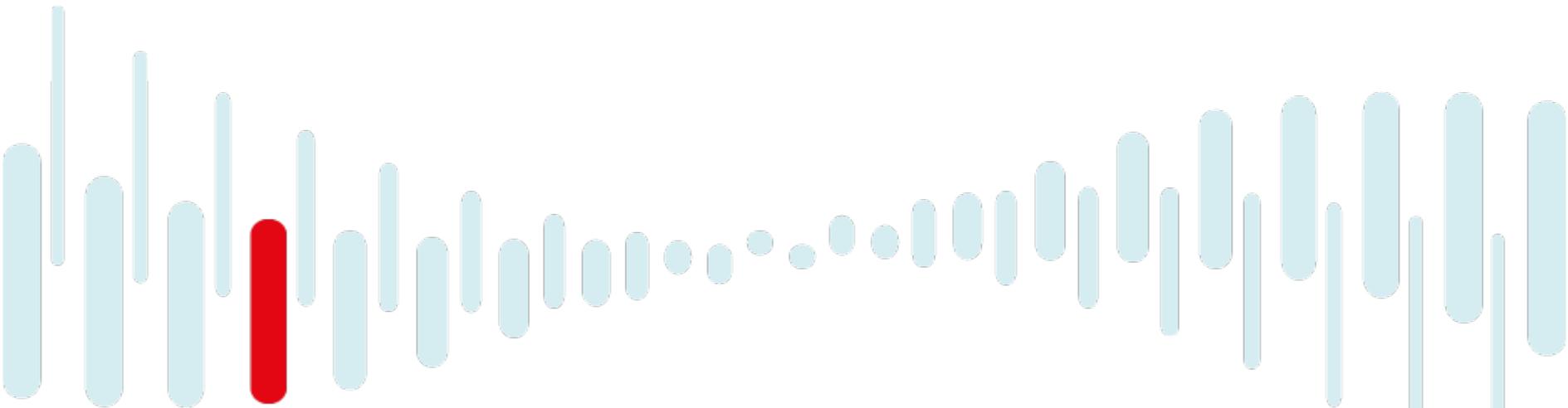


Déclaration des incidents de sécurité des systèmes d'information - Art L. 1111-8-2 du code de la santé publique

Cellule Accompagnement Cybersécurité des Structures de Santé (ACSS)



Sommaire

- **Présentation du dispositif - Art L. 1111-8-2 du code de la santé publique**
- **Projet d'arrêté d'application du décret n°2016-1214 du 12 septembre 2017**
- **Activités de la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS)**
- **Déclaration et traitement des incidents**
- **Présentation du portail de veille et d'échange**

Vidéo de présentation du dispositif accessible sur la chaîne Dailymotion de l'ASIP Santé

<https://www.dailymotion.com/asip-sante>

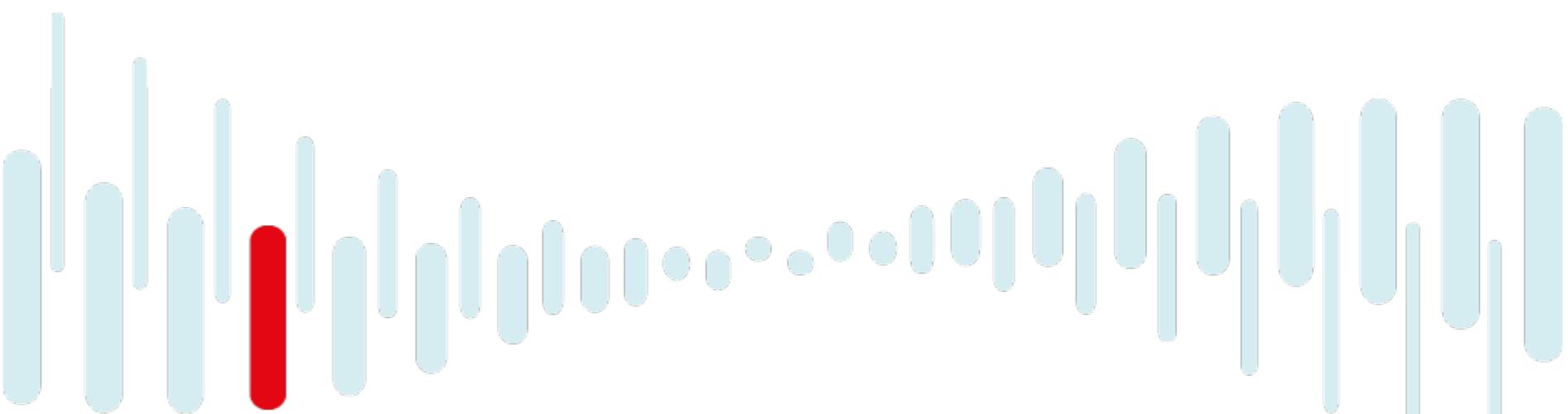


Dispositif de déclaration obligatoire et de traitement des signalements des incidents de sécurité

Ce qu'il faut retenir

- **ACSS : un dispositif de prévention et de traitement des signalements d'incidents de sécurité au profit des acteurs de santé (est mis en place depuis le 1^{er} octobre 2017)**
- **Il concerne les établissements de santé civiles et militaires, les centres de radiothérapie et les laboratoires de biologie médicale**
- **Il concerne 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 recommandé 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 signalements sont effectués via le portail de signalement des événements sanitaires indésirables – espace des professionnels de santé : <https://signalement.social-sante.gouv.fr>**

Projet d'arrêté d'application du décret n°2016-1214 du 12 septembre 2017



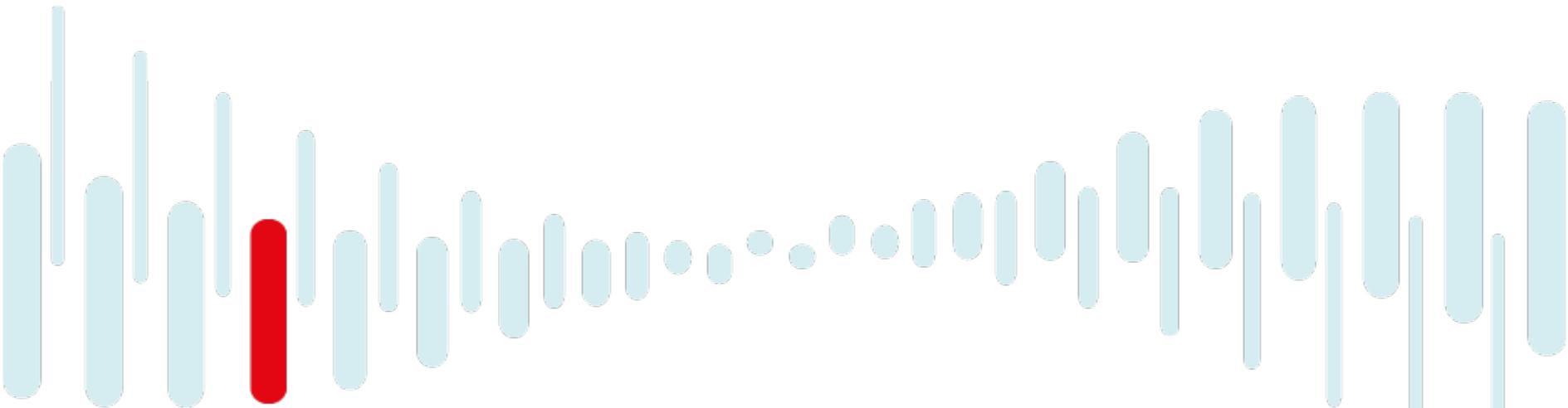
● Le projet d'arrêté contient les informations suivantes

- **Pour la déclaration** : « la déclaration d'un incident grave de sécurité mentionné à l'article L. 1111-8-2 du code de la santé publique est effectuée sur le portail de signalement des événements sanitaires indésirables prévu par l'arrêté du 27 février 2017 susvisé, au moyen du formulaire de déclaration figurant en annexe du présent arrêté. »

- **Pour le traitement des déclarations – répartition des responsabilités**
 - L'ARS compétente s'appuie sur l'ASIP Santé qui analyse la déclaration et qualifie les incidents signalés pour son compte
 - La structure concernée par l'incident est informée de la prise en compte et de l'analyse de son signalement par l'ASIP Santé
 - L'ASIP Santé et l'ARS compétente 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 et l'ARS compétente l'accompagnent dans la gestion de l'incident (échanges de la fiche de suivi, mesures d'urgence, recommandations, mesures de remédiation)

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

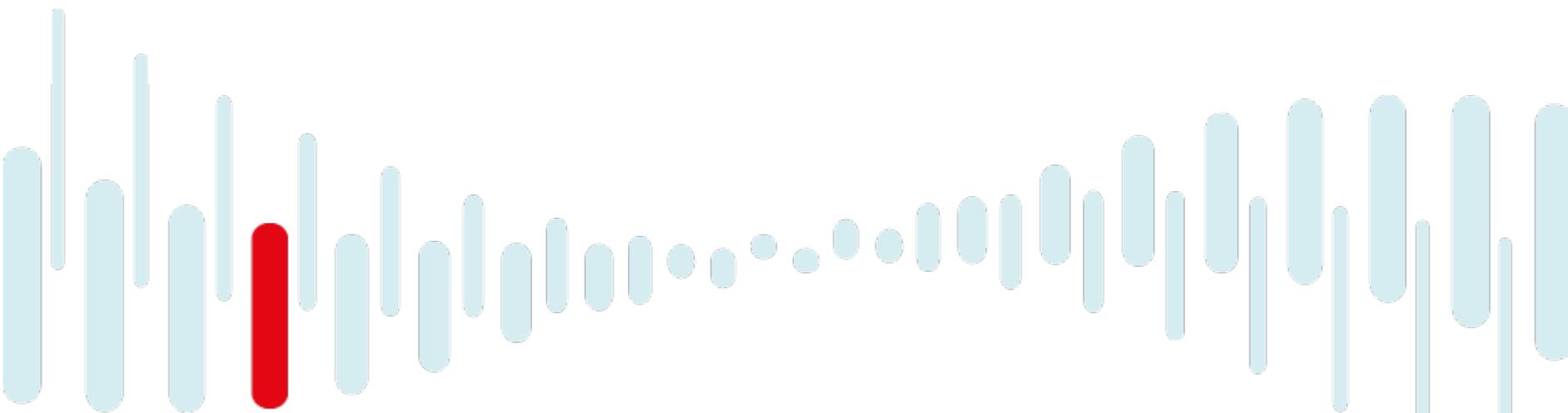
Activités de la cellule Accompagnement Cybersécurité des Structures de Santé (ACSS)



Mise en place d'une Cellule Accompagnement Cybersécurité des Structures de Santé

- **Le HFDS et l'ASIP Santé mettent en place une Cellule Accompagnement Cybersécurité des Structures de Santé (ACSS) qui va mener trois activités opérationnelles :**
 - **Analyse des signalements et accompagnement** des structures dans la gestion des incidents de sécurité (qualification de la criticité, proposition de mesures d'urgences et d'un plan de remédiation)
 - Mise à disposition **d'une veille quotidienne** sur l'actualité de la sécurité des SI et sur les menaces propres au secteur santé (émergence de menaces, incidents spécifiques au secteur santé) et sur certaines vulnérabilités matérielles et logicielles en particulier celles concernant la e-santé
 - **Animation de la communauté SSI** avec la mise en place d'un espace d'échange pour les correspondants SSI de la Cellule ACSS
- **La Cellule ACSS assure ses activités pendant les heures ouvrées (9h-18h) durant les jours ouvrés (cyberveille@sante.gouv.fr)**
- **En dehors des heures ouvrées et en cas d'incident critique suspecté, le FSSI pourra être saisi directement à l'adresse : ssi@sg.social.gouv.fr (PSSI-MCAS)**

Déclarer des signalements



Déclaration d'un incident de sécurité

Le Portail de signalement des événements sanitaires indésirables

Un Portail de déclaration

Le portail de signalement des événements sanitaires indésirables a été choisi pour permettre aux structures mentionnées par le décret de déclarer leurs incidents de sécurité.



Intégration du formulaire au Portail de signalement

- 1 -

Accéder au Portail des
signalements
et
Cliquer sur
« Professionnels de
Santé »

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr S'informer sur les événements sanitaires indésirables

Accueil

Signaler un événement indésirable, c'est 10 minutes utiles à tous

Vous êtes un particulier
Vous êtes la personne concernée, un proche, un aidant, un représentant d'une institution (maire, directeur d'école), une association d'usagers ...

Vous êtes un professionnel de santé
Vous êtes un professionnel de santé ou travaillez dans un établissement sanitaire ou médico-social (gestionnaire de risque, directeur d'Ehpad), ...

Déclaration d'un incident de sécurité des systèmes d'information de santé

- 2 -

Choisir « l'incident de sécurité des Systèmes d'Information »



LIBERTÉ • ÉGALITÉ • FRATERNITÉ
REPUBLIQUE FRANÇAISE



MINISTÈRE CHARGÉ
DE LA SANTÉ

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

[S'informer sur les événements sanitaires indésirables](#)

Accueil > Questionnaire

Merci de sélectionner la ou les cases correspondant à la situation que vous souhaitez signaler



1 — 2 — 3 — 4

Questionnaire

Vous souhaitez être guidé pour identifier la vigilance concernée (sinon cocher une ou plusieurs cases ci-dessous)

		
<input type="checkbox"/> Addictovigilance	<input type="checkbox"/> Maladies à déclaration obligatoire (MDO)	<input type="checkbox"/> Incident de sécurité des systèmes d'information
<input type="checkbox"/> AMP vigilance	<input type="checkbox"/> Matérovigilance	
<input type="checkbox"/> Biovigilance	<input type="checkbox"/> Nutrivigilance	
<input type="checkbox"/> Cosmétovigilance	<input type="checkbox"/> Pharmacovigilance	
<input type="checkbox"/> Défaut de qualité d'un médicament sans effet	<input type="checkbox"/> Pharmacovigilance vétérinaire	
<input type="checkbox"/> Événements indésirables graves associés aux soins - déclaration - 1ère partie	<input type="checkbox"/> Radiovigilance	
<input type="checkbox"/> Événements indésirables graves associés aux soins - analyse des causes - 2ème partie	<input type="checkbox"/> Réactovigilance	
<input type="checkbox"/> Erreur médicamenteuse sans	<input type="checkbox"/> Tatouage (vigilance sur les produits)	
	<input type="checkbox"/> Toxicovigilance	

Présentation faite dans le cadre de la Première Journée scientifique du SDB 10/10/2017

Déclaration d'un incident de sécurité des systèmes d'information de santé



LIBERTÉ • ÉGALITÉ • FRATERNITÉ
RÉPUBLIQUE FRANÇAISE

MINISTÈRE CHARGÉ
DE LA SANTÉ

Portail de signalement des événements sanitaires indésirables
signalement-sante.gouv.fr

[S'informer sur les événements sanitaires indésirables](#)

Accueil > Questionnaire



1 — 2 — 3 — 4

Questionnaire

 **Votre déclaration concerne un incident de sécurité des systèmes d'information**

Vous allez signaler un incident de sécurité des systèmes d'information ayant des conséquences potentielles ou avérées sur la sécurité des soins, sur la disponibilité, l'intégrité et/ou la confidentialité des données de santé, ou sur le fonctionnement normal de l'établissement.
Vous pouvez aussi signaler toute action ou suspicion d'action malveillante causant une indisponibilité partielle ou totale de systèmes informatiques, une altération ou une perte de données.

Tous les renseignements fournis seront traités dans le respect de la confidentialité des données à caractère personnel, du secret médical et professionnel.

COMMENCER

Déclaration d'un incident de sécurité des systèmes d'information de santé

- 3 -

Remplir le formulaire de déclaration

1 2 3 4

Déclaration

Vos informations personnelles

Profession du déclarant de l'incident grave de sécurité de systèmes d'information :

Nom * :

Prénom * :

Téléphone * : *votre numéro sans espace : 01XXXXXXXX*

Adresse électronique * : *le courriel permettra de vous envoyer l'accusé de réception de votre déclaration*

Nom de l'établissement ou de l'organisme : *pour les professionnels de santé n'exerçant pas dans un établissement de santé, écrire en toutes lettres 'Hors établissement de santé' ou 'hors ES'*

N° FINESS (si existant) :

Numéro de SIRET de la structure :

Adresse postale * :

Code postal / Commune * : *permet d'adresser votre signalement au CRPV dont vous dépendez géographiquement*

Service :

Type de la structure :

Localisation précise du ou des site(s) impacté(s) au sein de la structure :



Présentation faite dans le cadre de la Première Journée scientifique du SDB 10/10/2017

Déclaration d'un incident de sécurité des systèmes d'information de santé

Date de survenue de l'incident

Date à laquelle l'incident a été constaté* : 

Date du début de l'incident :  *(si connue, ou le cas échéant, estimée)*

Heure du début de l'incident :

Périmètre de l'incident de sécurité

Existe-t-il une mise en danger d'un ou plusieurs patients?* : Oui Non Je ne sais pas

Pensez-vous qu'une action malveillante soit à l'origine de l'incident de sécurité?* : Oui Non Je ne sais pas

A ce stade, l'incident a touché les composants techniques suivants* :

- Applications
- Serveurs
- Infrastructure de stockage
- Infrastructure réseau
- Postes de travail
- Dispositifs médicaux
- Objets connectés
- Automate / chaîne de production
- Infrastructure d'administration du SI
- Infrastructures d'accès au SI (annuaire type AD, portail d'authentification)
- Composants spécifiques SSI et infrastructure d'administration associée
- Téléphonie
- Liaisons réseau et télécom
- Archivage
- Autres équipements connectés au réseau (vidéosurveillance, système de chauffage, tout système de supervision d'équipements techniques connectés à Internet)

Des données ont-elles été touchées par l'incident, en termes de disponibilité, intégrité ou confidentialité? *Données patients, autres données*

Oui Non

* :

Déclaration d'un incident de sécurité des systèmes d'information de santé

Etat et suivi de l'incident de sécurité

L'incident est* :

Votre structure est-elle autonome (équipe interne ou prestataire) dans la résolution de l'incident* : Oui Non

Votre structure dispose-t-elle d'un service informatique* : Oui Non Je ne sais pas

Observations complémentaires (mesures entreprises et/ou actions envisagées) :

Souhaitez-vous bénéficier d'un accompagnement* : Oui Non

Observations complémentaires :

Etes-vous en mesure de donner plus d'informations concernant l'incident de sécurité* : Oui Non

Concernant l'impact de l'incident sur la sécurité de la structure, l'impact sur les données, ou l'action malveillante à l'origine de l'incident.

PRÉCÉDENT **SUIVANT**

 **Ministère chargé de la Santé**

CGU
Besoin d'aide

Déclaration d'un incident de sécurité des systèmes d'information de santé

Impacts de l'incident sur la sécurité de la structure

Quels sont les impacts sur le fonctionnement des systèmes?

- Fonctionnement dégradé du système de prise en charge d'un patient
- Interruption du Système de prise en charge d'un patient
- Fonctionnement dégradé de SI des activités support de la structure (RH, ...)
- Interruption de SI des activités support de la structure (RH, ...)

Observations complémentaires :

Quels sont les impacts sur l'organisation de la structure?

- Fonctionnement en mode dégradé
- Perte significative d'activité
- Re-planification des soins (activité de soins ou activité d'examen de biologie médicale) ou recours à des organismes tiers
- Arrêt prolongé d'une part importante ou de toute l'activité

Existe-t-il un risque de reproductibilité de l'incident de sécurité?

- Dans votre structure
- Pour d'autres structures
- Je ne sais pas

Observations complémentaires :

Déclaration d'un incident de sécurité des systèmes d'information de santé

Impacts de l'incident sur les données

Quelle est la nature des données impactées?

- Informations patients à caractère personnel (dossier patient, résultat d'analyses, ...)
- Informations à caractère personnel hors données patients (données relatives aux salariés de l'établissement, données d'accès de type identifiant/mot de passe, ressources humaines)
- Données techniques sensibles (mots de passe, clés cryptographiques, documents d'architecture et de configuration, ...)
- Informations confidentielles / stratégiques non personnelles (informations internes à l'établissement : financières, comptables, contractuelles, ...)
- Autres

Si vous avez saisi "Autres",
veuillez préciser :

Quel est l'impact sur ces données?

- Perte de données ou impossibilité d'accéder à des données
- Atteinte à l'intégrité des données, dégradation des données ou impossibilité de communiquer les données
- Divulcation ou accès non autorisé à d'informations à caractère personnel
- Divulcation ou accès non autorisé à des données relatives à la structure

Quels sont les impacts probables sur les personnes dont les données personnelles ont été impactées ?

- Préjudice moral, atteinte à la vie privée
- Vol, escroquerie, chantage, perte de preuves dans un contentieux
- Perte d'emploi, résiliation de contrat de prêt ou d'assurance
- Perte d'accès à des services publics ou commerciaux, à des services en ligne
- Discrimination, harcèlement, diffamation, perte de réputation
- Publicités ciblées et messages indésirables

Déclaration d'un incident de sécurité des systèmes d'information de santé

Origine de l'incident

Action malveillante suspectée :

- Défiguration de sites internet
- Compromission de systèmes d'information
- Attaques en dénis de service
- Messages électroniques malveillants
- Logiciels malveillants / virus
- Fuite d'information
- Autres

Si vous avez saisi "Autres",
veuillez préciser :

Intervention accidentelle sur
le SI :

Autre :

En cas d'action malveillante
identifiée, avez-vous
déconnecté les machines
potentiellement infectées? * : Oui Non

En cas d'acte malveillant,
envisagez-vous de déposer
plainte? : Oui Non

Pourquoi ? :

PRÉCÉDENT **SUIVANT**

Déclaration d'un incident de sécurité des systèmes d'information de santé

- 4 -

Validation

The screenshot shows the 'Récapitulatif de votre signalement' page. At the top, there are logos for the French Republic and the 'MINISTÈRE CHARGÉ DE LA SANTÉ'. The page title is 'Portail de signalement des événements sanitaires indésirables' with the URL 'signalement-sante.gouv.fr'. A breadcrumb trail reads 'Accueil > Questionnaire > Saisie du signalement > Récapitulatif'. Below the title, there is a photo of a doctor and a patient. A progress bar shows four steps, with the third step, 'Récapitulatif', highlighted in yellow. Below the progress bar, there is a section titled 'Vos informations personnelles' with a yellow person icon and an upward arrow.

The screenshot shows the 'Validation' page for an IT security incident report. The title is 'Pour l'incident de sécurité informatique'. It contains the following information:
ARS ILE-DE-FRANCE
INCIDENT SI
35 rue de la Gare
75019 Paris

ASIP Santé - Cellule ACSS
Accompagnement Cybersécurité des Structures de Santé
9 rue George Pitard
75015 PARIS

cyberveille@sante.gouv.fr

Below this information, there is a checkbox that is checked, with the text: 'En cochant cette case, je reconnais avoir lu et accepté les [conditions générales d'utilisation](#).'

At the bottom right, there is a reCAPTCHA widget with the text 'Je ne suis pas un robot' and the reCAPTCHA logo. Below the widget, it says 'Confidentialité - Conditions'.

Déclaration d'un incident de sécurité des systèmes d'information de santé

- 5 -

Envoi du signalement
à l'ARS compétente et
à l'ASIP Santé



CS 91704
33063 BORDEAUX CEDEX

ASIP Santé - Cellule ACSS
Accompagnement Cybersécurité des Structures de Santé

9 rue Georges Pitard
75015 PARIS 15
cyberveille@sante.gouv.fr



IMPORTANT !

Si vous voulez conserver une copie de votre signalement, vous devez cliquer sur la flèche pour le télécharger ou l'imprimer.

Le service de traitement des signalements de l'ASIP Santé est effectué en jours ouvrés (9h-18h). En cas d'incident critique suspecté, le FSSI pourra être saisi directement à l'adresse : ssi@sg.social.gouv.fr (PSSI-MCAS). Pour des informations sur des fiches réflexes, les bonnes pratiques et l'actualité SSI : <http://www.cybersecurite-sante.gouv.fr>

RETOUR À LA PAGE D'ACCUEIL

Traitement des signalements

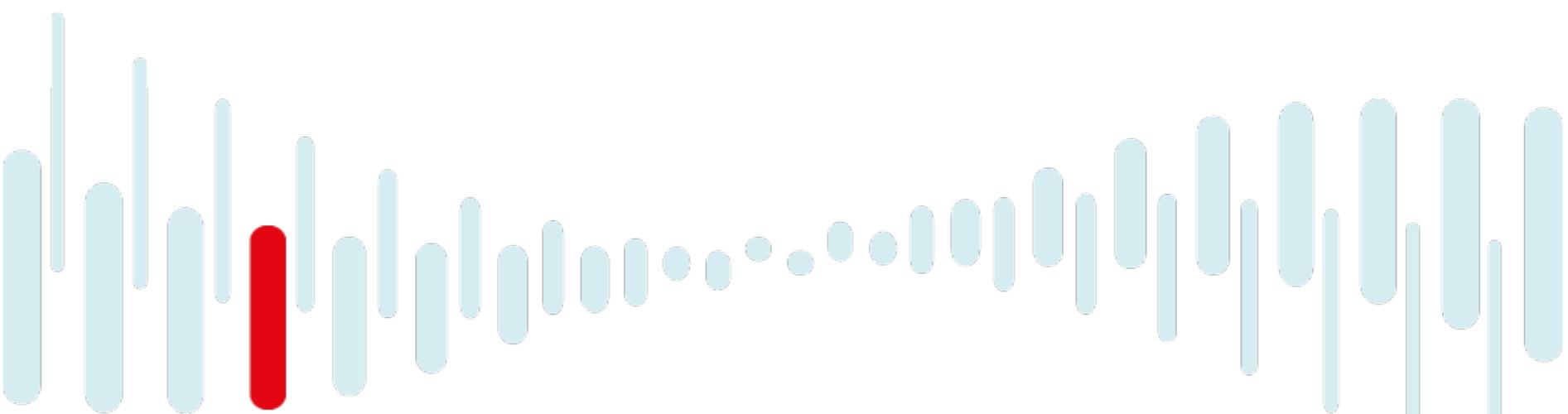


Traitement des signalements

Présentation des activités

- **Qualification du signalement avec éventuellement une prise de contact avec le déclarant si nécessaire**
- **Information systématique du FSSI et de l'ARS compétente territorialement**
- **Escalade vers la DGS en cas d'impact ou de suspicion d'impact sanitaire**
- **Escalade vers l'ANSSI en cas d'incident « particulier » (les modalités restent à définir)**
- **Actions immédiates auprès de la victime**
 - Mise à disposition de fiches reflexes adaptées à l'incident
 - orientation vers un acteur de proximité si disponible (portail sur la cybermalveillance, cybermalveillance.gouv.fr)
- **En cas de crise exceptionnelle et sur demande expresse du FSSI, mise à disposition d'une expertise pour une analyse technique approfondie voire une intervention sur site (analyse d'éléments techniques, plan de remédiation)**
- **Partage du retour d'expérience avec la communauté SSI du secteur (événements, difficultés dans la mise en place des contre-mesures, etc...)**
 - Préservation de la confidentialité sauf autorisation de l'organisme
- **Production d'un rapport d'activité annuel (Observatoire des incidents de sécurité dans le secteur santé) et d'indicateurs périodiques**

Présentation du Portail de veille et d'échange



Prévention et animation sectorielle

Présentation du Portail de veille et d'échange

- **Création d'un portail de veille et d'échange (animation d'une communauté afin de partager les informations) avec deux espaces :**
 - **Un espace commun avec de la veille spécifique sur la sécurité et le secteur santé ;**
 - **Un espace sécurisé avec un partage de retour d'expérience sur le traitement des incidents.**
- **Ce portail est animé quotidiennement par l'ASIP Santé :**
<https://www.cyberveille-sante.gouv.fr>
- **Un effort de rédaction particulier est apporté sur les alertes de sécurité pour que les recommandations formulées puissent être comprises par le grand public (structures ne disposant pas de service informatique)**
- **La sécurité du portail a été homologuée par le directeur de l'ASIP Santé le 2 octobre 2017 suite à un avis favorable de la commission d'homologation (Directeur de l'ASIP Santé, FSSI du ministère, RSSI délégué de l'ASIP Santé, SJ de l'ASIP Santé et directeur de programme)**

Prévention et animation sectorielle

Présentation du Portail de veille et d'échange



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère des
Solidarités et de la
Santé



L'AGENCE
FRANÇAISE
DE LA SANTÉ
NUMÉRIQUE

Portail d'Accompagnement Cybersécurité des Structures de Santé

ACCUEIL | ACTUALITÉS | ESPACE DOCUMENTAIRE | SIGNALER UN INCIDENT | LIENS UTILES | SE CONNECTER | Mots-clés

Abonnement au flux d'alertes

Connexion



Actualités



Espace documentaire



CYBERVEILLE SANTÉ

Amérique du Nord : Les établissements de santé représentent 26% des cyberattaques sur le deuxième trimestre
Lundi 2 octobre 2017 - 14:46

USA : Une attaque par ransomware menace les données de milliers de patients
Lundi 2 octobre 2017 - 09:25

USA : Une fuite de données de santé menace un millier de patients
Lundi 2 octobre 2017 - 09:22

CYBERVEILLE

De multiples vulnérabilités corrigées dans Mozilla Firefox
Lundi 2 octobre 2017 - 12:01

RedHat : Vulnérabilité du noyau Linux
Lundi 2 octobre 2017 - 09:54

Des évolutions sur le rançongiciel Locky
Vendredi 29 septembre 2017 - 19:39

Mois Européen de la Cyber Sécurité



EVÈNEMENTS

OpenStack Day France
Mardi 21 novembre 2017 - 09:00
<https://openstackdayfrance.fr/>
Espaces CAP 15, 1/13 Quai de Grenelle, Paris

3ème colloque sur la SSI secteur santé
Mercredi 29 novembre 2017 - 09:30

Contact | Mentions légales | Présentation de la cellule ACSS

Questions ?