MINISTÈRE
DU TRAVAIL, DE LA SANTÉ,
DES SOLIDARITÉS
ET DES FAMILLES

Liberté
Égalité
Fraternité

INSTRUCTION N° DNS/2025/12 du 22 janvier 2025 relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires

La ministre du travail, de la santé, des solidarités et des familles

à

Mesdames et Messieurs les directeurs généraux
des agences régionales de santé (ARS)

Référence	NOR : TSSL2502261J (numéro interne : 2025/12)
Date de signature	22/01/2025
Emetteurs	Ministère du travail, de la santé, des solidarités et des familles Délégation au numérique en santé
Objet	Mise en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires.
Action à réaliser	Mise en œuvre des actions listées dans l'instruction.
Résultat attendu	Amélioration de la cybersécurité des établissements et de leur résilience en cas d'attaque.
Echéances	Échéances précisées pour chaque action dans l'instruction.
Contacts utiles	Direction de projet Christophe MATTLER Mél. : christophe.mattler@sante.gouv.fr Nicolas VOSS Mél. : Nicolas.voss@sante.gouv.fr 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	5 pages et aucune annexe
Résumé	La présente instruction définit un ensemble d'actions devant être mises en œuvre par les établissements sanitaires dans le contexte d'une menace cyber persistante. Les actions visent : - à demander aux établissements de mesurer leur maturité et leur mobilisation (actions 2, 5 et 7) ; - à améliorer leur préparation et leur résilience (actions 1, 3 et 4) ; - à améliorer l'identification des professionnels (action 6).

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 ; sécurité ; cybersécurité ; contrat pluriannuel d'objectifs et de moyens ; budget numérique ; exercice de crise ; observatoire ; mesures prioritaires ; convergence ; GHT ; annuaire technique ; exposition internet ; audit ; continuité d'activité ; reprise d'activité; programme CaRE.
Classement thématique	Établissements de santé
Textes de référence	- Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé ; - Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé (référentiel sur la Politique Générale de Sécurité des Systèmes d'Information de Santé -PGSSI-S) ; - INSTRUCTION N° DGOS/PF/MSIOS/2012/347 du 25 septembre 2012 relative au renseignement de l'observatoire des systèmes d'information de santé ; - 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 ; - NOTE D'INFORMATION N° DGOS/PF2/2019/207 du 26 septembre 2019 relative à la définition et au suivi des ressources et des charges des systèmes d'information hospitaliers ; - NOTE D'INFORMATION N° DGOS/PF5/2022/268 du 14 décembre 2022 relative à la mise en place de l'Observatoire permanent de la sécurité des systèmes d'information des établissements de santé (OPSSIES) et du référentiel des mesures de sécurité prioritaires ; - Feuille de route du numérique en santé 2023-2027 ; - Programme CaRE - Le plan d'action pour protéger nos établissements face à la menace cyber - Décembre 2023 ; - Les mesures prioritaires de sécurité des systèmes d'information - Référentiel à destination des établissements de santé - DGOS - Octobre 2022.
Circulaire / instruction abrogée	Néant
Circulaire / instruction modifiée	Néant
Rediffusion locale	Les 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.
Validée par le CNP le 13 septembre 2024 - Visa CNP 2024-43	
Document opposable	Oui
Déposée sur le site Légifrance	Non
Publiée au BO	Oui
Date d'application	Immédiate

Objet

Conformément aux engagements pris par le ministre de la santé et de la prévention à la suite des incidents graves ayant touché des établissements en 2022, un programme de renforcement de la sécurité des systèmes d'information des établissements sanitaires (ES), publics et privés, a été construit sous le pilotage de la Délégation au numérique en santé (DNS), appuyé par l'Agence du numérique en santé (ANS) avec le soutien du Service du Haut fonctionnaire de défense et de sécurité (SHFDS).

Ce programme CaRE, pour Cybersécurité accélération et Résilience des Établissements, s'inscrit dans l'action 15 de l'axe 4 de la Feuille de route du numérique en santé 2023-2027 (« Renforcer massivement la cybersécurité dans les établissements, notre souveraineté sur l'hébergement et notre résilience face aux futures crises sanitaires »). Le programme capitalise sur les travaux déjà réalisés par l'ANS, les ARS et GRADeS.

En cohérence avec les chantiers lancés dans le programme CaRE, et afin de contribuer au renforcement de leur résilience en cas de cyberattaque, il est attendu de la part de tous les établissements sanitaires la mise en œuvre de plusieurs actions urgentes et prioritaires. Ces actions s'inscrivent dans la continuité de la mise en œuvre de la Directive NIS 1 et également dans la perspective de l'entrée en vigueur de la Directive NIS 2 qui s'appliquera à la grande majorité des établissements de santé.

Les actions urgentes ou prioritaires attendues de la part des établissements sanitaires sont présentées et détaillées dans le cadre de cette instruction.

Synthèse des actions à mettre en œuvre

Actions	Modalités de mise en œuvre
Action n° 1 – Réaliser chaque année un exercice de crise cybersécurité dans les établissements de santé	• Dans la prolongation de ce qui était demandé par l'instruction n° SHFDS/FSSI/2023/15, réalisation annuelle d'un exercice de crise cyber dans tous les établissements impliquant des participants au niveau décisionnel de la structure (ex : DG ou DGA, PCME, DSI, DIRCOM, ...) ; • Formalisation d'un retour d'expérience à la suite de l'exercice ; • Intégration des actions d'amélioration dans le plan d'amélioration de la qualité de l'établissement et mise en œuvre effective ; • Renseignement par les établissements de la réalisation de cet exercice de crise sur la plateforme nationale de suivi des systèmes d'information de santé.
Action n° 2 – Procéder à l'auto-évaluation de l'établissement vis-à-vis des mesures cyber dites prioritaires	• Déclaration *a minima* annuelle par les établissements de leur niveau de maturité sur la plateforme nationale de suivi des systèmes d'information de santé ; • Inclusion des actions relatives à ces mesures dans le plan d'amélioration de la qualité de l'établissement.
Action n° 3 – Réaliser régulièrement des audits de sécurité de certaines infrastructures IT dans l'ensemble des établissements sanitaires	• Les établissements doivent mettre en place les actions suivantes (étant à noter que les établissements privés à but lucratif doivent réaliser les actions suivantes pendant la durée du programme CaRE) : o Inscription pour tous les établissements, quel que soit le statut juridique, au club SSI (porté par l'ANSSI) ; o Inscription au service SILENE ; o Réalisation d'un audit ADS à fréquence trimestrielle minimum pour l'ensemble des annuaires de l'établissement ;

	• Dans le cadre de la mise en œuvre d'un système de management de la sécurité de l'information supervisé par le RSSI en lien avec le plan d'amélioration de la qualité de l'établissements (PAQ), intégration de la nécessité de mener des actions de remédiation des vulnérabilités détectées par des audits ADS et SILENE ; • Mise en œuvre des recommandations formulées au sein des rapports d'audit afin d'atteindre un niveau de sécurisation minimum des AD (il est demandé d'atteindre a minima un score de 2 à fin septembre 2025 et recommandé d'atteindre un score de 3 en cible fin mars 2026).
Action n° 4 – Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) pour tous les établissements sanitaires	• Fin juin 2025 au plus tard, mise en œuvre de la démarche PCA/PRA au sein de tous les établissements via la formalisation de la comitologie : désignation d'un responsable PCA/PRA, formalisation d'une lettre de cadrage de la démarche signée par la Direction du GHT/Direction de l'établissement et mise en œuvre d'un comité de pilotage (COPIL) en charge du suivi de la démarche ; • A fin juin 2026, pour tous les établissements, formalisation des bilans d'impact sur l'activité (BIA) pour l'ensemble des services critiques (urgences, chirurgie, etc.) et services médico-techniques (pharmacie, imagerie, laboratoire, etc.) ; • A fin juin 2027, pour tous les établissements, formalisation des bilans d'impact sur l'activité pour le reste des services de soin, les services administratifs et les services logistiques et formalisation du PCRA cadre pour l'ensemble des services.
Action n° 5 – Intégrer le volet cyber dans la qualité et la gestion des risques de l'établissement	Intégrer et suivre l'ensemble des actions cyber au sein du plan d'amélioration de la qualité de l'établissement (PAQ), notamment : • les actions de remédiations identifiées au travers des audits ; • les actions d'amélioration identifiées au travers des exercices de crise ; • les actions permettant la construction séquencée du PCRA ; • les actions à entreprendre pour satisfaire aux mesures prioritaires.
Action n° 6 – Se conformer aux référentiels d'identification et d'authentification	Les établissements doivent définir, en adéquation avec la réglementation en vigueur, une trajectoire de sécurisation des moyens d'identification électronique (MIE) des professionnels qui exercent sous leur responsabilité, conformément au Référentiel d'identification électronique de la PGSSI-S (RIE), rendu opposable par l'arrêté du 28 mars 2022, exigeant notamment : • L'utilisation de MIE fournis par l'ANS (cartes CPS ou Pro Santé Connect), de MIE de niveau de sécurité équivalent (2FA) homologués par l'établissement, ou de MIE déjà certifiés au niveau eIDAS substantiel ou élevé par l'ANSSI ; • La mise en œuvre d'une brique de SSO pour les établissements responsables de plus de 5 services sensibles ou comptant plus de 5000 utilisateurs ayant accès à au moins 1 service sensible ; • La mise en place d'un répertoire d'identité local synchronisé avec la GRH et le RPPS ; • La production d'un engagement de sécurisation de l'IE des personnes physiques accédant aux services sensibles (modèle annexé au RIE).

Action n° 7 – Calculer dans chaque établissement sanitaire la part du budget dédié au numérique et renseigner cette donnée sur la plateforme nationale de suivi des systèmes d'information de santé	• Calcul par tous les établissements sanitaires de la part du budget dédiée au numérique dans le budget général de l'établissement et du nombre d'ETP consacré à la SSI
	  ○ Pour les établissements publics, se référer à la Note d'information n° DGOS/PF2/2019/207 du 26 septembre 2019 ;
	• Saisie annuelle de ces données par tous les établissements sur la plateforme nationale de suivi des systèmes d'information de santé, après la clôture des comptes de l'établissement (fin du S1 de chaque année pour la part de l'année N-1)
	  ○ Pour les groupes d'établissements mutualisant des dépenses relatives au numérique, il est demandé d'intégrer dans le calcul une part de cette dépense mutualisée en répartissant cette dernière selon l'activité combinée de chaque établissement concerné par la mutualisation.
	Pour les établissements groupés avec des structures non sanitaires sous la même entité juridique (ex : ESMS, centre de recherche), compte-tenu de la difficulté d'identifier précisément la ventilation de chaque dépense, il est demandé de tenir compte de l'ensemble de la dépense pour le calcul de la part dédiée au numérique dans le budget général.

Vu au titre du CNP par la secrétaire générale des ministères chargés des affaires sociales,

signé

Sophie LEBRET

Pour la ministre et par délégation :
La déléguée au numérique en santé,

signé

Hela GHARIANI