MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

*Liberté*
*Égalité*
*Fraternité*

AGENCE
DU NUMÉRIQUE
EN SANTÉ

# DOSSIER D'INFORMATION


TOUS CYBER VIGILANTS

## Cybersécurité dans le secteur de la santé et du médico-social : une priorité nationale pour réussir la transformation numérique.

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

# EDITO

**La cybersécurité pour la santé et le médico-social, je m'engage.**

Comme médecin, comme parlementaire hier et comme ministre aujourd'hui, j'ai toujours eu la conviction que le numérique était un levier de transformation sans pareil. Aujourd'hui, le virage numérique n'est plus une construction théorique : il se confronte à la pratique, aux usages et aux organisations tant au niveau national que sur les territoires.

Il s'agit à présent d'aborder une vision numérique de la santé comme d'appliquer des usages sanitaires au numérique : c'est tout l'enjeu de cette transversalité. Pour cela, il nous faut renforcer la sécurité numérique de tout l'écosystème sanitaire, notamment hospitalier, et médico-social.

Le plan de renforcement de la cybersécurité des hôpitaux lancé en juin 2019 a permis d'accompagner établissements et ARS dans la conduite du changement. Malheureusement, nous avons fait face depuis quelques mois à une recrudescence d'attaques envers des établissements de santé. Ces évènements ont montré la nécessité pour le ministère de continuer, de renforcer et d'améliorer sa politique en matière de cybersécurité, pour aider les établissements à faire face à des actes de cyber malveillance de plus en plus sophistiqués et d'inciter les acteurs à plus de responsabilité et plus de pédagogie, sur le territoire métropolitain comme dans nos territoires d'outremer.

Avec le Ségur de la Santé, nous avons fait le choix d'investir massivement dans la sécurité des systèmes d'information de santé. Confirmé par les récentes annonces du Président de la République, notre engagement porte en premier lieu sur la prévention en donnant aux établissements la capacité de mettre en œuvre les outils pour augmenter leur niveau de protection. Cette prévention prend également la forme d'audits de sécurité des systèmes d'information et de sessions de sensibilisation. L'autre volet de notre engagement porte la réponse proprement dite aux incidents.

Ces activités sont déjà portées par l'Agence du Numérique en Santé mais elles seront renforcées avec la mise en place d'un CERT sectoriel, le CERT Santé, lancé au second trimestre 2021. Cette entité composée d'experts en cybersécurité sera dotée de moyens importants pour assister les acteurs dans la lutte contre les actes de cyber malveillance.

C'est par la pédagogie, la formation, le soutien en moyen humain et financier, l'accompagnement des acteurs, que nous sécuriserons ensemble les pratiques du numérique en santé.

Alors je vous le demande, soyons TOUS CYBERVIGILANTS !

**Olivier Véran**
Ministre des Solidarités et de la Santé

# ACCELERATION DE LA STRATEGIE NATIONALE EN MATIERE DE CYBERSECURITE

Alors que les attaques de ce type se multiplient depuis plusieurs mois, touchant tous les secteurs et en particulier celui de la santé, en France comme à l'international, le Président de la République a présenté le 18 février 2021 l'accélération de la stratégie nationale en matière de cybersécurité. Celle-ci vise à structurer l'écosystème cyber et à le rendre plus robuste pour permettre aux acteurs nationaux de se doter de moyens renforcés et souverains en matière de cybersécurité. Cette annonce a eu lieu en visioconférence avec les centres hospitaliers de Dax et de Villefranche-sur-Saône, dont l'activité a été fortement impactée par des cyberattaques. Les enjeux de protection contre la menace cyber sont donc à prendre très au sérieux.

## *« Nous en avons fait une priorité »*

*« Notre stratégie en matière de cybersécurité va accélérer. Car il nous faut aller plus loin, plus vite, être à l'avant-garde. Au total, 1 milliard d'euros seront investis.*

*Il nous faut renforcer les formations et doubler à l'horizon 2025 le nombre d'emplois dans ce secteur stratégique.*

*Les structures de santé seront invitées à consacrer systématiquement 5 à 10 % du budget à la cybersécurité, notamment au maintien en condition de sécurité des SI dans la durée. »*

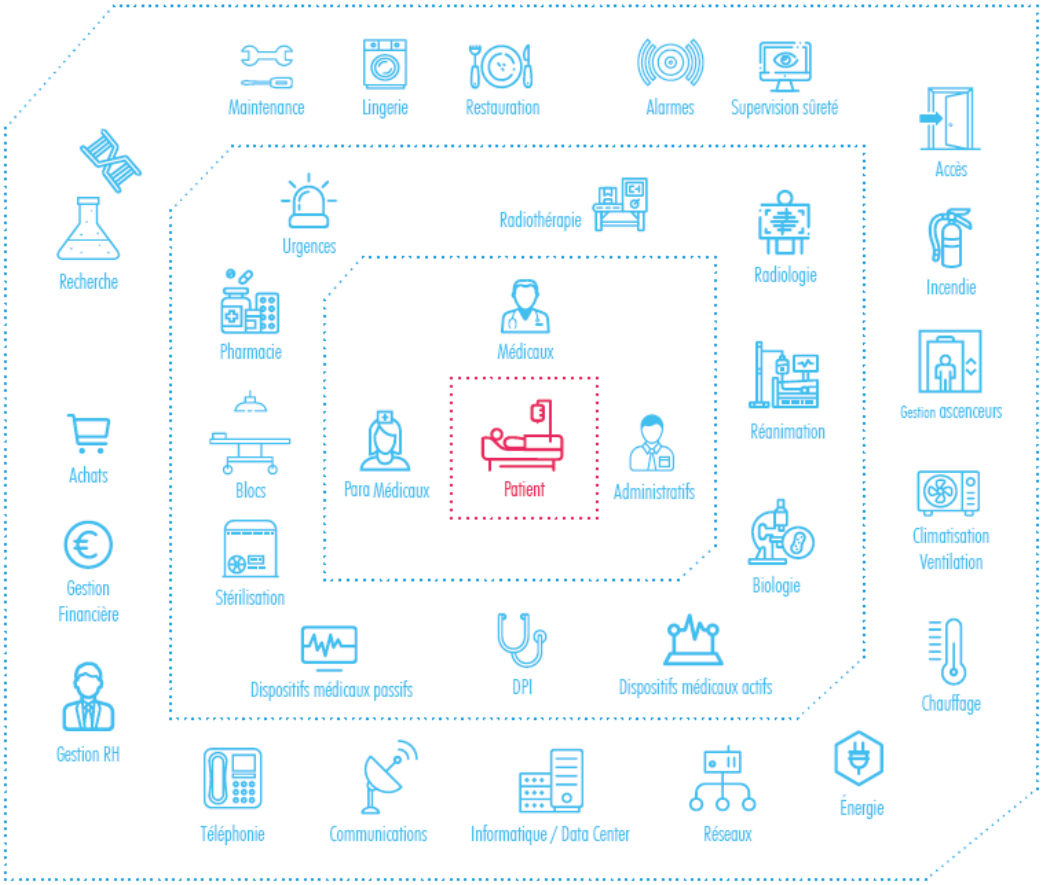
**Emmanuel Macron**
Président de la République
Extraits de la déclaration du 18 février 2021

# PARTIE 1/ SANTÉ NUMÉRIQUE : PRENDRE EN COMPTE LE RISQUE NUMERIQUE POUR RENFORCER LA SECURITE

## *L'essor du numérique en santé expose à des risques accrus*

Comme tous les secteurs, la santé connait aujourd'hui un formidable essor du numérique. Et ce, qu'il s'agisse des soins, de la gestion administrative ou des usages importés par les patients. Tout au long du parcours de soins, la donnée de santé est partout : au cabinet, comme à l'hôpital ou à la maison. Une omniprésence qui s'est accrue avec la crise sanitaire.

- 70 % des Français ont déjà pris RDV en ligne et 66 % ont déjà consulté ou reçu des résultats médicaux en ligne.
- 53 % des patients en téléconsultation y ont eu recours pour la 1ère fois pendant la crise et 91 % sont satisfaits.
- Dans les établissements la quasi-totalité des métiers de la santé et du médico-social sont concernés par le numérique. On pense aux résultats d'analyses ou aux dispositifs médicaux. Mais le numérique, c'est aussi le badge pour accéder à la cantine, le logiciel de paie ou le système de climatisation.[1]




[1] Étude quantitative OpinionWay juillet 2020_ 2100 personnes

Les cyber-risques sont à l'image de cet essor : ils augmentent. Et les établissements de santé y sont d'autant plus vulnérables qu'ils sont chaque jour particulièrement sollicités et sous tension. Stratégiques pour le pays, inégalement matures face au numérique et source exponentielle de données personnelles, ils constituent une cible privilégiée pour les attaques malveillantes. Avec un impact d'autant plus fort que la santé et la vie des patients sont en jeu.
Une cyberattaque peut en effet non seulement perturber le quotidien des professionnels, mais aussi mettre en péril la prise en charge des patients :

- Systèmes biomédicaux paralysés
- Plateaux techniques indisponibles
- Données de programmation des soins détruites
- Systèmes de messageries en panne
- Données de gestion et de ressources humaines perdues
- Données personnelles de santé usurpées.

En 2020, pas moins de 27 attaques[2] ont touché des hôpitaux français. Le secteur santé compte, depuis le début de l'année 2021, une cyberattaque par semaine. Les exemples ci-dessous témoignent de l'ampleur de ces attaques.

- *Dans la nuit du 8 au 9 février 2021, le CH de Dax a été victime d'une cyberattaque particulièrement massive, dite au « rançongiciel ». Un logiciel malveillant a crypté les données de l'établissement, paralysé son système informatique et coupé tous les appareils électroniques, dont les téléphones et ordinateurs. Ce qui a impacté les services de soins.*

- *Le 16 février 2021 à 4h30 du matin, le CH de Villeneuve-sur-Saône a été victime du rançongiciel RIUK qui touché les sites de Villefranche, Tarare et Trévoux. Les auteurs de l'attaque ont réclamé une rançon pour débloquer les données du système. Pour éviter que le virus se propage, les accès au système d'information et à internet ont été coupés et les interventions chirurgicales reportées...*

- *Le 21 décembre 2020, le CH d'Albertville-Moutiers a été victime d'une attaque par rançongiciel, qui les a contraint à travailler en mode dégradé pendant plusieurs semaines. A cause du chiffrement des données et par mesure de précaution, la quasi-totalité du SI a dû être arrêté affectant de nombreux services essentiels.*

- *Le 15 novembre 2019, le CHU de Rouen a été victime d'une attaque de grande ampleur qui a paralysé tous ses services pendant plusieurs jours, nécessité le transfert de certains patients dans d'autres établissements et provoqué le report de toutes les interventions programmées. L'attaquant avait déployé un logiciel malveillant qui a chiffré les données du système d'informations.*

[2] « 27 cyber-attaques majeures ont touché les hôpitaux français ». Source : https://www.lefigaro.fr/flash-eco/cybersecurite-des-hopitaux-27-attaques-majeures-en-2020-et-une-par-semaine-en-2021-20210217

• *Le 10 août 2019, le groupe de santé français Ramsay a été victime d'une cyberattaque à grande échelle, avec 120 sites touchés mais sans conséquence sur les soins ou la prise en charge des patients. Aucune donnée n'a été détournée ou détruite.*

## *La cybersécurité est indispensable pour transformer notre système de santé en toute confiance*

Lutter contre les déserts médicaux, décloisonner les parcours de soins, désengorger l'hôpital, faciliter la prévention, proposer une nouvelle offre de services ou accélérer la médecine personnalisée… Ces avancées ne pourront se développer que si notre système de santé est capable d'élever le niveau de sécurité de ses données et de ses échanges.
Plus le système sera performant, plus il devra être exigeant sur le plan technique comme dans les usages. La cybersécurité est un préalable au tournant numérique de notre système de santé et à la confiance de tous ses acteurs. **C'est pourquoi la résilience de chaque établissement de santé face à la menace cyber est devenue une priorité nationale.**

Or, les 3036 établissements de santé français sont loin de présenter le même niveau de sécurité numérique et la même prise de conscience des enjeux. Une partie d'entre eux ont élevé leur niveau d'alerte et construit des dispositifs de prévention et de réaction. D'autres manquent encore de ressources ou d'expertise. Cette grande disparité s'explique par des différences de taille, de budget et d'expérience. S'y ajoute un frein spécifique au secteur de la santé : par rapport aux enjeux sanitaires et à l'état critique de certains patients, le numérique apparaît souvent comme un risque secondaire, lointain et abstrait.

Symptôme de cette disparité dans la perception des enjeux, le nombre d'incidents graves déclarés par les établissements de santé reste encore faible et inférieur à la réalité estimée. Depuis la mise en place du nouveau dispositif de signalement en octobre 2017, seuls 847 incidents ont été déclarés, soit en moyenne 28 signalements par mois. Ce qui représente 10 à 15 % des établissements, dont une majorité d'établissements publics.

Ce faible nombre de signalements traduit encore une forme de crainte. Crainte d'être montré du doigt, crainte individuelle d'être tenu pour coupable, crainte d'être pris en faute. Pourtant, les signalements sont traités en toute confidentialité. Seules les personnes officiellement habilitées peuvent le faire. Cette crainte est une véritable faille pour tout le système.
En effet, les signalements immédiats d'incidents sont importants pour apporter un appui à la structure touchée, identifier une nouvelle menace cyber et proposer à l'ensemble des structures de santé des mesures de prévention et de réaction adaptées. Le CERT Santé a mis en place un espace de confiance où les structures de santé peuvent échanger en toute confidentialité et qui permet également de favoriser l'entraide.
Comme le confirment de récents exemples, quelques minutes suffisent en effet pour impacter jusqu'à 120 structures, du fait de l'interopérabilité des systèmes d'information.

## *La stratégie nationale de cybersécurité*

### > Le plan de renforcement 2021 de la cybersécurité en santé

La stratégie ministérielle pour la cybersécurité en santé se voit renforcée en 2021. Elle s'appuie sur la stratégie nationale pour la cybersécurité, présentée par le Président de la République le 18 février 2021, la feuille de route du numérique en santé de « Ma santé 2022 », et le « Ségur de la santé ».
Portée avec l'ANSSI, et en cohérence avec les actions déjà engagées, le plan de renforcement de la cyber sécurité 2021 concrétise les engagements du ministère des Solidarités et de la Santé pour faire face aux risques cyber, la nécessaire déclinaison territoriale et les efforts de mutualisation à poursuivre, en s'appuyant sur les GHT.

a. Déclinaison au niveau national

*Déclinaison de la Feuille de route du numérique en santé de « Ma Santé 2022 » et du volet numérique du « Ségur de la santé »*

- Pilotage national de la cybersécurité en santé (via un comité de pilotage ad-hoc) : Cabinet MSS, DNS, SG/HFDS, DGOS, ANS, en lien avec l'ensemble de l'écosystème de la santé et l'ANSSI.

*Création d'un observatoire national de maturité SSI des établissements de santé*

- Analyse du niveau de maturité des structures de santé, qui s'appuiera principalement sur le référentiel d'évaluation de la maturité numérique des systèmes d'information des structures de santé baptisé MaturiN-H (Maturité Numérique des Hôpitaux).

*Appui national des structures de santé opéré par le CERT Santé (ANS), en coordination avec le CERT-FR.*

- Veille et alerte au profit du secteur santé : https://esante.gouv.fr/securite/cert-sante, https://www.cyberveille-sante.gouv.fr/
- Service national de cybersurveillance en santé qui propose un service aux structures de santé pour détecter de façon préventive les vulnérabilités sur les domaines exposés sur Internet.
- Accompagnement et suivi des structures de santé dans le cadre de la réponse à un incident.

> *Campagne nationale régulière sur la cybersécurité en santé « **Tous cyber vigilants** »*, portée par le ministère des solidarités et de la santé pour accompagner les structures de santé dans la sensibilisation des personnels dans la durée et l'adoption de nouveaux comportements, individuel et collectif, nécessaires pour protéger le système de soins.

b. Déclinaison au niveau territorial

*ARS*

- Animation portée par les ARS sur leurs territoires de santé, pour accompagner le volet cyber du virage numérique des territoires : sensibilisation des acteurs, partage de pratiques, appui aux mutualisations, organisation de la réponse à incident.

*GHT*

- Montée en puissance des GHT comme accélérateur des nouveaux usages numériques, organisé autour de la sécurisation des SI partagés, de la mutualisation des moyens cybers et des capacités de réponse à incidents.

c. Déclinaison au niveau de chaque structure de santé

*Gouvernance*

- Prise en compte du risque cyber dans la politique de maîtrise des risques de l'établissement
- Existence ou désignation d'un RSSI ou correspondant SSI et d'un DPD (mutualisation à rechercher)
- Budget sécurité numérique :
  - Pour chaque programme numérique, il est demandé à chaque structure de consacrer de 5 à 10% du budget informatique à la cyber sécurité, notamment au maintien en condition de sécurité (MCS) des SI et des infrastructures sous-jacentes dans la durée

*Exigences de sécurité*

- Ensemble des structures de santé
  - Mise en œuvre des règles d'hygiène informatique[3]
- Opérateurs de services essentiels (dont CHU et ES support de GHT)
  - Mise en œuvre de règles de sécurité renforcée[4]

*Ces exigences de sécurité recouvrent les domaines suivants :*

1- *Maîtrise des SI*

- Élaboration et mise à jour d'une cartographie des SI
- Audits cybers réguliers (biennal) :
  - Sécurité des AD (ANSSI)
  - « Expositions de vulnérabilités sur Internet » (CERT Santé)
- Audits de conformité aux exigences applicables : « guide hygiène informatique » ou « NIS V1 »
- Plan d'action cyber pluriannuel de mise en conformité

[3] cf. ANSSI : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
[4] cf. directive NIS V1 : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037444012/

2- *Sensibilisation aux risques cyber*

- Sensibiliser l'ensemble des personnels aux enjeux de la cybersécurité et aux principes d'hygiène numérique.
  - Appui sur les supports nationaux et territoriaux (MSS, CERT Santé, ANSSI, ARS,etc.).

3- *Anticipation : Préparation à faire face aux incidents numériques et aux cyberattaques*

- Réaliser régulièrement des exercices de continuité d'activité en « mode numérique dégradé ».
- Disposer d'un plan de réponse en cas d'incident numérique ou de cybersécurité (mis à jour).

4- *Gestion des incidents*

- Déclaration systématique des incidents de sécurité des SI sur le portail de signalement des événements sanitaires indésirables :
  - https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil
- Réponse aux incidents graves de sécurité
  - Disposer d'un support contractuel permettant de pouvoir recourir à un spécialiste de la réponse à incidents de sécurité (Support propre à l'établissement ou mutualisé).

*Investissements - Mesures d'accompagnement financières*

- Plan de relance (ANSSI)
  - « Parcours de sécurisation » proposé prioritairement aux OSE.
- Programme HOP'EN
  - Pour les ES retenus, répondre aux prérequis cyber.
- Ségur de la santé
  - Les investissements au profit des établissements de santé et médico-sociaux couvrent les aspects liés à l'interopérabilité, la réversibilité, la convergence et la sécurité des systèmes d'information en santé, fondamentaux de la feuille de route nationale du numérique en santé.

*Contrôle*

- HAS – Certification pour la qualité des soins
  - Répondre aux exigences du « Critère 3.06-02 : "les risques numériques sont maîtrisés" ».

## > Des piliers opérationnels de cybersécurité pour le secteur santé

### a. Un portail numérique unique pour les signalements d'incidents de sécurité : https://signalement.social-sante.gouv.fr/.

Les établissements peuvent déclarer tous leurs événements indésirables via ce point d'entrée unique, qu'il s'agisse des incidents de sécurité survenus dans leurs systèmes d'information ou des événements sanitaires indésirables, afin qu'ils soient transmis aux acteurs en charge de l'évaluation.

### b. Le CERT Santé, une structure experte pour aider les établissements à répondre aux incidents de sécurité des systèmes d'information

Pour améliorer la résilience du secteur de la santé face à la menace cyber, le ministère des Solidarités et de la Santé a mis en place, le 1er octobre 2017, un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information (SSI) des structures de santé et aider les établissements à les gérer. Piloté par le FSSI des Ministères sociaux ce dispositif a été mis en place avec l'Agence du Numérique en Santé. Il intervient auprès des ARS et des établissements concernés, à travers une structure nationale d'assistance et d'appui : le CERT Santé. (Ex-cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS))[5].

### c. Un portail de veille et d'alerte pour informer les établissements de santé : https://www.cyberveille-sante.gouv.fr/

En coordination avec le CERT-FR (ANSSI), le CERT Santé exerce une veille permanente sur l'actualité de la sécurité des SI et sur les menaces propres au secteur de la santé. Il informe et alerte les acteurs de santé à travers des bulletins de sécurité publiés sur son portail.

### d. Un processus permanent de retour d'expériences pour anticiper et corriger

Le CERT Santé procède aussi à des audits de cyber-surveillance. Il s'agit de diagnostics de la sécurité des systèmes d'information vis-à-vis d'Internet. Les objectifs sont : identifier d'éventuelles vulnérabilités sur les machines exposées et alerter sur d'éventuelles fuites de données. Le service propose des recommandations pour améliorer la sécurité des serveurs et réduire les risques d'intrusion.

### e. Pourquoi il est fondamental de signaler tout incident puis de se faire accompagner

En 2020, près d'1 signalement sur 4 a débouché sur un accompagnement par le CERT Santé. C'est pourquoi il est fondamental que les établissements de santé et médico-sociaux déclarent leurs incidents de sécurité, dès qu'ils sont impactés.

[5] Voir p. 17

# PARTIE 2/ PANORAMA 2020 DES INCIDENTS DE SECURITE NUMERIQUE DANS LE SECTEUR SANTE ET MEDICO SOCIAL

Le CERT Santé produit chaque année un rapport public de son activité et communique chaque mois aux autorités ministérielles un indicateur sur l'état de la menace cyber. C'est grâce à cet observatoire des incidents de sécurité et à l'observatoire des vulnérabilités, que le ministère des Solidarités et de la Santé peut orienter ses actions stratégiques et opérationnelles, pour mieux accompagner les établissements en matière cybersécurité.

## *Quels incidents déclarés en 2020 ?*

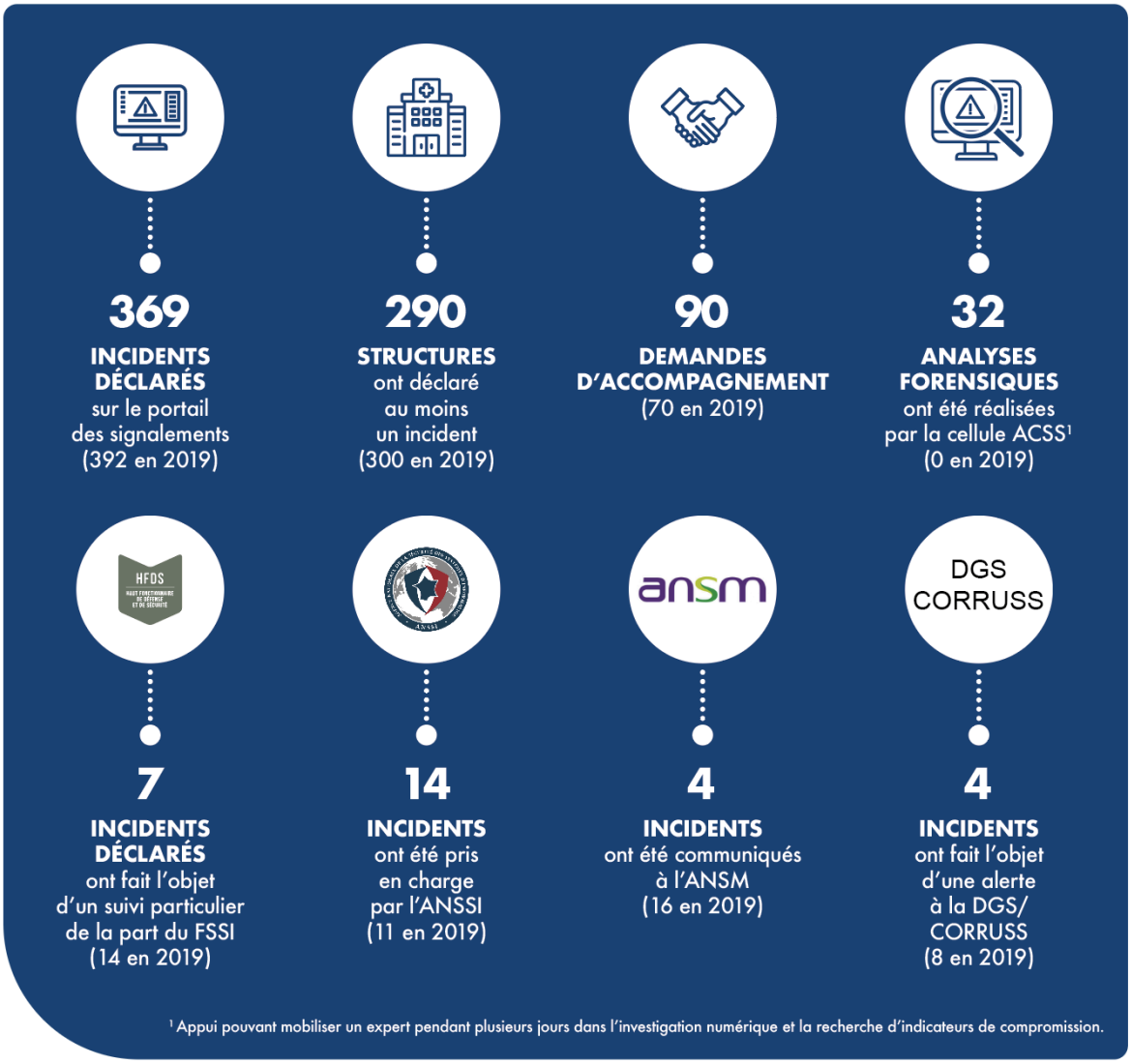
En 2020, **250 établissements ont déclaré 369 incidents**, soit une baisse d'environ 6% par rapport à 2019. Un taux de déclaration toujours faible par rapport au nombre d'établissements concernés par l'obligation de déclaration. Ils déclarent néanmoins de plus en plus leurs incidents d'origine malveillante, surtout lorsqu'ils ont impacté ou auraient pu impacter les soins, ce qui atteste de leur bonne compréhension du dispositif mis en place.
La hausse des actes de cyber malveillance dans le secteur santé se confirme en 2020, ce qui est cohérent avec la tendance globale. Ils représentent aujourd'hui 60 % des déclarations reçues par le CERT Santé, contre 41% en 2018 et 43% en 2019.
Par ailleurs, le CERT Santé a davantage été sollicité pour **aider les structures à répondre aux incidents de cybersécurité**. L'évolution de la menace et l'expertise nécessaire pour y faire face nécessitent en effet des moyens trop importants pour de nombreux établissements. Elles sollicitent notamment l'aide du CERT Santé pour conduire l'investigation numérique, c'est-à-dire analyser les artefacts et les journaux d'évènements puis pour remédier aux attaques, c'est à dire éradiquer la menace et mettre en place des plans spécifiques de protection.
Quant à l'ANSSI, elle est intervenue en appui pour des attaques à l'impact potentiellement fort sur la continuité des soins et en particulier auprès des Opérateurs de Services Essentiels (OSE).

La hausse significative des **attaques par maliciels** des structures de santé observée en 2019 s'est confirmée en 2020. Ces attaques représentent aujourd'hui près d'1 incident déclaré sur 4, dont plus de la moitié sont dus à des rançongiciels. Cette menace, qui concerne tous les secteurs d'activité, représente le risque le plus important pour la continuité des soins, surtout lorsque les sauvegardes ont été chiffrées. Car il faut alors souvent plusieurs semaines pour que le SI revienne à un fonctionnement normal, ce qui impacte durablement la prise en charge des patients.
Le **nombre d'incidents bloquant l'accès à distance a également augmenté en 2020**. En cause : des vols de mots de passe ou des faiblesses liées à une absence de mise à jour que les attaquants exploitent. C'est souvent par ce canal qu'ils accèdent au SI interne pour introduire un code malveillant (rançongiciel et cryptominer dans la majorité des cas). Cette hausse est étroitement liée à un usage accru de l'accès à distance durant la crise de la

COVID-19 et les difficultés que rencontrent les responsables informatiques pour corriger rapidement ces faiblesses sur un SI trop exposé sur Internet.
L'impact de ces actes de cyber malveillance est plus important lorsque les règles d'hygiène informatique n'ont pas été respectées pour protéger les actifs sensibles du SI. C'est-à-dire lorsque les services d'annuaire (Active Directory) sont insuffisamment sécurisés et les sauvegardes n'ont pas été cloisonnées.

Avec 40 % en 2020, contre 57 % en 2019, la **part des incidents d'origine accidentelle est en légère baisse**. Ils sont essentiellement dus, comme toujours, à des bugs logiciels, des dysfonctionnements ou des pannes de réseau, d'applicatifs ou de téléphonie. Ils impactent l'organisation des soins, puisqu'ils suspendent pour un temps l'accès au dossier informatisé des patients ou l'accès à des plateformes d'échanges de résultats médicaux (biologie, radiologie...). Les établissements comme les prestataires ont été globalement réactifs et autonomes pour les résoudre.

*Chiffres et infographies clés 2020 versus 2019*

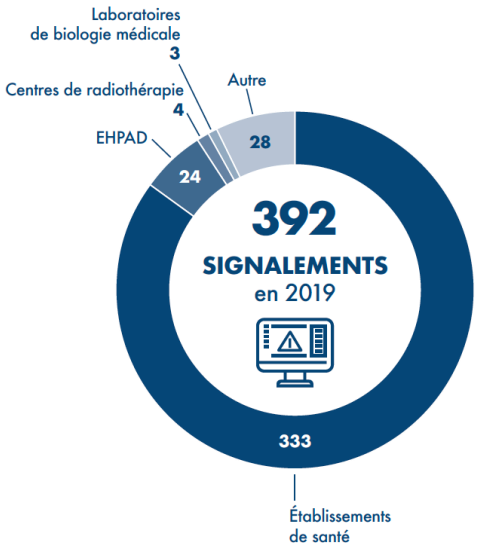


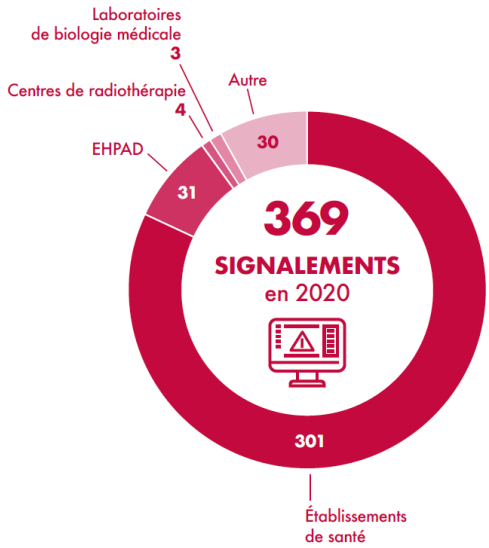
**369 incidents** ont été déclarés en 2020. Ce nombre est en légère baisse par rapport à 2019 (392) avec une moyenne de 20 par mois

En 2020, comme en 2019, près de la moitié des signalements sont résolus par la structure avant leur déclaration.

27% : c'est le pourcentage de **signalements pour lesquels a été demandé un accompagnement en 2020**. Il a **augmenté de 6% par rapport à 2019**.

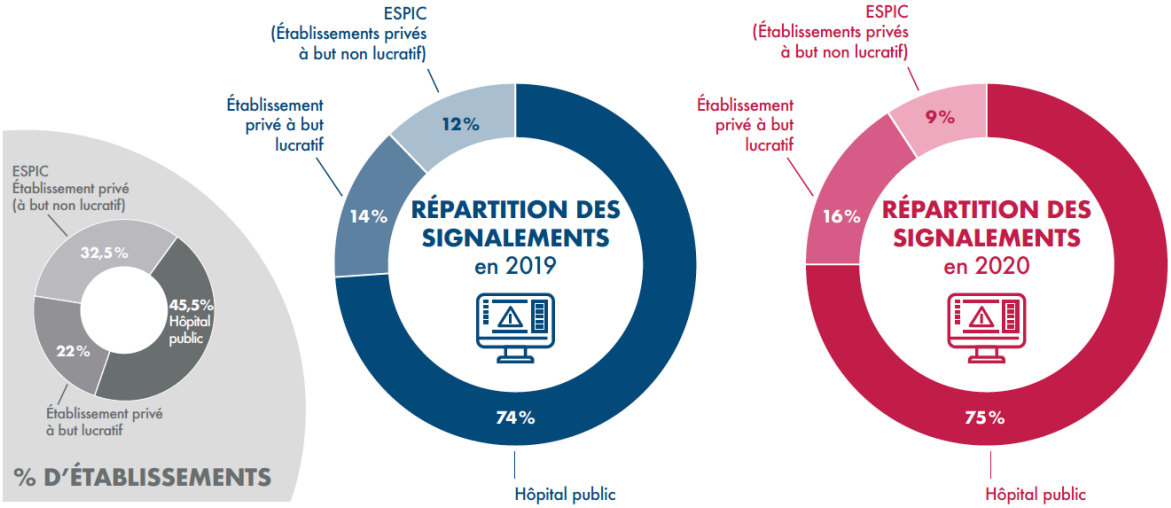
## Répartition des signalements selon le type de structure



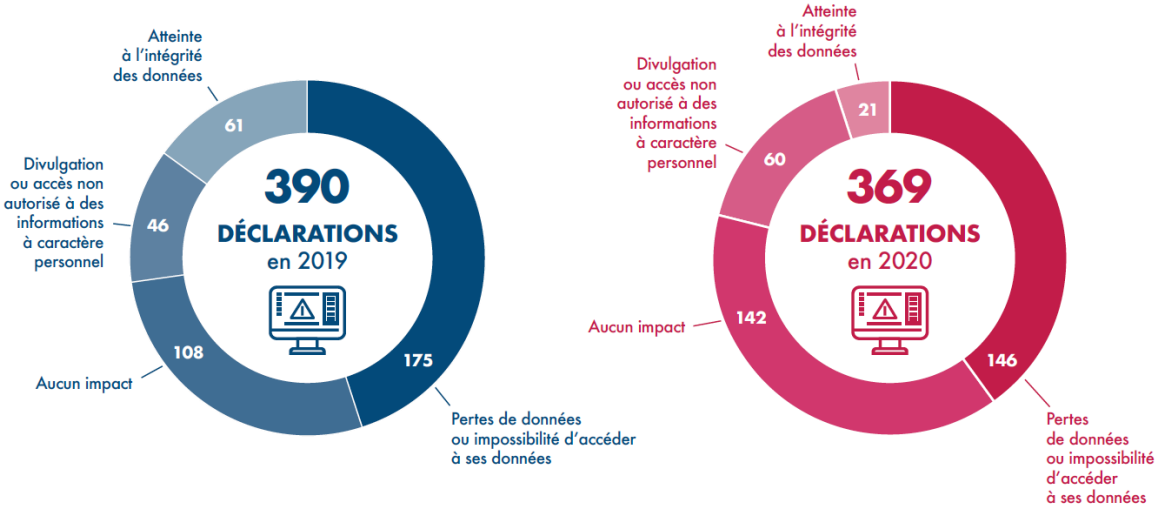




**81 %** des incidents de sécurité sont déclarés par les établissements de santé.

## Répartition des signalements comparée à la part des établissements de santé selon leur type

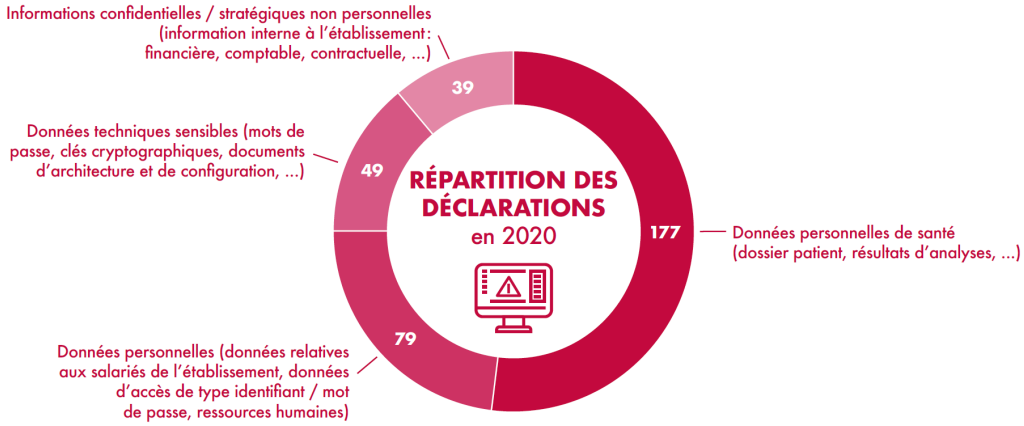



## Répartition des déclarations selon le type d'impact sur les données



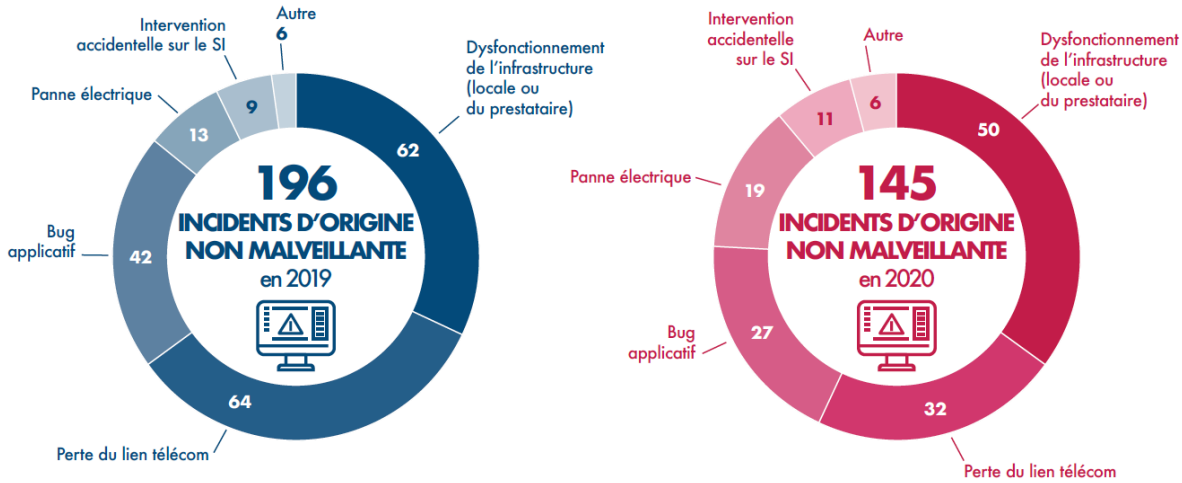

**45 %** C'est le pourcentage de structures qui ont été contraintes à mettre en place en 2020 **un fonctionnement en mode dégradé** du système de prise en charge des patients (5% de plus qu'en 2019).

## Répartition des déclarations selon le type de données impactées




**40%** C'est la part d'incident d'origine non malveillante en 2020, ce chiffre a baissé de 17% depuis 2019.

## Répartition des incidents d'origine non malveillante



# PARTIE 3 / CYBERSECURITE : LE RÔLE CENTRAL DU CERT SANTE

## *La cybersécurité, un enjeu essentiel dans la vie de nos établissements de santé*

Pour mettre en œuvre la stratégie nationale de sécurité numérique, le ministère des Solidarités et de la Santé, s'appuie sur l'Agence du Numérique en Santé et plus particulièrement sur la cellule ACSS - Accompagnement Cybersécurité des Structures de Santé - rebaptisée **CERT Santé en avril 2021** pour que ses missions soient plus facilement identifiables par les acteurs du secteur de la santé et du médico-social.

Cette cellule a rejoint en 2021 l'InterCERT-FR, un groupe d'organismes spécialisés dans l'analyse et le traitement des incidents. En intégrant cette structure, le CERT Santé bénéficie des retours d'expérience et de la coopération des autres acteurs, l'ANSSI notamment, et peut ainsi encore mieux accompagner les établissements.

L'ANSSI est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cybersécurité, l'ANSSI apporte son expertise et son assistance technique aux organismes publics comme l'ANS mais aussi aux entreprises. Avec une mission renforcée au profit des opérateurs de services essentiels (OSE), elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

Face à la menace qui pèse sur nos systèmes d'information, le collectif est un gage d'efficacité.

De manière très concrète, le CERT Santé :

- Enregistre les signalements des incidents de sécurité des systèmes d'information
- Analyse et qualifie les signalements
- Alerte les autorités compétentes
- Anime la communauté cyberveille santé
- Apporte son appui pour répondre aux incidents
- Anime un webinaire trimestriel sur la cybersécurité.

## *Le CERT Santé, un expert national reconnu au cœur du dispositif de lutte contre les cyberattaques*

Depuis 2017, la Cellule ACSS, devenu le CERT Santé, est l'interlocuteur privilégié des établissements sanitaires et médicosociaux en matière de sécurité opérationnelle. L'ANS a obtenu la reconnaissance par l'ANSSI et l'InterCERT-FR de la maturité du CERT Santé dans la réponse aux incidents et la veille sur la menace de cybersécurité pour les secteurs santé et médico-social. **L'ANS est aujourd'hui positionnée au cœur de l'expertise cyber française.** Grâce à l'appui de l'ANSSI, le CERT Santé a encore amélioré ses services en 2020 pour répondre aux incidents et rester en veille active face aux menaces de cyberattaques.

Au-delà de ses actions de soutien pour aider les structures à résoudre leurs incidents, le CERT Santé accompagne aussi les établissements à titre préventif. **Quarante GHT ont ainsi bénéficié de son service national de cybers-surveillance et plus de 800 établissements ont été alertées quant à la vulnérabilité ou la compromission potentielle de leur SI.**
Grâce aux actions préventives du CERT Santé, les systèmes d'information des structures de santé et du médico-social sont moins exposés aux menaces issues de l'Internet. Il est cependant fondamental que les établissements de santé continuent de déclarer leurs incidents le plus tôt possible pour bénéficier d'un appui du CERT Santé. Ils pourront ainsi mettre en œuvre des mesures de remédiation pour réduire de façon significative l'impact potentiel des actes de cyber malveillance.
Avec le Ségur de la Santé, le Ministère a fait le choix d'investir dans la sécurité des systèmes d'information de façon massive. Et le CERT Santé aura plus de moyens pour accompagner les structures les plus vulnérables du secteur.
Mais pour faire progresser les établissements en matière de prévention et de bonnes pratiques, il faut aussi les sensibiliser et les former. C'est pourquoi, le CERT Santé continuera à jouer un rôle central dans l'animation du secteur pour favoriser la coopération et l'entraide entre les acteurs, pour accompagner leur montée en compétence et pour contribuer à une plus grande résilience collective.

### *Le CERT Santé : des activités et des services opérationnels pour aider les acteurs de la santé numérique*

Le dispositif qui traite les signalements est un élément clé de la stratégie nationale de sécurité numérique portée par le ministère des Solidarités et de la Santé, en lien étroit avec les autorités gouvernementales en charge de la cybersécurité. La mise en œuvre opérationnelle de cette stratégie s'appuie sur le CERT Santé de l'Agence du Numérique en Santé, qui s'impose comme l'acteur principal de la sécurité du numérique en santé et de l'appui opérationnel aux structures de santé.

Le CERT Santé a mis en place une démarche méthodique pour améliorer la résilience des structures face aux actes de cyber malveillance. Les établissements peuvent compter sur son appui, en toute confiance.

> Un portail de signalement et un appui expert :
> https://www.cyberveille-sante.gouv.fr/

Le traitement des incidents reste de la responsabilité des établissements de santé. Mais le CERT Santé peut les accompagner dans le cadre de leur signalement. Cet appui comprend les missions suivantes.

- Traiter le signalement sur le portail des signalements des évènements sanitaires indésirables et notifier sa prise en compte.
- Analyser et qualifier le signalement pour le compte des autorités compétentes.
- Aider, si besoin, l'établissement à traiter l'incident de sécurité de ses systèmes d'information.

- Alerter les autorités compétentes de l'État, le cas échéant. C'est-à-dire les agences sanitaires, l'ANSSI ou la CNIL, selon la nature de l'incident.

Pour aider les établissements à répondre à un incident, le CERT Santé peut intervenir à différents niveaux.

- Il met à leur disposition des fiches de réflexes ou de recommandations de remédiation correspondant à la nature de l'incident.
- Il propose des mesures de confinement complémentaires au cours d'un premier entretien.
- Il les aide à identifier la menace et le scénario complet de la compromission puis propose les mesures de remédiation adaptées.

Le CERT Santé propose aussi un accompagnement dans la phase d'amélioration des mesures de sécurité.

- Il définit ou émet un avis sur des plans d'action sécurité.
- Il rappelle les bonnes pratiques de cloisonnement réseau, notamment via des guides et des supports de formation.

Une fiche récapitulant cet accompagnement est disponible sur le portail cyberveille-santé :

https://cyberveille-sante.gouv.fr/sites/default/files/documents/ACSS_Accompagnement_Reponse_Incident.pdf

### > Une communauté « cyberveille-santé » active

Pour faciliter le partage des bonnes pratiques, le portail cyberveille-santé offre un espace sécurisé au sein duquel les correspondants du CERT Santé peuvent échanger. Près de 600 Responsables de la sécurité des systèmes d'information (RSSI) peuvent partager leurs expériences sur tous les sujets touchant à la cybersécurité.

- La façon dont ils ont traité les incidents qu'ils ont rencontrés,
- Les indicateurs sur l'origine des incidents,
- Les documents publiés sur le portail, dont les bulletins de sécurité,
- Les actions ministérielles visant à encadrer ou accompagner les acteurs pour mettre en œuvre la sécurité numérique.

Par ailleurs, le CERT Santé organise une fois par trimestre un webinaire sur les menaces de cybersécurité (attaques à partir de l'Internet, rançongiciels, etc...), ses services d'appui (réponse à incident, prévention) et les bonnes pratiques de protection ou de cloisonnement pour renforcer la sécurité des systèmes numériques. 4 webinaires sont d'ores et déjà disponibles sur https://esante.gouv.fr/ans/webinaire/enjeux-de-la-cybersecurite-pour-la-transformation-numerique

### > Un dispositif d'alerte permanent

Via le portail cyberveille-santé, le CERT Santé alerte les établissements sur les nouvelles menaces de cybersécurité et propose des mesures réactives.

- Il informe et alerte les structures de santé quant aux vulnérabilités ou aux dysfonctionnements majeurs de leurs dispositifs médicaux, technologies de santé ou technologies standards : système d'exploitation, suite bureautique, base de données, etc.
- Il alerte les structures de santé en cas d'actes de cyber-malveillance : messages électroniques malveillants, rançongiciels, vols de données, etc.
- Il aide les établissements à gérer leur sécurité comme leurs incidents à travers des fiches réflexes, des fiches pratiques ou des guides de bonnes pratiques.

### > Un test en ligne pour améliorer la sécurité des messageries

Les attaquants qui cherchent à compromettre un SI utilisent souvent des courriels malveillants. Pour vérifier et améliorer la détection et le blocage de ces messages, et en particulier les attaques par hameçonnage, le CERT Santé propose aux établissements de tester en ligne la sécurité de leur serveur de messagerie. Ce service a pour but d'identifier les contrôles manquants et d'améliorer la configuration des règles de sécurité de la messagerie pour éviter que les utilisateurs soient victimes de ces contenus malveillants. Il permet de vérifier que la politique de contrôle des messages et de leur contenu a pris en compte les principales menaces issues de l'émetteur dans les métadonnées du message (en-tête, encodage, découpage en plusieurs partie), la pièce jointe (spam, virus) ou une URL (hameçonnage), etc. Ce service passe au crible plus de 170 points de contrôle.

# PARTIE 4 / TOUS CYBER-VIGILANTS : UNE CAMPAGNE D'INFORMATION POUR MOBILISER L'ENSEMBLE DES ACTEURS

## *Un kit de communication pour les **structures de santé***



*Un kit de communication à destination des* ***structures médico-sociales***


*Un kit de communication* ***générique (à destination des médecins libéraux, ARS, etc.)***

*Une campagne pour sensibiliser tous les métiers liés à la santé et mobiliser tous les établissements sur les enjeux de la cybersécurité.*

**La France dispose à la fois d'une expertise forte en cybersécurité et de structures d'accompagnement tels que l'ANSSI, CERT Santé ou des prestataires pour aider les établissements de santé**. Plusieurs outils sont accessibles, tant pour déclarer un incident ou trouver de l'aide, que pour s'informer sur les premiers gestes ou l'actualité en matière de cyberattaques. Mais pour que ce dispositif porte ses fruits, les acteurs de la santé doivent se saisir pleinement de la **cybersécurité comme d'un sujet quotidien et citoyen**. C'est tout l'enjeu de cette campagne nationale d'information lancée par le ministère des Solidarités et de la Santé pour mobiliser tout l'écosystème.

En effet, tous les acteurs du système de santé, du ministère des Solidarités et de la Santé jusqu'aux patients et leur famille, en passant par les établissements, les professionnels et la médecine libérale, sont parties prenantes de la sécurité numérique. On compte en France plus de 3 000 établissements de santé et 30 000 établissements et services médico-sociaux. Ils ont été choisis comme cible prioritaire de cette campagne parce qu'ils sont à la fois : au cœur du dispositif de santé, stratégiques pour leur territoire, et vulnérables.

En pratique, cette campagne veut mobiliser tous les acteurs des établissements de santé, c'est-à-dire aussi bien les équipes dirigeantes et les experts numériques que les professionnels de santé, les fonctions support et, de manière indirecte, les usagers. **Avec un ton positif et fédérateur qui mobilise tous ces publics autour d'un mot d'ordre engagé « TOUS CYBER VIGILANTS ».**

Les visuels montrent combien la prise en charge des patients est irriguée de numérique. On ne peut plus garantir la confiance dans le système de santé et la sécurité des individus sans garantir la sécurité des systèmes numériques des établissements. La campagne aura atteint son objectif si les professionnels des établissements de santé s'approprient pleinement le message central : ***« À l'hôpital, le numérique est partout. Ensemble, rendons-le plus sûr. Tous cyber vigilants »***. La campagne les incite à participer pleinement, en tant que professionnels comme en tant qu'individus, au fonctionnement des établissements de santé. Quand on se renseigne sur les techniques d'hameçonnage et les moyens de les éviter, quand on s'interroge sur les premiers gestes, on prend toute sa place dans ce collectif humain qui constitue la force réelle de toute démarche de cybersécurité.

La tonalité des visuels et des textes éveille la curiosité et impacte les consciences comme les comportements, sans engendrer de peur ou dramatiser. Car la peur n'est jamais un levier pour agir, que ce soit de façon individuelle ou collective.

Au-delà des établissements de santé, **« *Tous Cyber vigilants* » implique et mobilise l'écosystème au sens large**. Il se décline pour tous les métiers et se déploie partout sur le terrain, quelles que soient les structures (services, ARS ou GRADeS, ES, ESMS, etc.). Les

responsables de chaque structure et service peuvent s'en emparer et le répercuter autour d'eux, au sein de leurs équipes.

Et pour maximiser cet impact, la campagne joue résolument sur le décalage entre la taille des instruments qui permettent de prendre en charge les patients au quotidien et celle des individus qui œuvrent à la sécurité numérique. Ce décalage visuel valorise l'engagement collectif et l'implication de tous les métiers au service du bien commun.

### *Les détails opérationnels de la campagne*

La campagne nationale d'information sur la cybersécurité est déclinée par le ministère des Solidarités et de la Santé (DNS, HFDS, ANS et DGOS), en coordination avec l'ANSSI, les fédérations hospitalières, les conférences nationales et tout l'écosystème de la santé. Elle s'inscrit dans la continuité des actions de sensibilisation réalisées depuis 2019 sur cette thématique prioritaire.

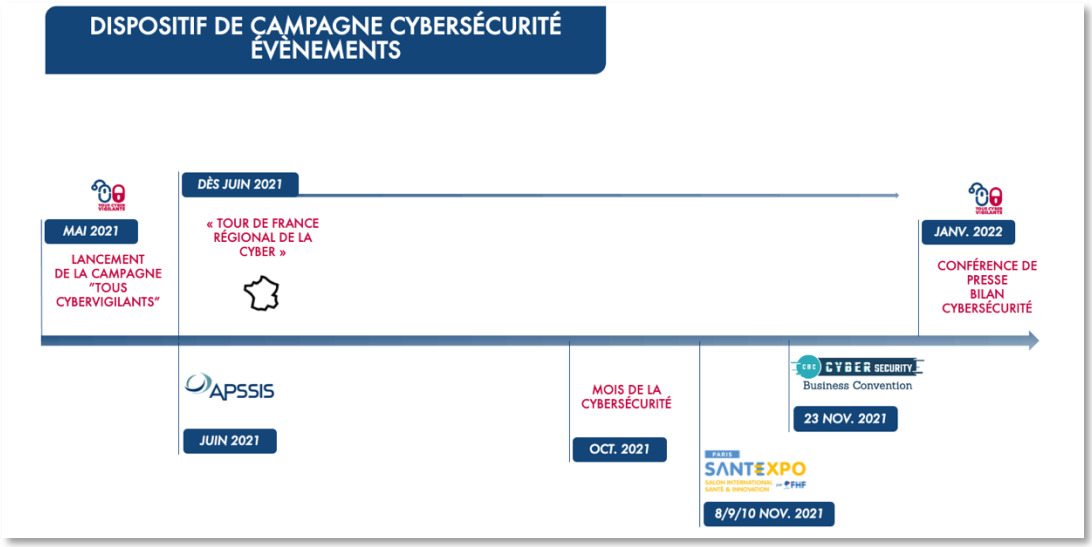
La campagne d'information est déployée sur différents supports de communication : presse professionnelle et spécialisée et ses versions en ligne, ainsi que sur les réseaux sociaux.

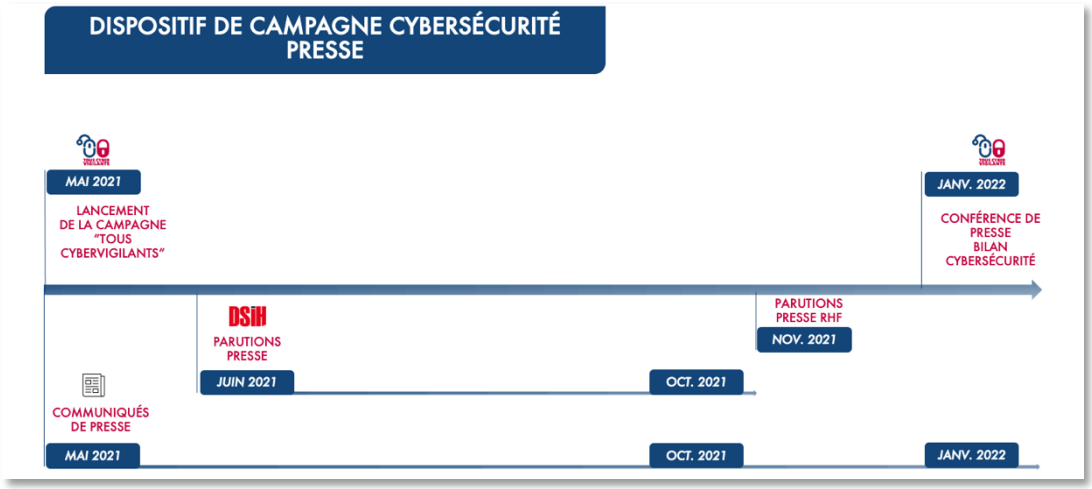
À partir du lancement de la campagne, le dispositif opérationnel de la campagne sera complété par des **actions concrètes au cœur des territoires** aussi bien en présentiel que sur les réseaux, avec :

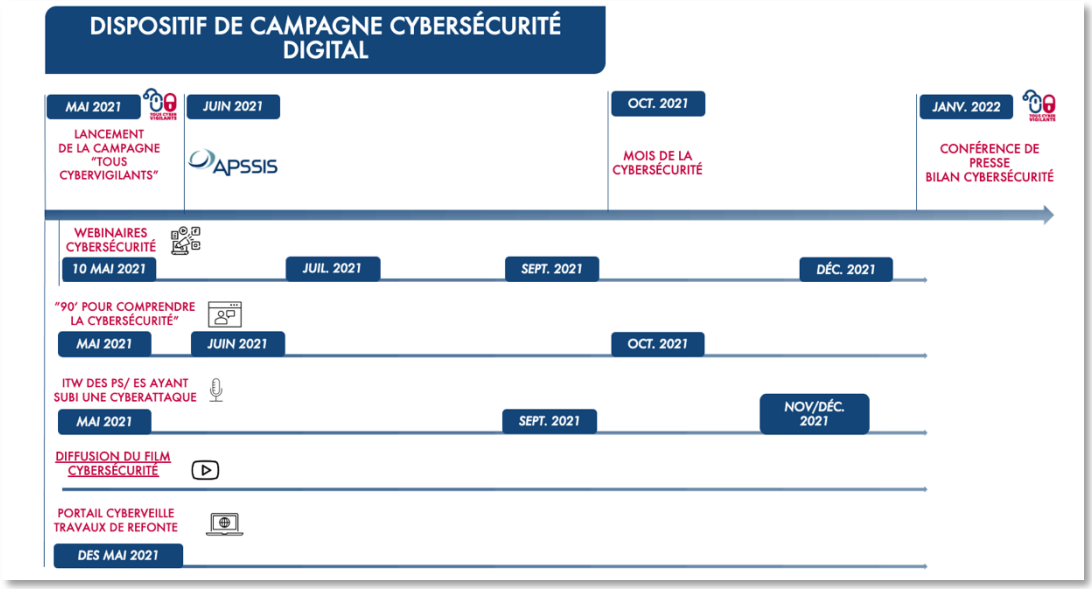

- Un « Tour de France Régional de la Cyber », en lien avec les ARS afin de sensibiliser sur les bonnes pratiques, partager, échanger sur des retours d'expériences et accompagner les acteurs.
- Des évènements qui seront l'occasion de prises de parole : comme le Congrès de l'APSSIS (juin), le colloque annuel de la cybersécurité (octobre), le mois européen de la cybersécurité, ou encore Sant'Expo (novembre)…
- Une présence renforcée de la cybersécurité sur les réseaux sociaux via la diffusion du film ou de messages sur Twitter/ Facebook et LinkedIn
- Des portraits-interviews réalisés sur le terrain pour montrer ceux qui font la cybersécurité sur le terrain.
- Un #Hashtag pour fédérer et animer une communauté mobilisée ;
- Des initiatives existantes renforcées et élargies : programmes de webinaires, interviews d'experts, mise à disposition de kit de communication…
- L'ensemble sera soutenu par un dispositif de promotion à forte visibilité dans la presse professionnelle (dont version numérique) tout au long de l'année.

**Le kit de communication à destination des structures de santé et du médico-social est disponible** (affichettes, dépliant, posts RS, film d'animation…) sur le site esanté.gouv.fr, dans la rubrique CyberSécurité et sur YouTube
Les supports sont téléchargeables à l'adresse www.touscybervigilants.fr

La campagne s'étalera tout au long de l'année 2021 avant un bilan lors d'une conférence de presse en janvier 2022 :



# LES ACTEURS DE LA CYBERSECURITE :

**L'Agence nationale de la sécurité des systèmes d'information (ANSSI)** assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

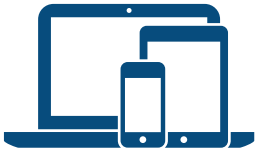
**Le secrétaire général des ministères sociaux - haut fonctionnaire de défense et de sécurité (HFDS)** -, anime et coordonne la politique en matière de défense et de sécurité, de vigilance, et de prévention de crise et de situation d'urgence, coordonne les mesures d'application et en contrôle la mise en œuvre. La sécurité numérique, est placée sous l'autorité du fonctionnaire en charge de la sécurité des systèmes d'information (FSSI), tête de chaîne fonctionnelle SSI ministérielle. En lien avec l'agence nationale de la sécurité des systèmes d'information (ANSSI), le FSSI anime et coordonne la politique de sécurité des systèmes d'information (SSI) et la stratégie de réponse aux cyberattaques pour les champs des ministères sociaux. Le FSSI assure le pilotage du traitement des incidents SSI, en s'appuyant sur le CERT Santé.

**La Délégation ministérielle au Numérique en Santé (DNS)** assure le pilotage de l'ensemble des chantiers de transformation du numérique en santé, dont le volet sécurité numérique, en lien avec le service du HFDS, en charge de coordonner la politique de sécurité numérique ministérielle. La doctrine technique de la feuille de route du virage numérique de Ma santé 2022 incorpore la sécurité et l'interopérabilité des SI en santé. La DNS assure le pilotage de l'Agence du Numérique en Santé (« ANS »), dont la mission est centrée sur la mise en œuvre opérationnelle de la politique du numérique en santé, dont la cybersécurité.

**Les agences régionales de santé (ARS)** s'assurent de la déclinaison territoriale de la politique de sécurité numérique en santé.
L'ARS anime et accompagne le volet cyber du virage numérique des territoires : sensibilisation des acteurs, partage de pratiques, recherche de mutualisations, organisation de la réponse à incident au niveau d'un territoire de santé, contrôle du niveau de maturité cyber et des plans d'actions continus des structures de santé.

**L'Agence du Numérique en Santé (ANS)** accompagne et accélère la transformation numérique du système de santé aux côtés de tous les acteurs concernés des secteurs sanitaire, social et médico-social, privés comme publics, professionnels ou usagers. Elle s'attache à fédérer les initiatives territoriales en s'appuyant sur les agences régionales de santé (ARS) et les structures de maîtrise d'ouvrage régionales.
Son activité s'articule autour de 4 rôles :

- Rôle de *régulateur* : elle améliore la performance numérique grâce à des règles communes de régulation et d'échanges
- Rôle *d'opérateur* : elle conçoit les grands e-programmes nationaux pour un service public de santé efficace et solidaire
- Rôles *de promoteur et de « valorisateur »* : elle stimule, accompagne, et évalue pour porter toutes les initiatives de e-santé »



TOUS CYBER VIGILANTS

## Plus d'informations sur :

touscybervigilants.fr
touscybervigilants@esante.gouv.fr

**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

ANS - Agence du Numérique en Santé
9, rue Georges Pitard 75015 Paris
01.58.45.32.50

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
*Liberté*
*Égalité*
*Fraternité*

AGENCE DU NUMÉRIQUE EN SANTÉ

l'agenceverte Mai 2021