SANTÉ

ÉTABLISSEMENTS DE SANTÉ

MINISTÈRE DES AFFAIRES SOCIALES
ET DE LA SANTÉ

Secrétariat général

Haut fonctionnaire de défense
et de sécurité

Direction générale de la santé

Sous-direction veille
et sécurité sanitaire

Direction générale de l'offre de soins

Délégué à la sécurité générale,
commissaire de police

Observatoire national des violences
en milieu de santé

Instruction n° SG/HFDS/2016/340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé

NOR : *AFSZ1633531J*

Validée par le CNP le 4 novembre 2016. – Visa CNP 2016-137.

Visée par le SG-MCAS le 28 septembre 2016.

Date d'application : 16 novembre 2016.

Catégorie : directives adressées par le ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.

Résumé : la présente instruction vise à instaurer une politique de sécurisation dans les établissements de santé.

Elle précise :

– le rôle des agences régionales de santé (ARS) dans l'animation et la coordination de la politique régionale de sécurité de l'offre de soins ;
– les mesures à mettre en œuvre par les établissements de santé ;
– les moyens financiers alloués aux établissements en mesures nouvelles pour renforcer leur sécurité ;
– les prescriptions spécifiques en matière de prévention de la radicalisation.

Mots clés : sécurité – plan Vigipirate – politique globale de sécurité des établissements – prévention des attentats – radicalisation.

Références :

Instruction n° SG/2016/14 du 8 janvier 2016 relative au cadre d'intervention des agences régionales de santé s'agissant des phénomènes de radicalisation.

Instruction DGS/DUS/SGMAS/SHFDS n° 2016-40 du 22 janvier 2016 relative aux principes d'organisation des missions de veille et de sécurité sanitaire et des missions relevant des domaines de la défense et de la sécurité au sein des agences régionales de santé.

Lettre conjointe des ministres des affaires sociales et de la santé et de l'intérieur du 16 novembre 2016 relative à la sécurisation des établissements de santé.

Annexes :

Annexe 1. – Lignes directrices pour l'élaboration d'un plan de sécurité d'établissement.

Annexe 2. – Mesures en matière de sécurité des systèmes d'information.

Annexe 3. – Recommandations particulières concernant la mise en œuvre des conventions sante-sécurité-justice.

Annexe 4. – Sensibilisation et formation des professionnels de santé.

Diffusion : agences régionales de santé, établissements de santé.

La ministre des affaires sociales et de la santé à Mesdames et Messieurs les directeurs généraux des agences régionales de santé ; copie à Mesdames et Messieurs les préfets de région ; Mesdames et Messieurs les préfets de département.

Le contexte de menace terroriste et les récents attentats imposent une vigilance accrue et nécessitent d'assurer, sur l'ensemble du territoire, la mise en œuvre effective de mesures particulières de sécurité au sein des établissements de santé. Cette instruction décline les orientations de la lettre conjointe des ministres des affaires sociales et de la santé et de l'intérieur relative à la sécurisation des établissements de santé du 16 novembre 2016.

Les établissements de santé publics et privés devront élaborer une politique globale de sécurité intégrant notamment la prévention des attentats. Dans ce domaine, la responsabilité des établissements s'exerce tant vis-à-vis du personnel, au titre de la responsabilité de l'employeur, que vis-à-vis des patients, usagers et prestataires.

Pilotée par les agences régionales de santé (ARS) au niveau régional, cette politique de sécurité des établissements de santé devra être réalisée en lien avec les préfets, les collectivités territoriales et les forces de sécurité intérieure et s'articuler autour de deux documents majeurs et complémentaires :

– l'élaboration d'un plan de sécurité d'établissement (PSE),
– la conclusion ou l'actualisation d'une convention « santé-sécurité-justice ».

1. **Le pilotage par les ARS**

Les directeurs généraux des agences régionales de santé élaboreront une politique régionale de sécurité qui couvrira notamment la prévention, la protection et la réaction face à des actes terroristes.

Ils désigneront un membre de leur équipe de direction chargé de :

– l'accompagnement de cette politique, fondée sur l'élaboration et la mise en œuvre d'un plan de sécurité par chacun des établissements et l'incitation à la signature ou à l'actualisation des conventions « santé-sécurité-justice » ;
– la cohérence des mesures de sécurité prises dans leur région ;
– la réalisation pour avril 2017 d'une cartographie des moyens les plus sensibles pour le secteur sanitaire sur le plan zonal, régional et local. Cet outil permettra d'identifier les activités, secteurs et sites stratégiques des établissements (plates-formes SAMU/Centre 15, service d'urgence, plateaux techniques, services spécialisés, pharmacies à usage intérieur, sites de stockage de produits stratégiques, etc.). C'est sur la base de cette cartographie que pourront être précisés avec les préfets les sites à protéger en priorité ;
– l'application des mesures de prévention de la radicalisation, en lien avec le référent radicalisation de l'ARS.

Afin de faciliter la mise en œuvre de cette démarche, un groupe d'appui technique sur la sécurité des établissements de santé pourra être constitué, avec pour missions :

– d'exercer une fonction consultative d'aide à la conception, à la mise en œuvre et au suivi de la politique de sécurité des établissements de santé sur le plan régional ;
– de participer à l'élaboration de la cartographie des sites à protéger en priorité ;
– de participer à la conception et au suivi d'actions d'information et de sensibilisation en direction du personnel hospitalier et des usagers ;
– dans le cadre du fonds de modernisation des établissements de santé publics et privés (FMESPP), de veiller à la cohérence des demandes d'appel à projet et à leur priorisation ;
– de faciliter le retour d'expériences et le partage de pratiques entre établissements.

Piloté par l'ARS, ce groupe inclurait notamment des représentants des fédérations hospitalières, des directeurs d'établissements de santé et des forces de sécurité intérieure.

2. **L'élaboration d'un plan de sécurité d'établissement (PSE)**

Pour la fin du 1er semestre 2017, chaque établissement devra se doter d'un « plan de sécurité d'établissement » (PSE) intégrant la menace terroriste. Ce plan s'appuiera sur une analyse de risques identifiant les éléments de vulnérabilité et centré sur les missions essentielles de l'établissement.

Chaque établissement établira ainsi une stratégie de protection en veillant à la cohérence avec les instructions gouvernementales (plan Vigipirate, directives nationales de sécurité, etc.), les préconisations du plan Blanc et leur plan de continuité d'activités.

Le PSE comprendra deux volets distincts :

– un volet de portée générale, comprenant les mesures globales de sécurisation liées à la protection de l'établissement dans la durée et intégrant les mesures du plan Vigipirate ;
– un volet de gestion de crise, traitant des mesures particulières et immédiates de sécurité à mettre en œuvre notamment en cas de survenance d'un attentat au niveau local et de risques potentiels de sur-attentat pour l'établissement.

Pour les accompagner dans leur démarche, les chefs d'établissements pourront solliciter l'appui :

– des préfectures et plus particulièrement les services chargés de la sécurité ;
– des forces de sécurité intérieure (référents sûreté de la police et de la gendarmerie et services spécialisés) ;
– des agences régionales de santé (conseillers de défense et de sécurité) ;
– le cas échéant, du ministère des affaires sociales et de la santé : service spécialisé du haut fonctionnaire de défense et de sécurité (hfds@sg.social.gouv.fr) et direction générale de l'offre de soins, par son délégué à la sécurité générale (sante-securite@sante.gouv.fr).

Pour élaborer leur PSE, les établissements s'appuieront sur le document joint en annexe n° 1, qui précise les grandes lignes directrices de ce plan et sur les guides réalisés à cet effet.

Des exercices annuels devront être effectués afin de tester le dispositif de sécurité élaboré par l'établissement en lien avec les services concernés et son appropriation par le personnel de l'établissement.

3. **Les conventions « santé-sécurité-justice »**

Vous inciterez les établissements à conclure ou à actualiser les conventions « santé-sécurité-justice », qui permettent d'assurer une démarche commune et formalisée entre les établissements, les forces de sécurité et les représentants du ministère de la justice, adaptée aux spécificités et aux priorités locales (*cf.* annexe 3).

Ces conventions doivent notamment comprendre les dispositions suivantes :

– la coordination de l'action dans le domaine de la sécurité ;
– les procédures d'information de l'autorité judiciaire, notamment du procureur de la République ;
– le diagnostic des situations à risques et des dispositifs de prévention notamment dans les établissements de santé ou les services les plus exposés à des risques d'incivilité et de violence ;
– les modalités d'intervention des forces de sécurité auprès des établissements et des professionnels de santé, ainsi que le renforcement de l'action des établissements en situation de crise ;
– les procédures d'information et sensibilisation des personnels hospitaliers à la prévention et à la gestion des conflits en milieu de santé.

Les conventions déjà signées seront mises à jour dans le cadre de la présente instruction, en y incluant les risques liés à la menace terroriste.

4. **La sensibilisation et la formation des professionnels et des usagers du système de santé**

Une attention particulière sera portée par les directeurs d'établissements à la sensibilisation de l'ensemble du personnel sur son rôle en matière de vigilance et de prévention au sein de son service et aux conduites à tenir en cas d'attentat sur site ou dans l'environnement immédiat de l'établissement.

Dans ce cadre, les directeurs d'établissements présenteront à l'ensemble du personnel leur plan de sécurité d'établissement et s'assureront que les consignes « alerte – attentat » et les mesures de protection propres à chaque site et à chaque service sont connues et maîtrisées.

Le personnel doit être préparé à réagir à une attaque terroriste. En lien avec les services spécialisés, un plan de sensibilisation et de formation approprié leur sera dispensé. Il doit être en cohérence avec les modules de formation à la sécurité qui vont être mis en place lors de la formation initiale et continue à destination du personnel de direction, médical et paramédical (*cf.* annexe 4).

Pour accompagner les établissements dans leurs actions de sensibilisation, des guides pédagogiques « réagir en cas d'attentat » à destination de l'ensemble des établissements ont été élaborés par les ministères chargés des affaires sociales, en partenariat avec le secrétariat général de la défense et de la sécurité nationale. Ils peuvent être adaptés au secteur concerné et au mode d'accueil du public (lieu fermé ou ouvert, accueil de mineurs, etc.).

Il convient également d'inciter les établissements à sensibiliser les usagers et les prestataires aux problématiques de sécurité, notamment par un affichage spécifique (« attentif ensemble ») et par un paragraphe dédié dans le livret d'accueil ou la diffusion de vidéo ou de film.

5. **La prise en compte de la sécurité des systèmes d'information**

Les menaces pesant sur les systèmes d'information numériques gagnent en intensité et en sophistication et constituent un risque majeur pour le fonctionnement des établissements.

Ce contexte nécessite une attention particulière afin d'identifier les vulnérabilités des systèmes d'information, de renforcer la vigilance et d'être en capacité de détecter dans les meilleurs délais tout incident ou cyber-attaque.

Des mesures afférentes à la sécurité des systèmes d'information (SSI) doivent être mises en œuvre, notamment celles recommandées dans le cadre de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS) et de sa déclinaison sectorielle au travers de la politique générale de sécurité des systèmes d'information de santé (PGSSI – S).

Le volet SSI est à intégrer dans le plan de sécurité d'établissement (*cf.* annexe n° 2).

6. **L'accompagnement financier**

Afin de faciliter la mise en œuvre des mesures de sécurité, un abondement spécifique de 25 millions d'euros par an durant 3 ans est prévu sur la base d'appel à projet dans le cadre du fonds de modernisation des établissements de santé publics et privés (FMESPP) dès 2017. Les ARS orienteront ce financement vers la sécurisation des sites à protéger en priorité (*cf.* cartographie des moyens). Par ailleurs, les établissements pourront recourir aux contrats locaux d'amélioration des conditions de travail (CLACT) en matière de santé et sécurité au travail, ainsi qu'au fonds interministériel de prévention de la délinquance (FIPD) pour la vidéosurveillance.

7. **Le suivi des actes de malveillance ou de violence dans le secteur santé**

Les directeurs d'établissements signaleront systématiquement à l'Observatoire national des violences en milieu de santé (ONVS) l'ensemble des atteintes aux personnes et aux biens qui surviennent dans leur établissement.

La plateforme de signalement extranet recense les déclarations qui sont ensuite traitées et analysées par les services de l'État. C'est aujourd'hui le principal moyen de connaître les situations locales permettant de faire évoluer les politiques publiques en fonction des événements survenant sur le territoire national.

8. **La prévention de la radicalisation**

La radicalisation de personnes ayant accès aux établissements de santé peut mettre en danger la sécurité de ces établissements. Il convient donc d'être attentif à ce phénomène et de mettre en place les mesures de prévention prévues dans l'instruction aux ARS du 8 janvier 2016 et dans la circulaire du Premier ministre du 13 mai 2016. La radicalisation de personnels de l'établissement est également possible.

Les responsables d'établissement doivent pour leur part réaliser des actions de sensibilisation au sein de leur établissement sur :

- les risques liés aux phénomènes de radicalisation ;
- le processus de transmission des informations ;
- le rôle que le personnel peut être amené à jouer dans la prise en charge médicale et le soutien psychologique des individus radicalisés, en voie de radicalisation ou de leurs familles.

Il est rappelé que le ministère de l'intérieur a édité un référentiel sur lequel l'ensemble des acteurs peut s'appuyer. Toutefois, toute personne a la possibilité de signaler des personnes en voie de radicalisation (personnel, usagers, prestataires) auprès du centre national d'assistance et de prévention de la radicalisation qui dispose d'un numéro vert : 0 800 00 56 96.

Je vous prie de bien vouloir vous assurer de la diffusion de cette instruction et de ses annexes à vos services et par leur intermédiaire aux établissements. Vous vous assurerez que chaque établissement a pris en compte la présente instruction, notamment par la mise en place d'un plan de sûreté d'établissement.

Pour la ministre et par délégation :

Le secrétaire général des ministères chargés des affaires sociales,
Haut fonctionnaire de défense et de sécurité,
P. Ricordeau

Le directeur général de la santé,
B. Vallet

La directrice générale de l'offre de soins,
A.-M. Armanteras de Saxcé

ANNEXE 1

LIGNES DIRECTRICES POUR L'ÉLABORATION D'UN PLAN DE SÉCURITÉ D'ÉTABLISSEMENT

PRÉAMBULE

Il revient à la direction de l'établissement de définir une politique globale de sécurité visant à protéger les personnes, les biens et les informations et à l'appliquer en priorité dans le domaine des activités essentielles. Cette politique doit indiquer clairement les objectifs généraux en termes de réduction et de gestion des risques et refléter l'engagement pris pour améliorer les performances de sécurité.

Cette politique doit :

- être appropriée à la nature et à l'étendue des menaces et vulnérabilités identifiées ;
- s'appuyer sur un responsable désigné en charge de la sécurité de l'établissement ;
- définir les principaux objectifs d'amélioration continue en matière de sécurité ;
- être communiquée à tout le personnel afin de le sensibiliser sur son rôle en matière de sécurité ;
- être consignée par écrit, mise en œuvre et revue périodiquement, pour s'assurer qu'elle reste pertinente et appropriée.

QU'EST-CE QU'UN PLAN DE SÉCURITÉ D'ÉTABLISSEMENT (PSE) ?

Le plan de sécurité d'établissement traduit la politique et l'organisation de la sécurité de l'établissement de santé :

- il précise les mesures organisationnelles à mettre en œuvre tant sur le plan de la vigilance, de la prévention que de la protection ;
- il est fondé sur une analyse de risques de l'ensemble des espaces (espaces périphériques, espace périmétrique et volumes intérieurs) ;
- il repose sur l'identification des vulnérabilités de l'établissement (personnes, infrastructures, informations, matériels sensibles) et fixe des priorités dans les sites à sécuriser ;
- il s'appuie sur le dispositif de sécurité existant et sur l'expérience déjà acquise par l'établissement dans la gestion des problématiques liées à la sécurité et prend en compte la particularité de son environnement ;
- il doit être élaboré en coordination avec les autorités préfectorales et les forces de sécurité intérieure, qui peuvent apporter leur concours dans l'élaboration du plan.

L'équipe de direction de l'établissement doit régulièrement passer en revue le système de gestion de la sécurité, pour s'assurer qu'il demeure pertinent, adéquat et efficace.

Il convient de distinguer :

- le dispositif de sécurité en temps normal ;
- le dispositif en cas d'attentat ou de crise locale.

En tout état de cause, le PSE devra s'articuler avec les plans et réglementations existants (plan Vigipirate, plan Blanc, etc.).

Le plan de continuité d'activité (PCA) de l'établissement décrit la stratégie adoptée par une organisation pour continuer à fonctionner puis rétablir ou reprendre son activité à la suite d'une perturbation importante. Il est primordial d'assurer une articulation et une cohérence entre le PCA et le PSE.

DESCRIPTION DE L'ATTENDU

Le plan de sûreté de l'établissement (PSE) s'articule autour de deux modes de fonctionnement.

1. **Sécurisation de l'établissement en temps normal**

L'établissement réalise un diagnostic initial qui lui permettra :

- d'identifier de façon régulière les menaces en lien avec les autorités préfectorales,
- d'évaluer les vulnérabilités de l'établissement de soins,
- de mettre en œuvre des mesures correctrices adaptées selon un calendrier et en fonction des priorités.

Ces actions doivent être planifiées, y compris leur maintenance et leur surveillance, afin d'assurer qu'elles sont réalisées dans les conditions requises en :

- élaborant et en tenant à jour des procédures formalisées permettant la définition des conduites à tenir en situation normale comme en mode dégradé (notamment la perte de fonction de sûreté telles que la surveillance le contrôle d'accès, etc.) ;
- stipulant des critères opératoires dans les procédures ;
- mettant en place un suivi des autorisations d'accès aux locaux réservés et aux informations sensibles ;
- définissant des zones contrôlées en fonction de leurs activités et de leurs vulnérabilités ;
- communiquant les procédures et les exigences pertinentes aux fournisseurs, aux sous-traitants et partenaires et vérifiant leur application ;
- établissant des procédures spécifiques d'accueil des personnes extérieures à l'organisme, notamment si celles-ci peuvent être en contact avec des informations et/ou des matériels évalués comme sensibles ;
- établissant des procédures d'identification et de traitement des incidents et des actes de malveillance ;
- élaborant les procédures avec les forces de sécurité intérieure ;
- sélectionnant les lieux de mise en sûreté adaptés pour le confinement ;
- élaborant un plan d'évacuation, comprenant notamment les cheminements, l'identification d'issues de secours, les lieux éventuels de rassemblement ou de confinement.

2. **Sécurisation complémentaire en situation d'attentat ou de crise locale**

Cette posture particulière nécessite le renforcement des mesures en vigueur et la mise en œuvre de mesures supplémentaires – en lien étroit avec les services préfectoraux et les forces de sécurité intérieure – afin d'assurer la prise en charge éventuelle d'un nombre important de victimes, de garantir le bon déroulement des soins et de prévenir le risque de sur-attentat visant l'établissement ou à proximité de ce dernier.

Un effort particulier devra être porté sur le renforcement de la sécurisation périmétrique et des accès[1] qui pourrait se traduire par :

- la fermeture partielle ou totale des accès de l'établissement. Sous le contrôle d'agents de sécurité ou des agents des forces de police ou gendarmerie : seuls les patients et les ambulances à destination des soins urgents seraient autorisés à entrer sur le site hospitalier, ainsi que les personnels rappelés[2] ;
- l'instauration d'un périmètre de sécurisation par filtrage des accès aux lieux critiques de l'établissement (SAMU, services des urgences, pharmacies à usage intérieur, etc.) ;
- une gestion des flux afin d'éviter un attroupement excessif aux portes ou un blocage des ambulances sur le site des urgences.

3. **Organisation d'exercices**

La réalisation d'exercices annuels de réaction à une attaque terroriste ou à une situation de sur-attentat peut prendre plusieurs formes :

- rappel simple des procédures et du rôle de chacun par le responsable du site ou son chargé de sûreté ;
- exercice « sur table » au cours duquel, dans une salle, les employés présentent la réaction qu'ils auraient en cas d'attaque. Celle-ci doit être scénarisée (lieu, nombre et armes des assaillants identifiés) ;
- test technique du système d'alerte ;
- organisation de reconnaissances exploratoires (lieux d'évacuation, salles de confinement, etc.) ;
- exercice de mise en situation avec des personnes simulant l'intrusion (les employés doivent être prévenus de la réalisation de l'exercice mais pas nécessairement de sa date exacte pour éviter des phénomènes de panique). La police ou la gendarmerie sont invités à apporter leur expertise. Ce type d'exercice doit être planifié et préparé en lien étroit avec les préfectures et les responsables des services locaux de sécurité concernés.

[1] Cette action doit être réalisée en lien avec le chef du pôle des urgences et le directeur du SAMU pour les établissements qui en disposent.

[2] Nécessité pour le personnel de l'établissement de disposer d'une carte professionnelle pour faciliter le filtrage.

4. **Mise à jour du PSE et des procédures**

Le PSE et les procédures de réaction du site font l'objet de mises à jour périodiques, notamment à la suite des enseignements tirés des exercices.

Ces retours d'expérience doivent pouvoir être partagés au niveau régional et local, en lien avec l'ARS et son groupe d'appui.

Documents de référence

Ministères sociaux :

Guides « Vigilance attentats : les bons réflexes » à destination des équipes de direction et du personnel des établissements de santé, sociaux et médicaux sociaux.

Guide de déclinaison des mesures de sécurisation périmétrique et bâtimentaire.

Guide de la DGOS relatif à la prévention des atteintes aux personnes et aux biens en secteur de soins (à paraître).

Points clefs d'une politique de sécurité (document DGOS/FHF).

Référentiels assurantiels du centre national de prévention et de protection :

Référentiel CNPP 1302 « Système de management de la sûreté - Lutte contre la malveillance et prévention des menaces ».

Référentiel CNPP 6011 « Analyse de vulnérabilité - Approche globale et méthode pour l'incendie ou la malveillance ».

Normes :

ISO 31000 « Management du risque – Principes et lignes directrices ».

ISO 27001 « Système de management de la sécurité de l'information ».

ISO 28000 « Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement ».

ISO 34001 « Système de management de la sûreté, la protection de ses actifs contre des actes malveillants et frauduleux ».

RECOMMANDATIONS EN MATIÈRE DE STRATÉGIE DE PROTECTION

1. **Identifier et évaluer les menaces et les risques**

Les sources de menaces et de risques pour l'établissement :

– actes de malveillance : importance et nombre des sous-traitants et prestataires, sensibilisation du personnel à la sécurité, actes de violence sur le personnel, occupation illicite de locaux (sous-sol, parking), vols, accueil des détenus, etc. ;
– risques techniques : locaux d'entreposage de matériels dangereux (azote, oxygène, etc.). ;
– risques liés aux structures : milieu urbain, multiplicité des sites et des accès, délimitation périmétrique par rapport à l'environnement, actes de malveillances, intrusion ;
– risques sur les systèmes d'information : vulnérabilités des systèmes d'information, etc.

L'évaluation qualitative ou quantitative et hiérarchisation : probabilité, gravité et acceptabilité des risques identifiés (prise en compte des mesures correctrices déjà mis en œuvre par exemple : restriction des accès, etc.).

2. **Définir les moyens de prévention et de protection en fonction de**

Espace périphérique (environnement immédiat, bâtiment voisin, espaces vert, voies de circulation piétonnes et automobile).

Espace périmétrique délimitant l'établissement (grillage, muret, façades, portes, escaliers de secours).

Espaces intérieurs : salles d'attente, locaux techniques, etc.

3. **Exemples de mesures de sécurité qui doivent être proportionnées aux risques identifiés**

Sensibilisation du personnel à la vigilance :

– rappel des consignes de sécurité : port du badge apparent, etc. ;
– rappel des bonnes pratiques en termes de vigilance ;
– fermeture systématique des portes et issues à la fin des activités journalières non permanentes ;

- réalisation de fiches réflexes en cas d'agression ;
- réorganisation des circuits d'accueil ;

Adapter le contrôle des accès :

- mise en place de systèmes anti-intrusion aux points névralgiques ;
- renforcer la surveillance périphérique du site (rondes, caméra, etc.) ;
- mettre en place ou renforcer la vidéo protection ;
- renforcer les contrôles d'accès :
  - dissocier les points d'entrées/sorties du personnel et du public ;
  - restreindre le nombre de points d'entrées/sorties du site ;
  - présence de personnels de sécurité aux points d'entrées/sorties :
    - vérifier l'identité des personnes entrantes ;
    - mise en service d'un scanner à rayon X ;
    - contrôle visuel des bagages ;
    - contrôle visuel du contenu des véhicules (coffres, intérieur des véhicules, etc.) ;
- définir les zones d'accès par type de flux (personnel, patients, familles, prestataires, etc.) :
  - fermeture partielle des accès de l'établissement ;
  - restriction d'accès aux seuls patients ;
  - circuit spécifique de l'accueil des détenus ;

Renforcer les mesures de sécurité des points critiques identifiés :

- dépôt air liquide, poubelles ;
- réorganisation du stationnement sur les parkings ;
- protection des éléments susceptibles d'être utilisés à des fins malveillantes (pierres, éléments métalliques, etc.) ;
- révision et adaptation de la signalétique interne à l'établissement ;

Renforcer les mesures en cas d'attentat (en coordination avec la préfecture et les forces de sécurité intérieure) :

- renforcement de la sécurisation périmétrique et des accès ;
- fermeture partielle ou totale des accès de l'établissement ;
- instauration d'un périmètre de sécurisation par filtrage des accès aux lieux critiques de l'établissement ;
- gestion des flux afin d'éviter un attroupement excessif aux portes ou un blocage des ambulances sur le site des urgences.

ANNEXE 2

LES MESURES EN MATIÈRE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

En matière de sécurité des systèmes d'information (SSI), l'ensemble des systèmes d'information et de communication (SIC) concourant au bon fonctionnement de l'établissement doivent être pris en considération : systèmes d'information hospitaliers, systèmes d'information embarquée ou associée aux dispositifs médicaux, informatique générale, systèmes de communication, gestion technique centralisée, etc.

Il est essentiel que l'ensemble des acteurs, directeurs d'établissement, professionnels de santé et responsables de la sécurité des systèmes d'information, soient impliqués et prennent les mesures qui s'imposent contre les malveillances et les négligences, internes et externes pouvant mettre en péril le bon fonctionnement des SIC d'un établissement.

Le rôle du directeur d'établissement est, à cet égard, stratégique dans la gouvernance de la SSI. Il doit établir un bilan des risques et des menaces pesant sur son établissement, définir ses priorités, proposer un plan d'action, s'entourer des compétences *ad hoc* et piloter la sécurité des systèmes d'information dont il porte la responsabilité.

Dans ce cadre, avec des systèmes de plus en plus ouverts et interconnectés, une vigilance particulière devra porter sur :

– les dispositions spécifiques pour prévenir les risques de piratage de tout ou partie des systèmes d'informations, en particulier ceux liés aux matériels biomédicaux, le contrôle d'accès, la gestion technique centralisée (GTC) et la gestion technique de bâtiment (GTB) ;
– les dispositions permettant de prévenir les risques liés à la perte du patrimoine informationnel de l'établissement notamment par la destruction physique ou logique des actifs indispensables à l'organisme (ex : gestion des flux médicaux) et au bon accomplissement de ses missions (ex : systèmes d'information hospitalier, infrastructures informatiques et de communication, biomédical, gestion technique centralisée ;
– les accès au réseau, en interne ou depuis l'extérieur, par les prestataires ;
– les privilèges de connexion accordés.

Les mesures relatives à la sécurité des systèmes d'information sont à intégrer dans le plan de sécurité d'établissement (PSE). Les mesures permettant de couvrir les risques les plus critiques sont à apprécier au regard des risques identifiés dans le PSE.

Les risques non couverts par des mesures (risques résiduels) doivent être identifiés et acceptés par le responsable légal de l'établissement.

Documents de référence

Ministères sociaux :

Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS)[1].

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)[2] : référentiels et guides pratiques qui traitent de la sécurisation de données de santé.

ISO 27000 « Management de la sécurité de l'information ».

Agence nationale de sécurité des systèmes d'information (ANSSI) :

Guides des bonnes pratiques ANSSI[3].

[1] Arrêté du 1er octobre 2015 portant approbation de la PSSI MCAS. NOR : AFSZ1523362A : https://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo/texte.

[2] http://esante.gouv.fr/.

[3] http://www.ssi.gouv.fr/administration/bonnes-pratiques/.

ANNEXE 3

RECOMMANDATIONS PARTICULIÈRES CONCERNANT LA MISE EN ŒUVRE DES CONVENTIONS SANTÉ-SÉCURITÉ-JUSTICE

Le ministère des affaires sociales et de la santé encourage la généralisation des conventions santé-sécurité-justice pour les établissements publics et privés, en cohérence avec le plan de sécurité d'établissement.

Sont notamment concernés dans cet accord :

– le diagnostic de sécurité effectué par les forces de l'ordre des établissements ;
– les procédures d'alerte spécifiques (objets et colis suspects, alertes à la bombe, le déclenchement de l'alerte en cas d'attentat…) ;
– l'enlèvement/déplacement des véhicules stationnés aux abords des sites sensibles ;
– l'intégration de l'établissement dans le dispositif de patrouille Vigipirate ;
– l'accueil des victimes d'attentat et leur protection ;
– le plan de protection de l'établissement en cas d'accueil de victimes d'attentat et leur famille ;
– la nomination d'un correspondant sécurité.

Les établissements n'ayant pas encore de convention sont invités à décliner les accords ministériels nationaux.

De manière générale, il est préconisé que cette convention soit courte. Elle sera par contre complétée par des annexes techniques chacune répondant par des mesures spécifiques aux problématiques rencontrées.

Vous trouverez des exemples de convention sur le site Internet du ministère des affaires sociales et de la santé[1].

Documents de référence

Ministères sociaux :

Protocole santé-sécurité-justice du 10 juin 2010.

Guide de la DGOS relatif à la prévention des atteintes aux personnes et aux biens en secteur de soins (à paraître).

Points clefs d'une politique de sécurité (document DGOS/FHF).

[1] http://social-sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante-medico-social/observatoire-national-des-violences-en-milieu-de-sante-onvs/article/onvs-les-bonnes-pratiques-contre-les-violences-en-milieu-de-sante.

ANNEXE 4

SENSIBILISATION ET FORMATION DES PROFESSIONNELS DE SANTÉ

Une attention particulière sera portée à la sensibilisation et à la formation de l'ensemble du personnel sur son rôle en matière de vigilance, de prévention et de réaction dans le cadre de l'amélioration de la sécurité de l'établissement. Il s'agit de développer une véritable « culture de la sécurité », propre à permettre une réaction collective face à des risques et à des menaces.

Le volet information :

- informez le personnel sur les risques et les menaces et sur le plan Vigipirate ;
- développez une stratégie de sensibilisation interne *via* l'affichage (*cf.* posture Vigipirate) et en diffusant des messages de vigilance sur le réseau interne et la vidéo « réagir en cas d'attaque terroriste »[1] ;
- présentez le plan de sécurité d'établissement au personnel en expliquant ses finalités et les zones et secteurs considérés comme les plus sensibles ;
- sensibilisez le personnel au respect des mesures de sécurité et de vigilance :
  - rappel des procédures et du rôle de chacun ;
  - information sur la procédure de signalement et l'identification des « signaux faibles » (incidents mineurs, comportements suspects, etc.) qui peuvent précéder un attentat ;
- diffusez les guides de bonnes pratiques en matière de vigilance.

Le volet formation :

Avec l'appui des écoles de formation professionnelles, dont l'École des hautes études en santé publique (EHESP) et les écoles de formation d'infirmiers, des modules de formation initiale et continue à destination des chefs d'établissement, du personnel de direction, médical et para-médical seront mis en place à partir de 2017.

En complément, des formations ciblées seront organisées par l'établissement visant à :

- la formation aux premiers secours ;
- la connaissance et la maîtrise par tous des moyens d'alerte (diffusion de l'alerte et connaissance des signaux d'alerte) ;
- la connaissance du site, en organisant des « reconnaissances exploratoires » afin d'identifier les cheminements, les issues de secours, les obstacles éventuels, et tout ce qui peut offrir une protection ;
- des mises en situation simples et des exercices collectifs, intégrant les différents partenaires, et en exploitant systématiquement les retours d'expérience de ces exercices (*cf.* annexe I, paragraphe 3).

Sur demande, les services de formation nationaux et locaux et les services spécialisés du ministère de l'intérieur pourront apporter leur concours à l'organisation de séances de sensibilisation et aux modules de formation développés par l'établissement.

Il est conseillé de s'appuyer sur les formations dispensées en local par les préfectures les forces de sécurité intérieure aux acteurs de l'ensemble des secteurs sociaux-économiques.

Documents de référence

Ministères sociaux :

Guides « Vigilance attentats : les bons réflexes » à destination des équipes de direction et du personnel des établissements de santé, sociaux et médicaux sociaux.

[1] http://www.gouvernement.fr/reagir-attaque-terroriste.
http://social-sante.gouv.fr/professionnels/gerer-un-etablissement-de-sante-medico-social/observatoire-national-des-violences-en-milieu-de-sante-onvs/article/onvs-les-bonnes-pratiques-contre-les-violences-en-milieu-de-sante.