Comité sectoriel de la sécurité sociale et de la santé
Section "Santé"

CSSSS/15/010

RECOMMANDATION N° 15/01 DU 20 JANVIER 2015 RELATIVE À UN PROJET DE CIRCULAIRE DU SPF SANTÉ PUBLIQUE PORTANT SUR L'UTILISATION DE SERVICES "CLOUD" DANS LES HÔPITAUX

La section santé du Comité sectoriel de la sécurité sociale et de la santé (dénommée ci-après « le Comité sectoriel »);

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;*

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*;

Vu la demande d'avis de la Commission de la protection de la vie privée reçue le 1er décembre 2014;

Vu le rapport d'auditorat de la Plate-forme eHealth du 9 janvier 2015;

Vu le rapport de monsieur Yves Roger,

Recommande le 20 janvier 2015, après délibération, ce qui suit:

I. OBJET DE LA DEMANDE

1. La Commission de la protection de la vie privée a reçu, le 18 septembre 2014, du Ministre des Affaires sociales et de la Santé publique de l'époque une demande d'avis concernant un projet de circulaire portant sur l'utilisation de services "cloud", rédigé par le SPF Santé publique.

2. Suite à la modification de l'article 20, § 1er, de la loi coordonnée du 10 juillet 2008 sur les hôpitaux et autres établissements de soins, les hôpitaux ont maintenant en effet la possibilité de recourir à des services "cloud". Le secteur hospitalier est toutefois demandeur d'un cadre de référence minimal permettant aux hôpitaux d'évaluer l'utilisation de services "cloud" de manière aussi rationnelle que possible, en respectant un niveau de sécurité technique et juridique maximal ainsi que la protection de la vie privée des patients.

3. Afin de satisfaire à cette demande, le SPF Santé publique a rédigé un projet de circulaire portant sur l'utilisation de services "cloud" au sein des hôpitaux.

4. Compte tenu de sa compétence spécifique en matière de protection des données relatives à la santé, notamment dans le secteur hospitalier, la Commission de la protection de la vie privée a transmis le projet de circulaire pour avis à la section santé du Comité sectoriel de la sécurité sociale et de la santé.

II. EXAMEN DE LA DEMANDE

5. Le projet de circulaire fournit une description circonstanciée du contexte de cloud computing, des risques potentiels et d'une série de points d'attention. Le Comité sectoriel constate toutefois que la circulaire n'apporte pas beaucoup d'aide aux hôpitaux dans des situations concrètes.

6. L'utilisation de services cloud comporte certains risques inhérents. Ainsi, le traitement de données dans le cloud peut conduire à une fragmentation physique des données sur différents serveurs et dans différents centres de données. Le responsable du traitement perd ainsi potentiellement le contrôle de ses données et la protection de ces données peut être compromise (protection insuffisante, perte, abus, consultation par des tiers ou des autorités étrangères, ...). Par ailleurs, il existe un risque que des autorités étrangères puissent consulter et réclamer des données selon leur propre législation.

7. Les acteurs des soins de santé qui envisagent d'adopter le cloud computing doivent vérifier au moyen d'une analyse de risques quelles seront les répercussions sur la sécurité et la confidentialité lorsque des données à caractère personnel des personnes concernées sont placées dans le cloud. Cette analyse de risques doit porter sur les points suivants:

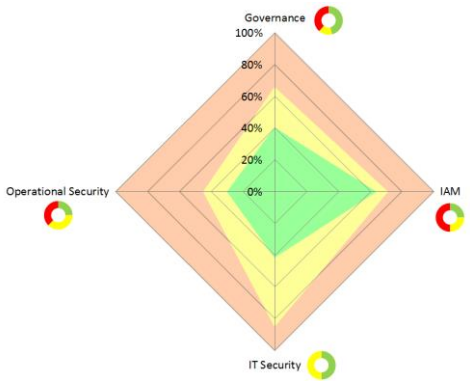
- une évaluation minutieuse des données à caractère personnel qui sont ou non enregistrées dans le cloud, en particulier pour les données dites "sensibles" telles que visées dans la LVP, dont les données à caractère personnel relatives à la santé;
- une analyse des conditions contractuelles;
- une évaluation de la conformité des conditions de sécurité proposées par le fournisseur de service "cloud", les mesures de référence établies par la Commission de la protection de la vie privée devant servir de norme minimale;
- la garantie du fournisseur de service "cloud" quant à certains droits, de l'exécution à la fin du contrat, afin qu'il puisse se concentrer sur ses propres obligations en matière de protection des données à caractère personnel: clause quant à la continuité et à la qualité du service, dispositions relatives à l'interopérabilité, à la réversibilité et à la portabilité des données, ... ;
- la prise en considération des conséquences d'un accès possible aux données par des personnes externes à l'établissement de soins, en particulier à des fins d'application de la loi et à d'autres fins;
- la possibilité de tenir compte des droits des patients concernés, comme le droit de consultation.

8. Pour permettre aux hôpitaux de réaliser une telle analyse de risques, le Comité sectoriel estime qu'il convient de mettre à la disposition des hôpitaux et des autres acteurs du secteur des soins de santé une méthode pratique visant à évaluer la sécurité des services "cloud".

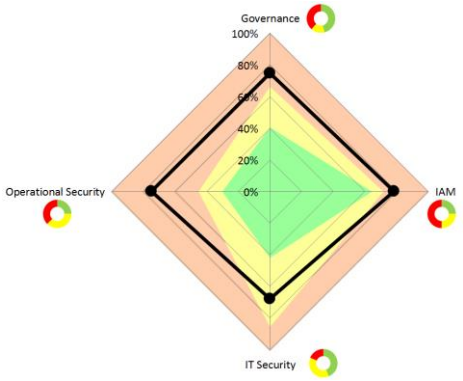
9. Ci-après un modèle à deux volets est décrit permettant à la base d'une grille simple et évolutive, d'une part, d'évaluer le niveau de maturité en ce qui concerne la sécurité d'un service cloud spécifique et, d'autre part, d'évaluer l'utilisation d'un service cloud spécifique en fonction du type de données qu'on souhaite y transférer.

10. Concrètement, la méthode proposée est composée de deux volets:

- un volet A constitué du questionnaire "Security-assessment-cloud-service.xlsm" qui permet d'évaluer le niveau de maturité en ce qui concerne la sécurité d'un service cloud spécifique. Cette évaluation doit reposer uniquement sur les données publiques que l'évaluateur a pu récolter au préalable (p.ex. sur le site web officiel du service cloud). La figure ci-dessous est un exemple du résultat d'analyse obtenu pour un service cloud une fois le questionnaire du volet A rempli. Le résultat est présenté sous forme de radar.



- un volet B constitué du questionnaire “Client-guide-cloud-assessment.xlsm” qui permet d’évaluer la possibilité d’utiliser un service cloud spécifique en fonction du type de données qu’on souhaite y transférer. La figure ci-dessous est un exemple du résultat de comparaison obtenu. La figure reprend le radar obtenu suite à l'application du volet A à un service cloud. La ligne noire correspond aux besoins et exigences de l'utilisateur ayant rempli le questionnaire du volet B. Le résultat final du volet B est donc basé sur un radar résultant du volet A, complété par l'évaluation de l'utilisateur.



11. Les points-clé de sécurité qui sont évalués par le modèle sont regroupés en 4 critères majeurs: gouvernance, gestion des identités et du contrôle d’accès, sécurité IT et enfin sécurité opérationnelle. Dans le contexte de la sécurité sociale et des soins de santé, le modèle évalue aussi la conformité du service cloud avec la "Politique de sécurité relative à des services de Cloud Computing" publiée par la Banque carrefour de la sécurité sociale[1]. Cette conformité est représentée dans les volets A et B par les bouées (une bouée par critère majeur).

12. Les codes couleur sont identiques pour les bouées ou les radars. La zone verte, dite “confidence zone“, représente le pourcentage de conformité totale d'un service cloud à un critère majeur. La zone jaune, dite “doubt zone“, représente le pourcentage de conformité potentielle d'un service cloud à un critère majeur. On parle de “conformité potentielle” pour ne pas pénaliser le service cloud évalué : la “doubt zone” représente donc les questions du questionnaire “Security-assessment-cloud-service.xlsm” où il est impossible de répondre avec certitude. Enfin, la zone rouge, dite “death zone“, représente le pourcentage de non-conformité d'un service cloud à un critère majeur.

13. Les figures ci-dessous présentent une comparaison entre 5 services cloud différents et les besoins/exigences d’un client ayant rempli le questionnaire du volet B. Le modèle compare ainsi les services cloud par critère pour faciliter l’analyse.

[1] https://www.ksz-bcss.fgov.be/binaries/documentation/fr/securite/policies/isms_050_cloud_computing_policy_fr.pdf

14. Les deux questionnaires du volet A et du volet B sont joints en annexe à la présente recommandation et seront publiés avec la recommandation à la page Web dédiée[2].

15. L'utilisation de ce modèle devrait permettre à un hôpital ou à tout autre acteur des soins de santé d'évaluer dans quelle mesure le niveau de sécurité d'un service cloud déterminé répond aux besoins spécifiques. Les acteurs des soins de santé concernés sont ainsi en mesure d'évaluer les divers risques avant d'avoir recours, sous leur propre responsabilité, à un service cloud déterminé.

Par ces motifs,

la section santé du Comité sectoriel de la sécurité sociale et de la santé,

recommande aux acteurs des soins de santé l'utilisation de la méthode décrite dans le présent document afin d'évaluer, sous leur propre responsabilité, la sécurité de services cloud.

Yves ROGER
Président

Le siège du Comité sectoriel de la sécurité sociale et de la santé est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11).

[2] https://www.ehealth.fgov.be/fr/a-propos-de-ehealth/organisation/comite-sectoriel/presentation.