Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère des Solidarités et de la Santé

asipsanté

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