependant, **le déploiement de ces technologies dans les hôpitaux soulève des défis majeurs en matière de cybersécurité et de conformité réglementaire**.

L’objectif du projet

L'objectif global de ce projet est de **renforcer la sécurité d’une IA de détection de lésions d'endométriose** afin de **protéger les données** sensibles des patientes, **garantir l'intégrité du système** et d'assurer une **utilisation éthique et conforme de l'IA** en routine clinique.

Les défis à que vous aurez à relever

- **Identifier les vulnérabilités potentielles** du système et évaluer les risques associés aux cyberattaques
- **Mettre en place des mécanismes de chiffrement** pour protéger les données médicales sensibles et implémenter des contrôles d'accès robustes
- **Garantir la sécurité des échanges de données** entre les différents composants du système (serveurs, interfaces utilisateur)
- **Développer des mécanismes de détection des intrusions** et des stratégies de réponse en cas d'attaque.
- **Se familiariser et assurer la conformité du système avec les différentes normes** (RGPD, ISO 27001, IEC 62304 …)
- **Rédiger un rapport détaillé** sur les solutions de sécurité mises en œuvre ainsi qu'un guide des bonnes pratiques pour les utilisateurs.

Pourquoi rejoindre ce projet ?

Rejoindre ce projet, c'est l'occasion de plonger dans un **domaine où la tech et la santé se rencontrent**. Vous travaillerez sur des technologies de pointe et serez au cœur des **enjeux actuels de protection des données** sensibles. Ce projet vous permettra de développer des solutions concrètes pour sécuriser un système d'IA, tout **en collaborant avec des experts** du domaine médical et technologique. Non seulement vous développerez des **compétences techniques qui seront transposables dans n’importe quel domaine**, mais vous travaillerez aussi sur un **projet à fort impact** pour la société.

Littérature scientifique

MINISTÈRE DE LA SANTÉ ET DE L'ACCÈS AUX SOINS

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Comprendre la stratégie nationale | Ségur du numérique en santé | Mon espace santé | Cybersécurité

Accueil › Stratégie nationale ›
Cybersécurité accélération et Résilience des Etablissements (CaRE)

Cybersécurité accélération et Résilience des Etablissements (CaRE)

Cybersécurité, une réponse collective, déterminée et coordonnée pour faire face à la menace !

Pour répondre à l'**augmentation de la cybermenace**, la **puissance publique réagit et mobilise des financements** pour rattraper et pérenniser le niveau cyber des établissements avec le **programme CaRE** (Cybersécurité accélération et Résilience des Etablissements), objectif prioritaire du plan d'action CaRE .

► Eur Radiol. 2023 Jul 7;33(12):8833–8841. doi: 10.1007/s00330-023-09860-1

Cybersecurity considerations for radiology departments involved with artificial intelligence

Brendan S Kelly [1,2,3,✉], Conor Quinn [4], Niamh Belton [2], Aonghus Lawlor [2], Ronan P Killeen [1,3], James Burrell [5]

► Author information ► Article notes ► Copyright and License information

PMCID: PMC10667413 PMID: 37418025

► J Digit Imaging. 2020 Oct 29;33(6):1527–1542. doi: 10.1007/s10278-020-00393-3

Cybersecurity in PACS and Medical Imaging: an Overview

Marco Eichelberg [1,✉], Klaus Kleber [2], Marc Kämmerer [2]

► Author information ► Article notes ► Copyright and License information

PMCID: PMC7728878 PMID: 33123867

ELSEVIER

Journal of the American College of Radiology
Volume 20, Issue 9, September 2023, Pages 828-835

Original Article

Keeping Patient Data Secure in the Age of Radiology Artificial Intelligence: Cybersecurity Considerations and Future Directions

Chintan Shah MD [a], Douglas Nachand MD [b], Christoph Wald MD, PhD, MBA [c], Po-Hao Chen MD, MBA [d]

Navigating the unseen peril: safeguarding medical imaging in the age of AI

Alexandra Maertens[1], Steve Brykman[2], Thomas Hartung[1,3], Andrei Gafita[4], Harrison Bai[4], David Hoelzer[5], Ed Skoudis[5] and Channing Judith Paller[6]*

[1]Center for Alternatives to Animal Testing (CAAT), Johns Hopkins Bloomberg School of Public Health, Baltimore, MD, United States, [2]Independent Creative Technologist, Boston, MA, United States, [3]CAAT Europe, University of Konstanz, Konstanz, Germany, [4]Radiology and Radiological Science, Johns Hopkins University School of Medicine, Baltimore, MD, United States, [5]SANS Technology Institute, Rockville, MD, United States, [6]Department of Oncology, Johns Hopkins University School of Medicine, Baltimore, MD, United States

---

La cybersécurité : un enjeu majeur pour les établissements de santé

mise à jour : **25.02.25**

Établissements de santé, sociaux et médico-sociaux |Professionnels |Système d'information

A+ A-

Les établissements de santé sont la cible de nombreuses attaques de leurs systèmes d'information (SI). Celles-ci peuvent les paralyser en tout ou partie et être à l'origine de fuites de données sensibles. Conscient de cette menace, le ministère chargé de la santé a engagé, à travers différents programmes, des moyens importants pour renforcer la sécurité informatique des établissements de santé et mieux les préparer face aux situations de crise.