Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

Arrêté du 30 octobre 2017 relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information

NOR : *SSAZ1730723A*

La ministre des solidarités et de la santé,

Vu le code de la santé publique, notamment ses articles L. 1110-4-1, L. 1111-8-2 et D. 1111-16-3 ;

Vu le code de la défense, notamment son article R. 1143-5 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information ;

Vu l'arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales ;

Vu l'arrêté du 27 février 2017 relatif au traitement automatisé de données à caractère personnel dénommé « portail de signalement des évènements sanitaires indésirables » ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 14 septembre 2017,

Arrête :

Art. 1er. – Sous réserve des dispositions relatives à la protection du secret de la défense nationale, 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 évènements sanitaires indésirables prévu par l'arrêté du 27 février 2017 susvisé, au moyen du formulaire de déclaration figurant en annexe du présent arrêté.

En cas d'impossibilité de déclaration par voie électronique, celle-ci peut se faire par tout moyen en respectant la forme et le contenu figurant en annexe auprès de l'agence régionale de santé territorialement compétente.

Le formulaire de déclaration permet au déclarant de fournir toutes les informations dont il dispose au moment de la découverte de l'incident. Il comporte les informations suivantes :

– 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, sur les personnes, sur les systèmes d'information et sur la structure ;
– les causes de l'incident, si celles-ci sont identifiées.

Art. 2. – Les déclarations reçues sur le portail de signalement des évènements sanitaires indésirables mentionné à l'article 1er du présent arrêté sont transmises à l'agence régionale de santé compétente et à l'agence des systèmes d'information partagés de santé, qui en informe les personnes mentionnées à l'article D. 1111-16-3 du code de la santé publique, selon les modalités prévues par cet article.

Art. 3. – L'agence régionale de santé compétente s'appuie sur l'agence des systèmes d'information partagés de 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'agence des systèmes d'information partagés de santé.

L'agence des systèmes d'information partagés de santé et l'agence régionale de santé 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'agence des systèmes d'information partagés de santé et l'agence régionale de santé compétente 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.

Art. 4. – Les catégories de données à caractère personnel susceptibles d'être enregistrées dans les traitements créés par le présent arrêté sont les suivantes :

1° Les données contenues dans le formulaire figurant en annexe du présent arrêté, comprenant notamment :

a) Les données relatives à l'identification des déclarants : nom, prénom, adresse électronique et numéro de téléphone professionnels, structure de rattachement ;

b) Le cas échéant, les données à caractère personnel pouvant être ultérieurement transmises par les déclarants dans le cadre de la gestion de l'incident grave de sécurité ;

2° Les données relatives à l'identification des personnes chargées du traitement du signalement : nom, prénom, adresse électronique et numéro de téléphone professionnels, structure de rattachement ;

3° Les données relatives à l'identification des personnes au sein des structures souhaitant bénéficier du service d'information prévu à l'article 5 du présent arrêté : nom, prénom, adresse électronique et numéro de téléphone professionnels, structure de rattachement.

Art. 5. – L'agence des systèmes d'information partagés de santé est responsable du traitement de données à caractère personnel mentionné à l'article D. 1111-16-3 du code de la santé publique, dans le respect des orientations stratégiques définies par le haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales.

Ce traitement a pour finalités :

1° Le recueil, l'analyse et, le cas échéant, la qualification et la transmission des signalements des incidents de sécurité mentionnés à l'article L. 1111-8-2 du code de la santé publique aux agences ou aux autorités compétentes de l'Etat ;

2° La mise en œuvre d'un service d'information et d'accompagnement des établissements de santé, des organismes et services exerçant des activités de prévention, de diagnostic ou de soins, des agences régionales de santé et des autorités compétentes de l'Etat, concernant la prévention et la gestion des incidents de sécurité, ainsi que la sécurité des systèmes d'information.

Pour réaliser ces finalités, l'agence des systèmes d'information partagés de santé met en place un système d'information afin d'enregistrer et de traiter les déclarations reçues conformément à l'article 2 du présent arrêté.

Ces déclarations sont uniquement accessibles au sein de l'agence des systèmes d'information partagés de santé et des services du haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales, au personnel individuellement désigné et spécialement habilité par le directeur ou le responsable de chacun de ces organismes.

L'agence des systèmes d'information partagés de santé est responsable de la mise en œuvre des mesures de sécurité destinées à garantir la confidentialité et l'intégrité de la conservation, de la sauvegarde et des transmissions de données à caractère personnel dans le système d'information mentionné au premier alinéa du présent article.

Des moyens d'authentification et de gestion des habilitations sont mis en œuvre pour encadrer l'accès aux déclarations par les personnes habilitées.

Art. 6. – Les déclarations transmises à l'agence régionale de santé compétente sont enregistrées dans le système d'information prévu à cet effet par celle-ci.

Au sein de l'agence régionale de santé compétente, ces déclarations sont directement accessibles au personnel nominativement habilité par le directeur général de l'agence régionale de santé.

L'agence régionale de santé 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.

Elle met en œuvre les mesures de sécurité destinées à garantir la confidentialité et l'intégrité de la conservation, de la sauvegarde et des transmissions de données à caractère personnel dans le système d'information mentionné au premier alinéa du présent article.

Art. 7. – L'ensemble des déclarations reçues, des opérations réalisées et des documents associés à la gestion des incidents sont enregistrés dans les systèmes d'information visés aux articles 5 et 6 du présent arrêté.

Les données mentionnées aux 1° et 2° de l'article 4 du présent arrêté sont conservées pendant la durée nécessaire à la gestion de l'incident de sécurité puis font l'objet d'un archivage.

Art. 8. – Le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 susvisée ne s'applique pas au traitement ayant pour finalité le recueil, l'analyse, la qualification, la transmission et la gestion des signalements des incidents de sécurité mentionnés à l'article L. 1111-8-2 du code de la santé publique par les agences ou les autorités compétentes de l'Etat.

L'agence des systèmes d'information partagés de santé et les agences régionales de santé procèdent à l'information des personnes concernées, conformément aux dispositions du I de l'article 32 de la loi du 6 janvier 1978 susvisée.

Les droits d'accès et de rectification prévus par les articles 39 et 40 de la loi du 6 janvier 1978 susvisée auprès de l'agence des systèmes d'information partagés de santé ou auprès des agences régionales de santé.

Art. 9. – L'arrêté du 27 février 2017 relatif au traitement automatisé de données à caractère personnel dénommé « portail de signalement des évènements sanitaires indésirables » est modifié comme suit :

I. – Le 1° de l'article 1er est remplacé par les dispositions suivantes : « 1° De promouvoir et recueillir le signalement d'évènements sanitaires indésirables ou d'incidents graves de sécurité des systèmes d'information

mentionnés à l'article L. 1111-8-2 du code de la santé publique en mettant à la disposition du public et des professionnels un service d'information sur les vigilances, les déclarations et de manière générale sur la veille et la sécurité sanitaire ; »

II. – Le 2° de l'article 1er est remplacé par les dispositions suivantes : « 2° D'orienter le public, les professionnels de santé, les professionnels des secteurs sanitaire et médico-social ainsi que les industriels et autres professionnels vers le formulaire permettant de déclarer l'évènement sanitaire indésirable constaté et figurant sur la liste mentionnée au premier alinéa de l'article D. 1413-58 du code de la santé publique ou vers le formulaire destiné à recueillir les déclarations d'évènements sanitaires indésirables ne figurant pas sur la liste mentionnée au premier alinéa de l'article D. 1413-58 précité et relevant de la compétence des agences régionales de santé, ou vers le formulaire permettant de déclarer l'incident grave de sécurité des systèmes d'information mentionné à l'article L. 1111-8-2 du code de la santé publique ; »

III. – Après les mots : « L. 5311-1 du code de la santé publique », le premier alinéa de l'article 3 est complété par les mots : « , à l'agence des systèmes d'information partagés de santé pour les seules données relevant de la déclaration des incidents graves de sécurité des systèmes d'information mentionnés à l'article L. 1111-8-2 du code de la santé publique, et ».

Art. 10. – Le secrétaire général des ministères chargés des affaires sociales, haut fonctionnaire de défense et de sécurité et le directeur général de la santé sont chargés de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait le 30 octobre 2017.

Pour la ministre et par délégation :

Le secrétaire général des ministères chargés des affaires sociales,
P. Ricordeau

Le directeur général de la santé,
B. Vallet

ANNEXE

De l'arrêté relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information

Formulaire de déclaration d'un incident de sécurité

* Informations à fournir obligatoirement

1. Personne déclarant l'incident (contacter cette personne afin d'obtenir des informations complémentaires)

Nom et Prénom*		Fonction	
Adresse électronique*		Téléphone*	
Raison sociale la structure		Numéro de SIRET de la structure	
Numéro FINESS Juridique si existant		Adresse de la structure* Code postal commune*	
Type de structure* (ES, labo, etc.)			
Service			

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

2. Date de survenue de l'incident

Date de la déclaration * :

Date à laquelle l'incident a été constaté *

Date et heure du début de l'incident (si connues, ou le cas échéant, estimées)

3. 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
  - ○ logiciel d'aide à la prescription
  - ○ logiciel d'aide à la dispensation
  - ○ logiciels utilisés en biologie médicale
  - ○ autres

- □ Serveurs
- □ Infrastructure de stockage
- □ Infrastructure réseau
- □ Postes de travail
- □ Dispositifs médicaux
- □ Objets connectés
- □ Automate / chaine 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 personnelles, données techniques sensibles) ? *

- □ Oui
- □ Non

- ☐ Je ne sais pas

4. Etat et suivi de l'incident de sécurité

L'incident est* :

- ☐ Pas encore pris en charge
- ☐ En cours de résolution
- ☐ Résolu
- ☐ Bilan effectué

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

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 ? *
(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)

- ☐ Oui
- ☐ Non

Les volets suivants sont à remplir lorsque le déclarant répond positivement à la question précédente.

5. 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, etc.)
- ☐ Interruption de SI des activités support de la structure (RH, etc.)

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

6. Impact de l'incident sur les données

Quelle est la **nature des données impactées** ?

- ☐ Informations patients à caractère personnel (dossier patient, résultats 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, etc.)
- ☐ Informations confidentielles / stratégiques non personnelles (informations internes à l'établissement : financières, comptables, contractuelles, etc.) ;
- ☐ Autres (précisez)

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 ;
- ☐ Divulgation ou accès non autorisé à des informations à caractère personnel ;
- ☐ Divulgation 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.

7. 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
  - ○ Autre

- ☐ 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 ?