SPF SANTÉ PUBLIQUE
SÉCURITÉ DE LA CHAÎNE ALIMENTAIRE
ET ENVIRONNEMENT

Direction générale Soins de santé

CONSEIL FÉDÉRAL DES
ÉTABLISSEMENTS HOSPITALIERS

Bruxelles, le 29 juin 2021

Réf. : CFEH/D/536-2 (*)

Avis du CFEH suite à la demande du ministre Vandenbroucke du 19/05/2021 concernant les BMUC et la cybersécurité

Au nom du Président,
Margot Cloet

Annick Poncé
Directeur général ad interim

Isabelle Van der Brempt (Signature)
Digitally signed by Isabelle Van der Brempt (Signature)
Date: 2021.07.07 22:59:30 +02'00'

(*) Le présent avis a été approuvé (par e-mail) par la plénière le 29/06/2021 et ratifié par le Bureau à cette même date.

Par le présent avis, le CFEH souhaite répondre à la demande d'avis du ministre Vandenbroucke du 19/05/2021 concernant les BMUC et la cybersécurité.

Avant tout, le CFEH souhaite souligner que l'avis rendu porte à la fois sur les hôpitaux généraux et les hôpitaux psychiatriques.

Procédure

Dans le cadre de cette demande d'avis, deux groupes de travail ont été mis sur pied au sein du CFEH afin de se prononcer sur cette demande d'avis.

Dans un premier temps, un groupe de travail BMUC a été créé, composé de membres du CFEH ainsi que des experts nécessaires du secteur. Le groupe de travail a décidé, en partie à la demande du ministre, de rendre un avis avant le 1er juillet sur le financement BMUC pour l'année 2022. L'objectif est de pouvoir ainsi rendre un avis sur les objectifs à court terme de 2022 concernant le financement du DPI dans les hôpitaux sur la base des BMUC. Par la suite, ce groupe de travail se penchera en détail sur les modalités pour 2023 et 2024, partant du contexte et des axes prioritaires visés dans l'approche ultérieure tels qu'ils sont formulés dans l'avis.

Dans un deuxième temps, un second groupe de travail axé sur la cybersécurité a vu le jour. Ici aussi, la composition du groupe est un mélange entre membres du CFEH et experts du secteur. Comme indiqué dans la demande d'avis du ministre, le présent avis se concentre sur les axes prioritaires mentionnés : conscientisation par la sensibilisation et élaboration d'une politique visant à accroître la maturité de la cybersécurité en milieu hospitalier. Le groupe de travail souhaite également identifier les principaux coûts liés au développement de la cybersécurité dans les hôpitaux. Le présent avis renvoie à une nouvelle directive européenne relative à la sécurité des réseaux et des systèmes d'information. De plus, ce groupe de travail se penchera ensuite sur les modalités pour les années à venir, en s'appuyant à cet égard sur les priorités énoncées dans la demande d'avis.

Avis relatif au financement du DPI via le BMF 2022

Contexte

Les hôpitaux font face à la pandémie de COVID-19 depuis mars 2020 à ce jour. Le secteur hospitalier consacre presque toute son attention aux mesures nécessaires pour maîtriser cette pandémie. Les hôpitaux bénéficient dès lors d'une marge très limitée pour poursuivre le développement structuré et coordonné du DPI et son évaluation selon les BMUC. Le CFEH est conscient que c'est déjà la deuxième année que le déploiement du DPI prend du retard en termes de rapidité en raison de la pandémie qui sévit.

Il est dès lors difficile d'introduire de nouveaux critères dans le suivi de l'évolution du déploiement du DPI sur lesquels on s'appuie pour déterminer le financement dans le BMF 2022, de fixer les valeurs de référence à atteindre, de procéder à la conversion en actions concrètes au sein des hôpitaux et enfin d'effectuer les mesures nécessaires pour pouvoir objectiver les réalisations.

Proposition d'avis

En 2020, le CFEH a rendu deux avis sur ce dossier : le premier avis sur le financement du BMF au 1er juillet 2020 (CFEH/D/507-3) a été approuvé par la plénière du CFEH du 23/04/2020 et le deuxième avis sur le financement du BMF au 1er juillet 2021 (CFEH/D/522) a été approuvé par la plénière du CFEH du 10/12/2020.

Le CFEH propose de reprendre ces deux avis et de les appliquer tels quels dans le financement de 2022. En ce qui concerne le financement du DPI dans le cadre du BFM de juillet 2022, le CFEH recommande que les modalités de financement de 2020 et 2021 soient prolongées d'un an et, par conséquent, que le financement en 2022 soit calculé de la même manière qu'en 2020 et 2021.

Approche ultérieure

Le groupe de travail BMUC s'engage toutefois à établir en juillet 2021 un agenda en vue de l'approche ultérieure portant sur les années de financement 2023 et 2024. À cet égard, les axes prioritaires fixés dans la demande d'avis serviront de principes directeurs. Ceci s'inscrira dans le cadre de l'approche progressive conformément à ce qui est aussi formulé dans la demande d'avis. Le CFEH tente de rendre un avis à ce sujet avant la fin de l'année 2021, pour pouvoir informer les hôpitaux à temps, lancer et développer la mise en œuvre et effectuer les mesures nécessaires dans un délai raisonnable. À cet égard, la différenciation actuelle des critères entre les hôpitaux généraux et les hôpitaux psychiatriques doit continuer à être prise en compte.

Avis relatif à la cybersécurité

Contexte

Le CFEH souscrit pleinement à la vision selon laquelle la cybersécurité dans les hôpitaux belges doit être une priorité. Plusieurs incidents récents ont montré clairement que le secteur des soins de santé est la cible d'actes malveillants dont les conséquences sont lourdes. L'énorme masse de données à caractère hautement sensible requiert une protection aussi efficace que possible contre l'utilisation abusive de ces données. Les leçons tirées de ces récents incidents incitent les hôpitaux à réfléchir en profondeur sur une stratégie adaptée pour gérer la problématique de la cybersécurité. Le CFEH se réjouit de l'attention portée à ce sujet qui ressort de cette demande d'avis, avec la promesse d'un soutien organisationnel et administratif de la part de l'autorité. En outre, le SPF a également précisé au cours des réunions qu'une indemnité financière serait prévue à cet effet en 2022.

Priorité du CFEH

Comme indiqué dans la demande d'avis du ministre, le CFEH s'est concentré dans son premier avis sur les points suivants : « sensibilisation » et « accroissement de la maturité en ce qui concerne la politique de cybersécurité ».

À cet égard, le CFEH a souhaité élaborer un trajet qui intègre de manière logique ces éléments dans l'approche de la cybersécurité. La directive européenne NIS et la norme ISO/CEI 27001 sont le fil conducteur utilisé pour cette approche. Comme le souligne la demande d'avis du ministre, l'Europe planche actuellement sur une nouvelle version de la directive NIS. Cependant, cette version n'est pas encore connue à l'heure actuelle et ne peut donc pas servir pour l'instant de ligne directrice pour l'approche proposée. Le CFEH s'appuiera dans un premier temps sur des considérations génériques

qui peuvent être intégrées dans tout cadre normatif. En outre, le CFEH prendra progressivement en compte les développements de la nouvelle version de la directive NIS, y compris les conséquences de la désignation des opérateurs de santé comme O.E.S. (Operators of Essential Services) (voir à ce sujet la lettre du CFEH au Ministre réf. CFEH/C/41-2021, datée du 11/03/2021).

Propositions d'étapes dans le cadre du lancement d'une culture sur la cybersécurité en milieu hospitalier

- Le CFEH souligne que la première étape dans l'approche sur la cybersécurité passe nécessairement par une évaluation interne approfondie dans chaque hôpital général et psychiatrique. La position de départ de chaque hôpital peut très fortement varier. Cette diversité est liée aux actions prises par le passé, à l'ampleur du service ICT interne, aux investissements déjà réalisés, aux processus élaborés ... En résumé, avant de pouvoir évaluer la meilleure approche dans les étapes à venir, il convient d'identifier et d'évaluer en profondeur la situation actuelle.

- Le CFEH préconise la réalisation d'un audit externe où une partie externe évaluera la conformité aux règles existantes et le degré de protection. Plusieurs angles d'approche sont possibles à cet égard : le cadre à évaluer, le recours ou non au test d'intrusion (*pentest*), le hacking éthique, etc. Il s'agit d'un audit effectué par une partie externe pour établir la situation « as is » et l'écart avec le cadre normatif. Il faut toutefois souligner à cet égard que cette étape n'aboutit pas immédiatement à un renforcement de la cybersécurité mais elle permet de détecter les failles du système. On peut éventuellement opter ici pour un audit ciblé sur la base de la récente enquête du gouvernement concernant la cybersécurité dans les hôpitaux Un deuxième point d'attention important est le caractère répétitif de certaines actions, comme le hacking éthique pour continuer à suivre la sécurité du système. Compte tenu de la nature évolutive de la menace, cette étape sera également réitérée avec une certaine régularité, par ex. tous les trois ans. Le CFEH propose d'établir les accords nécessaires à ce sujet avec Belac, l'Organisme belge d'Accréditation.

- Une prochaine étape du trajet consiste à élaborer un plan pour remédier aux failles observées dans le système, en se basant sur les résultats de l'audit externe et sur d'éventuelles mesures complémentaires. À nouveau, cette étape doit être réalisée en interne, au sein de l'organisation (sous la supervision ou non de partenaires externes). Il convient d'élaborer une politique de sécurité à l'échelle de l'organisation, il va sans dire dans le but de protéger le système contre toute menace interne et externe.

- Le CFEH propose aussi d'évaluer l'approche de la cybersécurité en tenant compte des expériences à l'étranger. À cet égard, il est fait référence aux expériences menées par ex. aux Pays-Bas ou en France[1].

- Le CFEH prend également connaissance d'une analyse de risques qui a été effectuée dans le passé par le SPF Santé publique et qui peut donner un aperçu de la situation en Belgique. Il est

[1] La France vient de dévoiler son programme pour aider les hôpitaux en matière de cybersécurité : 2 milliards pour la transformation numérique des hôpitaux, dont 350 millions pour la cybersécurité. Les 135 GHT (groupements hospitaliers de territoire) deviendront officiellement des O.E.S. (https://www.patientnumerique.com/actus/actualites/2021/04/la-france-devoile-un-programme-dassistance-aux-hopitaux-en-matiere-de-cyber-securite/).

possible d'utiliser ces informations pour détecter de manière plus ciblée les besoins des hôpitaux et pour définir de manière plus ciblée des points d'action à un niveau supérieur.

Conscientisation par la sensibilisation au sein de l'organisation

Le CFEH préconise une approche approfondie dans les hôpitaux pour procéder, à tous les niveaux de l'organisation et partout sur le lieu de travail, à la sensibilisation requise pour la problématique et aux actions à entreprendre nécessairement pour garantir la cybersécurité. Les potentielles menaces pour les systèmes numériques varient et peuvent surgir n'importe où dans un hôpital. Chacun doit donc être conscient de ces éventuels risques et des protocoles qui sont convenus en la matière.

Les formations qu'il faut dispenser à cet égard doivent être adaptées aux différentes circonstances en fonction de l'environnement. Il importe dès lors que cette sensibilisation et ces formations soient répétées régulièrement. Des outils de formation permanente et des actions de sensibilisation peuvent être utilisés à cette fin. Le CFEH préconise le développement d'un programme e-learning constitué de plusieurs modules.

Assurabilité du risque

Le CFEH relève un problème spécifique concernant l'assurabilité du risque de violation de la cybersécurité. Le secteur de l'assurance augmente les primes pour couvrir ce genre de risques. Sur demande, il est souligné ici qu'il s'agit d'une tendance du marché international. Le secteur estime qu'il est très important de pouvoir maintenir un système d'assurabilité abordable. On renvoie à cet égard à la mobilisation des équipes d'assistance en cas de cyber-attaque externe, mais aussi à la couverture de potentielles réclamations financières, non seulement liées à cette cyber-attaque externe, mais aussi en raison d'éventuels manquements dans la prestation de soins comme conséquence de la défaillance complète ou partielle des systèmes.

Partage de connaissance

Le CFEH tient à souligner que le partage de connaissances dans cette matière importante et délicate revêt une importance cruciale. La cybersécurité n'est pas une compétition entre hôpitaux, mais bien une attitude commune par rapport à de potentielles agressions toxiques qui ciblent les données de santé de nos patients. Par conséquence, il importe que les hôpitaux se réunissent autour de cette question et partagent autant que possible leurs connaissances en la matière. On envisage à cet égard une structure organisationnelle, par exemple au niveau du réseau pour partager les informations. Mais comme la problématique dépasse le cadre des réseaux, cela doit être examiné à un niveau beaucoup plus large.

Plusieurs canaux informels permettent l'échange d'informations, mais le CFEH estime que continuer à favoriser la coopération, en particulier en matière de cybersécurité, est une tâche importante de l'autorité. L'échange de bonnes pratiques, mais aussi le partage des plans d'action sont des éléments importants. Le CFEH préconiserait à cet égard une implication des représentants de la cellule nationale de Cybersécurité pour participer à cette plateforme faîtière. Enfin, le CFEH tient aussi à préciser que d'autres groupes importants de la société sont confrontés à cette problématique (par ex. les services de police) et que le partage des connaissances pourrait dès lors s'effectuer sur une plateforme très étendue.

Éléments récapitulant l'avis

- Trajet dans chaque institution : évaluation interne, évaluation externe, élaboration d'un plan d'action ;
    - comparaison avec les expériences à l'étranger ;
    - feed-back de l'analyse des risques par le SPF Santé publique dans le secteur ;
- conscientisation dans l'organisation grâce aux formations et à la sensibilisation ;
- assurabilité des risques ;
- partage des connaissances dans le secteur, mais aussi entre les secteurs.

Aspects financiers de la cybersécurité

Le CFEH prend note de la possibilité de prévoir en prévision un financement visant à soutenir le déploiement d'un plan d'approche Cybersécurité au sein des hôpitaux. Il est dès lors important que ce premier avis sur la cybersécurité trace une première ébauche des éventuels coûts auxquels sont confrontés les hôpitaux à cet égard.

Fonctions existantes avec valeur ajoutée

Depuis mai 2018, chaque organisation doit disposer d'un délégué à la protection des données (*Data Protection Officer* - DPO), en sus de conseil de sécurité de l'information. Ces fonctions et leurs coûts d'exploitation n'ont pas fait l'objet d'une rétribution supplémentaire de la part du gouvernement. Entre-temps, les exigences en matière de connaissances et l'ensemble des tâches de ces fonctions, notamment l'instauration de règles RGPD, s'est fortement élargi. Ces fonctions ont vu leur éventail de tâches s'élargir encore plus dans le cadre de la problématique liée à la cybersécurité et des étapes nécessaires qui ont été détectées par le CFEH pour évaluer la conscientisation et la maturité de l'organisation. Le CFEH tient à souligner que l'autorité doit prendre en compte ces fonctions et leurs coûts d'exploitation (37,5 millions[2] d'euro, calculé sur une base annuelle pour tous les hôpitaux), dans l'optique de prévoir un financement structurel approprié. Dans ce contexte, le DPO et le conseiller de sécurité de l'information occupent une position centrale et cruciale. Il semble dès lors inadmissible que cette position clé essentielle dans la coordination de la cybersécurité ne soit pas compensée.

Coûts liés au trajet

- L'exécution de l'évaluation externe engendre des frais supplémentaires. Le CFEH constate que la totalité des coûts d'une telle évaluation externe varie d'un hôpital à l'autre, ainsi que le contenu de cette évaluation externe. Les montants oscillent entre 11 000 et 80 000 euros pour un audit externe, et entre 26 000 et 150 000 euros pour une évaluation ISO27001). Comme il s'agit d'une étape essentielle du trajet qu'un hôpital doit suivre, il s'agira certainement d'un montant fixe, avec une composante supplémentaire récurrente annuelle (maintenance). En outre, l'installation d'un SIEM ("Security Information Event Management")/SOC ("Security Operations Center") assure un niveau élevé de cybersécurité et coûte au moins 50 000 euros par an et par hôpital. Le CFEH propose dès lors d'intégrer un montant dans l'intervention financière en s'appuyant sur une étude comparative ultérieure et sur une concrétisation ultérieure du trajet.

- L'assurabilité du risque lié à la cybersécurité est pour l'instant estimée à un montant compris entre 40 000 et 180 000 euros. Ici aussi , on observe une variation en fonction de la taille de l'établissement et du risque à assurer. Étant donné que le CFEH considère l'assurabilité du

[2] Voir fiche 8 de l'avis FRZV/D/514-2 besoins prioritaires 2021, du 9 juillet 2020.

risque comme un élément très important, il convient de le préciser dans la détermination de l'intervention financière.

- La sensibilisation requise auprès du personnel de l'ensemble de l'organisation doit s'effectuer par le biais de formations et par des sessions de répétition régulières. Pour illustrer l'impact financier d'une formation à l'échelle de l'hôpital, nous donnons un exemple. Pour une formation en classe de 2 heures destinée à tous les employés de l'organisation, on calcule un coût total de 15 millions d'euros. Le coût d'opportunité, c'est-à-dire le remplacement du personnel de santé lorsqu'il suit la formation, est le facteur le plus important. D'autres voies de formation sont bien sûr possibles, par exemple passer par un court module d'e-learning pendant 10 minutes par mois est moins coûteux pour l'absence de personnel soignant, mais cela signifie une "absence" annuelle de 2 heures par employé. Le CFEH tient donc à souligner que les nombreux "petits bouts" qui éloignent le personnel soignant de son chevet ont également un impact lourd et entraînent un coût.
- Le partage des connaissances est un élément crucial aux yeux du CFEH. Outre les canaux informels existants permettant l'échange d'expériences, le CFEH demande également que l'autorité mette en place une plateforme plus englobante qui permettra aussi l'échange requis d'expériences et de connaissances dans un cadre social plus large. Néanmoins, le CFEH demande aussi à l'autorité de soutenir les initiatives prises à un échelon plus local, comme celui des réseaux.

Modalités de la rémunération

Concernant la répartition des moyens financiers qui seraient mis à la disposition des hôpitaux, le CFEH n'a pas d'objections de procéder de la même manière que dans le cadre du financement du DPI.

La structure du financement consiste en un financement-socle de base (composé d'un montant fixe indépendant de la taille de l'hôpital et d'un montant par lit), un financement accélérateur (également composé d'un montant fixe indépendant de la taille de l'hôpital et d'un montant par lit) et – éventuellement et de manière limitée - un financement de partage des connaissances. L'objectif est de disposer d'un système simple et transparent. Les critères de financement doivent également être communiqués aux hôpitaux en temps utile.

Toutefois, il est important que dans la phase initiale (lancement de l'approche), le financement-socle de base soit suffisamment important pour soutenir les premières mesures prises par les hôpitaux. Après ce coup de pouce nécessaire, il devrait ensuite être possible d'affiner progressivement les modalités de financement en fonction de critères.

Futur plan d'approche

Le groupe de travail Cybersécurité établira un plan d'approche en juillet/septembre 2021 en vue d'élaborer le futur avis, en se concentrant à cet égard sur les fers de lance et les priorités qui sont formulés dans la demande d'avis. L'objectif est de soumettre d'ici la fin de l'année 2021 un deuxième avis sur la future approche en matière de cybersécurité.

***