MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

INSTRUCTION N° SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et à leur financement

Le secrétaire général des ministères chargés des affaires sociales
à
Mesdames et Messieurs les directeurs généraux
des agences régionales de santé

Référence	Numéro interne : 2023/15
Date de signature	30/01/2023
Emetteur	Ministère de la santé et de la prévention Sécrétariat général des ministères chargés des affaires sociales (SGMCAS) Service du haut fonctionnaire de défense et de sécurité (SHFDS)
Objet	Obligation de réaliser des exercices de crise cyber dans les établissements de santé et leur financement.
Commande	Rappeler aux établissements de santé la nécessité de réaliser des exercices de crise cyber.
Action à réaliser	Transmission par les agences régionales de santé (ARS) de la présente instruction aux correspondants sécurité des systèmes d'information (SSI).
Echéance	Prise en compte du contenu de cette instruction dès sa réception.
Contact utile	Fonctionnaire de sécurité des systèmes d'information Pôle « Sécurité des systèmes d'information » Patrice BIGEARD Tél. : 01 40 56 69 73 Mél. : patrice.bigeard@sg.social.gouv.fr
Nombre de pages et annexe	3 pages + 1 annexe (3 pages) Annexe - Information sur les modalités de financement des exercices de crise cyber
Résumé	L'objet de cette instruction est de rappeler l'objectif assigné le 14 décembre 2021 à l'ensemble des établissements de santé, de réaliser des exercices de crise cyber et de préciser les modalités d'un accompagnement financier forfaitaire destiné à la mise en œuvre de ces exercices de crise. Cet accompagnement financier s'intègre dans le Ségur numérique entièrement pourvu par des fonds européens, dans le cadre du plan de relance et de résilience européen. Le bénéfice de ce financement est donc exclusif de tout autre financement européen.

Mention Outre-mer	Ces dispositions s'appliquent aux Outre-mer, à l'exception de la Polynésie française, de la Nouvelle-Calédonie et de Wallis et Futuna.
Mots-clés	Système d'information ; établissement de santé ; médico-social ; soutien financier ; cyber sécurité ; exercice ; continuité d'activité.
Classement thématique	Etablissements de santé
Textes de référence	- Note d'information N° SG/SHFDS/2021/253 du 14 décembre 2021 relative à la mise en œuvre d'exercices cyber (PCA NUM) dans les établissements de santé ; - Note aux directeurs généraux des ARS du 30 juillet 2021 portant sur le Plan de renforcement 2021 de la cyber sécurité des établissements de santé ; - Instruction N° SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'Action SSI ») dans les établissements et services concernés.
Circulaire / instruction abrogée	Néant
Circulaire / instruction modifiée	Néant
Rediffusion locale	Les correspondants SSI en ARS devront assurer une diffusion de cette instruction auprès des groupements régionaux d'appui au développement de la e-santé (GRADeS) et des établissements de santé et médico-sociaux.
Validée par le CNP le 9 décembre 2022 - Visa CNP 2022-135 **Visée par le SGMCAS le 30 janvier 2023**	
Document opposable	Non
Déposée sur le site Légifrance	Non
Publiée au BO	Non
Date d'application	Immédiate

Une note d'information transmise aux directions générales des ARS le 14 décembre 2021 demandait que chaque établissement organise, avant fin 2023, au moins un exercice de crise cyber puis de façon permanente, au moins une fois par an. La persistance d'un niveau élevé de menace justifie le besoin de préparation et d'anticipation pour faire face à des attaques et incidents d'origine malveillants.

Pour ces raisons, je vous demande de relayer dans les établissements de santé de vos régions la nécessité de réaliser ces exercices de crise cyber.

Pour rappel, cette nécessité est mise en évidence dans deux volets de l'action globale conduite par le ministère de la santé et de la prévention et les ARS en matière de cyber sécurité.

- La réalisation des exercices de crise fait partie des mesures prioritaires de renforcement demandées aux établissements de santé et qui constituent l'un des principaux volets de l'Observatoire de la sécurité des systèmes d'information des établissements de santé (OPSSIES). La remontée par les établissements de santé de leur niveau de maturité en sécurité des systèmes d'information dans l'OPSSIES, au travers de ces mesures prioritaires, fera également l'objet une demande du ministère.

- Ces exercices de crise sont inscrits dans les actions du Plan de renforcement 2021 de la cyber sécurité des établissements de santé qui prévoit d'organiser de manière régulière, et au moins une fois par an, un exercice de crise cyber, dont le retour d'expérience sera présenté au comité de direction de l'établissement et pris en compte dans le Plan de continuité d'activité (PCA).

Les moyens mis à disposition des ARS et des établissements de santé sont les suivants :

- Un financement de 10 M€ est mis en place pour la réalisation des exercices. Les règles européennes d'usage de ce financement relèvent de la Facilité pour la reprise et la résilience (FRR, point 3 de l'annexe).
- 3 kits de scénario d'exercices, adaptés à la typologie des acteurs, ont été produits et sont disponibles sur le portail de l'Agence du numérique en santé (ANS). Ceux-ci peuvent être utilisés par les établissements en toute autonomie mais une prestation d'accompagnement est recommandée pour la première réalisation, par un GRADeS ou un prestataire spécialisé.
- Il est à noter que ces kits d'exercices de crise proposent également des scénarii adaptés spécifiquement aux établissements médico-sociaux.

L'objectif fixé par la note d'information N° SG/SHFDS/2021/253 du 14 décembre 2021 relative à la mise en œuvre d'exercices cyber dans les établissements de santé reste applicable. L'indicateur du taux d'établissements de santé ayant conduit dans l'année un exercice de continuité d'activité en mode « numérique dégradé » vise une cible de 100 % à l'horizon **mai 2023 pour les opérateurs de services essentiels (OSE)**. La priorisation des autres établissements, publics et privés, avec une cible de 100 % à fin 2024 pourra se faire sur des critères de types d'activités comme la médecine chirurgie obstétrique (MCO) et les établissements ayant la plus forte activité combinée.

Les éléments relatifs au financement sont détaillés en annexe. Une foire aux questions (FAQ) sera mise à disposition sur le portail Cyberveille de l'ANS pour détailler cette démarche.

Le service du HFDS et son pôle FSSI sont à votre disposition pour toute question relative à a mise en œuvre de cette instruction.

Le secrétaire général et haut fonctionnaire
de la défense et de la sécurité des
ministères chargés des affaires sociales,

Pierre PRIBILE

Annexe

Information sur les modalités de financement des exercices de crise cyber

1 Le plan de renforcement en cyber sécurité 2021 prévoit une action spécifique destinée aux exercices de crise cyber et de continuité d'activité en « mode numérique dégradé »

Pour rappel, cette action se décompose en deux volets (4.3 et 4.4) traitant de la réalisation l'exercice et de l'évaluation du Plan de continuité d'activité de l'établissement au travers de cet exercice.

> Action ARS 4.3 : veiller à la réalisation d'exercices de continuité d'activité en établissement.

Le Plan de renforcement de la cyber sécurité prévoit la réalisation d'exercices de crise ayant un impact sur le volet sanitaire, afin de se préparer à des incidents de fonctionnement, en vérifiant l'adéquation des plans de continuité d'activité des établissements de santé et leur capacité à s'adapter à un fonctionnement en mode numérique dégradé.

> Action ARS 4.4 : intégrer la notion de risque cyber dans les « plans de perturbation de l'offre de soins »

Le Plan de renforcement de la cyber sécurité prévoit également d'intégrer les impacts d'un risque cyber sur la gestion et la prise en charge des usagers dans les « plans de perturbation de l'offre de soins ».

Les exercices de crises doivent in fine permettre d'évaluer cette adéquation et la préparation des de la structure sanitaire pour y faire face, tant par les équipes de direction que par les directions des systèmes d'informations ou les équipes soignantes.

2 Un accompagnement financier ciblé pour aider à la réalisation des exercices de continuité d'activité

2.1 Principes généraux

Dans le cadre du Ségur du numérique, un montant de 10 millions d'euros a été décidé pour soutenir la mise en œuvre de ces exercices sur les années 2022/2023. Ce montant est exclusivement dédié à des prestations d'animation de ces exercices de crises en priorité par les établissements supports de groupements hospitaliers de territoire (GHT), désignés OSE, et par les établissements de santé (publics, privés) suivant les modalités prescrites ci-dessous.

Ces financements seront octroyés aux ARS dans le cadre d'un abondement au Fonds d'intervention régional (FIR).

Ce soutien est destiné à financer la réalisation des exercices par le recours à une maîtrise d'œuvre en charge de l'animation et de la conduite opérationnelle des exercices de crise, s'appuyant sur les kits mis à disposition par l'ANS.

Ces fonds ne sont pas fongibles et sont destinés au seul accompagnement à la réalisation de ces exercices.

2.2 Soutien financier 2022/2023

Pour ces deux années, les règles d'attribution du soutien financier sont les suivantes :

- Une enveloppe globale de crédits de 10 millions d'euros sera déléguée aux ARS selon une répartition en fonction du nombre d'établissements sanitaires à la maille FINESS PMSI (Fichier national des établissements sanitaires et sociaux - Programme de médicalisation des systèmes d'information).
- Chaque ARS décidera de la stratégie régionale quant à l'utilisation de ces fonds et pourra opérer une délégation de crédits :
    - Soit auprès de son groupement régional d'appui au développement de la e-santé (GRADeS), pour mettre en œuvre une offre régionale d'accompagnement à la réalisation des exercices de crise ;
    - Soit directement auprès d'un établissement qui se sera appuyé sur un accompagnement auprès d'un prestataire spécialisé pour réaliser son exercice, idéalement au travers de l'utilisation de l'un des kits mis à disposition.

Dans les deux cas, le financement fera l'objet d'une convention précisant, outre le montant alloué, les règles d'utilisation du financement ainsi que les principes associés à la maîtrise des risques listés au point 3.

Si, dans le premier cas de figure, la délégation de crédit par l'ARS pourra intervenir directement auprès du GRADeS, dans le second cas, les établissements seront destinataires des crédits afin de prendre en charge le coût de l'accompagnement de la réalisation de l'exercice.
Dans ce second cas, le principe d'un forfait fixe, plafonné, s'appliquera, indépendamment de la taille de l'établissement et cela pour garantir à chaque établissement un niveau de financement adéquat. Ce niveau de financement, défini sur la base du kit d'exercice mis en œuvre, vise à tenir compte de la complexité de la simulation à réaliser :

- 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.

Il appartient à l'ARS de définir l'organisation de la stratégie de financement entre ces deux mécanismes, voire en mode mixte.

2.3 Éligibilité au financement pour l'accompagnement à la réalisation des exercices de continuité d'activité

L'attribution du forfait s'appuiera sur la complétion d'une grille d'évaluation de la maturité cyber sécurité des établissements de santé produite en complément des kits d'exercices par l'Agence du numérique en santé.

Cette grille permettra d'établir la bonne adéquation entre la typologie d'un établissement et l'un des kits proposés.

Les kits d'exercices de crises (débutant, intermédiaire, confirmé) ont été produits avec le concours du fonctionnaire de sécurité des systèmes d'information, de l'ANS, des ARS et des GRADeS avec l'appui d'un prestataire spécialisé. Tout en déclinant un scénario préconçu et

adapté à la typologie des acteurs, ils incluent les documents supports de l'exercice tant pour l'animateur que pour les participants.

2.4 Contrôle de la réalisation des exercices par les établissements financés

Les ARS auront pour mission de centraliser la liste des établissements ayant bénéficié d'un financement. Cette liste intègrera la date de l'exercice et la nature du kit d'exercice mis en œuvre.

Seul l'accompagnement à la mise en œuvre de ces kits pourra faire l'objet d'un financement, tout autre type de prestation devant être pris en charge par l'établissement concerné.

La liste régionale des établissements s'étant exercés fera l'objet par les ARS d'une transmission semestrielle au fonctionnaire de sécurité des systèmes d'information qui assurera la bonne remontée de ces informations auprès du comité de pilotage (COPIL) Cyber national deux fois par an.

3 Un accompagnement financier qui s'inscrit dans le cadre de la Facilité pour la reprise et la résilience (FRR)

Comme indiqué au point 2.2, l'attribution du financement, que ce soit par complément de dotation au GRADeS ou à travers un financement du bénéficiaire final de l'aide, devra faire l'objet d'un conventionnement.

La convention permet de préciser l'objet, l'origine du financement, l'interdiction du double financement par des fonds européens, les conditions d'usage du financement, les modalités de reversement en cas de non usage ou d'usage non conforme à l'objet de la convention, ainsi qu'un certain nombre de règles nationales et européennes.

Au-delà du conventionnement, la protection des intérêts financiers de l'Union européenne doit conduire les ARS à mettre en place des mesures adaptées pour détecter et prévenir les risques suivants auprès des établissements financés :

- Fraude et conflits d'intérêts, plus particulièrement dans le processus de sélection du prestataire pour la réalisation de l'exercice de continuité d'activité ;
- Double financement au titre de la FRR et d'autres programmes de l'Union européenne ;
- Non-respect de la réglementation relative à la commande publique pour les opérateurs qui y sont soumis ;
- Non-respect des règles nationales d'éligibilité définies au point 2.3 ;
- Non recouvrement des sommes indues dans l'hypothèse où les exercices ne seraient pas réalisés.

Par ailleurs, l'attention des services instructeurs en ARS et des bénéficiaires est attirée sur :

- Les obligations relatives à la conservation des dossiers (article 132 du règlement financier applicable au budget général de l'Union) ;
- L'origine des fonds, la visibilité du financement de l'Union européenne (article 34-2 du Règlement UE 2041/2021) devant être assurée au niveau de la convention de financement.

Enfin, dans le cadre du traitement de ces exercices, les prestataires devront apporter aux GRADeS ou aux établissements, des garanties de respect du Règlement général sur la protection des données.