Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

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

NOR : *SSAZ2123175D*

Publics concernés : *établissements de santé ; organismes et services exerçant des activités de prévention, de diagnostic ou de soins ; établissements médico-sociaux.*

Objet : *conditions et modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information.*

Entrée en vigueur : *le texte entre en vigueur le lendemain de sa publication.*

Notice : *le texte définit les catégories d'incidents de sécurité des systèmes d'information des établissements de santé, des hôpitaux des armées, des organismes et services exerçant des activités de prévention, de diagnostic ou de soins et des établissements médico-sociaux devant faire l'objet d'un signalement aux autorités compétentes de l'Etat, ainsi que les conditions et modalités selon lesquelles ils sont traités.*

Références : *le décret est pris pour l'application de l'article L. 1111-8-2 du code de la santé publique, dans sa rédaction issue de l'article 1er de l'ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé. Le décret ainsi que les dispositions du code de la santé publique qu'il modifie peuvent être consultés, dans leur rédaction issue de cette modification, sur le site Légifrance (https://www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport du ministre des solidarités et de la santé,

Vu l'ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des agences régionales de santé ;

Vu le code de la santé publique, notamment ses articles L. 1111-8-2, L. 1111-24 et D. 1413-58 ;

Vu le code de la défense, notamment ses articles R.* 1132-3 et R. 1143-1 ;

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

Vu le décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »,

Décrète :

Art. 1er. – Le code de la santé publique est ainsi modifié :

1° Dans l'intitulé de la sous-section 4 de la section 1 du chapitre Ier du titre Ier du livre Ier de la première partie réglementaire, les mots : « et conditions » sont remplacés par les mots : « , conditions et modalités » et, après les mots : « des incidents », sont insérés les mots : « significatifs ou » ;

2° L'article D. 1111-16-2 est ainsi modifié :

a) Le 1° du I est complété par les mots : « ou permettant d'assurer la continuité de la prise en charge sanitaire » ;

b) Au 2° du I, après les mots : « survenue d'incidents », sont insérés les mots : « significatifs ou » ;

c) Au premier alinéa du II, après les mots : « comme incidents », sont insérés les mots : « significatifs ou » ;

d) Le II est complété par deux alinéas ainsi rédigés :

« – les incidents ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé ;

« – les incidents susceptibles de toucher d'autres établissements, organismes ou services. » ;

3° L'article D. 1111-16-3 est remplacé par les dispositions suivantes :

« *Art. D. 1111-16-3.* – I. – La déclaration des incidents significatifs ou graves de sécurité des systèmes d'information, sans préjudice des autres déclarations obligatoires, est effectuée sans délai par le directeur de l'établissement de santé, de l'organisme ou du service exerçant des activités de prévention, de diagnostic ou de

soins, de l'établissement médico-social ou la personne déléguée à cet effet, auprès du groupement d'intérêt public mentionné à l'article L. 1111-24.

« Le groupement d'intérêt public assure :

« – 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. Il peut 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 ;

« – la relation avec l'Agence nationale de sécurité des systèmes d'information, notamment en cas d'incident concernant un opérateur de service essentiel ou qui pourrait avoir un impact de portée nationale ;

« – la prévention des incidents, en organisant les retours d'expérience au niveau national, et la proposition de mesures d'aide au traitement des incidents ;

« – la gestion et la mise en œuvre du traitement de données à caractère personnel relatif aux signalements, dont les caractéristiques sont précisées par un arrêté du ministre chargé de la santé.

« Le groupement d'intérêt public informe sans délai le service du haut fonctionnaire de défense et de sécurité des ministères sociaux de tout signalement analysé. Il informe également sans délai les services compétents de la direction générale de la santé, ainsi que les agences régionales de santé concernées, de tout signalement susceptible d'avoir un impact sanitaire direct ou indirect, notamment en cas de dysfonctionnement de l'offre de soins.

« Le groupement d'intérêt public est informé sans délai de la résolution des incidents par l'une des personnes mentionnées au premier alinéa du présent I.

« Il établit, au vu des informations communiquées par les établissements et organismes concernés, un rapport annuel à caractère statistique relatif aux signalements anonymisés des incidents de sécurité des systèmes d'information. Ce rapport est rendu public.

« II. – Sous réserve des dispositions relatives à la protection du secret de la défense nationale, la déclaration d'un incident significatif ou grave de sécurité mentionné à l'article L. 1111-8-2 est effectuée via le site internet mentionné à l'article D. 1413-58.

« Le déclarant fournit toutes les informations dont il dispose au moment de la découverte de l'incident et notamment 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.

« Le groupement d'intérêt public mentionné à l'article L. 1111-24 peut 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. » ;

4° L'article D. 1111-16-4 est ainsi modifié :

a) Au premier alinéa, après les mots : « établissements de santé, », est inséré le mot : « les » et, après les mots : « article D. 1111-16-2 », sont insérés les mots : « et les établissements médico-sociaux » ;

b) Il est ajouté un alinéa ainsi rédigé :

« – les établissements médico-sociaux. »

Art. 2. – La ministre des armées et le ministre des solidarités et de la santé sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 27 avril 2022.

JEAN CASTEX

Par le Premier ministre :

Le ministre des solidarités et de la santé,
OLIVIER VÉRAN

La ministre des armées,
FLORENCE PARLY