AGENCE DU NUMÉRIQUE EN SANTÉ

La régulation en cyber dans le numérique en santé

Health Innovation Intensive Training

21 mai 2026

Vincent Croisile

La cybersécurité, enjeu majeur pour l'écosystème du numérique en santé

Contexte

- L'actualité fait régulièrement état de cyberattaques concernant des logiciels et applications de santé
- Cela peut impacter le fonctionnement du système de santé (établissement de santé, activité libérale, etc.) avec des conséquences parfois **graves voire même irréversibles pour l'acteur concerné**
- Cela peut également avoir pour conséquence des fuites de données de santé à **caractère personnel au sein des systèmes d'information concernés**, données particulièrement **sensibles** et qui doivent être protégées en conséquence.

Enjeux de sécurité

- Les solutions logicielles font partie des **vecteurs d'attaque** qui peuvent être utilisés pour **accéder au SI de santé**
- Les applications utilisées sont progressivement amenées à s'interconnecter avec **Mon Espace Santé (DMP)**
- L'application des **bonnes pratiques de sécurité dans la conception et tout au long du cycle de vie des logiciels et applications utilisées en santé** est essentielle et fait notamment l'objet de réglementations : Cyber Resilience Act, Hébergement de données de santé, Référentiel d'identification électronique…

La **régulation cyber en e-santé** est nécessaire afin de **sécuriser les données sensibles**, **garantir la confiance des usagers** et **encadrer les pratiques** numériques des acteurs du secteur **dans une logique d'écosystème**.

Les principaux acteurs de la régulation cyber

L'ANS au cœur de la transformation numérique en santé

Régulateur

Nous améliorons la sécurité des systèmes numériques grâce à des règles communes en termes de régulation et d'échange.

Opérateur

Nous concevons de grands e-programmes nationaux (Ségur numérique, Programme CaRE, etc.) pour un service de santé sécurisé, efficace et solidaire.

Promoteur, valorisateur

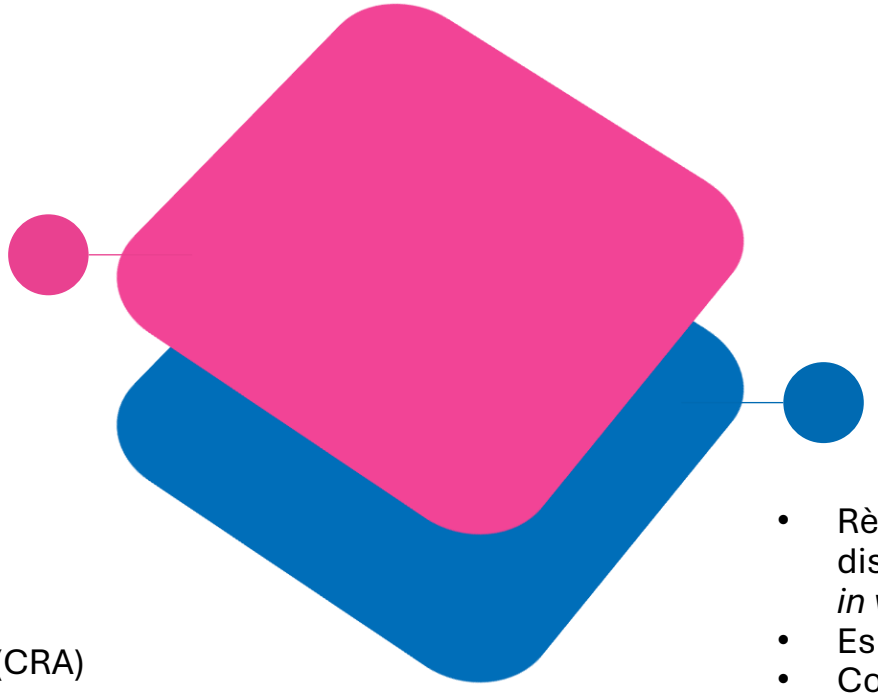
Nous stimulons, accompagnons et évaluons la sécurité de toutes les initiatives de e-santé pour les faire évoluer et grandir.

Au sein de l'ANS, nous apportons notre accompagnement pour renforcer la sécurité de vos produits et structures organisationnelles, notamment au travers de la sensibilisation et de l'acculturation aux enjeux cyber.

Principales réglementations applicables au secteur de la e-santé

Textes non-spécifiques au secteur de la santé

- Règlement Général sur la Protection des Données (RGPD)
- Loi Informatique et Libertés
- Directives européennes sur la Sécurité des réseaux et de l'information (NIS 1 et NIS2)
- Directive européenne sur la Résilience des Entités Critiques (REC)
- Règlement européen sur la cyberrésilience (CRA)
- Dispositif national de Sécurité des Activités d'Importance Vitale (SAIV)
- Lois de Programmation Militaire (LPM)



Textes spécifiques au secteur de la santé

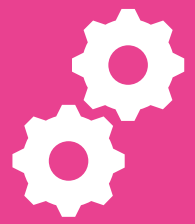
- Règlements européens portant sur les dispositifs médicaux et les dispositifs médicaux *in vitro*
- Espace européen des données de santé
- Code de la Santé Publique
  - Disposition des données de santé
  - Hébergement des données de santé
  - Signalement des incidents de sécurité
  - Services numériques en santé
  - …
- Politique de Gestion de la Sécurité des Systèmes d'Information de Santé (PGSSI-S)
  - Référentiel d'identification électronique
  - Guides pratiques
  - …

Les questions essentielles à se poser

Gouvernance

- Quelles sont mes obligations réglementaires ? (ex : RGPD, HDS, PGSSI-S, CRA)
- Quelles sont les données sensibles que je traite ? Comment est-ce que je les protège ?
- Mes collaborateurs sont-ils sensibilisés à la cybersécurité ?
- La sécurité de mes partenaires est-elle évaluée ?

Sécurisation du SI



- Quels mécanismes de contrôle d'accès ai-je mis en place ?
- Comment la sécurité de mon parc informatique est-elle assurée ?
- Comment mes développements sont-ils sécurisés ?

Gestion des incidents

- Quels outils de surveillance et de détection ai-je déployés ?
- Mon entreprise sait-elle comment réagir en cas de cyberattaque ?
- Quels sont nos processus pour garantir la continuité de service en cas d'attaque ou de panne ?

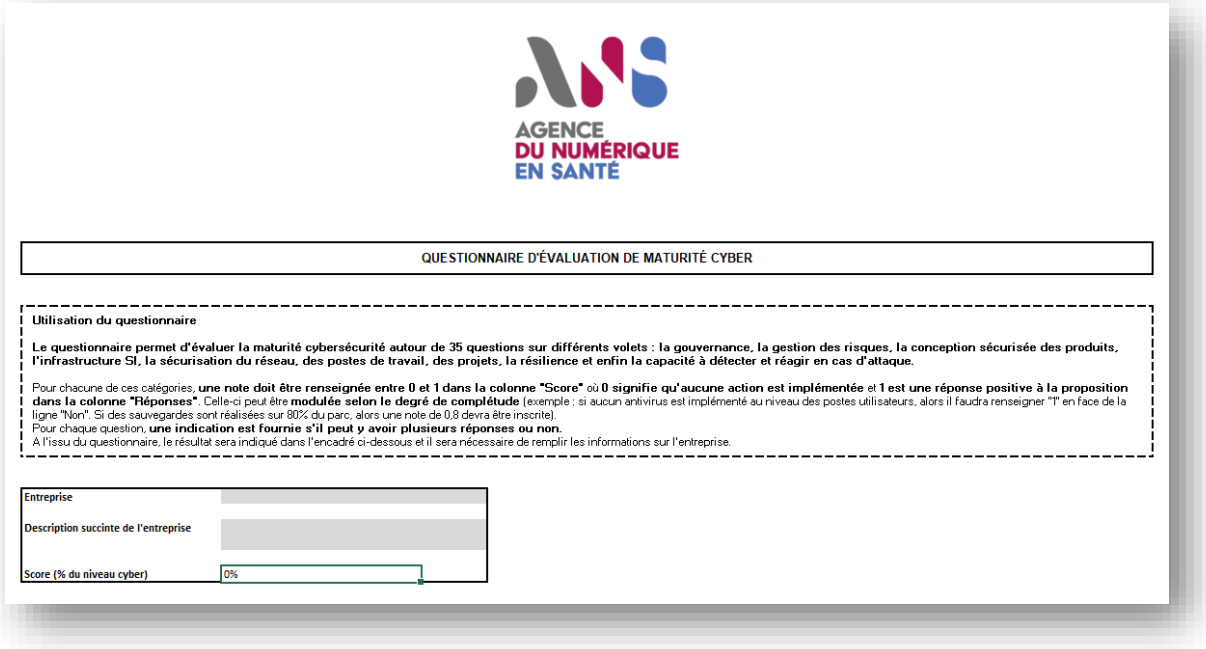
Pour aller plus loin : le Cyber-diag

Le Cyber-diag est un **questionnaire simple** conçu pour **évaluer le niveau de sécurité d'une organisation et de son produit**. Il permet, **en 2 heures d'entretien avec un expert**, d'avoir un **aperçu de votre maturité** et d'identifier des **mesures de sécurité** pouvant améliorer votre posture cyber.

Une **évaluation déclarative de la maturité organisationnelle et technologique** au travers de **35 questions** réparties en **8 thématiques**

Une note attribuée qui **tient compte du type de mesures de sécurité** mises en œuvre à la fois **pour le produit développé et l'organisation interne** de l'entreprise

Un **outil** qui a déjà permis d'évaluer la maturité de la SSI d'**une vingtaine de start-ups depuis 2023** et qui permet **des échanges et un suivi personnalisés**



QUESTIONNAIRE D'ÉVALUATION DE MATURITÉ CYBER

Utilisation du questionnaire

Le questionnaire permet d'évaluer la maturité cybersécurité autour de 35 questions sur différents volets : la gouvernance, la gestion des risques, la conception sécurisée des produits, l'infrastructure SI, la sécurisation du réseau, des postes de travail, des projets, la résilience et enfin la capacité à détecter et réagir en cas d'attaque.

Pour chacune de ces catégories, **une note doit être renseignée entre 0 et 1 dans la colonne "Score"** où **0 signifie qu'aucune action est implémentée** et **1 est une réponse positive à la proposition dans la colonne "Réponses"**. Celle-ci peut être **modulée selon le degré de complétude** (exemple : si aucun antivirus est implémenté au niveau des postes utilisateurs, alors il faudra renseigner "1" en face de la ligne "Non". Si des sauvegardes sont réalisées sur 80% du parc, alors une note de 0,8 devra être inscrite).
Pour chaque question, **une indication est fournie s'il peut y avoir plusieurs réponses ou non.**
A l'issu du questionnaire, le résultat sera indiqué dans l'encadré ci-dessous et il sera nécessaire de remplir les informations sur l'entreprise.

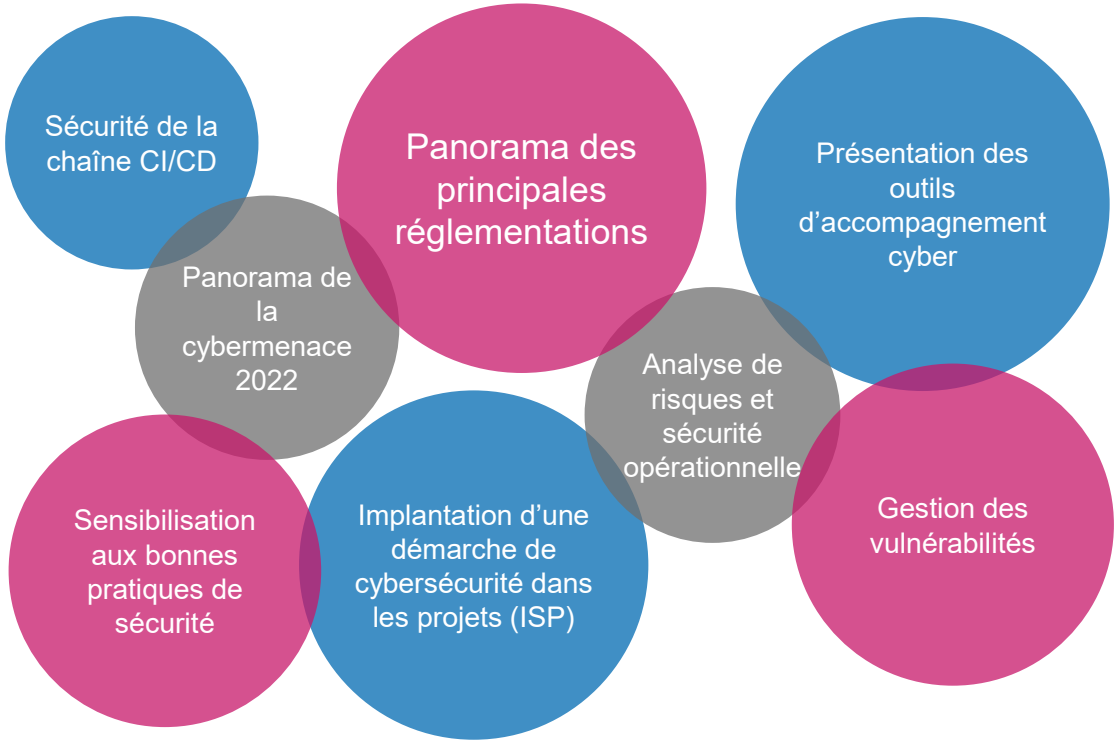
Entreprise	
Description succinte de l'entreprise	
Score (% du niveau cyber)	0%

Intéressés pour réaliser un Cyber-diag de votre organisation et de votre produit ? Vous pouvez contacter l'équipe ANS Innovation **:** **innovation@esante.gouv.fr**

Pour aller plus loin : des ressources à votre disposition

L'ANS propose régulièrement des **sessions collectives de cyber sensibilisation et d'acculturation aux bonnes pratiques** en matière de cybersécurité et met à disposition fiches thématiques pour accompagner les entreprises du numérique en santé.

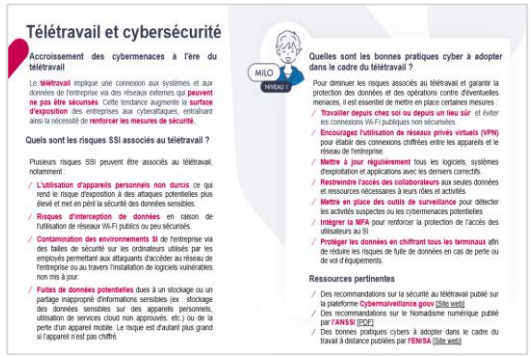
Des webinaires disponibles en Replay



Des fiches thématiques accessibles en ligne

Des supports **concis** et structurés à destination de **publics spécialistes ou non** :

- **Contextualisation** de la thématique cyber abordée
- **Identification des risques** auxquels être attentifs
- **Conseils pratiques** et concrets sur les actions à entreprendre
- **Liste de ressources** accessibles en un clic



AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Avez-vous des questions ?

Liens utiles

- Cybersécurité : Panorama des principales réglementations pour les start-ups de la e-santé – ANS – Lien
- Corpus documentaire PGSSI-S – ANS – Lien
- Règlement Général sur la Protection des Données (RGPD) – CNIL – Lien
- Sensibiliser et Former – ANS – Lien
- Fiches synthétiques sur la Sécurité du SI – ANS – Lien
- Guide d'hygiène informatique – ANSSI – Lien
- Recommandations relatives à l'administration sécurisée des SI – ANSSI – Lien
- Top 10 de l'OWASP – Lien

AGENCE DU NUMÉRIQUE EN SANTÉ

Doctrine du numérique en santé - Cybersécurité

Health Innovation Intensive Training

Atelier

21 mai 2026

Evolution de la menace cyber

- Auparavant : plutôt des attaques cyber opportunistes qui touchaient les solutions les plus vulnérables et pouvaient impacter le secteur de la santé sans qu'il soit directement visé
- Aujourd'hui menace additionnelle : groupe d'attaquants qui cible les données de santé

Schéma d'attaque type

Vol d'identifiants pour prendre la main sur le compte d'un PS

↓

Utilisation de faiblesses liées à une mauvaise mise en œuvre du cloisonnement et de la gestion des privilèges pour accéder à des données non légitimes

↓

Exfiltration massive des données de santé exposées via API en l'absence de blocage

Mettre en œuvre l'authentification multifacteurs (MFA)

Il s'agit du principal point d'entrée des attaquants, c'est notamment indispensable pour les solutions les plus exposées (SaaS).

- Mise à disposition de l'authentification PSC pour les professionnels de santé
- Mise en œuvre de l'authentification MFA requise a minima pour les accès distants dans le cadre du référentiel d'identification électronique. Renforcement en cours avec le RIEv2

Eviter l'utilisation d'un ID prévisible

Pour les ressources sensibles telles que les dossiers patients/usagers : il ne doit pas être possible d'incrémenter l'ID d'un dossier pour accéder successivement à l'ensemble des dossiers patients/usagers.
Un accès aux dossiers de façon massive pourrait alors être automatisé très simplement par un attaquant avec le développement d'un script dédié.

Respecter le principe du moindre privilège

L'utilisateur ne doit être en mesure d'accéder qu'aux ressources minimales auxquelles il a besoin d'accéder dans le cadre de son activité.

Ex : Un professionnel de santé ne doit a priori pouvoir accéder qu'aux dossiers patients/usagers qui le concernent, tout accès à des dossiers qui concerneraient d'autres établissements et professionnels est à proscrire.
De même un patient ne doit pouvoir accéder qu'à ses informations personnelles, attention au cloisonnement!

Eviter l'exposition de données en masse via API

Des contrôles doivent être mis en œuvre pour bloquer tout accès abusif aux données et alerter le cas échéant les personnes concernées.

Ex : En cas de téléchargement de dossiers patients/usagers en masse qui ne correspond pas à l'usage nominal de la solution

AGENCE
DU NUMÉRIQUE
EN SANTÉ

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante