Appel à projet

Financement d’un exercice de continuité d’activité en mode numérique dégradé au profit des établissements sanitaires

18 septembre 2023

Contexte de l'appel à projet (AAP)

Entre 2020 et 2023 on a recensé un nombre croissant de cyberattaques : à titre d'exemple, en 2021, le CERT Santé (Computer Emergency Response Team Santé)[1] a géré plus de 733 déclarations d'incident, soit plus du double par rapport à 2020.[2]

Les établissements sanitaires au même titre que toute autre organisation doivent être en capacité d'anticiper la survenance de cyberattaques pour limiter leur impact et continuer du mieux possible à exercer leurs missions.

Objectifs de l'AAP

Dans le cadre de la feuille de route du numérique en santé et au regard des récents évènements cyber, **il est attendu des établissements sanitaires qu'ils réalisent chaque année un exercice de continuité d'activité en mode numérique dégradé**.

L'exercice à réaliser est un exercice de continuité d'activité dont l'élément déclencheur est un incident cyber sécurité. A ce titre, il doit permettre d'évaluer la capacité de l'établissement à poursuivre son activité de prise en charge des patients dans un mode numérique dégradé. En conséquence, au-delà de la DSI, cet exercice doit impliquer la direction générale et les directions métiers de l'établissement.

Des kits « exercices de crise cyber sécurité » prêts à l'emploi et autoporteurs ont été élaborés. Trois niveaux de kits sont proposés en fonction du niveau de maturité de l'établissement en termes de cyber sécurité :

- Kit débutant
- Kit intermédiaire
- Kit expert

Ils sont disponibles sur le site cyberveille-santé.

Afin de choisir le kit adapté, le niveau de maturité cybersécurité de l'établissement doit être évalué grâce à la grille d'auto-évaluation également disponible sur le site cyberveille santé.

[1] Le CERT Santé est un service de réponse à incident 24h/24 et 7j/7. Il s'agit d'accompagner les bénéficiaires du CERT Santé confrontés à un incident majeur ayant déjà affecté un ou plusieurs services numériques et contraignant l'établissement à mettre en place un mode dégradé de fonctionnement.

[2] Les incidents de sécurité ont doublé en un an | esante.gouv.fr

Afin que les établissements puissent être accompagnés dans cette démarche, l'ARS Ile-de-France a ouvert un premier appel à projets entre janvier et juillet 2023, recueillant plus de 200 candidatures. Afin de maintenir la dynamique, un second appel à projets est ouvert entre le 18 septembre et le 30 novembre 2023.

Une allocation forfaitaire sera versée pour couvrir totalement ou partiellement le coût de l'accompagnement par un prestataire référencé et ce avant fin mai 2024 :

- De 4 000 euros maximum pour des exercices de niveau 1 ou 2
- De 5 000 euros maximum pour des exercices de niveau 3

Cette allocation est réalisée par exercice et par établissement dont le personnel, notamment métier, est effectivement mobilisé dans l'exercice.

A qui s'adresse cet appel à projet ?

L'appel à projet s'adresse à tous les établissements sanitaires d'Ile-de-France (avec une priorisation des OSE, établissements assurant de la MCO et établissements à forte activité combinée), qu'ils aient déjà candidaté ou non au premier appel à projets.

Ces exercices devront être programmés au plus tard fin mai 2024 (fin décembre 2023 pour les OSE).

Modalités de candidature

Les étapes de candidature sont les suivantes :

- Renseigner la grille d'autoévaluation de la maturité en matière de cyber sécurité (niveau 1, 2 ou 3) ;
- En fonction du résultat, si besoin d'accompagnement pour réaliser l'exercice, passer une commande d'accompagnement auprès de la Centrale d'achat de l'informatique hospitalière (CAIH) (adhésion à prévoir), du GRADeS SESAN (adhésion à prévoir), du RESAH (adhésion à prévoir) ou de toute autre centrale/prestataire et joindre le bon de commande ;
- Renseigner l'Observatoire Permanent de la Sécurité des Systèmes d'Information des Établissements de Santé (OPSSIES) ;
- Renseigner le formulaire de candidature sur démarches simplifiées avec toutes les informations demandées et joindre la grille d'autoévaluation, le bon de commande et la date de mise à jour de l'observatoire (moins de 3 mois) : https://www.demarches-simplifiees.fr/commencer/appel-a-projets-vague-2-hopital-et-cybersecurite-e

Les instructions des candidatures auront lieu au fil de l'eau et donneront lieu à la production d'une convention de financement liant l'ES à l'ARS ou liant l'ARS à SESAN pour les établissements passant par SESAN.

Il s'agira pour l'établissement de transmettre dès la candidature le bon de commande de la prestation, puis la justification du service fait (par exemple facture) qui déclenchera le paiement de l'ARS. Ainsi, le paiement sera effectué dès lors que l'exercice a été réalisé.

Les notifications et paiement seront réalisés en fonction des dates de dépôt des candidatures : les premiers candidats seront les premiers notifiés.

Calendrier

Les candidatures peuvent être déposées entre le 18 septembre et le 30 novembre 2023 minuit.

Les exercices devront être réalisés le plus rapidement possible et au maximum d'ici le 31 mai 2024 (31 décembre pour les OSE).

Conditions de candidature

Les candidats sont invités à renseigner les éléments demandés concernant leur établissement à partir du lien suivant : https://www.demarches-simplifiees.fr/commencer/appel-a-projets-vague-2-hopital-et-cybersecurite-e

Les pré requis sont la réalisation de l'autoévaluation sur la base de la grille de maturité, la mise à jour de l'OPSSIES de manière récente et la transmission du bon de commande.

D'autre part, il convient de veiller au renseignement correct et exhaustif du formulaire *démarches simplifiées*.

Pour toute question, nous vous invitons à contacter charline.auzou@ars.sante.fr