Appel à projets national

Mise en œuvre de mesures de cybersécurité pour les établissements et services du secteur social et médico-social (ESSMS) – phase exploratoire (POC)

Cahier des charges

Réponse possible jusqu'au 4 juin 2026 à 16h00 - heure de Paris).

Statut : Finalisé | Classification : Public | Version finale

Table des matières

1. Enjeux et contexte

Vers une cybersécurité renforcée pour le médico-social

Le numérique occupe une place de plus en plus centrale dans le secteur social et médico-social. De nombreux établissements et services sociaux et médico-sociaux (ESSMS) s'engagent dans l'informatisation ou la modernisation de leur système d'information, avec pour objectifs d'améliorer la qualité de l'accompagnement, de faciliter les échanges avec les partenaires et le secteur sanitaire, ainsi que d'optimiser leur fonctionnement interne.

Cette transformation est soutenue par le Ségur du numérique, et plus particulièrement les programmes SONS et ESMS Numérique. Ces dispositifs visent à favoriser l'interopérabilité des outils numériques et à renforcer la coordination entre acteurs, en accompagnant les ESSMS dans le déploiement d'un Dossier Usager Informatisé (DUI) référencé Ségur et dans l'adoption des services et référentiels socles.

A la faveur de ces programmes, le niveau d'équipement en DUI référencés Ségur s'est significativement élevé : près de deux tiers des ESSMS sont dorénavant équipés ou en passe d'être équipés d'un DUI référencé Ségur.

Si cette transformation est essentielle pour mieux accompagner les personnes et fluidifier leur parcours, la dématérialisation croissante des données sensibles et leur circulation entre professionnels augmentent les risques d'atteinte à la confidentialité, suppression ou altération, dus à des attaques ou à des erreurs humaines. Le manque de sensibilisation, notamment chez les professionnels mobiles, accentue la vulnérabilité des ESSMS.

En 2024, 153 incidents ont été déclarés pour les ESSMS. En 2025, ce nombre atteint 204 déclarations d'incidents dont 113 d'origine malveillante..

Faute d'investissement ciblé, la cybersécurité repose sur des bases fragiles : des effectifs experts des sujets cyber trop peu nombreux, des investissements financiers trop faibles, peu de formation à l'hygiène informatique et des équipements informatiques souvent obsolètes. Un incident cyber peut donc se produire et gravement perturber les services, bloquer la paie ou interrompre l'accompagnement et les soins. Les données personnelles, très convoitées et cibles privilégiées des cyberattaquants, exposent les usagers à des risques d'usurpation d'identité et les structures à des coûts de récupération pouvant atteindre plusieurs dizaines de milliers d'euros. Les ESSMS doivent aussi faire face à un cadre réglementaire exigeant (RGPD, PGSSI-S, NIS 2), souvent mal maîtrisé.

Le programme CaRE : une réponse collective et structurée face au risque cyber

Pour donner suite aux cyberattaques subies par plusieurs établissements de santé, une Task Force dédiée a été mise en place sur décision de Matignon en décembre 2022. Celle-ci :

- Avait pour objectif de construire un plan cyber pluri annuel massif ;
- Devait s'appuyer sur l'expérience du Ségur et des mécanismes mis en place : déploiement massif et généralisé faisant suite à des phases pilotes, trajectoire itérative, travail avec

l'ensemble des acteurs concernés, activation de l'ensemble des leviers à disposition (réglementaires, incitatifs, coercitifs, référencements, objectifs).

La Task Force est coordonnée par la Délégation au Numérique en Santé (DNS) et rassemble le Haut Fonctionnaire de Défense et de Sécurité (HFDS), le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI), l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), la Direction Générale de l'Offre de Soins (DGOS), l'Agence du Numérique en Santé (ANS), des représentants des Agences Régionales de Santé (ARS) et des Groupements Régionaux d'Appui au Développement de la e-Santé (GRADeS) et les fédérations hospitalières et médico-sociales. La DNS s'appuie sur l'ANS pour piloter les travaux du programme CaRE (Cybersécurité accélération Résilience des Etablissements).

Le programme CaRE décline un plan d'action concret et ambitieux pour la période de 2023 à 2027. Le programme se décline en 4 axes et 20 objectifs :

1. Gouvernance et résilience
2. Ressources et mutualisation
3. Sensibilisation
4. Sécurité opérationnelle

Ce dernier axe, Sécurité opérationnelle, vise à renforcer la sécurité technique des systèmes d'information des établissements, en améliorant la détection des failles, la correction des vulnérabilités et la capacité de reprise après incident. Cela passe par le financement d'actions ciblées. Plusieurs dispositifs de financement ont d'ores et déjà été lancés :

- Domaine 1 : sécurisation des annuaires d'établissements et de leur exposition à Internet.
- Domaine 1 bis : extension du domaine 1 visant à étendre le dispositif de financement à des structures non couvertes par le domaine 1.
- Domaine 2 : stratégie de sauvegarde des données et continuité d'activité.
- HospiConnect : déploiement de moyens d'identification électroniques (MIE) permettant la sécurisation des accès au système d'information.

Des travaux sont en cours pour le lancement d'autres domaines qui viendront compléter cette stratégie, notamment sur la protection des postes de travail et la sécurisation des pratiques liées aux accès distants.

Le volet social et médico-social intègre pleinement le programme et nécessite une adaptation pour répondre aux enjeux spécifiques du secteur.

Un appel à projets de cybersécurité dédié exclusivement au secteur social et médico-social

L'intégration des ESSMS dans les dispositifs de financement a d'abord été envisagée à partir du domaine 2. Toutefois, au regard de la forte hétérogénéité du secteur, tant en matière de typologie d'établissements que de niveaux de maturité en cybersécurité, cette approche a été réévaluée.

À l'issue de plusieurs ateliers de construction des objectifs du domaine 2 dédiés aux ESSMS, il a été décidé de ne pas les intégrer aux appels à financements sanitaires existants, mais de concevoir un appel à projets spécifique, mieux adapté aux réalités du secteur, à sa complexité organisationnelle, ainsi qu'à l'hétérogénéité de sa maturité en matière de cybersécurité.

Cet appel à projets adopte un format itératif, avec plusieurs cycles prévus sur plusieurs années, permettant une mise en œuvre progressive et ajustable.

Face aux interrogations sur la manière d'impliquer l'ensemble du secteur, la **première itération sera lancée sous la forme d'un POC (preuve de concept)**. Pensée comme une phase exploratoire, elle a pour objectif d'étudier les conditions de généralisation de l'appel à projets à l'ensemble du secteur social et médico-social. Pour tenir compte de l'hétérogénéité des structures, plusieurs parcours de cybersécurité sont proposés. Cette diversité d'approches permettra de sélectionner un panel de lauréats aussi représentatif que possible du secteur, dans un premier temps en nombre limité, afin de tirer des enseignements concrets de cette phase pilote.

Les retours issus de cette première étape permettront d'ajuster les itérations suivantes, qui viseront à élargir à la fois le nombre de bénéficiaires et les thématiques abordées. Ces prochaines phases intégreront également de nouveaux parcours cyber complémentaires, afin de mieux répondre aux besoins variés du secteur et de renforcer progressivement sa maturité en cybersécurité.

Cet appel à projet repose sur l'arrêté du 11 mai 2020 modifiant l'arrêté du 9 décembre 2009 fixant les modalités d'attribution par l'ASIP Santé de financements visant à favoriser le développement des systèmes d'information partagés de santé, pris sur le fondement et pour l'application du troisième alinéa de l'article L. 1111-24 du code de la santé publique.

Les conditions et les modalités de sa mise en œuvre, approuvées par délibération du conseil d'administration de l'ANS du 11/03/2026, sont définies dans le présent cahier des charges

A noter : Le présent cahier des charges s'applique exclusivement à cette première phase exploratoire. Les critères, modalités et parcours décrits sont susceptibles d'évoluer dans le cadre des itérations ultérieures, au regard des enseignements tirés de cette phase d'expérimentation.

2. Conditions d'éligibilité à l'itération d'expérimentation de l'appel à projets

Est éligible à l'appel à projets « Mise en œuvre de mesures de cybersécurité pour les établissements et services du secteur social et médico-social (ESSMS) » tout projet qui respecte les conditions cumulatives suivantes.

2.1. Thématique et objectifs du projet

Le présent appel à projets s'inscrit dans les objectifs globaux du programme CaRE, qui vise notamment à :

- Améliorer la résilience des systèmes d'information en développant des capacités pour détecter, répondre et se remettre rapidement de cyber-attaques ;
- Développer les connaissances et compétences des professionnels du secteur sur les pratiques de cybersécurité ;
- Réduire l'exposition des structures aux menaces ;
- Renforcer la capacité des structures du secteur à se doter de ressources SSI via la mutualisation ;
- Engager l'ensemble du secteur médico-social dans une démarche de progression de leurs pratiques cyber.

Pour répondre à ces enjeux, cet appel à projets propose **trois parcours de cybersécurité** axés sur le niveau de maturité initial des candidats. Chaque parcours propose des objectifs à atteindre obligatoirement regroupés dans trois thématiques et des objectifs à atteindre « à la carte » relatifs à la mise en œuvre d'un socle minimal et essentiel de mesures techniques et organisationnelles de cybersécurité.

Avant de pouvoir accéder aux trois parcours, les structures candidates doivent remplir plusieurs prérequis pour candidater à l'appel à projets :

- Disposer d'un **dossier usager informatisé (DUI) référencé Ségur** ;
- Formaliser un **engagement** écrit de la part de la Direction de la structure porteuse pour la mise en œuvre des projets de cybersécurité à laquelle elle s'engage, et engage tous les ESSMS de son regroupement le cas échéant ;
- Réaliser un **cyberdiagnostic** : un premier autodiagnostic est effectué via l'Observatoire Permanent de la Sécurité des Systèmes d'Information dans le médico-social (OPSSIMS[1]), puis

[1] https://esante.gouv.fr/essms/cybersecurite

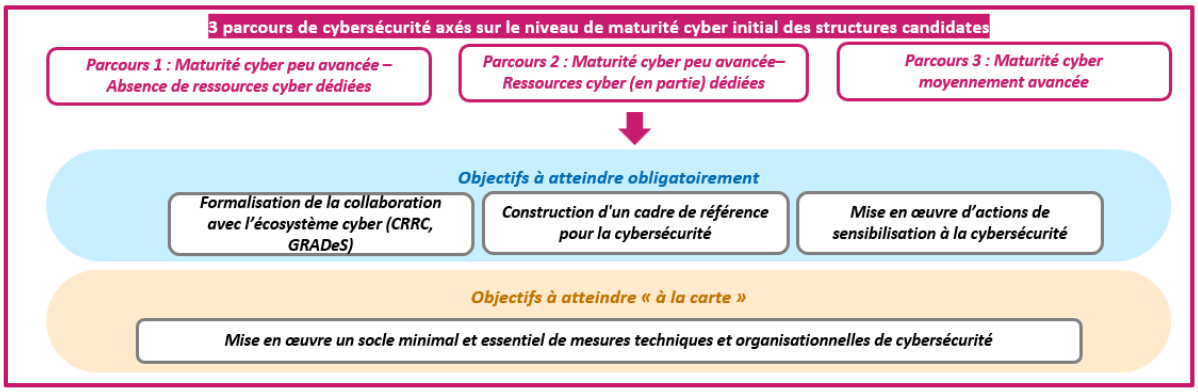
validé avec le CRRC[2] (éventuellement via l'outil régional de cyber diagnostic) afin de confirmer et d'orienter le candidat vers un parcours de cybersécurité adapté.

Le diagnostic OPSSIMS à réaliser correspond à la version du 26 janvier 2026.

Le choix du parcours de cybersécurité s'inscrit directement dans la lignée des prérequis d'accès au dispositif, et en particulier dans la réalisation du cyberdiagnostic préalable. En effet, les CRRC accompagnent les structures candidates dans l'analyse des résultats du diagnostic et dans l'orientation vers le parcours de cybersécurité le plus adapté à leur situation, afin de garantir une entrée réaliste dans le dispositif et une capacité effective à atteindre les objectifs du parcours choisi.

Le candidat ne peut se positionner que sur un seul parcours pour le POC. Il pourra toutefois se porter candidat à un autre parcours (plus avancé) sur les itérations ultérieures de l'appel à projet.
L'ANS se réserve la possibilité, en lien avec les régions, d'autoriser un changement de parcours de cybersécurité en cours d'expérimentation, lorsque les difficultés rencontrées par un lauréat ne lui permettent pas d'atteindre les cibles initialement fixées, afin de privilégier l'atteinte d'objectifs adaptés plutôt qu'une interruption des travaux engagés.

Les différents parcours et objectifs à atteindre sont présentés ci-après :



[2] Centre régional de ressources cybersécurité, créé par l'instruction n° DNS/2024/54 du 2 juillet 2024 relative aux missions des centres régionaux de ressources cybersécurité (CRRC).

Parcours 1 : Niveau de maturité peu avancé – Absence de ressource cyber dédiée

Ce parcours s'adresse aux candidats ayant un niveau de maturité cyber peu avancé, et ne disposant pas de ressource cyber interne, externe ou mutualisée dédiée.

Pour ce parcours, les lauréats devront choisir 2 objectifs à la carte.

Les objectifs à atteindre sont décrits ci-après :

Objectifs à atteindre obligatoirement	*Formalisation de la collaboration avec l'écosystème cyber (CRRC, GRADeS)*	POC.P1.O1.1 : Signer un acte de partenariat (format juridique libre) avec le GRADeS / CRRC
		POC.P1.O1.2 : Désigner un Correspondant SSI
	Construction d'un cadre de référence pour la cybersécurité	POC.P1.O2.1 : Élaborer une charte informatique et l'annexer au règlement intérieur
		POC.P1.O2.2 : Définir et appliquer une politique globale de sécurisation des modalités d'authentification
		POC.P1.O2.3 : Définir et appliquer une procédure formalisée de gestion des comptes utilisateurs nominatifs et mettre en place la matrice d'habilitation
	Mise en œuvre d'actions de sensibilisation à la cybersécurité	POC.P1.O3.1 : Mettre en œuvre des actions de sensibilisation *informative* auprès des Directions et du personnel
		POC.P1.O3.2 : Mettre en œuvre des actions de sensibilisation *applicative* auprès des Directions et du personnel
Objectifs à atteindre « à la carte »	*Mise en œuvre un socle minimal et essentiel de mesures techniques et organisationnelles de cybersécurité*	POC.P1.O4.A : Réaliser un inventaire du parc informatique et formaliser un plan de renouvellement sur les équipements obsolètes
		POC.P1.O4.B : Réaliser une cartographie applicative et fonctionnelle
		POC.P1.O4.C : Disposer d'un accès internet délivré par une offre professionnelle
		POC.P1.O4.D : Rédiger une procédure formalisée de signalement et d'alerte en cas d'accident cyber, et la diffuser auprès de l'ensemble du personnel
		POC.P1.O4.E : Mettre en place au moins une mesure identifiée comme prioritaire suite au diagnostic d'entrée dans les parcours. L'action doit

		être sélectionnée suite à un échange avec le GRADeS.

Parcours 2 : Niveau de maturité peu avancé – Ressources cyber dédiées

Ce parcours s'adresse aux candidats ayant un niveau de maturité cyber peu avancé, et disposant de ressources cyber internes, externes ou mutualisées (en partie) dédiées.

Pour ce parcours, les lauréats devront choisir 3 objectifs à la carte.

Les objectifs à atteindre sont décrits ci-après :

Objectifs à atteindre obligatoirement	*Contractualisation avec l'écosystème cyber*	POC.P2.O1.1 : Signer un acte de partenariat (format juridique libre) avec le GRADeS / CRRC
	Construction d'un cadre de référence pour la cybersécurité	POC.P2.O2.1 : Elaborer une charte de sécurité des SI et la diffuser auprès de l'ensemble du personnel
		POC.P2.O2.2 : Définir et appliquer une politique globale de sécurisation des modalités d'authentification
		POC.P2.O2.3 : Définir et appliquer une procédure formalisée de gestion des comptes utilisateurs nominatifs et mettre en place la matrice d'habilitation
		POC.P2.O2.4 : Mettre en place une comitologie cyber récurrente
	Mise en œuvre d'actions de sensibilisation à la cybersécurité	POC.P2.O3.1 : Mettre en œuvre des actions de sensibilisation *informative* auprès des Directions et du personne
		POC.P2.O3.2 : Mettre en œuvre des actions de sensibilisation *applicative* auprès des Directions et du personnel
Objectifs à atteindre « à la carte »	*Mise en œuvre un socle minimal et essentiel de mesures techniques et organisationnelles de cybersécurité*	POC.P2.O4.A : Réaliser un inventaire des composants du SI à l'aide d'un outil automatisé et retirer/remplacer tous les composants obsolètes
		POC.P2.O4.B : Réaliser une cartographie applicative et technique
		POC.P2.O4.C : Sécuriser le réseau Internet professionnel
		POC.P2.O4.D : Définir et appliquer une politique d'identification et de gestion des authentifications

		POC.P2.O4.E : Mettre en place au moins une mesure identifiée comme prioritaire suite au diagnostic d'entrée dans les parcours. L'action doit être sélectionnée suite à un échange avec le GRADeS
		POC.P2.O4.F : Définir une politique de sauvegarde et de restauration des données cohérentes avec les besoins métiers, à valider avec la direction
		POC.P2.O4.G : Rédiger une fiche « processus métier » en suivant la méthodologie de construction du PCRA, et la diffuser auprès du personnel concerné

Parcours 3 : Niveau de maturité moyennement avancé

Ce parcours s'adresse aux candidats ayant un niveau de maturité cyber moyennement avancé.

Pour ce parcours, les lauréats devront choisir 3 objectifs à la carte.

Les objectifs à atteindre sont décrits ci-après :

Objectifs à atteindre obligatoirement	*Formalisation de la collaboration avec l'écosystème cyber (CRRC, GRADeS)*	POC.P3.O1.1 : Signer un acte de partenariat (format juridique libre) avec le GRADeS / CRRC
	Structuration des référentiels de cybersécurité	POC.P3.O2.1 : Elaborer une PSSI
		POC.P3.O2.2: Elaborer des procédures de sécurité des SI
		POC.P3.O2.3 : Définir et appliquer une procédure formalisée de gestion des comptes utilisateurs nominatifs et mettre en place la matrice d'habilitation
	Mise en œuvre d'actions de sensibilisation à la cybersécurité	POC.P3.O3.1 : Mettre en œuvre des actions de sensibilisation *informative* auprès des Directions et du personnel
		POC.P3.O3.2 : Mettre en œuvre des actions de sensibilisation *applicative* auprès des Directions et du personnel
	Mise en œuvre un socle minimal et essentiel de	POC.P3.O4.A : Utiliser un réseau dédié et cloisonné pour l'administration

Objectifs à atteindre « à la carte »	*mesures techniques et organisationnelles de cybersécurité*	POC.P3.O4.B : Mettre en place un système d'enregistrement des logs de connexion internet, et de surveillance quotidienne du réseau et des équipements.
		POC.P3.O4.C : Réaliser un test d'intrusion, à renouveler annuellement
		POC.P3.O4.D : Mettre en place au moins deux mesures identifiées comme prioritaires suite au diagnostic d'entrée dans les parcours. Les actions doivent être sélectionnées suite à un échange avec le GRADeS
		POC.P3.O4.E : Mettre en place un système de sauvegarde intègre et immuable
		POC.P3.O4.F : Instaurer une organisation et des procédures pour assurer le suivi efficace des sauvegardes ainsi qu'un plan d'action pour gérer les alertes.
		POC.P3.O4.G : Mettre en œuvre la politique de sauvegarde et de restauration des données et tester les sauvegardes et les restaurations à fréquence régulière (tests techniques et fonctionnels)
		POC.P3.O4.H : Elaborer un PCRA sur le scénario d'indisponibilité des Systèmes d'Information

A noter : L'atteinte des objectifs définis dans le cadre des parcours de cybersécurité peut s'appuyer sur des actions réalisées ou engagées par la structure via d'autres dispositifs d'accompagnement. Ces actions peuvent être prises en compte pour valider l'atteinte des objectifs. En revanche, les actions déjà réalisées ou financées par d'autres dispositifs ne peuvent donner lieu à un financement au titre du présent appel à projets.

2.2. Profil et engagement du candidat

Profil du candidat

L'expérimentation est ouverte à l'ensemble des établissements et services sociaux et médico-sociaux (ESSMS) relevant de l'article L.312-1 du Code de l'action sociale et des familles (CASF).

Les ESSMS rattachés à des structures hybrides (sanitaire et médico-social) sont éligibles, dès lors que la candidature porte exclusivement sur le périmètre médico-social. Toute structure strictement sanitaire est exclue de cet appel à projets.
Sont également acceptés tous types de regroupements d'ESSMS, notamment :

- Organismes gestionnaires (OG),
- Grappes d'établissements formées dans le cadre du programme ESSMS numérique (en incluant tous les établissements composant la grappe),
- Groupements de coopération sociale ou médico-sociale (GCSMS),
- Groupements territoriaux sociaux ou médico-sociaux (GTSMS),
- Tout groupement constitué par une convention de partenariat spécifiquement signée dans le cadre de l'appel à projets médico-social.

A noter :

- Les différents types de groupement peuvent porter une candidature, cependant seuls les établissements et services du périmètre concerné sont éligibles au financement et pris en compte au titre du dispositif ;
- Les candidatures mono-établissement (mono-EJ) sont acceptées.

Porteur du projet et organisation du projet

Dans le cadre d'un groupement ou d'un organisme gestionnaire, le projet est porté collectivement par l'ensemble des établissements et services sociaux et médico-sociaux constituant le groupement.
Une entité est désignée comme porteuse de projet, agissant pour le compte de l'ensemble des établissements du groupement. Le porteur de projet assure la responsabilité administrative du dépôt de la candidature, de la contractualisation et de la gestion des subventions attribuées, sans préjudice de l'implication et de la responsabilité de chacun des établissements membres dans la mise en œuvre du projet.
Le porteur de projet devra correspondre à une structure appartenant aux établissements et services sociaux et médico-sociaux énumérés au I. de l'article L. 312-1 du CASF.

De manière générale (et pas uniquement pour les groupements), le candidat/groupement candidat s'appuiera sur sa propre organisation pour la mise en œuvre du projet et s'il en a le besoin sur un ou plusieurs fournisseurs de services numériques et de cybersécurité, ainsi qu'éventuellement sur des prestataires de services publics ou privés (expertise technique, pilotage de projet, conduite du changement, support, etc.).

Engagements du candidat

En candidatant à l'appel à projets, la structure s'engage :

- À mobiliser les équipes nécessaires au bon déroulement du projet, en mettant en œuvre les moyens nécessaires pour sa bonne réalisation. Elle s'engage notamment à mobiliser un chef de projet (mise en œuvre du projet, évaluation, puis partage d'expérience).
- À participer activement aux échanges réguliers avec l'équipe projet de l'ANS, à partager ses retours d'expérience selon les modalités définies et à contribuer à l'évaluation finale du projet.
- À accepter sans réserve la publication large et transparente des résultats du projet au sein de l'écosystème du numérique en santé, par exemple sur le site de l'ANS.

2.3. Début et durée du projet

Dans le cadre de la phase exploratoire, la durée du projet est fixée à 8 mois, à compter de la signature de la convention prévue à l'article 4.3 du présent cahier des charges, quel que soit le parcours de cybersécurité sélectionné.

Pour les itérations ultérieures, la durée pourra être ajustée au regard des retours d'expérience issus de la phase exploratoire.

L'ANS se réserve la possibilité de proposer une prolongation de la période d'exécution du projet, notamment afin de tenir compte des contraintes opérationnelles rencontrées ou des enseignements tirés de la phase d'expérimentation.

3. Critères de sélection des projets

Un jury désignera jusqu'à 21 lauréats parmi les candidatures éligibles.
L'ANS sera sensible durant sa sélection à :

- Assurer une répartition équilibrée entre les régions,
- Assurer une certaine représentativité et diversité des établissements choisis (secteur public / privé…),
- Viser la plus grande diversité possible des mailles de mutualisation,

tout en se réservant la possibilité de s'en écarter afin de retenir les projets les plus pertinents au regard de la qualité et de la solidité des dossiers déposés.

L'ANS sera également sensible durant sa sélection aux points suivants :

- La capacité du porteur de projet à s'inscrire dans une logique d'échange et de coordination avec la région sera évaluée, notamment au travers des échanges réalisés en amont avec l'ARS et le CRRC, afin d'assurer l'alignement de la candidature avec les objectifs du programme et le choix d'un parcours cyber adapté ;
- L'adéquation stratégique et la pertinence du projet seront appréciées au regard de la cohérence entre le parcours de cybersécurité choisi, le niveau de maturité issu du diagnostic, la clarté de la situation actuelle, ainsi que la définition d'objectifs et d'une situation cible réalistes à l'issue du POC ;
- La capacité de réalisation et la gouvernance du projet, seront évaluées au regard de l'identification d'un pilotage clair, de la mobilisation réaliste des équipes internes ou de prestataires, de la faisabilité du projet sur la durée du POC, de l'existence de modalités de suivi adaptées, ainsi que de la capacité opérationnelle des ESSMS à engager effectivement les travaux de cybersécurité dès le démarrage de la phase d'expérimentation ;
- L'impact sectoriel et la représentativité du projet seront appréciés au regard de son potentiel de transférabilité et de mutualisation, du nombre de professionnels et/ou d'usagers concernés, ainsi que de la contribution de la structure à la diversité des lauréats du secteur médico-social ;
- La soutenabilité financière du projet sera analysée au regard du caractère réaliste et proportionné du budget prévisionnel, en cohérence avec les objectifs poursuivis et les actions prévues dans le cadre du POC.

L'instruction des candidatures peut donner lieu à une phase de présélection sur la base des critères d'éligibilité et de recevabilité définis au présent cahier des charges.

4. Organisation de la procédure de l'appel à projets

4.1. Dossier de candidature

Le dossier de candidature est composé notamment de :

- une lettre d'intention signée par la direction de la structure porteuse, attestant du soutien au projet et de la participation au POC ; lorsque la candidature est portée par un groupement, cette lettre précise la mobilisation de l'ensemble des établissements concernés et est complétée, le cas échéant, par un document formalisant l'engagement des parties ;
- la liste des ESSMS inclus dans la candidature, accompagnée des justificatifs d'équipement en DUI référencé Ségur pour l'ensemble des sites concernés ;
- le résultat du cyberdiagnostic réalisé (à minima l'autodiagnostic OPSSIMS [3]) ; et les éléments attestant d'un échange avec la région et orientant le candidat vers un parcours.

Les attendus détaillés, ainsi que les autres éléments constitutifs du dossier de candidature, sont précisés dans le guide des prérequis et objectifs de chaque parcours. Ces guides seront publiés sur le site de l'ANS.

Le dossier de candidature doit être déposé sur la plateforme Convergence[4] avant le 4 juin 2026 à 16h00 (heure de Paris), sous peine de rejet de celui-ci.

Les dossiers de candidature devront être déposés complets avant la date et l'heure limites indiquées dans le présent appel à projets.

La date et l'heure prises en compte sont celles de la réception effective du dossier par l'ANS, telles qu'enregistrées par le système de dépôt ou, à défaut, par tout moyen permettant d'en attester.

Tout dossier transmis après la date et l'heure limites sera rejeté.

Sauf dysfonctionnement technique avéré de la plateforme ou incident imputable à l'ANS, aucune régularisation d'un dépôt tardif ne sera admise.

4.2. Instruction des candidatures

Le choix des projets lauréats s'effectue au regard des critères d'éligibilité et de sélection définis dans le présent cahier des charges.

L'instruction des candidatures mobilise un comité d'engagement dont la composition a été définie par délibération du Conseil d'administration de l'ANS du 11 mars 2026.

[3] https://esante.gouv.fr/essms/cybersecurite

[4] La plateforme Convergence, autrement appelée eCaRE, est la plateforme dédiée à la candidature aux guichets d'appels à financement et d'appels à projets du programme CaRE.

L'instruction des candidatures se déroule en 2 phases :

- Les dossiers de candidature sont déposés par les candidats sur la plateforme Convergence, mise en œuvre par l'ANS. Les candidatures sont réceptionnées par l'ANS au fil de l'eau, jusqu'à la date limite de dépôt.
- Analyse des dossiers de candidature reçus sur Convergence par un jury (composé d'acteurs ANS, DNS et CNSA) sur la base d'une grille d'analyse commune reprenant les critères mentionnés dans le cahier des charges et proposition d'une présélection de dossiers au comité d'engagement.
- Les dossiers des candidats conformes aux critères et les analyses correspondantes sont remis au comité d'engagement qui propose une liste de lauréats à l'issue d'une séance de délibération organisée par l'ANS ;

  Sur la base des avis et recommandations du comité d'engagement, le directeur de l'ANS sélectionne les projets lauréats de l'appel à projets « Mise en œuvre de mesures de cybersécurité pour les établissements et services du secteur social et médico-social (ESSMS) », susceptibles de faire appel à un financement. Les avis rendus par le comité d'engagement sont des avis simples qui ne lient pas la Direction de l'ANS.

Le choix des projets lauréats relève du pouvoir d'appréciation de l'ANS au regard des critères définis dans le présent cahier des charges, dans le respect des principes d'égalité de traitement, d'objectivité et de transparence.

4.3. Conventionnement

Une convention est signée entre l'ANS et chaque lauréat du présent appel à projets.
Cette convention fixe les objectifs, les moyens, le calendrier et les conditions de réalisation du projet ainsi que les modalités d'évaluation des résultats et de contrôle par l'ANS de la bonne utilisation des crédits, moyens ou services mis à disposition.
Dans le cadre de cette convention, le lauréat qui souhaite bénéficier du soutien financier s'engage à respecter les obligations suivantes :

- L'atteinte des prérequis et objectifs précisés dans le cahier des charges ;
- La déclaration de l'atteinte des objectifs sur la plateforme « Convergence » et le dépôt des pièces justificatives ;
- La déclaration des coûts exposés pour l'atteinte des objectifs matérialisée par la remise d'un bilan financier établi conformément à la trame qui aura été fournie aux établissements au moment de leur candidature, accompagnée des factures justificatives afférentes ;
- En vue des opérations de contrôle de conformité menées par l'ANS, la mise à disposition de toute pièce complémentaire qui permettrait de justifier de l'atteinte des objectifs ;

- La possibilité pour l'établissements de participer à un temps d'échange en visio-conférence avec les équipes de l'ANS ou d'accueillir sur site les équipes de l'ANS pour la vérification des éléments de preuve fournis et de l'atteinte des objectifs.

4.4. Suivi et livrables des lauréats

L'ANS, avec l'appui des ARS et des CRRC, assure le suivi de la mise en œuvre des projets sélectionnés.
Dans le cadre de l'expérimentation, le lauréat s'engage à respecter les modalités de suivi prévues par les instances nationales nécessaires au bon déroulement de l'expérimentation.
Les lauréats sélectionnés participent aux points d'avancement réguliers organisés par leur région, y partagent les difficultés rencontrées et les avancées réalisées dans la mise en œuvre des travaux de cybersécurité engagés.
A mi-parcours, les lauréats sélectionnés produisent un premier retour d'expérience selon le modèle qui sera fourni au préalable.
En fin d'expérimentation, ils transmettent un retour d'expérience final rendant compte des travaux mis en œuvre et des résultats obtenus.
L'un des objectifs de cette expérimentation est de pouvoir formaliser et valoriser des retours d'expérience (réussites, leviers, freins, recommandations…) au travers d'un comité de fin d'expérimentation organisé au niveau national invitant l'ensemble des lauréats.

Dans une logique d'accompagnement et de progression, l'ANS se réserve la possibilité, en lien avec les régions, d'autoriser un changement du parcours de cybersécurité en cours d'expérimentation, lorsque les difficultés rencontrées par un lauréat ne lui permettent pas d'atteindre les cibles initialement fixées, afin de privilégier l'atteinte d'objectifs adaptés plutôt qu'une interruption des travaux engagés.

5. Règles de financement

5.1. Cadre juridique du financement

Les subventions attribuées au titre de la présente itération d'expérimentation de l'appel à projets sont accordées sur le fondement du règlement (UE) n° 2023/2831 relatif aux aides de minimis - dit « règlement de minimis » dans la suite du document - dans la limite du plafond d'aides fixé à 300 000 € par entreprise sur une période de trois années glissantes.

Le candidat s'engage à remettre, au moment du dépôt de sa candidature, une déclaration sur l'honneur précisant :

- le montant total des aides de minimis perçues au cours des trois dernières années, cette période s'appréciant de manière glissante ;
- la nature, la date d'octroi et l'autorité ayant attribué ces aides ;
- et qu'il n'a pas dépassé, avec la subvention demandée, le plafond précité. L'absence ou l'inexactitude de cette déclaration pourra entraîner le rejet de la candidature ou, le cas échéant, le retrait de la subvention accordée.

Lorsque le candidat est un groupement d'entité juridique, les dispositions ci-dessus s'appliquent à chacun des membres du candidat.

5.2. Montant du financement

Pour chaque parcours retenu et selon l'atteinte des objectifs cibles visés, une aide est attribuée sous la forme d'une subvention. Conformément au règlement de minimis applicable, qui autorise l'octroi d'aides sans définition préalable des coûts éligibles, le soutien financier octroyé dans le cadre du présent appel à projets prendra la forme d'un forfait. Ce montant forfaitaire sera attribué dans la limite des plafonds définis dans le tableau ci-dessous.

Les montants forfaitaires sont calculés en fonction du nombre d'entités géographiques (EG) incluses dans la candidature et du parcours de cybersécurité retenu parmi les trois parcours proposés pour ce POC. Ce calcul intègre un mécanisme de dégressivité du montant financé au-delà d'un certain nombre d'EG, afin de mieux tenir compte des effets de mutualisation au sein des groupements.

Le montant forfaitaire par EG a été défini à partir d'une étude de coûts, reposant sur l'identification des principaux postes de dépenses associés aux objectifs des parcours.

Le modèle de calcul de la subvention repose ainsi sur un financement attribué :

- à 100 % du montant unitaire pour les premières EG,
- puis selon des taux dégressifs appliqués par tranche d'EG,
- jusqu'à un plafond maximal de subvention par groupement, variable selon le parcours retenu.

Règle de calcul (commune aux 3 parcours) :

Nombre d'EG dans la candidature	Taux de financement
EG 1 à 4	100 %
EG 5	80 %
EG 6	60 %
EG 7	40 %
EG 8 à 12	20 %
À partir de l'EG 13	0 %

Montants unitaires et plafonds par parcours :

Parcours	Montant unitaire par EG	Montant maximal de subvention par groupement
Parcours 1	9 400 €	63 920 €
Parcours 2	17 000 €	115 600 €
Parcours 3	17 000 €	115 600 €

Les financements attribués dans le cadre du présent appel à projets ne peuvent couvrir des actions ou dépenses ayant déjà fait l'objet d'un financement public au titre d'un autre dispositif. Les modalités de non-cumul et de contrôle afférentes sont précisées dans la convention de financement.

Ils relèvent du règlement de minimis. À ce titre, le bénéficiaire déclare et garantit que le montant total des aides de minimis perçues au cours des trois exercices fiscaux glissants, toutes autorités publiques confondues, y compris la présente aide, ne dépasse pas le plafond réglementaire en vigueur.

Une attestation sur l'honneur relative aux aides de minimis perçues ou sollicitées est exigée préalablement à la signature de la convention de financement.

En cas de dépassement du plafond réglementaire ou de déclaration inexacte, l'ANS pourra respectivement procéder au rejet de la candidature, au retrait de l'aide ou au reversement total ou partiel des sommes versées.

Le recours au régime de minimis pour la présente édition est spécifique à cet appel à projet exploratoire et ne préjuge pas du cadre juridique qui pourra être retenu pour les appels à projets ultérieurs.

5.3. Modalités de versement du financement

Le financement est versé à la fin du projet, en une fois, après la période de pilote terminée et sur la base des pièces justificatives suivantes à fournir à l'ANS :

- Le rapport d'évaluation et le rapport financier final ;
- La convention signée entre l'ANS et la structure porteuse de la candidature ;
- Le procès-verbal de réalisation des bilans du retour d'expérience intermédiaire et final visé par l'ANS.

Dans le cadre du régime de minimis applicable à la présente édition, le financement est attribué sous forme forfaitaire et n'est pas ajusté en fonction des dépenses effectivement engagées, sous réserve de la réalisation des engagements et objectifs définis par le dispositif.

Le récapitulatif des recettes dans la trame financière devra clairement distinguer l'ensemble des financements déjà perçus ou attribués.

La convention précise les conditions dans lesquelles le financement peut être retiré par l'ANS et le remboursement de tout ou parties des sommes, notamment en cas de méconnaissance des dispositions du cahier des charges, des stipulations conventionnelles ou en cas de fraude.

6. Confidentialité et communication

L'ANS s'assure que les documents transmis dans le cadre du présent appel à projets sont soumis à la plus stricte confidentialité. L'ensemble des personnes ayant accès aux dossiers de candidatures est tenu à la plus stricte confidentialité.

Une fois le projet sélectionné, les lauréats sont tenus de mentionner le soutien apporté par le Ministère de la Santé, des familles, de l'autonomie et des personnes handicapées (délégation au numérique en santé) et de l'ANS dans leurs actions de communication et la publication de leurs résultats avec la mention unique « ce projet a été soutenu par la délégation au numérique en santé (DNS) et l'agence du numérique en santé (ANS) ».

Toute opération de communication doit être concertée entre les lauréats et l'ANS, afin de vérifier notamment le caractère diffusable des informations et la conformité des références.

L'Etat et l'ANS pourront communiquer sur les objectifs généraux de l'appel à projets, ses enjeux et ses résultats, ainsi que sur les projets retenus, dans le respect des secrets des affaires. Ils pourront notamment utiliser à cette fin une « fiche communication » qui sera établie par le lauréat, une fois celui-ci sélectionné.

Enfin, les lauréats sont tenus à une obligation de transparence et de reporting vis-à-vis de l'Etat et de l'ANS, nécessaire à l'évaluation ex-post des projets ou de l'appel à projets.