# Appel à projets portant sur le financement d'exercices de continuité d'activité en mode numérique dégradé au profit des établissements sanitaires du Grand Est

## 1 - Contexte de l'appel à projet (AAP)

Entre 2020 et 2022, un nombre croissant de cyberattaques a été recensé. À titre d'exemple, en 2021, le CERT (Computer Emergency Response Team) Santé a géré plus de 733 déclarations d'incident, soit plus du double par rapport à 2020.

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

Sur la base de l'instruction N° SHFDS/FSSI/2023/15 (Février 2023) portant sur la réalisation prioritaire d'exercices de continuité d'activité en mode dégradé numérique par les établissements sanitaires.

## 2 - 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. À 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 : https://www.cyberveille-sante.gouv.fr/dossier-thematique/exercice-de-crise-cyber

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 :

https://www.cyberveille-sante.gouv.fr/sites/default/files/media/document/2022-11/ANS_Grille%20d%27%C3%A9valuation%20de%20la%20maturit%C3%A9_V.1.xlsx

Afin que les établissements puissent être accompagnés dans cette démarche, l'ARS allouera une subvention forfaitaire aux structures qui réaliseront un exercice de continuité d'activité en 2023.

Celle-ci permettra de couvrir le coût de l'accompagnement par un prestataire référencé par l'ANSSI.

Les financements sont dimensionnés de la façon suivante :

- Attribution d'un forfait maximal de 4,5 K€ pour la réalisation d'un exercice de crise s'appuyant sur le kit débutant ;
- Attribution d'un forfait maximal de 7 K€ pour la réalisation d'un exercice de crise s'appuyant sur le kit intermédiaire ;
- Attribution d'un forfait maximal de 10 K€ pour la réalisation d'un exercice de crise s'appuyant sur le kit confirmé.

### 3 - A qui s'adresse cet appel à projets ?

L'appel à projets s'adresse à tous les établissements sanitaires MCO du Grand Est (avec une priorisation des OSE (Opérateurs de Services Essentiels), des établissements assurant de la MCO et établissements à forte activité combinée), qu'ils aient déjà réalisé ou non un exercice de continuité d'activité en mode dégradé.

L'objectif est que 100% des OSE (Opérateurs de Services Essentiels) aient réalisé un exercice pour fin mai 2023, ainsi que les établissements MCO des GHT et des établissements privés MCO à forte activité, dans la proportion au total de 25% des établissements comptabilisés en Grand Est sur la base du FINESS PMSI, soit environ 60 établissements au total.

L'objectif est que 50% des établissements sanitaires (base FINESS PMSI) aient réalisé un exercice au cours de l'année 2023, soit environ 120 établissements au total.

Il est attendu que :

- Dans le cas d'un GHT, le RSSI du GHT pilote le projet d'exercice de crise et porte le dossier de candidature pour l'OSE (Opérateur de Services Essentiels) mais aussi pour les autres établissements MCO du GHT,
- Dans le cas d'un groupe d'établissements privés, un RSSI du groupe (basé dans un établissement du Grand Est) pilote le projet d'exercice de crise et porte le dossier de candidature pour son établissement de rattachement mais aussi pour les autres établissements MCO du groupe,
- Dans le cas d'un établissement MCO isolé en Grand Est, son RSSI pilote le projet d'exercice de crise et porte le dossier de candidature pour son établissement de rattachement.

### 4 - 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 de l'autoévaluation, l'établissement devra passer une commande d'accompagnement à la réalisation de l'exercice (niveau 1, 2 ou 3) auprès de la Centrale d'achat de l'informatique hospitalière (CAIH) (adhésion à prévoir) ou autre centrale d'achat ou après dans le cadre d'un marché spécifique et joindre le bon de commande.
- Renseigner l'Observatoire Permanent de la Sécurité des Systèmes d'Information des Établissements de Santé (OPSSIES).

Les candidatures seront ensuite à déposer sur le site **Démarches simplifiés** à **partir de mi-mars 2023**. Les coordonnées de la démarche seront communiquées aux établissements sanitaires du Grand Est par les chargés de mission Ségur Numérique.

Les candidatures seront traitées au fil de l'eau. Les candidatures conformes se verront notifiées au fil de l'eau. Le principe du premier arrivé, premier servi s'applique à cette procédure, excepté pour les OSE, ES GHT et ES privés à forte activité qui sont prioritaires.

La date limite de candidature est fixée au **31 août 2023**.

Les exercices devront être réalisés le plus rapidement possible et au plus tard d'ici fin décembre 2023.
La réalisation de ces exercices sera un prérequis des appels à projet à venir concernant la cybersécurité.