Démarche : Appel à Manifestation d'Intérêt (Vague 3) relatif à un programme de financement d'un parcours cybersécurité axé sur la réalisation d'un exercice de gestion de crise cyber au profit des établissements médico-sociaux bretons

Organisme : Département Innovation en Santé - Direction de Cabinet

Identité du demandeur

Email

Etablissement
SIRET

Dénomination

Forme juridique

Formulaire

Les établissements continuent à être la cible d'attaques informatiques, touchant aussi bien le secteur sanitaire que le médico-social. Ce risque croissant depuis plusieurs années s'est encore renforcé en raison des tensions internationales. L'augmentation de l'usage du numérique dans la santé augmente l'exposition des établissements du secteur aux cyberattaques, plaçant ainsi la santé dans le top 5 des secteurs les plus touchés.

L'impact de ces attaques est considérable. Elles entraînent des coûts importants pour remettre en service les SI en mobilisant prestataires et éditeurs. Elles mobilisent jour et nuit des équipes techniques mais aussi métiers, sans compter les impacts sur la disponibilité de l'offre de soins et en conséquence les pertes de chance.

La cybersécurité nécessite aujourd'hui un investissement certes important mais qui se révèlera rentable en évitant les incidents ou en minimisant leurs impacts.
Cet engagement est d'autant plus nécessaire que le domaine de la santé hérite d'une dette technique dans le numérique et dans la cybersécurité : nous devons donc réaliser un effort particulier pour rattraper ce retard.

Organisé par l'Agence Régionale de Santé Bretagne et le Groupement Régional E-santé Bretagne, cet appel à manifestation d'intérêt (Vague 3) s'inscrit dans le cadre du financement d'un parcours cybersécurité axé sur la réalisation d'un exercice de gestion de crise cyber au profit des établissements médico-sociaux bretons.

RGPD
<i>Les données personnelles recueillies sur ce formulaire feront l'objet d'un traitement par l'ARS Bretagne et le GRADES e-Santé Bretagne afin d'assurer le suivi et la gestion de cet appel à manifestation d'intérêt nécessaire à l'exécution d'une mission d'intérêt public ((article 6 1. e) RGPD). Vos données seront conservées pendant toute la durée du plan de renforcement cybersécurité et sont uniquement destinées aux services internes de l'ARS Bretagne et du GRADeS e-santé Bretagne. Elles ne feront l'objet d'aucune diffusion.
Pour la réalisation de ce formulaire, l'ARS Bretagne et le GRADeS e-Santé Bretagne utilisent Démarches-Simplifiées, service fourni par la DINUM (direction interministérielle du numérique).

Vous pouvez accéder aux données vous concernant, vous opposer au traitement de ces données, les faire rectifier ou geler leur utilisation en exerçant votre demande auprès du délégué à la protection des données de l'ARS Bretagne : <A HREF="mailto:ARS-BRETAGNE-DPO@ars.sante.fr">ARS-BRETAGNE-DPO@ars.sante.fr</A> ou par voie postale. Vous disposez également du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) si vous estimez que le traitement de vos données constitue une violation de la réglementation.</i>

Données administratives

1.1 - Merci de renseigner ci-dessous les informations concernant l'établissement
<h1>Etablissement médico-social<h1>

Raison sociale de l'établissement

Adresse complète

SIRET

FINESS JURIDIQUE

FINESS GEOGRAPHIQUE

Statut juridique
Cochez la mention applicable, une seule valeur possible
- ☐ Établissement public
- ☐ Établissement privé à but lucratif
- ☐ Établissement privé associatif

Nombre de salariés
Cochez la mention applicable, une seule valeur possible
- ☐ Moins de 50
- ☐ Entre 51 et 100
- ☐ Entre 101 et 200
- ☐ Entre 201 et 300
- ☐ Plus de 300

Civilité du Chef d'établissement
- ☐ Mme
- ☐ M.

Nom du Chef d'établissement

Prénom du Chef d'établissement

Courriel du Chef d'établissement

1.2 - Merci de renseigner ci-dessous les informations concernant l'équipe systèmes d'information
<h1>Equipe SI<h1>

Civilité du DSI (Directeur des Systèmes d'Information) ou RSI (Responsable des Systèmes d'Information)
- [ ] Mme
- [ ] M.

Nom

Prénom

Courriel

1.3 - Merci de renseigner ci-dessous les informations concernant l'équipe sécurité des systèmes d'information
<h1>Equipe SSI<h1>

Votre établissement dispose-t-il d'un RSSI (Responsable Sécurité des Systèmes d'Information) formellement identifié ?
Cochez la mention applicable
- [ ] Oui
- [ ] Non

Civilité du RSSI
- [ ] Mme
- [ ] M.

Nom du RSSI

Prénom du RSSI

Téléphone du RSSI

Courriel du RSSI

Parcours "Exercice de gestion de crise cyber" (Vague 3)

2.1 - Rappel concernant le parcours "Exercice de gestion de crise cyber" (Vague 3)

Le parcours "Exercice de gestion de crise cyber" (Vague 3) s'inscrit avant tout dans une démarche qualité axée sur la cybersécurité de la structure qui s'engage à le réaliser dans son intégralité. En candidatant à ce parcours, vous engagez votre établissement sur une durée de 10 mois à la réalisation des actions suivantes :
- Un exercice de gestion de crise cyber
- 2 campagnes de phishing
- 3 sessions de sensibilisation (e-learning)
- 1 session de sensibilisation en présentielle
- 14 supports de sensibilisation à diffuser au sein de votre structure.

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

Un exercice de gestion de crise cyber au niveau établissement n'est pas :

- un exercice de continuité informatique
- un test de plan de reprise informatique au niveau groupe
- un test du mode dégradé lors des opérations de maintenance du système d'information
- une bascule régulière entre systèmes de secours
- un test de restauration
- une restauration de l'annuaire Active Directory ou de la messagerie

Votre établissement a-t-il déjà réalisé un exercice de gestion de crise cyber ?
Cochez la mention applicable
- [ ] Oui
- [ ] Non

Si oui en quelle année ?

Vous n'avez jamais réalisé d'exercice de gestion de crise cyber
Dans ce cas, quelque soit votre niveau de maturité cybersécurité, il est conseillé de commencer par un exercice "débutant" (avec une cellule de gestion de crise).

Dans le cas ou votre candidature serait retenue, l'exercice de gestion de crise cyber devra être réalisé au plus tard au 30 novembre 2026. Quand prévoyez vous de le réaliser ?
Cochez la mention applicable, une seule valeur possible
- [ ] Mars 2026
- [ ] Avril 2026
- [ ] Mai 2026
- [ ] Juin 2026
- [ ] Juillet 2026
- [ ] Aout 2026
- [ ] Septembre 2026
- [ ] Octobre 2026
- [ ] Novembre 2026

2.2 - Référent interne à votre structure désigné pour assurer la réussite du Parcours "Exercice de gestion de crise cyber" (Vague 3) au sein de votre établissement

Merci de renseigner ci-dessous les informations concernant le référent interne à votre structure désigné pour assurer la réussite du Parcours "Exercice de gestion de crise cyber" (Vague 3) au sein de votre établissement; le référent sera l'interlocuteur et le contact privilégié de l'ARS Bretagne et du Groupement régional e-santé Bretagne.

Civilité du référent

☐ Mme

☐ M.

Nom du référent

Prénom du référent

Téléphone du référent

Courriel du référent

Profession du référent

2.3 - Niveau de maturité cybersécurité

A l'aide de la grille OPSSIMS, merci de renseigner les informations ci-dessous et de joindre le fichier de résultat de votre auto-évaluation.

Pièce justificative à joindre en complément du dossier

☐ Grille OPSSIMS

Merci de joindre le fichier renseigné

Dépôt des éléments justificatifs

3.1 - Eléments justificatifs

Une attention particulière sera portée aux candidatures pouvant justifier des éléments suivants (sans caractère obligatoire) :

1 - Procès-Verbal de vérification d'aptitude (VA) ou de validation de service régulier (VSR) concernant la mise en œuvre d'un dossier de l'usager informatisé (DUI) référencé Ségur numérique
2 - Attestation signée par le directeur de l'OG désignant le référent interne à la structure en charge de la réalisation du parcours cyber
3 - Relevé d'Identité Bancaire de l'établissement candidat

1 - Procès-Verbal de vérification d'aptitude (VA) ou de validation de service régulier (VSR) concernant la mise en œuvre d'un dossier de l'usager informatisé (DUI) référencé Ségur numérique

Cochez la mention applicable

☐ Oui

☐ Non

Pièce justificative à joindre en complément du dossier

☐ Merci de joindre le procès-verbal de vérification d'aptitude (VA) ou validation de service régulier (VSR) concernant la mise en œuvre d'un dossier de l'usager informatisé (DUI) référencé Ségur numérique

2 - Attestation signée par le directeur de l'OG désignant le référent interne à votre structure en charge d'assurer la réussite du Parcours "Exercice de gestion de crise cyber" au sein de votre établissement

Cochez la mention applicable

☐ Oui

☐ Non

Pièce justificative à joindre en complément du dossier

☐ Merci de joindre l'attestation signée par le directeur de l'OG désignant le référent interne à votre structure en charge d'assurer la réussite du Parcours "Exercice de gestion de crise cyber" au sein de votre établissement

3 - Relevé d'Identité Bancaire de l'établissement candidat

Cochez la mention applicable

☐ Oui

☐ Non

Pièce justificative à joindre en complément du dossier

☐ Merci de joindre le Relevé d'Identité Bancaire de l'établissement candidat