Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère des Solidarités et de la Santé

Secrétariat général des ministères chargés des affaires sociales

Service spécialisé du haut fonctionnaire de défense et de sécurité

Fonctionnaire de sécurité des systèmes d'information

Personne chargée du dossier : Philippe LOUDENOT
Tél : 01 40 56 63 36
Mél. : philippe.loudenot@sg.social.gouv.fr

La ministre des solidarités et de la santé

à

Mesdames et Messieurs les directeurs généraux des agences régionales de santé

INSTRUCTION N° SG/SHFDS/FSSI/2017/ 281 du 26 septembre 2017 relative au rôle des ARS dans la mise en œuvre du dispositif de déclaration obligatoire et de traitement des signalement des incidents graves de sécurité des systèmes d'information des structures de santé

Date d'application : Immédiate
NOR : SSAZ1727191J
Classement thématique : établissements de santé - gestion.
Validée par le CNP le 15 septembre 2017 - Visa CNP 2017-105

Catégorie : Directives adressées par la ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.
Résumé : Présentation du dispositif de déclaration obligatoire et de traitement des signalements des incidents graves de sécurité des systèmes d'information et rôle des ARS. Information des directeurs de structures de santé sur le dispositif de déclaration obligatoire et traitement des signalements des incidents de sécurité par les ARS.
Mots-clés : sécurité des systèmes d'information, SSI, signalement, déclaration obligatoire, incident, veille, protection des données de santé.
Textes de référence : Article L. 1111-8-2 du code de la santé publique, créé par l'article 110 de la loi n° 2016-41 du 26 janvier 2016 de modernisation du système de santé français, instituant l'obligation de signalement des incidents de sécurité des systèmes d'information par les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins

Décret n° 2016-1214 du 12 septembre 2016 (JORF n° 0214 du 14 septembre 2016) relatif aux conditions de traitement des incidents graves de sécurité des systèmes d'information du secteur santé (article D. 1111-16-2-I et suivants du code de la santé) Arrêté prévu par le décret n° 2016-1214 du 12 septembre 2016. Instruction DGS/VSS1/PP1/PP4/EA1/SG/DGOS/PF2/2017/78 du 3 mars 2017 relative à l'organisation régionale des vigilances et de l'appui sanitaires
Annexes : - Annexe 1 : Processus global de traitement des signalements d'incidents graves de sécurité : - Annexe 2 : Fiche de présentation du dispositif destiné aux structures de santé
Diffusion : directions des établissements de santé, des hôpitaux des armées, des laboratoires de biologie médicale et des centres de radiothérapie.

La présente instruction précise les modalités pratiques de mise en place du dispositif de traitement des signalements des incidents de sécurité des systèmes d'information prévu par le décret n° 2016-1214 du 12 septembre 2016, dans le cadre de l'obligation de déclaration des incidents de sécurité faite aux établissements de santé, aux hôpitaux des armées, aux centres de radiothérapie ainsi qu'aux laboratoires de biologie médicale par l'article L. 1111-8-2 du code de la santé publique. Dans la suite du document, ces différents acteurs du système de santé sont désignés sous le terme générique de « structures ». Sous la responsabilité du haut fonctionnaire de défense et de sécurité et notamment du fonctionnaire de sécurité des systèmes d'information (HFDS/FSSI), l'Agence des systèmes d'information partagés de santé (ASIP Santé) est l'opérateur du ministère des solidarités et de la santé dans la mise en œuvre de ce dispositif.

1. Enjeu

L'interconnexion croissante des réseaux et les besoins de dématérialisation exposent les systèmes d'information à des incidents de sécurité. Dans le secteur de la santé, ces systèmes apparaissent comme critiques, que ce soit au regard de leur disponibilité ou vis-à-vis de l'intégrité et de la confidentialité des données qu'ils manipulent. La mise en défaut de ces systèmes pourrait impacter fortement l'activité de l'ensemble des acteurs du secteur et la prise en charge des patients.

2. Règlementation applicable

La règlementation applicable pour la mise en place de ce dispositif de traitement des signalements est la suivante :

- **L'article L.1111-8-2 du code de la santé publique** (créé par l'article 110 de la loi précitée du 26 janvier 2016), qui institue l'obligation pour les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins de déclarer les « incidents graves de sécurité des systèmes d'information » ;
- **Le décret n° 2016-1214 du 12 septembre 2016,** qui pose les conditions dans lesquelles les incidents graves de sécurité des systèmes d'information doivent être signalés et traités (déclaration sans délai par la structure concernée, qualification par l'Agence régionale de santé, transmission des incidents jugés significatifs par l'ARS à l'ASIP Santé).
- **L'arrêté du 1er octobre 2015** portant approbation de la politique de sécurité des systèmes d'information (PSSI) des ministères chargés des affaires sociales (JO du 27 octobre 2015), dont l'annexe précise les mesures à mettre en œuvre par les services et par les structures.

3. Objectifs du dispositif

Les objectifs du dispositif sont :

- **de renforcer le suivi des incidents** pour le secteur santé des établissements concernés ;
- **d'alerter et d'informer** l'ensemble des acteurs de la sphère santé dans le cas d'une menace pouvant avoir un impact sur le secteur ;
- **de partager des bonnes pratiques** concernant les actions de prévention ainsi que les réponses à apporter aux incidents, afin de réduire les impacts et de mieux protéger les systèmes.

Pour répondre à ces objectifs, un **dispositif de prévention et de traitement des incidents de sécurité au profit des acteurs de santé** est mis en place pour être opérationnel le **1er octobre 2017.**

Il vous est donc demandé d'informer dans les meilleurs délais les responsables des structures concernées sur les modalités de mise en place de ce dispositif obligatoire ainsi que sur la gamme des services proposés dans ce cadre.

4. Mise en place du dispositif de traitement des signalements des incidents de sécurité

Dans le cadre de la mise en œuvre du décret du 12 septembre 2016 précité, l'ASIP Santé est désignée comme le groupement d'intérêt public en charge d'apporter un appui au traitement des incidents de sécurité du système d'information.

Sous la responsabilité du HFDS/FSSI, l'ASIP Santé met en place une Cellule Accompagnement Cybersécurité des Structures de Santé (ACSS), dispositif opérationnel dont l'organisation, les activités et les moyens permettent de répondre aux modalités du décret (ce dispositif est décrit dans l'annexe 1).

5. Traitement des signalements des incidents de sécurité SI : rôle des ARS et des structures

A partir du 1er octobre 2017, les signalements des incidents de sécurité sur les systèmes d'information sont obligatoires. Ils sont effectués via le portail de signalement des évènements sanitaires indésirables – espace des professionnels de santé :

https://signalement.social-sante.gouv.fr

Le traitement des signalements est directement réalisé par la cellule ACSS. Si le signalement est effectué en heures non ouvrés (au-delà de 18h) ou jours non ouvrés et que le déclarant estime, au regard des impacts constatés et de l'évolution de l'incident de sécurité, avoir besoin d'une aide à la gestion de l'incident dans les plus brefs délais il doit, en parallèle du signalement sur le portail des vigilances, en informer le FSSI au travers de la BAL : ssi@sg.social.gouv.fr, afin d'en assurer son traitement et qui, le cas échéant ,alerte le centre opérationnel de la sécurité des systèmes d'information de l'agence nationale de sécurité des systèmes d'information.

Le décret du 12 octobre 2016 précité précise que les structures doivent signaler les incidents graves de sécurité ayant des conséquences :

- potentielles ou avérées sur la **sécurité des soins** ;
- sur la disponibilité, l'intégrité ou la confidentialité des **données de santé** ;

- sur le **fonctionnement normal** de l'établissement.

D'une façon plus générale, il est demandé que les structures signalent toute action ou suspicion d'action malveillante causant une **indisponibilité partielle ou totale** de systèmes informatiques, **une altération ou une perte de données**.

Les **directeurs des structures** sont chargés de réaliser cette déclaration ou désignent une personne déléguée responsable du signalement des incidents.

Les agences régionales de santé s'appuient sur l'ASIP-Santé/cellule ACSS qui est chargée d'analyser la déclaration et de qualifier les incidents signalés.

La structure concernée par l'incident est informée de la prise en compte et de l'analyse de son signalement par l'**ASIP Santé/cellule ACSS**.

L'ASIP Santé et l'agence régionale de santé peuvent demander à la structure concernée par l'incident toute information complémentaire permettant la qualification de l'incident et la mise en place d'une réponse adaptée.

A la demande de la structure concernée par l'incident, **l'ASIP Santé et l'agence régionale de santé** l'accompagnent dans la gestion de l'incident. Elles peuvent formuler des **recommandations** et notamment proposer des **mesures d'urgence** pour limiter l'impact de celui-ci, des **mesures de remédiation** ainsi que des **mesures destinées à améliorer la sécurité** du ou des systèmes d'information concernés.

Les **agences régionales de santé** doivent mettre en place une organisation interne appropriée pour suivre le traitement des signalements d'incidents de sécurité.

L'ensemble des actions à réaliser sont précisées en annexe 1.

6. Mise en place d'un portail de veille et d'échange

Dans le cadre des actions de sensibilisation et d'accompagnement des structures, l'ASIP/cellule ACSS met en place un portail Web dédié d'information sur l'actualité SSI, les menaces sectorielles et les bonnes pratiques. Il présente des bulletins de veille sur les vulnérabilités logicielles critiques, des fiches réflexes, des guides pour répondre à différents types d'incidents et des analyses sur la mise en œuvre de nouvelles technologies.

Ce portail met aussi à disposition de la communauté SSI du secteur un espace accessible uniquement par authentification, sur lequel d'autres services sont disponibles : forum de discussion, possibilité de commenter des documents mis en ligne sur l'espace public, ... Ce portail est accessible à partir de l'adresse suivante : https://www.cyberveille-sante.gouv.fr

7. Présentation des dispositifs de déclaration et de traitement des incidents aux structures : rôle des ARS

Il vous est demandé de mettre en place, en lien avec le HFDS/FSSI et l'ASIP Santé/cellule ACSS, des actions de communication adaptées afin de présenter aux responsables des structures concernées **le dispositif de déclaration des incidents de sécurité** en vigueur à partir du 1er octobre 2017, ainsi que **le dispositif de traitement des signalements des incidents** de sécurité, présenté dans l'annexe 2.

Vous veillerez à la mise en place de boîtes fonctionnelles dédiées à la SSI au sein des établissements concernés ainsi qu'au niveau de vos ARS (SSI-[région]@ars.sante.fr) permettant la réception d'alertes spécifiques en matière de cybersécurité.

8. Contacts

Toute question sur la présente instruction est à adresser aux boites fonctionnelles suivantes :

- Fonctionnaire de Sécurité des Systèmes d'Information : ssi@sg.social.gouv.fr
- ASIP Santé : cyberveille@sante.gouv.fr

Vous pouvez également vous rendre sur le Portail esante.gouv.fr sur lequel un espace est réservé à la présentation de la mise en place du dispositif de traitement des signalements des incidents de sécurité.

Pour la ministre et par délégation

Le secrétaire général des ministères
chargés des affaires sociales,

signé

Pierre RICORDEAU

ANNEXE 1

Processus global de traitement des signalements d'incidents graves de sécurité des systèmes d'information

Sommaire

1 Introduction

Ce document présente le processus de traitement des signalements d'incidents graves de sécurité ainsi que le rôle des acteurs en charge d'apporter une réponse aux signalements.

2 Processus général

2.1 Déroulement

La gestion (déclaration et traitement) des signalements d'incidents graves de sécurité repose sur les activités suivantes :

- Le signalement d'un incident de sécurité par une structure observant des impacts tels que définis par le décret 2016-1214 (le directeur de la structure ou une personne désignée par le directeur de la structure) : le déclarant décrit son évènement au travers d'un formulaire ;
- La qualification de l'incident par une ARS et par l'ASIP Santé;
- La réponse circonstanciée à un incident de sécurité pour limiter les impacts et accompagner les structures dans la mise en place de mesures curatives ;
- L'analyse des performances de signalement de chaque incident de sécurité et de la pertinence de la réponse apportée dans le cadre d'un retour d'expérience ;
- L'activité de suivi et de reporting de l'ensemble des signalements traités ;
- L'accompagnement des acteurs de santé dans l'amélioration de leurs mesures de sécurité et de gestion des incidents à l'aide de :
    - Fiches réflexes en cas d'incident ;
    - Bonnes pratiques et moyens de prévention ;
    - Bulletins de sécurité créés à partir d'une veille sur des vulnérabilités des composants logiciels et matériels du secteur santé.

La déclaration d'un incident de sécurité au sein d'une structure doit présenter les faits avérés de l'observation d'un évènement. Elle doit décrire l'incident de manière la plus détaillée possible, afin de permettre sa qualification et de pouvoir ajuster la rapidité et l'intensité des actions d'appui et d'accompagnement.

Le traitement du signalement d'un incident de sécurité consiste à accompagner la structure dans le cadre de la réponse à apporter à l'incident.

Le suivi de la réponse apportée au sein de la structure déclarante permet de connaitre le niveau d'exposition aux risques relatif à chaque vulnérabilité identifiée et ainsi améliorer l'aide au traitement apporté par les ARS et l'ASIP Santé/cellule ACSS en coordination avec le HFDS/FSSI.

L'ASIP Santé communique aux personnes en charge de piloter la réponse aux incidents et d'améliorer le niveau de protection du système face aux nouvelles menaces, des retours d'expérience, des recommandations et des bonnes pratiques.

2.2 Exception pour les hôpitaux militaires

Tous les incidents de sécurité impactant les hôpitaux militaires remontent dans et uniquement dans la chaine de traitement « CYBER » du ministère des armées, qui les qualifie et les traite suivant ses procédures. Selon la nature de l'incident et de son niveau de confidentialité, le ministère des armées en informe soit le HFDS, soit l'ASIP Santé. L'ARS compétente sera uniquement informé de son

existence par un message type. Cependant, si l'incident a des conséquences sur l'offre de soins, l'ARS en sera immédiatement informée.

2.3 Présentation synthétique du rôle des acteurs au sein du processus

2.3.1 Le Ministère de la Santé :

2.3.1.1 HFDS/FSSI

Afin de respecter la cohérence globale en matière d'animation de la politique de sécurité des systèmes d'information, de contrôle et de mutualisation des actions, le HFDS/FSSI assure le pilotage de ce dispositif. Le FSSI est le correspondant des structures interministérielles spécialisées en matière de SSI et facilite les échanges et le traitement des exigences multiples.
Les principales actions menées par le HFDS/FSSI sont les suivantes :

- Pilote les actions d'appui dans le cadre des incidents significatifs
- Assure le traitement des signalements ou demandes urgentes d'accompagnement en heure non ouvrées (à partir de 18h) et les jours non ouvrés au travers de la boîte ssi@sg.social.gouv.fr ,
- Pilote les alertes vers les structures du périmètre des ministères sociaux en cas de risque important et/ou de propagation d'une menace,
- Pilote les actions de communication en lien avec la DICOM du ministère,
- Assure la liaison avec l'ANSSI et les partenaires interministériels.

2.3.1.2 DGS

Les principales actions menées par la DGS sont les suivantes :

- Analyse de l'impact sur la prise en charge des patients et l'organisation des soins à partir d'une alerte émise par l'ASIP Santé et en informe le HFDS,
- Gère les conséquences sanitaires,
- Diffuse des recommandations / mesures palliatives en mode dégradé (hors SI),
- Reçoit du HFDS une analyse de l'impact interministériel.

La DSSIS, la DGS et la DGOS contribuent également à la mise en place du dispositif pour le compte du Ministère.

2.3.2 L'ASIP Santé/Cellule ACSS

Le HFDS/FSSI s'appuie sur l'ASIP Santé pour mettre en place ce dispositif de traitement des signalements des incidents de sécurité au travers de la création de la Cellule Accompagnement Cybersécurité des Structures de Santé (Cellule ACSS).

Les principales actions menées par la cellule ACSS sont les suivantes :

- Reçoit les signalements et notifie au déclarant sa prise en compte,
- Analyse et qualifie le signalement pour le compte de l'ARS compétente,
- Apporte si besoin un accompagnement dans le traitement de l'incident « numérique »,
- Informe le HFDS de tout signalement analysé et lui apporte un appui pour les actions d'accompagnement relatives aux incidents significatifs et dans le cadre d'une gestion de crise,
- Assure le traitement des signalements en heures ouvrés (9h-18h),
- Alerte sans délai la DGS dans le cas d'un incident ayant un impact sanitaire potentiel,

- Corrèle les évènements en cas de signaux faibles concordant sur le territoire,
- Diffuse les alertes vers les ARS et structures relevant de l'article 110 de la loi n° 2016-41 du 26 janvier 2016
- Assure l'interface avec les éditeurs dans le cadre de vulnérabilités identifiées et de demandes de correctifs (à l'exclusion des logiciels suivis par l'ANSM).

2.3.3 Les ARS

Les ARS reçoivent les signalements d'incident grave de sécurité. Le signalement des incidents par les structures sera simultané tant vers les ARS que l'ASIP Santé, le temps que les ARS adaptent ou complètent leur organisation.
Les principales actions menées par les ARS sont les suivantes :

- Reçoit les signalements et demande une analyse à l'ASIP en vue de leur qualification,
- Participe à l'analyse effectuée par l'ASIP Santé,
- Apporte si besoin un accompagnement dans le traitement de l'incident « numérique »,
- Prend les mesures nécessaires pour faire face aux conséquences éventuelles de l'incident sur l'offre de soins de son territoire.
- Sensibilise l'ensemble des professionnels du secteur à la sécurité des systèmes d'information et à la déclaration des incidents graves de sécurité des systèmes d'information.

2.3.4 L'ANSM

L'ANSM traite les signalements relatifs aux incidents concernant les dispositifs médicaux (DM), les dispositifs médicaux de diagnostic in vitro (DMDIV), les logiciels d'aide à la prescription (LAP) et les logiciels d'aide à la dispensation (LAD)

Le FSSI, l'ASIP Santé et l'ANSM coordonnent leurs actions lorsque des incidents de sécurité de système d'information mettent en jeu les dispositifs et logiciels cités ci-dessus.

Une convention ANSM-HFDS-ASIP/ACSS doit être réalisée.

2.3.5 L'ANSSI

En tant que CERT National, l'ANSSI est un partenaire privilégié pour des échanges relatifs à la mise en place des processus et des outils.
Pour les SI classifiés en SIIV, le signalement des incidents doit être signalé au HFDS/FSSI et à l'ANSSI. Les conditions et les modalités de traitement des signalements des incidents émis par des structures de santé OIV devront être définies par l'ANSSI, le FSSI et l'ASIP Santé.

Une convention ANSSI-HFDS-ASIP/ACSS doit être réalisée.

2.3.6 Les organismes cités par le décret

Les organismes cités par le décret sont les établissements de santé, les organismes et services exerçant des activités de prévention, de diagnostic ou de soins : les établissements de santé, les hôpitaux des armées, les laboratoires de biologie médicale et les centres de radiothérapie.
La déclaration des incidents graves de sécurité des systèmes d'information est effectuée par le directeur de la structure ou la personne déléguée.
Lors de la phase de spécification et de mise au point du dispositif de gestion des incidents, quelques structures seront approchées afin de leur proposer d'être des pilotes pour éprouver les processus mis en œuvre.

2.3.7 Le ministère des armées

Le ministère de la défense intervient au titre du traitement opérationnel des incidents de sécurité pour le compte des hôpitaux militaires.

2.3.8 Les éditeurs et industriels du secteur

Les structures font appel à des éditeurs spécialisés pour la mise en place de systèmes participant à la prise en charge du patient : systèmes logiciels hospitaliers, logiciels GAM, DPI, plateaux techniques de biologie, d'imagerie médicale, SI de gestion des repas, gestion des gaz médicaux, des composants du SI directement liés aux activités de prévention, de diagnostic ou de soins, de prise en charge d'un patient, facturation, etc..

Ces éditeurs sont responsables du maintien en condition de sécurité de leurs logiciels et peuvent faire l'objet de sollicitations particulières de la part de la Cellule ACSS lors de la découverte d'une vulnérabilité affectant leur logiciel dans le cadre d'un incident de sécurité.

De nombreux établissements font appel à des hébergeurs de données de santé ou à des prestataires de services pour assurer la protection de leurs données ou de leurs systèmes. A ce titre, ils sont identifiés par la Cellule ACSS comme des acteurs participant directement au traitement des incidents et à la prise en compte des alertes. Ils feront donc l'objet d'une attention particulière dans le cadre de la sensibilisation des acteurs.

3 Détail des phases du processus

3.1 Phase 1 : Signalement de l'incident de sécurité

Cette étape correspond au signalement d'un incident de sécurité. Les structures doivent être en capacité d'identifier les incidents de sécurité affectant les systèmes sous leur responsabilité et de les déclarer sans délais aux acteurs en charge de la qualification désignés par le décret.

3.1.1 Acteurs

Les structures devant déclarer les incidents de sécurité sont :

- Les établissements de santé ;
- Les hôpitaux militaires ;
- Les laboratoires de biologie médicale ;
- Les centres de radiologie.

Dans chaque structure, le directeur de la structure désigne la ou les personnes en mesure de déclarer les incidents de sécurité.

3.1.2 Élément déclencheur

Les personnels d'une structure ciblée par le décret observent un incident de sécurité touchant à la sécurité des systèmes d'information.

3.1.3 Tâches

Le directeur de la structure ou la personne désignée déclare l'incident sur le portail de signalement des évènements sanitaires indésirables via un formulaire de déclaration des incidents de sécurité.

Tâche A : Identifier le périmètre de l'incident de sécurité

- repérer les éléments du système d'Information concernés par l'incident (matériel, logiciel) ;

Tâche B : Identifier l'impact de l'incident sur la sécurité de la structure et des données

- identifier l'impact sur le fonctionnement des systèmes et sur l'organisation de la structure ;

Tâche C : Evaluer la capacité à traiter l'incident de sécurité

- identifier si une action malveillante est à l'origine de l'incident ;

Tâche D : Remplir et valider le contenu du formulaire sur le portail de signalement des évènements sanitaires indésirables

Lorsque la déclaration est validée, la notification de signalement est transmise aux acteurs en charge de la qualification.

Le déclarant reçoit un message électronique l'informant de la prise en compte de sa déclaration sur le portail de signalement des évènements sanitaires indésirables et précisant les entités alertés.

Si le signalement est effectué en heures non ouvrés (au-delà de 18h) ou jours non ouvrés et que le déclarant estime, au regard des impacts constatés et de l'évolution de l'incident de sécurité, avoir besoin d'une aide à la gestion de l'incident dans les plus brefs délais il doit, en parallèle du signalement sur portail de signalement des événements sanitaires indésirables**, en informer le FSSI au travers de la BAL ssi@sg.social.gouv.fr.**

3.1.4 Délai d'exécution

La déclaration d'un incident de sécurité doit s'effectuer sans délai après son observation en vue d'obtenir une réponse rapide et adaptée par les ARS et la Cellule ACSS à l'évènement ciblé.

3.1.5 Éléments en sortie

- le formulaire de déclaration d'incident de sécurité renseigné est disponible sur le portail de signalement des évènements sanitaires indésirables.

3.1.6 Phase suivante

Phase 2 : Prise en compte du signalement de l'incident de sécurité par les ARS et la Cellule ACSS.

3.2 Phase 2 : Communication et prise en compte du signalement par l'ARS et la Cellule Accompagnement Cybersécurité des Structures de Santé (ACSS)

L'ARS en responsabilité sur le territoire où se situe la structure impactée ainsi que la Cellule ACSS sont informés d'un signalement sur le portail de signalement des évènements sanitaires indésirables.

La Cellule ACSS ouvre un dossier de traitement suite à la récupération du contenu de la déclaration sur le portail de signalement.

3.2.1 Acteurs

- L'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité
- La Cellule ACSS

3.2.2 Éléments en entrée

- Le formulaire de déclaration stocké temporairement sur le portail de signalement des évènements sanitaires indésirables regroupant toutes les informations communiquées par le déclarant concernant l'incident de sécurité.

3.2.3 Tâches

Tâche A : Notification du dépôt sur le portail de signalement des évènements sanitaires indésirables du signalement d'un incident de sécurité par mail à destination des acteurs en charge de la qualification (ARS et la Cellule ACSS)

Tâche B : Récupération de la déclaration de l'incident de sécurité sur le portail de signalement des évènements sanitaires indésirables par les acteurs en charge de la qualification.

Tâche C : Ouverture d'un dossier de traitement du signalement par la Cellule ACSS

Tâche D : Notification au déclarant de la prise en compte de sa déclaration par la Cellule ACSS

3.2.4 Délais

La prise en compte de la déclaration par les acteurs en charge de la qualification doit être réalisée dans les meilleurs délais suivant la notification.

3.2.5 Eléments en sortie

La Cellule ACSS créé et initialise un dossier de traitement du signalement de l'incident de sécurité puis informe le déclarant de la prise en compte de sa déclaration.

3.3 Phase 3 : Qualification du signalement

L'ARS compétente s'appuie sur l'ASIP Santé qui analyse la déclaration et qualifie les incidents signalés pour son compte. La Cellule ACSS analyse chaque signalement et sollicite si besoin le déclarant pour pouvoir réaliser sa qualification. Cette analyse peut nécessiter un échange entre la Cellule ACSS et les structures. Le contenu de cet échange fait l'objet d'une fiche d'aide au traitement d'un incident de sécurité qui sert de support d'échanges entre la Cellule ACSS et les structures durant les étapes de qualification des signalements et d'aide au traitement des incidents de sécurité.

La qualification d'un incident est basée sur les définitions du décret mais aussi sur la base de la fiche d'aide au signalement diffusée par la Cellule ACSS.

La Cellule ACSS informe l'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité de la qualification du signalement.

3.3.1 Acteur

- L'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité
- La Cellule ACSS
- Le FSSI

3.3.2 Éléments en entrée

- Le dossier de traitement du signalement de l'incident de sécurité à l'état « en attente de qualification »

3.3.3 Tâches

La qualification du signalement est prise en charge par un expert sécurité qui analyse et juge de la criticité de l'incident de sécurité.

Tâche A : Qualification de l'incident
Elle permet de définir la criticité de l'incident qui conditionnera les modalités d'appui et d'accompagnement. Elle peut nécessiter une prise de contact avec le déclarant et l'initialisation d'une fiche de suivi de l'aide au traitement d'un incident.

En fonction du résultat de l'analyse, l'une ou plusieurs des tâches suivantes est à exécuter :

Tâche B1 : Il ne s'agit pas d'un incident de sécurité : la Cellule ACSS en informe le déclarant et lui indique qu'il n'y aura pas de suite particulière apportée au signalement.

Tâche B2 : Il s'agit d'un incident grave ou significatif : la Cellule ACSS en informe le HFDS qui assure ensuite le pilotage du traitement en cas d'incident significatif (phase 4).

Tâche B3 : Il s'agit d'un incident susceptible d'avoir un impact sanitaire direct ou indirect : la Cellule ACSS alerte, outre le FSSI, la DGS.

3.3.4 Délai d'exécution

La qualification doit être réalisée dans les meilleurs délais suivant la création du dossier de traitement du signalement.

3.3.5 Éléments en sortie

- L'incident est qualifié
- Le dossier de traitement du signalement de l'incident de sécurité à l'état « à traiter ».

3.3.6 Phase suivante

Si le signalement ne correspond pas à un incident de sécurité, il faut clore le dossier (phase 5 « Clôture du dossier de traitement »).
S'il s'agit d'un incident grave ou significatif, il faut passer aux étapes de traitement (Phase 4 ou 4 bis).

3.4 Phase 4 : Appui au traitement des incidents graves

L'ARS compétente informe la Cellule ACSS si elle souhaite lui confier, lui déléguer une partie, ou prendre totalement en charge l'appui au traitement de l'incident.

L'appui au traitement des incidents de sécurité consiste à proposer aux structures venant de subir un incident des actions concrètes pour stopper l'éventuelle progression de l'incident et protéger leur système d'information.

La Cellule ACSS utilise la fiche de suivi de l'appui au traitement d'un incident comme support d'échange pour partager sur l'analyse de l'incident, sur les actions d'aide au traitement et disposer de l'état d'avancement du traitement de l'incident par la structure.

Si la prise en charge de l'appui au traitement de l'incident lui est confiée, la Cellule ACSS informe l'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité des actions entreprises. La fréquence des retours de l'ASIP Santé vers l'ARS se fera au cas par cas selon le degré de criticité de l'incident, de son impact et de son évolution dans le temps. Toutefois l'ARS sera informée au moins une fois par semaine de l'avancement des actions menées.

3.4.1 Acteurs

- L'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité
- La Cellule ACSS
- La structure impactée par l'incident

3.4.2 Éléments en entrée

Pour l'appui au traitement des incidents, les experts en réponse aux incidents de sécurité disposent du dossier de traitement du signalement contenant :

- Les informations communiquées par le déclarant ;
- La qualification par les experts de la Cellule ACSS;
- L'analyse contextuelle si d'autres incidents du même type ont déjà été traités.

3.4.3 Tâches

Tâche A : Vérification si d'autres incidents du même type ont été remontés et sont toujours en cours de traitement (passage à significatif)

Si un ou plusieurs autre(s) incident(s) similaire(s) est (sont) en cours de traitement, il faut immédiatement passer à la phase 4bis.

Tâche B: Analyse des causes de l'incident de sécurité

L'analyse de l'incident a pour objectif de préciser le périmètre technique impacté et les causes malveillantes ou non de son origine.

- Demande d'informations complémentaires au déclarant permettant d'approfondir l'analyse et d'apporter un meilleur accompagnement ;
- Le cas échéant, demande de préservation des traces numériques.

Tâche C : Accompagnement de la structure

Suite à la qualification et aux premières analyses, des mesures d'urgence peuvent être prises pour limiter les impacts et préserver les traces numériques. En effet, même sans connaitre précisément l'impact réel de l'incident qui fait l'objet d'une analyse approfondie, l'identification des causes de l'incident permet de recommander les actions immédiates ou déclencher des mesures à prendre au sein de la structure, comme par exemple :

- Un confinement (débranchement du réseau d'un poste infecté) ;
- Une isolation (couper les flux de messagerie internet) ;
- Une communication ciblée de recommandations ;

Ces mesures d'urgence doivent être documentées dans les procédures du support informatique de chaque structure sous forme de fiches réflexes et de mesures de sécurité.

La Cellule ACSS met à disposition des structures des fiches réflexes sur son portail SSI sectoriel. Elles seront régulièrement mises à jour et de nouvelles fiches pourront être créées.

Ces fiches décrivent l'ensemble des informations/actions à réaliser par les exploitants. Elles seront classées par type d'incident et adaptées au niveau de compétence de l'interlocuteur ainsi qu'au type de structure.

L'objectif est d'obtenir un traitement simple et efficace des actions à mettre en œuvre. De plus, les réponses aux incidents liées aux fiches réflexes doivent être revues régulièrement afin de s'assurer de leur efficacité.

La Cellule ACSS accompagne les structures au cas par cas. Lorsque la Cellule ACSS estime ne pas pouvoir apporter un appui suffisant à la structure au regard de la nature de l'incident et de son impact, elle communiquera une liste de prestataires qui pourront aider la structure à confiner l'incident et mettre en œuvre des mesures de protection. Cette liste de prestataire sera disponible sur son portail SSI sectoriel.

L'ARS compétente prend les mesures nécessaires pour faire face aux conséquences éventuelles de l'incident sur l'offre de soins de son territoire.

3.4.4 Délai d'exécution

La structure doit être contactée dans les meilleurs délais après la qualification de l'incident. L'appui et l'accompagnement sont réalisés en jours ouvrés dans les délais compatibles avec la criticité de l'incident.

3.4.5 Éléments en sortie

- Fiche(s) réflexe(s) correspondant(es) au type d'incident rencontré par la structure ;
- Accompagnement personnalisé au cas par cas ;
- Communication d'une liste de prestataires référencés par l'Etat ;
- Dossier de traitement à l'état « A clôturer ».

3.4.6 Phase suivante

Phase 5 : Clôture du dossier de traitement

3.5 Phase 4 Bis : Appui au traitement de l'incident significatif par la Cellule ACSS

L'aide au traitement des incidents significatifs est pilotée par le HFDS/FSSI. Cette démarche est globalement identique à celle menée dans le cadre du traitement des incidents graves.

La Cellule ACSS utilise la fiche de suivi de l'aide au traitement d'un incident comme support d'échange pour partager sur l'analyse de l'incident, sur les actions d'aide au traitement et disposer de l'état d'avancement du traitement de l'incident par la structure.

La Cellule ACSS informe l'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité des actions entreprises dans l'aide au traitement de l'incident. La fréquence des retours de l'ASIP Santé vers l'ARS se fera au cas par cas selon le degré de criticité de l'incident, de son impact et de son évolution dans le temps. Toutefois l'ARS sera informée au moins une fois par semaine de l'avancement des actions menées.

3.5.1 Acteurs

- HFDS/FSSI
- L'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité
- DGS
- La Cellule ACSS
- La structure impactée par l'incident

3.5.2 Éléments en entrée

- Le dossier de traitement du signalement de l'incident contenant :
    - Les informations communiquées par le déclarant ;
    - La qualification par les experts de la Cellule ACSS;
    - L'analyse contextuelle si d'autres incidents du même type ont été signalés.

3.5.3 Tâches

Tâche A : Analyse des causes de l'incident de sécurité

- L'analyse de l'incident a pour objectif de préciser le périmètre technique impacté et les causes malveillantes ou non à son origine ;
- Demande d'informations complémentaires au déclarant permettant d'approfondir l'analyse et d'apporter un meilleur accompagnement ;
- Préservation des traces

Tâche B : Coordination des actions auprès des structures impactées

Le HFDS/FSSI coordonne le plan d'action auprès des structures impactées et du plan de communication éventuel auprès du grand public.
L'incident peut être traité selon deux modalités : « normal » c.-à-d. comme un incident grave soit en mode « gestion de crise ».

Tâche C1 : Appui et accompagnement des structures en mode normal

Suite à la qualification et aux premières analyses, des mesures d'urgence peuvent être prises pour limiter les impacts et préserver les traces. En effet, même sans connaitre précisément la nature de l'incident, son origine ou son impact réel qui font l'objet de la phase d'analyse, l'identification des causes de l'incident permet de recommander les actions immédiates ou déclencher des mesures à prendre au sein de la structure, comme par exemple :

- Un confinement (débranchement du réseau d'un poste infecté) ;
- Une isolation (couper les flux de messagerie internet) ;
- Une communication ciblée de recommandations

Ces mesures d'urgence doivent être documentées dans les procédures du support informatique de chaque structure sous forme de fiches réflexes et de mesures de sécurité.

La Cellule ACSS met à disposition des structures des fiches réflexes sur son portail SSI sectoriel. Elles seront régulièrement mises à jour et de nouvelles fiches pourront être créées.

Ces fiches décrivent l'ensemble des informations/actions à réaliser par les exploitants. Elles seront classées par type d'incident et adaptées au niveau de compétence de l'interlocuteur ainsi qu'au type de structure.

L'objectif est d'obtenir un traitement simple et efficace des actions à mettre en œuvre. De plus, les réponses aux incidents liées aux fiches réflexes doivent être revues régulièrement afin de s'assurer de l'efficacité de la réponse.

La Cellule ACSS accompagne les structures au cas par cas. Lorsque la Cellule ACSS estime ne pas pouvoir apporter un appui suffisant à la structure au regard de la nature de l'incident et de son impact, elle communiquera une liste de prestataires qui pourront l'aider à confiner l'incident et mettre en œuvre de mesures de protection.

L'ARS compétente prend les mesures nécessaires pour faire face aux conséquences éventuelles d'un incident significatif de sécurité des systèmes d'information sur l'offre de soins de son territoire.

Tâche C2 : Incident significatif nécessitant la mise en place d'un plan de crise

Si le HFDS met en place une gestion de crise, la Cellule ACSS applique alors le plan de crise qui reste à définir.

Tâche D : en cas de risque important et/ou de propagation d'une menace particulière, le HFDS/FSSI pilote la diffusion d'une alerte vers les ARS et les structures du périmètre des ministères sociaux relayée par la Cellule ACSS

3.5.4 Délai d'exécution

La structure doit être contactée dans les meilleurs délais après la qualification de l'incident. L'appui et l'accompagnement sont réalisés en jours ouvrés dans les délais compatibles avec la criticité de l'incident.

3.5.5 Éléments en sortie

- Fiche(s) réflexe(s) correspondant(es) au type d'incident rencontré par la structure
- Accompagnement personnalisé au cas par cas
- La liste des prestataires spécialisés dans l'analyse en profondeur des causes de l'incident
- [Facultatif] Communication auprès du grand public
- Dossier de traitement à l'état « à clôturer »

3.5.6 Phase suivante

Phase 5 : Clôture du dossier de traitement

3.6 Phase 5 : Clôture du dossier de traitement

La Cellule ACSS, l'ARS, (le HFDS/FSSI en cas d'incident significatif) et la ou les structures impactée(s) conviennent ensemble de la fin des actions d'accompagnement.

La fin des actions d'accompagnement et la fin du traitement de l'incident par la structure permettent la clôture du dossier de traitement.

3.6.1 Acteurs

- L'ARS responsable du territoire au sein duquel est déclaré l'incident de sécurité
- La Cellule ACSS
- Le HFDS/FSSI
- La ou les structures impactées

3.6.2 Éléments en entrée

- Le dossier de traitement du signalement contenant :
    - Les informations communiquées par le déclarant ;
    - La qualification ;
    - Les actions d'aide au traitement de la ou des structures impactées.
- L'information selon laquelle la structure a mené à terme ses actions de traitement de l'incident.

3.6.3 Tâches

<u>Tâche A</u> : Clôturer

- Acter la fin de l'intervention de la Cellule ACSS (et du HFDS/FSSI en cas d'incident significatif) auprès de la structure impactée

<u>Tâche B</u> : Faire un bilan du traitement de l'incident

- Réaliser une synthèse des actions menées et des résultats obtenus
- Faire une synthèse des vulnérabilités et risques résiduels

3.6.4 Délai d'exécution

La clôture de l'incident doit être réalisée dans les meilleurs délais après la phase d'aide au traitement.

3.6.5 Éléments en sortie

- Clôture de la fiche de suivi
- Bilan de la fiche de suivi
- Clôture du dossier de traitement du signalement

3.6.6 Phase suivante

Retour d'expérience

3.7 Phase 6 : Retour d'expérience

Le retour d'expérience permet de capitaliser l'expérience engrangée après chaque incident de sécurité afin d'enrichir la base de connaissances de façon à mieux qualifier les incidents et accompagner les établissements de santé.

Le bilan contient des informations relatives aux :

- causes de l'incident,
- facteurs ayant potentiellement augmenté les impacts,
- difficultés rencontrées lors du traitement,
- mesures mises en place,
- recommandations.

3.7.1 Acteurs

- ARS
- La Cellule ACSS
- HFDS/FSSI

3.7.2 Éléments en entrée

- Bilan de la fiche de suivi

3.7.3 Tâches

Tâche A : Enrichir le bilan pour en faire un retex en s'appuyant sur des éléments similaires éventuels précédemment archivés ou provenant de la veille sectorielle

Tâche B : Enrichir la base de connaissances de façon à mieux qualifier les incidents à l'avenir

Tâche D : Mettre le retex de l'incident dans la base de partage des retex entre la Cellule ACSS et les ARS afin de pouvoir en tirer des statistiques sur le traitement des signalements

Tâche E : Anonymiser le retex pour le partager avec la communauté SSI de la Cellule ACSS

3.7.4 Délai d'exécution

Le retour d'expérience doit être réalisé dans les meilleurs délais après la clôture de l'incident.

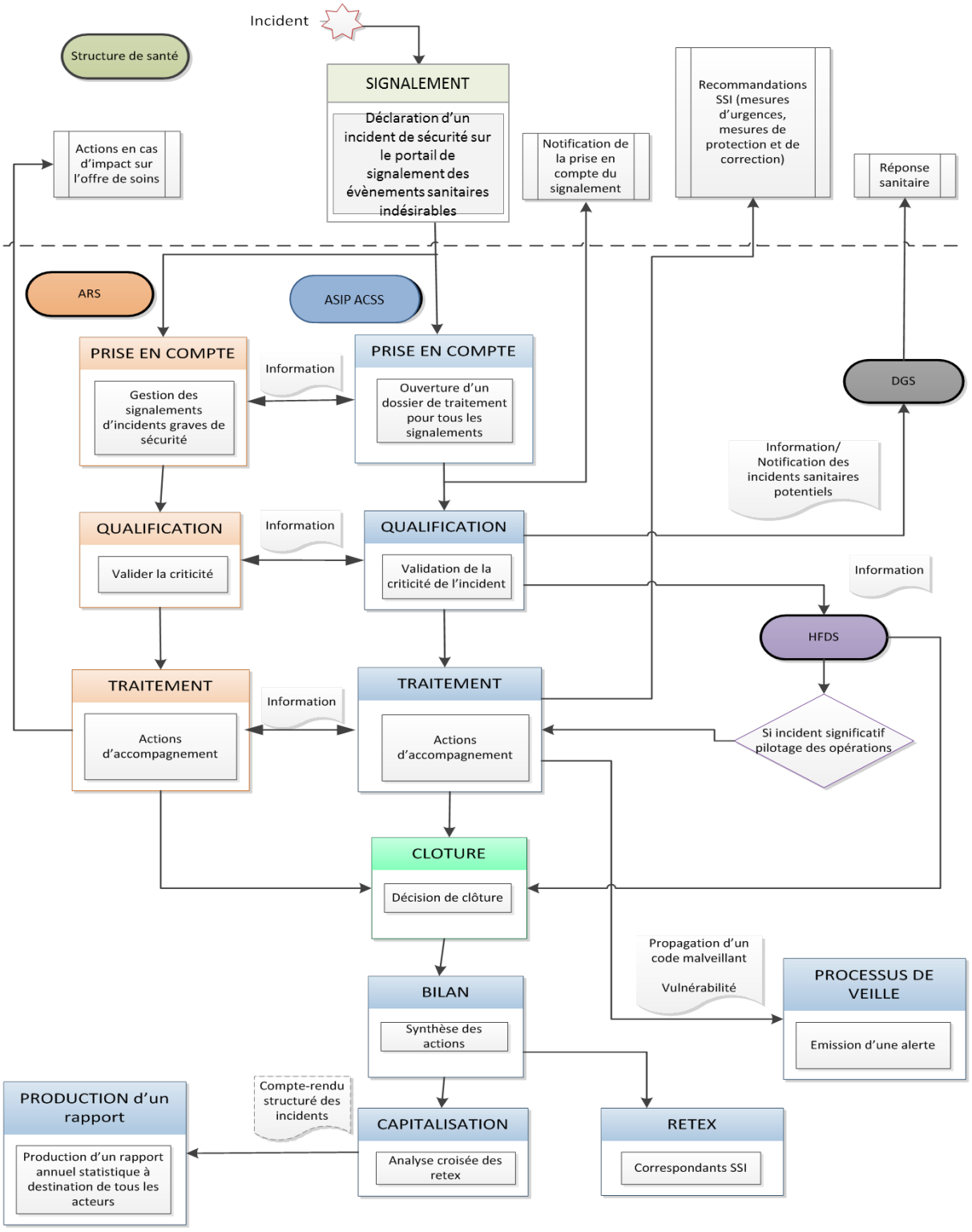
3.7.5 Éléments en sortie

- Synthèse structurée de la gestion de l'évènement de sécurité par les ARS ou la Cellule ACSS pour la capitalisation
- Recommandations, sensibilisation

3.7.6 Phase suivante

Néant

4 Logigramme



5 Métadonnées

IDENTIFICATION DU DOCUMENT			
Titre :	Titre du document		
Auteur :	Auteur	**Version :**	V 0.4
Date de création :	Date de création	**Date de dernière mise à jour :**	2017-10-03

ARCHIVAGE			
Durée d'Utilité Administrative :	DUA (15 ans)	**Sort final :**	Sort final

VALIDATION ET DIFFUSION			
Classification* :	Non sensible public	**Etat :**	Etat
Emetteur :	Nom de l'émetteur	**Vérificateur :**	Nom du vérificateur
Validation :	Nom du valideur	**Date de validation :**	Date de validation

PROJET			
Nom du projet :	Nom du projet	Type de document :	Choisissez un élément.
Phase du projet :	Phase du projet	Version applicative :	Version applicative

MARCHE			
Nom du prestataire :	Nom du prestataire		
Numéro de bon de commande :	Numéro de BC	Numéro du marché :	Numéro de marché
Date de réception du document	Date de réception	Date de début de marché :	Début du marché

* liste déroulante : Non sensible public – Interne - Confidentiel

Les éléments des trois premiers tableaux doivent obligatoirement être remplis

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère des Solidarités et de la Santé

ANNEXE 2

Dispositif de traitement des incidents graves de sécurité des systèmes d'information dans le secteur santé

LE CONTEXTE REGLEMENTAIRE

L'interconnexion croissante des réseaux et les besoins de dématérialisation **exposent les systèmes d'information numériques à des incidents de sécurité**. Dans le secteur santé, ces systèmes apparaissent comme critiques, que ce soit au regard de leur **disponibilité** ou vis-à-vis de **l'intégrité et la confidentialité des données** qu'ils manipulent. La mise en défaut de ces systèmes pourrait **impacter fortement l'activité** de l'ensemble des acteurs du secteur et la prise en charge des patients.
Au travers de l'article 110 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, le Ministère des Solidarités et de la Santé introduit **l'obligation de signalement des incidents de sécurité pour :**

- les établissements de santé,
- les hôpitaux des armées,
- les centres de radiothérapie,
- les laboratoires de biologie médicale.

Le décret d'application n°2016-1214 du 12 septembre 2016 précise que les **incidents graves de sécurité des systèmes d'information du secteur santé devront être signalés sans délai à partir du 1er octobre 2017.**

LES INCIDENTS DE SECURITE A SIGNALER

Les incidents graves de sécurité à signaler sans délai ont des conséquences :

- potentielles ou avérées sur **la sécurité des soins ;**
- sur la **disponibilité, l'intégrité ou la confidentialité des données** de santé ;
- sur le **fonctionnement normal** de l'établissement.

Ces signalements devront être effectués par le directeur de la structure ou une personne qu'elle aura désigné via le portail de signalement des évènements sanitaires indésirables – espace des professionnels de santé: **https://signalement.social-sante.gouv.fr**

LA MISE EN PLACE D'UN DISPOSITIF SPECIFIQUE

Afin d'apporter un accompagnement aux structures de santé concernées par la déclaration de ces incidents, le Ministère des Solidarités et de la Santé (service du HFDS/FSSI) un dispositif pour traiter les signalements. La gestion opérationnelle est déléguée à l'ASIP Santé en collaboration étroite avec les ARS.
Les objectifs visés par ce dispositif sont de :

- **Renforcer le suivi des incidents** pour le secteur santé ;
- **Alerter et informer l'ensemble des acteurs** de la sphère santé dans le cas d'une menace pouvant avoir un impact sur le secteur ;
- **Partager des bonnes pratiques** sur les actions **de prévention** ainsi que sur les **réponses à apporter suite aux incidents**, afin de réduire les impacts et de mieux protéger les systèmes.

La mise en place du dispositif est guidée par les principes suivants :

- **une logique de sensibilisation et d'accompagnement** afin de favoriser les déclarations spontanées des établissements hospitaliers ;
- un **rôle de conseil ou d'orientation** vers les acteurs adéquats, mais en aucun cas une prise en charge de l'incident à la place de la structure victime ;
- une attention particulière portée sur **la sécurité du dispositif pour assurer la confidentialité des informations** communiquées par les établissements.

UNE ANALYSE ET UN ACCOMPAGNEMENT

Le HFDS/FSSI et L'ASIP Santé au travers de la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) apportent un appui aux agences régionales de santé et des structures concernés dans les domaines suivant :

- **Analyse des signalements et accompagnement des structures dans la gestion des incidents de sécurité** ;
- **Veille sur l'actualité de la sécurité** des SI et sur les menaces propres au secteur santé (via un portail dédié : https://www.cyberveille-sante.gouv.fr);
- **Animation de la communauté SSI** avec la mise en place d'un espace d'échange pour les correspondants SSI du secteur.

Toute information complémentaire peut être obtenue sur demande à cyberveille@sante.gouv.fr ou ssi@sg.social.gouv.fr