MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

INSTRUCTION N° SHFDS/FSSI/2023/78 du 23 mai 2023 relative au traitement des incidents significatifs ou graves de sécurité des systèmes d'information

Le secrétaire général des ministères chargés des affaires sociales

à

Mesdames et Messieurs les directeurs généraux
des agences régionales de santé

Copie à :

Madame la directrice de l'Agence du numérique en santé

Référence	NOR : SPRZ2313568J (numéro interne : 2023/78)
Date de signature	23/05/2023
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	Traitement des incidents significatifs ou graves de sécurité des systèmes d'information.
Commande	Application du décret du 27 avril 2022 relatif au traitement des incidents significatifs ou graves de sécurité des systèmes d'information.
Action à réaliser	Diffusion de cette instruction auprès des établissements sociaux et medico sociaux des régions.
Echéance	Immédiate.
Contact utile	Fonctionnaire de sécurité des systèmes d'information (FSSI) 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	Des modifications récentes ont été opérées au cadre juridique relatif au signalement des incidents significatifs ou graves de sécurité des SI. L'obligation de déclaration a été étendue aux établissements médico-sociaux et la procédure associée au traitement de ces signalements a également été modifiée. La présente instruction détaille ces évolutions et clarifie les obligations qui s'imposent aux établissements concernés.

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	Incident de sécurité, système d'information, signalement.
Classement thématique	Établissements de santé
Textes de référence	Code de la santé publique : article L. 1111-8-2, articles D. 1111-16-2 à D.1111-16-4.
Circulaire / instruction abrogée	Néant
Circulaire / instruction modifiée	Néant
Rediffusion locale	Établissements sanitaires, sociaux ou médico-sociaux.
Validée par le CNP le 27 janvier 2023 - Visa CNP 2023-03	
Document opposable	Non
Déposée sur le site Légifrance	Non
Publiée au BO	Oui
Date d'application	Immédiate

La présente instruction précise les évolutions apportées par l'ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé (ARS) et par le décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information. Ces textes, qui ont modifié les dispositions législatives et réglementaires du Code de la santé publique, ont principalement élargi l'obligation de signalements d'incidents significatifs ou graves de sécurité des systèmes d'information aux établissements médico-sociaux et modifié les procédures de traitement des signalements de ces incidents.

Depuis le décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions de traitement des incidents graves de sécurité des systèmes d'information du secteur santé, les établissements de santé - mais également les hôpitaux des armées, des organismes et services exerçant des activités de prévention, de diagnostic ou de soins (notamment les laboratoires de biologie médicale et les centres de radiothérapie) - sont soumis à l'obligation de signaler ces incidents.

Ce signalement se fait sur le portail des signalements opéré par l'Agence du numérique en santé (ANS) qui pilote, en coordination avec le Service du haut fonctionnaire de défense et de sécurité (HFDS), la mise en œuvre de ce dispositif pour les incidents concernant les systèmes d'information.

1- Elargissement de l'obligation de signalement aux établissements médico-sociaux

Conformément aux dispositions des articles D. 1111-16-3 et D. 1111-16-4 du Code de la santé publique, « les établissements médico-sociaux » sont dorénavant soumis à l'obligation de déclarer la survenue d'incidents significatifs ou graves de sécurité de leurs systèmes d'information.

Cette obligation s'applique également aux incidents susceptibles de toucher d'autres établissements, organismes ou services, notamment en cas d'attaque pouvant se propager vers d'autres entités soit par rebond depuis l'établissement touché soit à la suite d'un incident provoqué par un sous-traitant victime d'une attaque et fournissant des services à plusieurs établissements.

2- Évolution dans le dispositif de signalement

Le nouveau dispositif place l'ANS (CERT Santé) au centre de la gestion des signalements des établissements de santé et médico-sociaux. Tous les signalements lui remontent directement via le Portail des signalements des évènements sanitaires indésirables (PSIG).

Il est désormais de la responsabilité du CERT Santé d'informer sans délai tout signalement à la fois vers l'ARS concernée et vers le pôle FSSI du SHFDS, que l'incident soit de nature malveillante ou non, avec ou sans impact sanitaire.

Les ARS (et les groupements régionaux d'appui au développement de la e-santé [GRADeS] dans certaines régions) continueront à disposer d'un compte d'accès au PSIG pour récupérer les signalements d'incident de sécurité des systèmes d'information. Elles seront toujours alertées par le PSIG lors du dépôt d'une nouvelle déclaration par une structure localisée sur leur territoire. Elles seront également systématiquement informées des échanges entre le CERT Santé et les structures déclarantes pour intervenir si besoin auprès des établissements en d'impact de l'incident sur l'offre de soins.

Dans le scénario d'un incident susceptible d'avoir un impact sanitaire direct ou indirect, notamment en cas de dysfonctionnement de l'offre des soins, le signalement doit être également remonté sans délai par le CERT Santé au CORRUSS (Direction générale de la santé [DGS]).

a. Modalités de déclaration sur le site internet de l'ANS

Les modalités de déclaration restent inchangées. La déclaration est effectuée sans délai auprès du CERT Santé. Le formulaire de déclaration doit être renseigné sur le portail des signalements : https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil (espace professionnel de santé).
Le déclarant fournit toutes les informations dont il dispose au moment de la découverte de l'incident et notamment :

- les informations permettant d'identifier la structure concernée par l'incident ainsi que le déclarant ;
- la description de l'incident, notamment la date du constat, le périmètre de l'incident, les systèmes d'information et données concernées et l'état de la prise en charge ;
- la description de l'impact de l'incident sur les données, les personnes, les systèmes d'information et la structure ;
- les causes de l'incident si celles-ci sont identifiées.

b. Rôle de l'ANS (CERT Santé)

Au regard du Code de la santé publique, l'ANS (CERT Santé) assure les missions suivantes :

- l'analyse des incidents significatifs ou graves de sécurité des systèmes d'information et la proposition des mesures à prendre pour faire face à cet incident ;
- l'appui de la structure déclarant l'incident ;
- la relation avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) (en l'occurrence le CERT-FR) notamment en cas d'incident concernant un opérateur de service essentiel ou qui pourrait avoir une portée nationale ;
- la prévention des incidents ;
- la gestion et la mise en œuvre du traitement de données à caractère personnel relatif aux signalements.

Le CERT Santé assure dès réception du signalement un travail de qualification de l'incident afin d'identifier une éventuelle cause malveillante. Dans un tel cas où se confirme une attaque cyber, un protocole adapté est déroulé par le CERT Santé en appui de la structure déclarante afin de la prémunir contre un risque de propagation de l'attaquant dans ses réseaux et au-delà à l'échelle du groupement hospitalier de territoire (GHT) ou vers un échelon régional ou national. La préservation de preuves numériques s'inscrit dans les mesures d'urgence préconisées par le CERT Santé.
Si la phase de qualification aboutit à un incident de nature non malveillante, le CERT Santé en informe le déclarant et lui indique qu'il n'y aura pas de suite particulière apportée au signalement. Ces incidents non malveillants, d'origine technique ou humaine, apparaissent néanmoins dans les statistiques annuelles du CERT Santé.

De plus, dans le cadre de ses actions de prévention, l'ANS (CERT Santé) :

- met à disposition des fiches et des guides pour améliorer la sécurité des systèmes et réduire le risque d'être victime d'un acte de cyber-malveillance ;
- offre un service de cyber surveillance permettant aux structures de tester à la demande les vulnérabilités exposées sur internet ;
- alerte les structures en cas de vulnérabilité critique détectée sur la base de scans périodiques de l'exposition sur internet des structures ;
- propose un accompagnement pour le renforcement du niveau de sécurité.

3- Cas des opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE) du secteur santé

L'évolution de ce dispositif de signalement se fait sans préjudice des autres déclarations obligatoires, en particulier de l'obligation de signalement à l'ANSSI (CERT-FR) par les OIV des incidents affectant leurs systèmes d'information d'importance vitale (SIIV) et par les OSE des incidents affectant leurs systèmes d'information d'importance essentielle (SIE).

Il s'agit donc pour cette catégorie d'établissements de signaler leurs incidents à la fois au CERT-FR et au CERT Santé, qui remontera le signalement aux autorités ministérielles (DGS et SHFDS) et ARS concernées.

4- Cas des incidents survenant hors heures ouvrées et jours ouvrés

Depuis le 17 octobre 2022, le CERT Santé a étendu son service de réponse à incident aux heures non ouvrées. Une astreinte est mobilisée pour 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 de ses activités.

La personne d'astreinte au sein du service informatique ou de la direction des systèmes d'information (DSI) de l'établissement devra déclarer son incident au CERT Santé en appelant le 09 72 43 91 25, accueil téléphonique du CERT Santé. Elle bénéficiera d'un appui dans la qualification de l'incident et la mise en œuvre de mesures permettant de stopper la propagation d'une activité malveillante au sein de son système d'information.

5- Exception pour les hôpitaux militaires

Tous les incidents de sécurité impactant les hôpitaux militaires remontent uniquement dans la chaîne de traitement cyber du Ministère des Armées. Selon la nature de l'incident et son degré de confidentialité, le Ministère des Armées en informe le SHFDS et le CERT Santé qui, en cas d'impact sanitaire, en informera sans délai l'ARS concernée.

6- Déclaration à la Commission nationale de l'informatique et des libertés (CNIL) par l'établissement

L'obligation de déclaration à la CNIL directement par l'établissement victime d'un incident ayant entraîné l'indisponibilité, le vol ou la perte de données de santé demeure, dans les conditions prévus au Règlement général sur la protection des données (RGPD) Notifier une violation de données personnelles | CNIL.

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

Pierre PRIBILE