



Cybersécurité en santé

Enjeux & Bonnes pratiques

24/11/2022 – Semaine Sécurité Patient

 Sant & Numérique
Hauts-de-France

Sant& Numérique Hauts-de-France

Qui sommes nous ?



- Sant& Numériques Hauts-de-France
 - GRADeS
 - Rôle & missions

- Zoé BOUDRY
Cheffe de projets (référente Identitovigilance)

- Cédric BOUCHER
Chef de projets (référent Cybersécurité)

Enjeux de la cybersécurité



Cybersécurité

Enjeux

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l'appelle également sécurité informatique ou sécurité des systèmes d'information.

Elle peut être divisée en plusieurs catégories :

- La sécurité des réseaux.
- La sécurité des applications.
- La sécurité des informations.
- La sécurité opérationnelle.
- La reprise après sinistre et la continuité des opérations.
- La formation des utilisateurs.

La cybersécurité est la mise en œuvre d'un ensemble de techniques et de solutions de sécurité pour protéger la confidentialité, l'intégrité et la disponibilité des informations.

Cybersécurité

Enjeux

En santé, plusieurs facteurs ont une incidence sur la sécurité du patient :

- l'ergonomie de l'environnement de soins,
- les systèmes de soin,
- la communication au sein de l'équipe comme entre les équipes, etc...

Désormais, un nouveau facteur doit être prise en compte : la cybersécurité.

- Les données de santé sont intéressantes car elles contiennent des données à la fois personnelles et financières et, sont vendues sur le « dark web » au prix fort.
- Les établissements de santé deviennent des cibles attractives.
- Amplification du phénomène avec la pandémie de COVID-19.

Cybersécurité

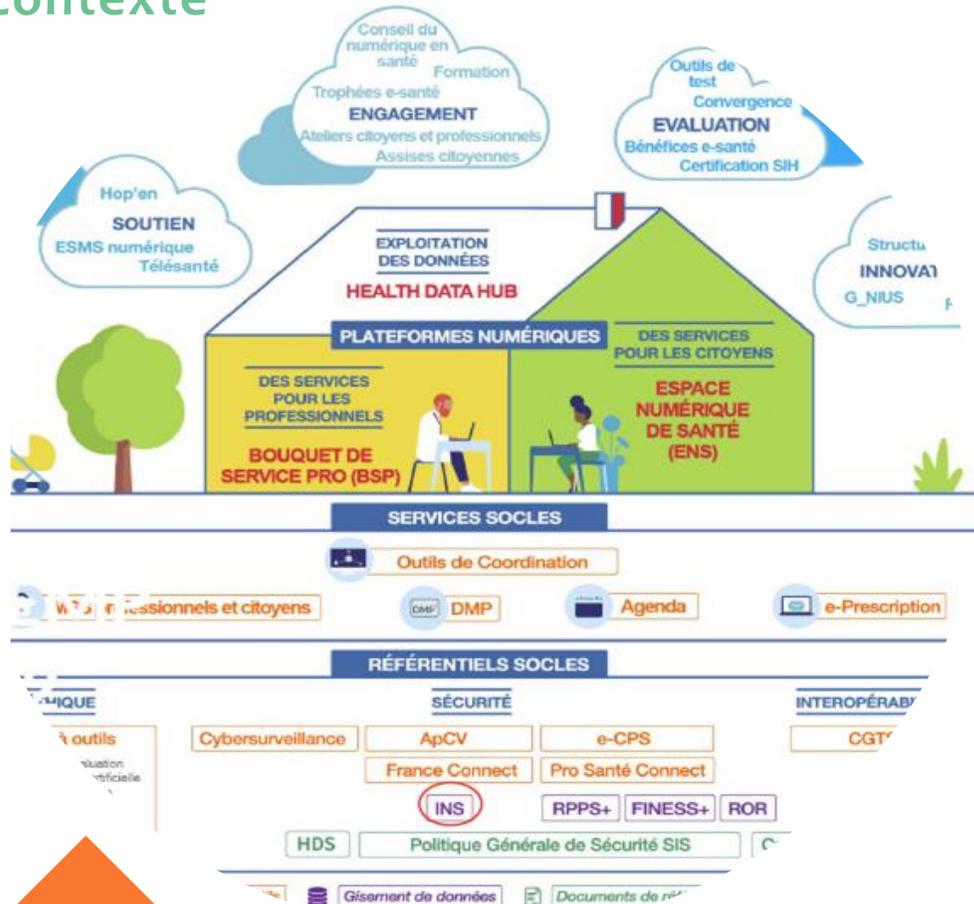
Enjeux

La stratégie Cyber présentée le 18 février 2021 par le président de la République a pour objectif de renforcer cette dernière à destination des établissements sanitaires et médico-sociaux :

- Le Ségur de la Santé a prévu 350 M€ spécifiquement dédiés au renforcement de la cybersécurité des établissements de santé et médico-sociaux.
- L'enveloppe budgétaire pour renforcer la cybersécurité de l'État prévoit 25 M€ spécifiquement dédiés à la réalisation d'audits de cybersécurisation des établissements ainsi qu'au déploiement du service national de cyber surveillance en santé, en partenariat avec l'Agence du numérique en santé (ANS).
- Le soutien de la part de l'État est possible si une part de 5 à 10% du budget informatique est dédiée à la cybersécurité.
- La sensibilisation à la cyber sécurité sera intégrée dans tous les cursus de formation des acteurs en santé pour développer les pratiques « d'hygiène numérique ».
- 135 groupements hospitaliers français intégrés à la liste des opérateurs de service essentiels, qui implique des règles de sécurité informatique plus strictes et le contrôle par l'ANSSI du bon respect de ces règles.

L'identité Nationale de santé (INS)

Contexte



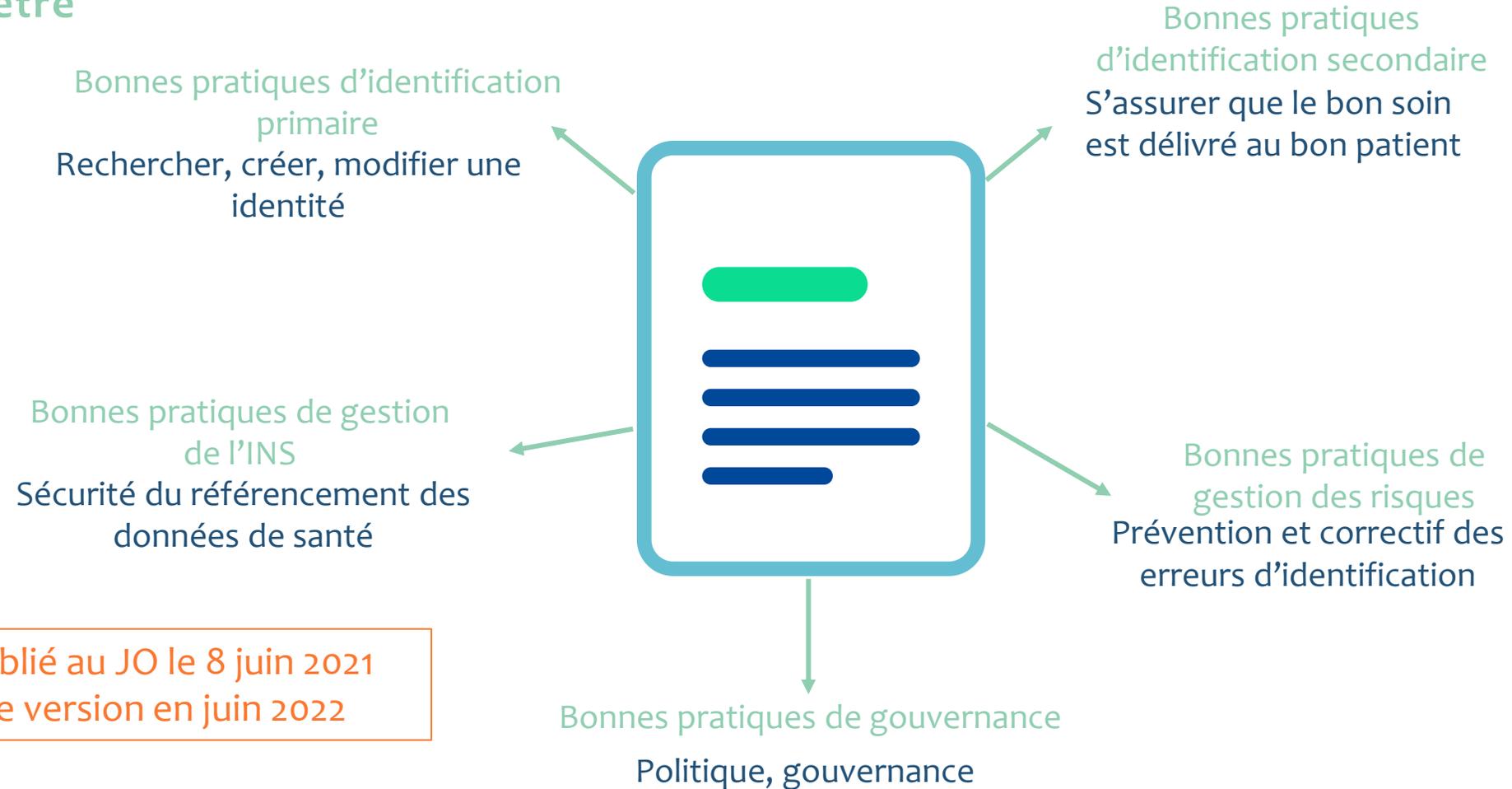
- L'identité INS constitue l'un des projets socles de la feuille de route nationale du numérique en santé (mesure n°6): il garantit que l'ensemble des projets de la feuille de route soient construits sur des **fondations solides**.

- Le **volet numérique du SEGUR**, accélérateur du développement du numérique en santé, confirme le positionnement de l'INS comme un service socle indispensable

- Depuis le **1er janvier 2020**, toutes les données de santé doivent être référencées avec l'INS et les traits d'identité de référence. La récupération de l'INS s'accompagne de bonnes pratiques d'identitovigilance inscrite dans le Référentiel National d'IdentitoVigilance.

Périmètre du Référentiel National d'Identitovigilance (RNIV)

Périmètre



Arrêté publié au JO le 8 juin 2021
Nouvelle version en juin 2022

L'identité Nationale de santé (INS)

Enjeux

L'INS est un identifiant unique et pérenne :

- Fiabiliser l'identité de l'utilisateur/patient accueilli dans une structure de santé
- Faciliter l'échange et le partage des données de santé
- Contribue à la qualité de prise en charge de l'utilisateur et à la sécurité des soins

Politique Générale de Sécurité des Systèmes d'Information de Santé

Enjeux

Le corpus documentaire de la PGSSI-S, Politique Générale de Sécurité des Systèmes d'Information de Santé, offre le cadre de référence nécessaire à la mise en œuvre des règles de sécurité en matière de e-santé.

Les référentiels sont opposables !

Ses objectifs :

- Aider les porteurs de projet dans la définition des niveaux de sécurité attendus
- Permettre aux industriels de préciser les niveaux de sécurité de leurs offres
- Soutenir les établissements de santé dans le choix et l'application de leur politique de sécurité
- La PGSSI-S s'applique aussi bien au secteur public qu'au secteur privé, aux professionnels de santé du sanitaire, du médico-social et social, aux établissements de soin et aux offreurs de service.

Bonnes pratiques et référentiels

Cybersécurité / INS



Bonnes pratiques

PGSSI-S

Référentiel « Identification électronique des acteurs sanitaire, médico-social et social »

- CPx
- E-CPS (Pro Santé Connect)
- Authentification à double facteur (2FA)

Référentiel « Identification électronique des usagers »

- INS

Les référentiels sont opposables !

Bonnes pratiques

Création d'identités patientes et récupération de l'INS

<i>Matricule INS</i>	<i>Nom</i>	<i>Prénom(s)</i>	<i>Sexe</i>	<i>DDN</i>	<i>Lieu nais.</i>	<i>OID</i>
260058815400233	DARK	JEANNE MARIE CECILE	F	30/05/1960	88154	1.2.250.1.213.1.4.8

NIR

NIA

1. Récupérer un document à haut niveau de confiance afin de créer une identité
2. Rechercher au préalable l'identité du patient accueillis afin de ne pas créer de doublon
3. Si le patient n'existe pas dans votre référentiel d'identité (GAM/GAP), le créer en respectant des règles de saisies précisées dans le RNIV
4. Réaliser l'appel au téléservice INSi afin de récupérer l'INS du patient accueilli

Bonnes pratiques

Les guides d'hygiène de l'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) met à disposition des guides d'hygiènes à la sécurité informatique :

1. Les 10 règles de bases
2. Les 12 règles essentielles
3. Renforcer la sécurité de son système d'information en 42 mesures



SOMMAIRE

AVANT-PROPOS
MODE D'EMPLOI DU GUIDE

I - SENSIBILISER ET FORMER - P.4

II - CONNAÎTRE LE SYSTÈME D'INFORMATION - P.8

III - AUTHENTIFIER ET CONTRÔLER LES ACCÈS - P.13

IV - SÉCURISER LES POSTES - P.20

V - SÉCURISER LE RÉSEAU - P.26

VI - SÉCURISER L'ADMINISTRATION - P.36

VII - GÉRER LE NOMADISME - P.40

VIII - MAINTENIR LE SYSTÈME D'INFORMATION À JOUR - P.45

IX - SUPERVISER, AUDITER, RÉAGIR - P.48

X - POUR ALLER PLUS LOIN - P.55

OUTIL DE SUIVI
BIBLIOGRAPHIE

2

Bonnes pratiques

Focus sur cas concrets

Sensibiliser et former

- La plateforme de formation e-santé de l'ANS (<https://esante-formation.fr/>)

The screenshot shows the homepage of the ANS e-health training platform. At the top, there is a blue header with the ANS logo and the text 'La plateforme de formation e-santé'. Below the header, there is a navigation bar with 'Accueil' and 'Thématiques'. A search bar is located on the right side of the header. The main content area features a welcome message: 'Bienvenue sur la plateforme de formation de la communauté e-santé. Venez découvrir les modules de formation réalisés par l'Agence du Numérique en Santé et ses partenaires.' Below this, there are six featured modules, each with a title, a representative image, and a brief description:

- COVID-19**: Logiciels métiers et téléconsultation : tutoriels des éditeurs. Description: TUTORIELS mis à disposition par les éditeurs de solutions.
- Référentiels**: Cadre d'interopérabilité. Description: Des systèmes d'information communicants pour favoriser la coopération des professionnels.
- Référentiels**: Politique Générale de Sécurité. Description: Un Cadre commun pour garantir la sécurité des systèmes d'information de santé.
- Accompagnement Cybersécurité**: Sécurité opérationnelle des SI. Description: Sécurité opérationnelle des systèmes d'information de santé.
- Services numériques nationaux**: Signalement-sante.gouv.fr. Description: Portail de signalement des événements indésirables graves.
- Services numériques nationaux**: Simphonie. Description: Simplification et dématérialisation du parcours patient.

On the right side of the page, there are two additional boxes:

- Besoin d'aide ?**: A box with a question mark icon and a list of links: 'Pourquoi créer un compte ?', 'Comment se connecter ?', 'Poster un commentaire ?', and 'Je n'arrive pas à créer mon compte'.
- Votre avis nous intéresse**: A box with a speech bubble icon and the text: 'Contribuez à l'amélioration de eSante-formation.fr. Déposez vos avis et suggestions'.

Bonnes pratiques

Focus sur cas concrets

Sensibiliser et former

- MOOC de l'ANSSI
(<https://secnumacademie.gouv.fr/>)



SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

Bienvenue sur le MOOC de l'ANSSI.

Vous y trouverez l'ensemble des informations pour vous **initier à la cybersécurité**, approfondir vos connaissances, et ainsi **agir efficacement sur la protection de vos outils numériques**. Ce dispositif est accessible gratuitement. Le suivi intégral de ce dispositif vous fera bénéficier d'une attestation de réussite.

[Accéder au MOOC de l'ANSSI](https://secnumacademie.gouv.fr/)

Bonnes pratiques

Focus sur cas concrets

Choisir avec soin ses mots de passe

- Nouvelles recommandations de la CNIL (octobre 2022) venant remplacer celles établies en 2017.

Le tableau ci-dessous recense les 3 cas d'authentification par mot de passe identifiés par la CNIL dans sa nouvelle recommandation. Le contrôle d'accès devra reposer sur des règles plus robustes selon les risques auxquels le système est exposé.

	EXEMPLE D'UTILISATION	ENTROPIE MINIMUM	MESURES COMPLÉMENTAIRES
Mot de passe seul	FORUM, BLOG	80	Conseiller l'utilisateur sur un bon mot de passe
Avec restriction d'accès (le plus répandu)	SITES DE E-COMMERCE, COMPTE D'ENTREPRISE, WEBMAIL	50	Mécanisme de restriction d'accès au compte : (exemples) <ul style="list-style-type: none">• Temporisation d'accès au compte après plusieurs échecs ;• Nombre maximal de tentatives autorisées dans un délai donné ;• "Captcha" ;• Blocage du compte après 10 échecs assorti d'un mécanisme de déblocage choisi en fonction des risques d'usurpation d'identité et d'attaque ciblée par déni de service.
Avec matériel détenu par la personne	CARTE BANCAIRE OU TÉLÉPHONE	13	Matériel détenu en propre par la personne (ex: carte SIM, carte bancaire, certificat) + Blocage au bout de 3 tentatives échouées

Bonnes pratiques

Focus sur cas concrets

Protégez votre messagerie professionnelle

- Hameçonnage (ou phishing)

Comment se protéger contre une tentative de phishing ?



1. Ne communiquez jamais d'informations sensibles par messagerie ou téléphone :

aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.



2. Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien

(sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.



3. Vérifiez l'adresse du site qui s'affiche dans votre navigateur.

Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.



4. En cas de doute, contactez si possible directement l'organisme concerné

pour confirmer le message ou l'appel que vous avez reçu.



5. Utilisez des mots de passe différents et complexes pour chaque site et application

afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques de type [KeePass](#) pour stocker de manière sécurisée vos différents mots de passe.



6. Si le site le permet, vérifiez les date et heure de dernière connexion à votre compte

afin de repérer si des accès illégitimes ont été réalisés.



7. Si le site vous le permet, activez la double authentification pour sécuriser vos accès.

Bonnes pratiques

Focus sur cas concrets

- Budget dédié à la cyber 5 à 10% du budget informatique
- Identifier / nommer un RSSI (prérequis HOP'EN, SEGUR)
- Existence de procédures dégradées (+ test de ces dernières)
- Déclaration des incidents auprès de la CNIL et du CERT Santé
 - CNIL : <https://notifications.cnil.fr/notifications/index>
 - CERT Santé : https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html

Questions





Merci !
