AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

MINISTÈRE DU TRAVAIL, DE LA SANTÉ, DES SOLIDARITÉS ET DES FAMILLES
Liberté
Égalité
Fraternité

Direction générale de la recherche, de l'innovation et du numérique en santé

Financé par l'Union européenne
NextGenerationEU



Webinaire de clôture du Cybermois

Prévenir, se conformer, progresser

2 novembre 2026

Domaine Cybersécurité

Webin-aire

Nos webinaires pour construire la e-santé de demain !

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Webinaire, les bonnes pratiques



Le micro et la caméra sont automatiquement coupés sauf pour les intervenants.



Je pose mes **questions** dans **l'espace Questions/Réponses.**



Je ne pose **pas mes questions dans l'espace conversation.** Celles-ci ne seront pas traitées.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Déroulé du webinaire

1. **Fuites de données :**
   état de la menace et bonnes pratiques pour réduire les risques
2. **Régulation cyber des solutions numériques en santé :**
   dispositif incitatif et réglementation européenne
3. **Programme CaRE :**
   point d'étape
4. **Ressources mises à disposition**

Nos intervenants



Steven GARNIER
Directeur de domaine



Estelle NICAUD
Directrice de programme



Thomas DAMONNEVILLE
Analyste menaces



Vincent CROISILE
Expert sécurité



Ange HIRSCH
Expert sécurité

AGENCE DU NUMÉRIQUE EN SANTÉ



Christophe MATTLER
Directeur de programme

MINISTÈRE DU TRAVAIL DE LA SANTÉ ET DES SOLIDARITÉS
Liberté
Égalité
Fraternité

Direction générale de la recherche, de l'innovation et du numérique en santé

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

1. Fuites de données :

État de la menace et bonnes pratiques pour réduire les risques

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Le constat

Partie 1 · Des fuites en forte hausse

Des fuites en hausse, des attaques simples

196 violations de données suivies par le CERT-FR en 2025

Contre 130 en 2024, tous secteurs confondus

99 violations signalées par les services de l'État depuis le 1er août 2026

Dont 67 confirmées (opération REACTIV)

La plupart des fuites ne mettent en œuvre aucune faille technique

- **Identifiants légitimes réutilisés**
- **Ingénierie sociale**
- **Données exposées sans contrôle d'accès**

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

État de la menace

Partie 2 · Comment les données fuitent

État de la menace : Quatre grands scénarios de fuite

Usurpation d'identifiants

Des comptes légitimes volés, puis rejoués par l'attaquant : le scénario le plus fréquent

Vulnérabilités applicatives

Des failles connues exploitées, souvent bien après la publication du correctif

Accès direct aux données

Une erreur de configuration expose un stockage ou un service sans contrôle d'accès

Internes et tiers

Collaborateur malveillant, compte non révoqué après un départ, prestataire compromis

Webin-aire
Nos webinaires pour construire la e-santé de demain !

L'usurpation d'identifiants, une chaîne industrialisée



Un marché organisé

Des acteurs spécialisés infectent les postes, d'autres achètent et exploitent les accès.
Les identifiants volés se vendent en lots ou par abonnement.

Invisible pour la victime

Rien n'est chiffré ni détruit et la connexion paraît normale : pour le système, l'attaquant est un utilisateur légitime.

Webin-aire
Nos webinaires pour construire la e-santé de demain !

CE QU'ILS VOLENT

- **Mots de passe enregistrés dans le navigateur**
- **Cookies de sessions déjà ouvertes**
- **Certificats, portefeuilles et autres secrets**

COMMENT

- **Logiciels gratuits, faux installeurs**
  Cracks, utilitaires, faux convertisseurs de documents
- **Publicités piégées**
  Y compris en tête des résultats de recherche
- **Phishing**
  Liens et pièces jointes malveillants
- **ClickFix**
  Une commande à copier-coller « pour corriger un problème »

Ce qui transforme un compte volé en fuite massive

MFA absente ou faible

Un simple mot de passe, ou un code facilement contournable

Accès depuis des postes non administrés

Les identifiants pro se retrouvent sur des appareils personnels infectés

Droits trop larges, sans quotas

Un compte ordinaire peut consulter et extraire des volumes massifs

Exposition et cloisonnement insuffisants

Applications sensibles joignables depuis Internet ou des réseaux tiers

Journalisation et supervision lacunaires

Des exfiltrations de plusieurs gigaoctets passent inaperçues

Remédiation et correctifs tardifs

Sessions non révoquées, comptes oubliés, failles corrigées trop tard

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Bonnes pratiques

Partie 3 · Réduire les risques

Identité : sortir du login / mot de passe



MFA sur toutes les applications, résistante

Passkeys, clés FIDO ou application d'authentification ; pas de code par e-mail ; second facteur sur un autre appareil

Aucun appareil personnel pour les accès pro

Accès depuis des postes administrés et durcis uniquement ; séparation perso / pro contrainte techniquement

Des sessions courtes, liées au contexte, révocables

Réauthentification si l'IP, le pays ou le navigateur change ; toute réinitialisation révoque les sessions ouvertes

Bonnes pratiques – Droits et exposition : limiter la portée d'un vol

Mesure	Impact
Moindre privilège par profil métier	Un compte ordinaire n'accède plus à des volumes massifs
Quotas de volume et de requêtes	Le scraping est freiné, et devient visible
Restrictions horaires	Une connexion nocturne est bloquée ou signalée
Applications internes derrière VPN, segmentation	Plus d'accès direct depuis Internet ou un réseau tiers
Filtrage sur la réputation et la géolocalisation IP	VPN commerciaux, Tor et IP malveillantes bloqués ou signalés
Revue des comptes, désactivation des inactifs	Plus de comptes oubliés exploitables

Journaliser

- Chaque action attribuée à un compte et une IP
- Toutes les applications dans le SIEM
- Au moins six mois de rétention

Détecter et réagir

- Volumes et rythmes anormaux
- Connexions nocturnes, Tor, VPN
- Seuils métier, blocage automatique

Remédier jusqu'au bout

- Réinitialiser le mot de passe
- Révoquer toutes les sessions
- Analyser l'activité et nettoyer le poste

À retenir

MFA résistante au phishing sur toutes les applications

Corriger vite les applications exposées, revoir régulièrement les comptes

Aucun accès professionnel depuis un appareil personnel ou non administré

6 réflexes

Chaque application journalisée et supervisée, avec des alertes automatiques

Des droits au plus juste, des quotas de consultation et de requêtes

Réinitialiser un mot de passe
= révoquer les sessions et analyser l'activité

Pour aller plus loin

- RETEX du CERT-FR sur les violations de données applicatives
- Rapport d'incident DGFiP de l'ANSSI
- Fiches réflexes du CERT Santé

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

2. Régulation cyber des solutions numériques en santé

Dispositif incitatif et réglementation européenne

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Dispositif incitatif

Le Ségur du numérique en santé

Un programme national pour partager de façon fluide et sécurisée les données de santé

2 Md€ financés par l'État

Un investissement inédit pour intervenir dans la mise à jour des logiciels et le développement des usages

Le SONS - Système Ouvert et Non Sélectif

État finance
Achat pour le compte des structures

Éditeurs référencés
Conformité vérifiée par l'ANS

Structures équipées
Pas de surcoût sur le périmètre financé

Enjeux de sécurité

- **Les logiciels, vecteurs d'attaque vers le SI des structures**
- **Interconnexion croissante : Mon espace santé, MSSanté**
- **Données de santé sensibles, activité des structures exposée**

Ségur vague 2 : Un socle d'exigences cyber, à démontrer pour être référencé

Pour la première fois, des exigences de cybersécurité harmonisées sont intégrées aux REM de tous les couloirs

Gestion des vulnérabilités

Détecter, traiter et suivre les failles

Sécurisation de l'hébergement

Intégration du PAS ou HDS, processus de sauvegarde défini

Développement sécurisé

Réduire les risques dès la conception

Authentification et contrôle d'accès

Limiter les accès non autorisés

Journalisation et traçabilité

Faciliter la détection et l'analyse d'incidents

Documentation SSI

Formaliser les mesures de sécurité

Gouvernance sécurité

Piloter la cybersécurité et sensibiliser les équipes projet

Test d'intrusion indépendant

Attester l'absence de vulnérabilités critiques du Top 10 OWASP

Un référentiel commun et vérifiable, pour la sécurité sur tout le cycle de vie du logiciel

Le Ségur fait monter en maturité les éditeurs, au bénéfice direct des établissements

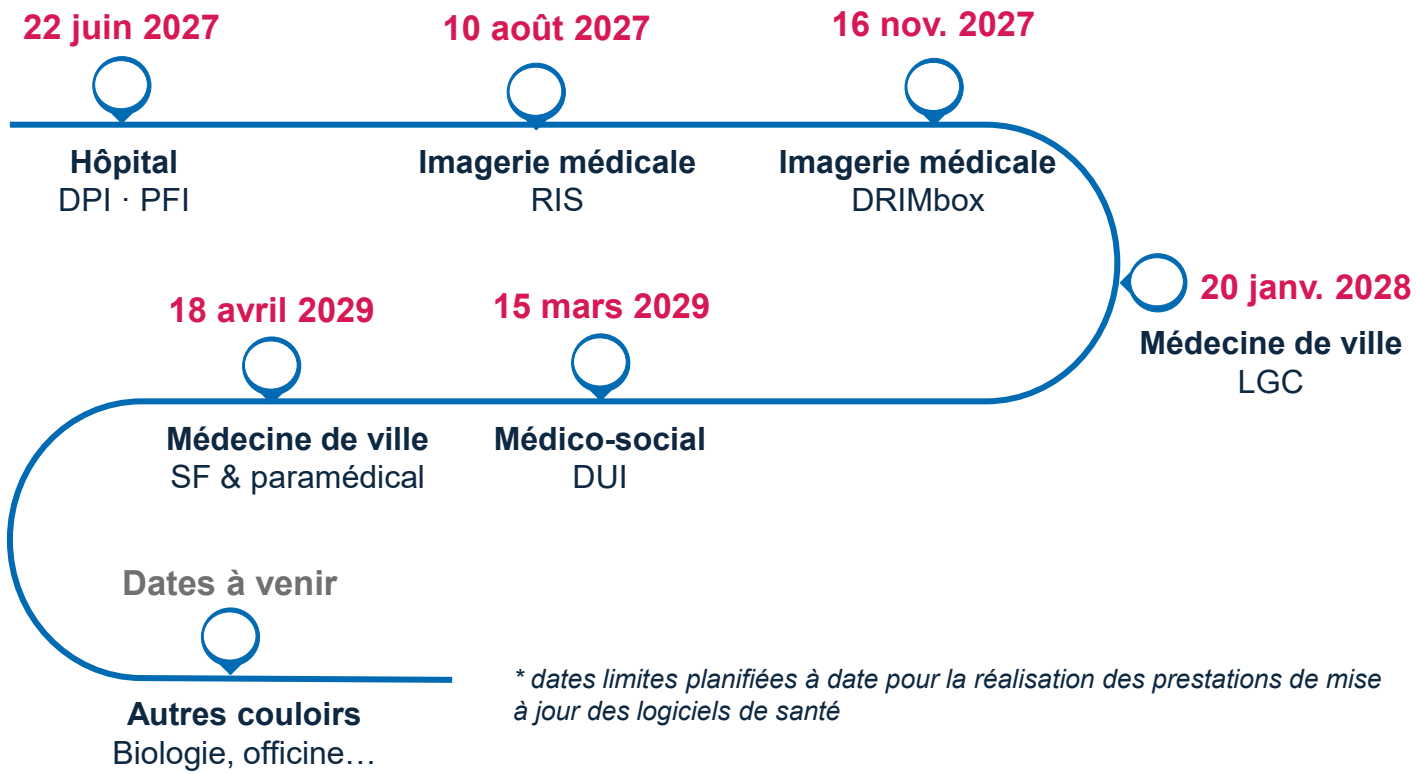
Établissements
Moins de risques de compromission

Logiciels robustes
Mieux maintenus, correctifs rapides

Éditeurs candidats
Démontrer, tester, corriger

Exigences REM
Socle cyber commun à tous les couloirs

Calendrier de déploiement*



** dates limites planifiées à date pour la réalisation des prestations de mise à jour des logiciels de santé*

À l'hôpital, le programme CaRE complète le Ségur : financement, accompagnement et montée en maturité cyber

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Réglementation européenne

Le Cyber Resilience Act

Un niveau minimal de cybersécurité pour tous les produits numériques mis sur le marché de l'UE

Qui est concerné ?

- Éditeurs de logiciels de santé, y compris certaines solutions intégrant des services SaaS/cloud
- Fabricants de dispositifs médicaux numériques (hors marquage CE)
- Fabricants d'objets connectés de santé
- Intégrateurs commercialisant sous leur propre marque

Trois obligations clés

Sécuriser dès la conception
Sécurité intégrée au développement, paramètres sûrs par défaut

Gérer les vulnérabilités
Détecter, corriger, diffuser les correctifs, divulguer de façon coordonnée

Démontrer la conformité
Documentation technique, preuves, surveillance après mise sur le marché

Du produit à son maintien en condition de sécurité : « by design » et « by default »

Le meilleur moment pour se préparer : maintenant

Déjà applicable

11 septembre 2026

Notifier les vulnérabilités activement exploitées et les incidents graves, via la plateforme unique de l'ENISA

24 h Alerte initiale → **72 h** Informations complémentaires → **Fin** Rapport final

11 décembre 2027

Application complète du CRA

Toutes les autres obligations : conception, vulnérabilités, conformité et maintien en conditions de sécurité

À engager dès aujourd'hui

1. Identifier les produits entrant dans le champ du CRA
2. Mettre en place une gouvernance cyber produit
3. Formaliser la gestion des vulnérabilités et incidents
4. Maîtriser les composants logiciels (SBOM)
5. Savoir détecter, qualifier et notifier vulnérabilités et incidents
6. Intégrer le CRA dans le cycle de développement

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

3. Programme CaRE : point d'étape

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Revue des axes du programme

Les 4 axes du plan d'action CaRE

Gouvernance et résilience

Renforcer la gouvernance et la résilience en cybersécurité dans le secteur de la santé, en articulation avec les niveaux national, régional et local

Ressources et mutualisation

Prise en compte de la pénurie de talents et de ressources dans les établissements, et mise en avant du besoin de mutualiser et de pérenniser les ressources humaines.

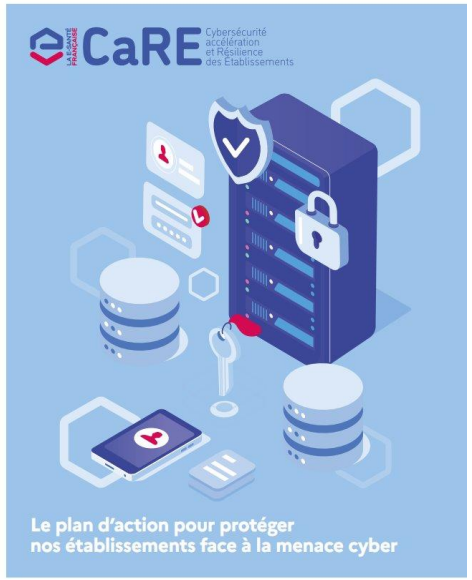


Sensibilisation

Encourager un engagement fort de chacune des parties prenantes de la cybersécurité dans les établissements de santé.

Sécurité opérationnelle

Soutenir financièrement les investissements jugés prioritaires via des « Domaines » (via des appels à financements et/ou appels à projets).



Le plan d'action du programme CaRE se décline autour de 4 axes

Webin-aire
Nos webinaires pour construire la e-santé de demain !

AXE 1 Gouvernance et résilience

Préparation de la réponse aux crises cyber

- Portage des actions d'élaboration des **PCRA** et de leurs **tests au** travers des **kits PCRA** et de l'**intégration** d'un **volet numérique** au plan blanc au **domaine 2**
- **Publication** des **kits exercices de crise v2** pour maintenir la dynamique de réalisation

Démarche d'auto-évaluation de la maturité par les ES et ESSMS

- **Publication d'une nouvelle version de l'OPSSIMS** destiné aux ESSMS
- Evaluation de la **maturité sur l'identification électronique intégrée à HospiConnect**

AXE 2 Ressources et mutualisation

Catalogue des offres cyber ***mis à jour mensuellement***

- **493** offres publiques et **549** offres d'industrielles recensées

CRRC

- **Développement et ancrage** des CRRC lancés en 2024 et soutenus à hauteur de **26 M€** dont **8 M€** dédiés au secteur médico-social

AXE 3 Sensibilisation

Etude de perception des risques cyber dans les ES

- **Publication** de l'étude répondue par **719 directeurs d'établissements**

Témoignages

- **Partage** de plusieurs **RETEX** d'établissements sur **la gestion de cyberattaques**

AXE 4 Sécurité opérationnelle

Domaines prioritaires

- **Atteinte des cibles du Domaine 1** « Annuaires techniques et exposition sur internet » par 939 candidats payés sur 1181 engagés
- **Lancement du Domaine 2** « Stratégie de continuité et de reprise d'activité »
- **Lancement de la généralisation HospiConnect,** portant sur les thématiques d'identification électronique
- **Lancement du POC de l'AAP médico-social** avec 3 parcours déclinés selon la maturité des ESSMS

Webinaire
Nos webinaires pour construire la e-santé de demain !

Le programme CaRE a déployé un appui méthodologique et financier afin d'accompagner les établissements dans leur préparation à la crise de manière durable selon 3 volets.



S'ENTRAÎNER

+ de 2 220

exercices de crise réalisés

Publication d'un kit ANS "Exercice de crise" v1, soutien financier pour leur réalisation en 2023-2024 et publication d'un kit v2 en 2025



ANTICIPER

1 kit PCRA

méthodologique

Adaptation aux besoins des ES et des ESSMS, du cadrage au maintien en condition opérationnelle



ANCRER

641

visites de certification HAS en 2025

Intégration de critères numériques et cyber dans la certification HAS depuis 2024

Les CRRC proposent des services mutualisés et personnalisables, pour mieux prévenir et gérer la cybersécurité des établissements de santé

- **Aider** les structures sanitaires et médico-sociales à renforcer leur cybersécurité
- **Concevoir des services** pour prévenir et réagir aux cyberattaques
- **Proposer des formations et sensibiliser** aux bonnes pratiques en cybersécurité
- **Mobiliser** les capacités de soutien nécessaires en cas d'incident cyber

Prenez contact avec votre CRRC pour être accompagné dans le renforcement de votre cybersécurité



Cartographie des GRADeS portant les CRRC

Webin-aire
Nos webinaires pour construire la e-santé de demain !

Dans le cadre de l'axe 2 du programme CaRE, les ARS mettent en place des Centres Régionaux de Ressources Cyber (CRRC) depuis 2024 afin d'accompagner les établissements sanitaires et médico-sociaux dans le renforcement de leur cybersécurité.

Objectifs des CRRC

O.G.1
Soutenir les ES/ESMS dans l'atteinte des objectifs des différents domaines

O.G.2
Promouvoir les domaines CaRE auprès des ES/ESMS

O.G.3
Construire un échelon de réponse régional lors des incidents cyber (Hors CERT)

O.G.4
Accompagner les établissements dans le déploiement du PCRA « CaRE »

O.G.5
Animer la communauté cyber de la région

O.G.6
Sensibiliser les acteurs sanitaires et médico-sociaux en région

O.G.7
Accompagner la formation cyber des professionnels informatiques

O.G.8
Favoriser l'émergence d'initiatives autour de la cybersécurité
Objectif optionnel

O.MS.1
Diagnostic cyber

O.MS.2
Renforcement de la maturité

O.MS.3
Accompagnement aux exercices de crise cyber

Exemples d'actions menées

- Réalisation de diagnostics de maturité cyber
- Réalisation d'exercices de crise
- Sensibilisation auprès des professionnels de santé et administratifs des établissements
- Organisation de formations
- Diffusion de la méthodologie PCA/PRA
- Communication sur le programme
- Mise en place de marchés de prestation cyber
- Mise en œuvre de projets innovants

Les CRRC, à l'issue de leurs 2 premières années, participent directement à la montée en maturité cyber des établissements sanitaires et médico-sociaux.

Axe 3 : Sensibilisation – Étude de perception

Une étude nationale a été menée en mai-juin 2025 auprès des directeurs d'établissements de santé afin d'analyser leur perception du risque cyber, de mieux comprendre les arbitrages auxquels ils sont confrontés et d'identifier les leviers susceptibles de renforcer la résilience du secteur. Cette démarche s'inscrit dans l'ambition du programme CaRE de placer la cybersécurité au cœur du pilotage des établissements.

Mobilisation nationale

- **719 directeurs d'établissements de santé ont répondu dans le cadre d'une enquête nationale sur la perception du risque cyber**
- **Association des fédérations hospitalières, ARS et GRADeS pour relayer et promouvoir l'enquête auprès des établissements**
- **Expression directe des directions d'établissements, afin de mieux comprendre leurs enjeux, leurs arbitrages et leurs attentes**

1. **La cybersécurité : une compétence technique à une compétence stratégique au cœur des arbitrages des Directeurs des établissements de santé**
2. **La continuité des soins, priorité des Directeurs d'établissements de santé en cas de cyber attaque : un atout pour renforcer la confiance des usages**
3. **La coopération et la mutualisation des expertises territoriales considérées comme levier de performance par les directeurs d'établissements de santé**
4. **Le soutien financier du programme considéré comme nécessaire et à pérenniser**

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Zoom sur l’axe 4

L'axe 4 du programme CaRE, consacré à la **sécurité opérationnelle**, est décliné en plusieurs domaines spécifiques.
Chacun de ces domaines vise à **traiter une problématique technique précise** et **à combler les lacunes existantes en matière de cybersécurité**, afin de renforcer la protection des systèmes d'information des établissements de santé.

Les domaines de financement

Terminé
Domaine « Annuaire techniques et exposition internet »

En cours
Domaine « Stratégie de continuité et de reprise d'activité »

À venir
Domaine « Sécurisation des accès distants »

À venir
Domaine « Supervision des postes de travail »

En cours
HospiConnect

En cours
Appel à projet médico-social

Webin-aire
Nos webinaires pour construire la e-santé de demain !

Des résultats concrets ont été atteints grâce à la mise en œuvre de ce premier domaine de financement.

1er dispositif de financement dédié à la cybersécurité pour les établissements de santé

1er AAF du programme CaRE, ayant mis en visibilité le programme auprès des ES

1er dispositif de financement d'ampleur porté par l'ANS de « bout en bout »



x3

Part des AD répondant au niveau de sécurité attendu



x11

Nombre de collecte ADS réalisées mensuellement sur le service de l'ANSSI



÷14

Nombre d'ES avec une vulnérabilité critique exposée



+237%

Nombre d'établissements inscrits au service SILENE



1504

Entités juridiques ayant atteint les objectifs du domaine



43 M€

Délégués aux établissements pour les soutenir dans leur action



86%

Des directions générales s'impliquent dans les exercices de crises cyber

Pour les établissements, le domaine 1 du programme CaRE a donné "**un cadre et des moyens**" pour accélérer le renforcement de la cyber-résilience

Guillaume Coquet – DSI, Groupe Santelys

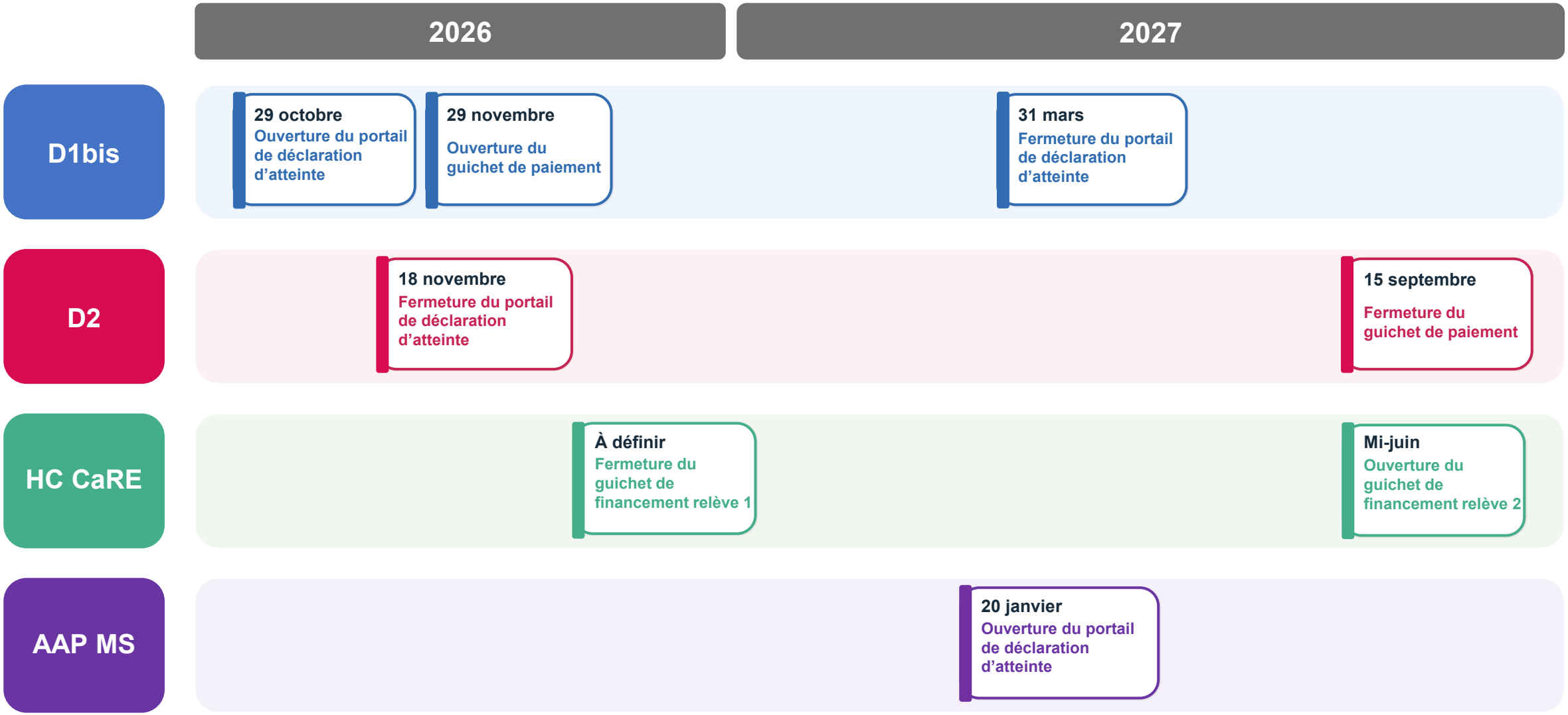
Bilan du domaine 1 (2/2)

Pour rappel, le domaine a été lancé le **18 mars 2024** avec la publication de l'arrêté portant création de l'appel à financement. Ce lancement à permis la mise en œuvre d'une plateforme de candidature pour **1428 candidats éligibles (65 millions d'euros).** Il a atteint une dernière étape lors de la clôture du guichet de paiement survenue le **30 juin 2026**. Les chiffres présentés ci-dessous illustrent **les résultats obtenus à chaque phase** du domaine :

Phase 1 Candidature	Phase 2 Dépôt des dossiers d'atteinte	Phase 3.A Contrôle de conformité	Phase 3.B Contrôle financier
1182 Dossiers de candidatures validés	**1049** Dossiers d'atteinte transmis	**943** Dossiers validés par la conformité	**939** Dossiers payés*
81% Des candidats éligibles	**89%** Des candidats engagés Soit 73 % des candidats éligibles	**89%** Des candidats dont le dossier a été transmis Soit 66 % des candidats éligibles	**99%** Des candidats validés par la conformité Soit 66 % des candidats éligibles
63,5M Montant plafond des validés	**58,5M** Montant plafond des déposés	**52M** Montant plafond validé par la conformité	**43M** Montant validé par la DAF et l'AC

** Montant supérieur à 0*

Prochains jalons des domaines



La direction du programme CaRE réalise une enquête afin d'orienter les travaux à venir

Objectifs

1. Évaluer la perception du programme
2. Mesurer l'appropriation des dispositifs déployés
3. Identifier les éventuelles difficultés rencontrées
4. Recueillir des propositions d'amélioration

Cibles



DG et RSSI d'établissements



ARS et GRADeS



Fédérations hospitalières

Diffusion

Enquête réalisée sur la plateforme Grist fournie par la DINUM

- Envoi par la direction du programme aux ARS, RSSI et fédérations
- Envoi par les ARS aux DG d'établissements et aux GRADeS

Réponses attendues avant le 27/11

7

articles publiés dans le cadre du Cybermois

Face aux cyberattaques : les enseignements de 2 établissements pour mieux se préparer

Continuité et reprise d'activité : trois établissements partagent leur démarche

Du diagnostic à l'action : le retour d'expérience de 2 établissements engagés dans le domaine 1

Cybersécurité dans le médico-social : adapter l'accompagnement aux réalités du terrain

Cyber Resilience Act : une nouvelle étape pour la cybersécurité des produits numériques

Décryptage RIE v2

Ségur du Numérique Vague 2 : la cybersécurité devient un critère de référence

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

4. Ressources mises à disposition

Webin-aire
Nos webinaires pour construire la e-santé de demain !

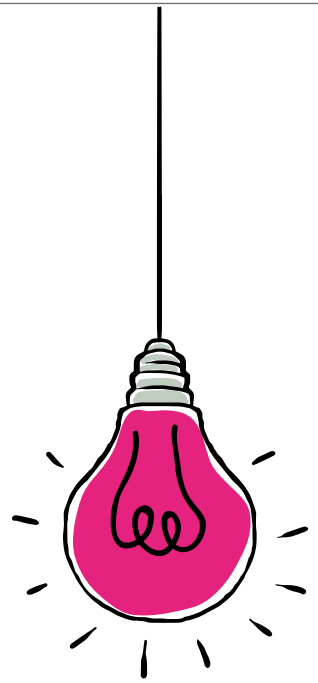


Fiche sécurité 2026 de la Doctrine du numérique en santé :
https://esante.gouv.fr/doctrine/securite

Page web dédiée à la PGSSI-S :
https://esante.gouv.fr/produits-services/pgssi-s

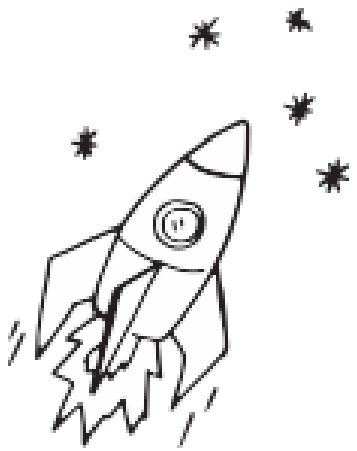
Site internet du CERT Santé :
https://cyberveille.esante.gouv.fr/

Page web dédiée au Programme CaRE :
https://esante.gouv.fr/strategie-nationale/cybersecurite



Ce webinaire est enregistré et le replay sera mis à disposition sur la chaine Youtube de l'ANS



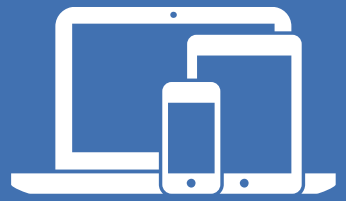


MERCI POUR VOTRE ATTENTION

ET A BIENTÔT

AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici



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