Pre-print en diffusion libre autorisée
Publication consultable ici : https://doi.org/10.1016/j.irbmnw.2012.04.006

Sécurité de l'information en santé : Grille d'autodiagnostic d'après l'ISO 27799

Ayoub BOUDMANE, Léa GUIBON, Mei LI, Emilie SILVI, Anisseh ZARJI, Jean-Pierre CALISTE, Gilbert FARGES

Université de Technologie de Compiègne - Master Management de la Qualité
BP 60319- 60203 Compiègne Cedex France
Tél. : +33 (0)3 44 23 44 58 - Email : gilbert.farges@utc.fr - Site web : http://www.utc.fr/master-qualite

Contexte et problématique :

Le secteur hospitalier est un lieu de création, de circulation et d'échange important d'informations, qu'elles soient sous format informatique ou papier. Ces informations doivent être disponibles, intègres et rester confidentielles.

Les récentes statistiques dans le domaine de la sécurité de l'information montrent qu'actuellement, l'utilisation du référentiel GMSIH (Groupement pour la Modernisation des Systèmes d'Information Hospitalier) a augmenté de +14% et qu'un responsable sécurité est clairement identifié dans plus d'un tiers des hôpitaux [1]. Par contre, ces mêmes statistiques révèlent que seulement 7% des hôpitaux disposent d'un tableau de bord sécurité. De plus, d'après une enquête du Club de la Sécurité de l'Information Français (CLUSIF, [2]) de juin 2010, 60% des hôpitaux ne font pas d'analyse de risque, un tiers ont un contrôle inopiné des mots de passe et 31% n'ont pas connaissance que leur système de sécurité de l'information est soumis à une réglementation. Or, la loi de 1978 relative à la sécurité des systèmes d'information [3] préconise le respect de la confidentialité, se traduisant par une charte de respect de la confidentialité. La loi du 4 mars 2002 (dite "Loi Kouchner") consolidée le 26 février 2010, impose le secret professionnel avec une confidentialité des dossiers [4]. Enfin le référentiel de la Haute Autorité de Santé HAS [5], précise au chapitre 1, partie 2, référence 5 et critère E3 que « le dispositif de sécurité du système d'information est évalué et fait l'objet d'actions d'amélioration ».

Aussi, pour permettre aux hôpitaux d'évaluer le niveau de sécurité de leur système d'information, un outil d'autodiagnostic a été réalisé en interprétant et synthétisant les exigences de la norme **NF EN ISO 27799 "Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002"** [6]. Ce nouvel outil, accessible gratuitement sur internet, offre ainsi un moyen rapide pour se positionner, identifier les axes prioritaires d'amélioration, évaluer les résultats des actions entreprises et ainsi mieux répondre aux exigences de la HAS, relatives à la

sécurité des systèmes d'information et à leur amélioration continue.

Méthodologie et résultats :

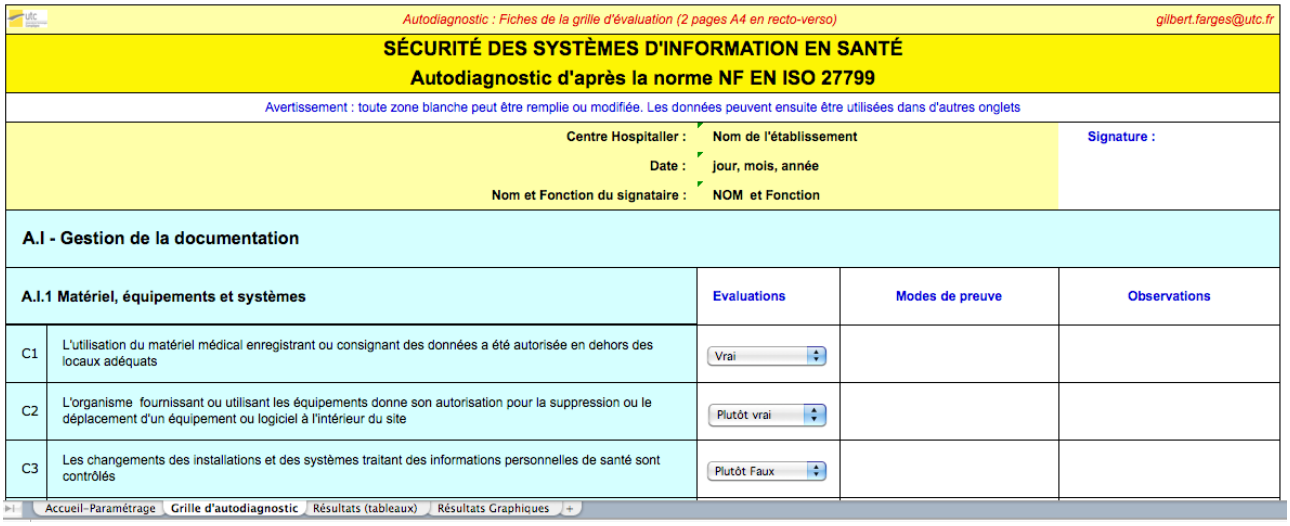
Dans un premier temps, une approche a été réalisée auprès de quelques établissements de santé afin d'identifier les problèmes-clefs liés à la sécurité de l'information. Les retours recueillis ont montré que les problèmes pouvaient survenir principalement soit à cause des structures d'exploitation de l'information (réseau informatique non sécurisé), soit de la mauvaise adéquation des moyens mis en œuvre, soit des compétences inadéquates du personnel, soit des méthodes de management de l'information en santé (organisation, ordinateurs en accès libre). Suite à ce recensement, les exigences du manuel de certification de la HAS [5] et de la norme ISO 27799 [6] ont été étudiées, mutualisées et déclinées en 54 critères dont le niveau de réalisation peut être évalué.

L'outil d'autodiagnostic est destiné à toute personne en charge de la sécurité de l'information en santé. Il exploite un tableur automatisé de type Excel© conçu pour se positionner rapidement en évaluant chacun des critères à l'aide d'une échelle de véracité à 4 niveaux paramétrables par l'utilisateur via un onglet "Accueil-Paramétrage" (figure 1) :

- Faux : L'action n'est jamais réalisée (0%)
- Plutôt faux : L'action est réalisée aléatoirement (33%)
- Plutôt vrai : L'action est réalisée sytématiquement (66%)
- Vrai : L'action est réalisée, tracée et améliorée en continu (100%)

L'évaluation se réalise via l'onglet "Grille d'autodiagnostic" où des champs "modes de preuve" et "observations" sont prévus pour aider à la prise de décision ou mémoriser les interventions ultérieures à entreprendre (Figure 1). Les 54 critères sont regroupés en 17 thèmes, eux-mêmes intégrés dans 3 catégories :

- Gestion de la documentation
- Gestion des risques
- Amélioration continue



Autodiagnostic : Fiches de la grille d'évaluation (2 pages A4 en recto-verso) — gilbert.farges@utc.fr

SÉCURITÉ DES SYSTÈMES D'INFORMATION EN SANTÉ
Autodiagnostic d'après la norme NF EN ISO 27799

Avertissement : toute zone blanche peut être remplie ou modifiée. Les données peuvent ensuite être utilisées dans d'autres onglets

Centre Hospitalier : Nom de l'établissement — Signature :
Date : jour, mois, année
Nom et Fonction du signataire : NOM et Fonction

A.I - Gestion de la documentation

A.I.1 Matériel, équipements et systèmes		Evaluations	Modes de preuve	Observations
C1	L'utilisation du matériel médical enregistrant ou consignant des données a été autorisée en dehors des locaux adéquats	Vrai		
C2	L'organisme fournissant ou utilisant les équipements donne son autorisation pour la suppression ou le déplacement d'un équipement ou logiciel à l'intérieur du site	Plutôt vrai		
C3	Les changements des installations et des systèmes traitant des informations personnelles de santé sont contrôlés	Plutôt Faux		

Accueil-Paramétrage | Grille d'autodiagnostic | Résultats (tableaux) | Résultats Graphiques

Figure 1 : Grille d'autodiagnostic pour évaluer le système de sécurité de l'information en santé [7]

Le résultat de l'autodiagnostic est obtenu immédiatement avec un traitement automatique en temps réel des réponses fournies. Des onglets permettent d'accéder aux tableaux de valeurs ou graphiques des résultats par catégories (figure 2) ou par thèmes (figure 3). Les évaluations graphiques par catégories devraient permettre, au responsable de la sécurité de l'information en santé et à son équipe, d'identifier rapidement des axes stratégiques prioritaires, tandis que les résultats par thèmes permettront de focaliser davantage sur les plans d'action précis à mettre en œuvre et à suivre.

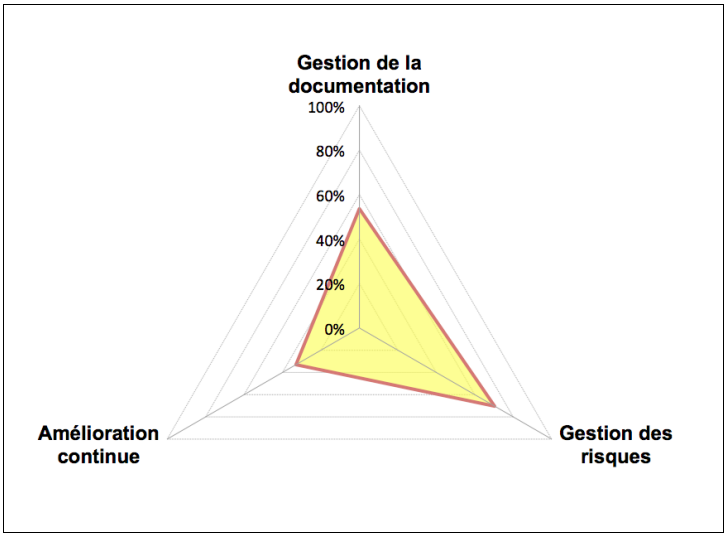


Figure 2 : Exemple des résultats présentés par catégorie d'un autodiagnostic d'après l'ISO 27799 [7]

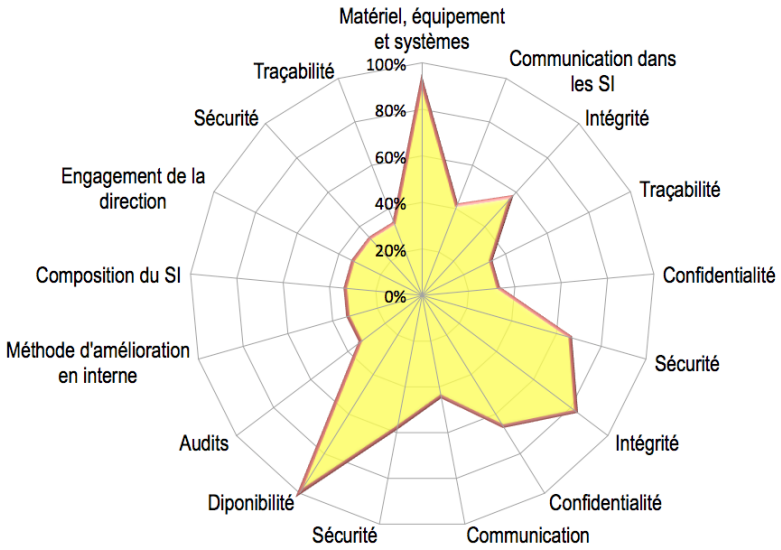


Figure 3 : Exemple des résultats présentés par thèmes du même autodiagnostic [7]

Ces éléments peuvent alors être imprimés en format A4, signés et archivés dans le système documentaire qualité. Ils peuvent aussi servir de modes de preuve crédibles pour une autodéclaration de conformité selon la norme internationale ISO 17050 [8, 9] ou présentés lors d'un visite de renouvellement de la certification HAS [5].

Conclusion :

L'outil d'autodiagnostic réalisé permet à toute personne en charge de la sécurité de l'information en établissement de santé de connaître rapidement sa position vis à vis des exigences de la norme NF EN ISO 27799 - Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002. Il est téléchargeable gratuitement sur internet [7] et entièrement paramétrable pour s'adapter aux différents contextes ou besoins hospitaliers. Il comprend 54 critères d'action à réaliser, regroupés en 17 thèmes ou processus, eux-mêmes intégrés dans 3 catégories ou axes stratégiques (gestion de la documentation, gestion des risques et amélioration continue). Chaque critère s'évalue au moyen d'une échelle de véracité à 4 niveaux paramétrables sur leurs termes et leurs valeurs.

L'outil d'autodiagnostic ISO 27799 devrait aider les acteurs hospitaliers dans leur gestion des données médicales numériques et faciliter l'identification des critères de décision quant aux actions prioritaires à mettre en œuvre pour satisfaire les exigences réglementaires de l'HAS [5].

Il est conseillé de dresser un constat de situation initiale afin d'établir une référence à partir de laquelle les effets des actions d'amélioration pourront être mesurés. L'outil sert alors de pilotage de la dynamique de progrès en permettant d'évaluer très rapidement (environ 1 heure) toute situation et surtout en montrant de manière concrète et factuelle les écarts avec les états antérieurs. Cette approche permet d'augmenter notablement la crédibilité face à des auditeurs externes, mais aussi de favoriser les prises de conscience en interne sur les efforts à consentir.

En intégrant l'amélioration continue dans leurs pratiques quotidiennes, les acteurs hospitaliers en charge de systèmes gérant l'information en santé augmenteront leurs capacités intrinsèques de maîtrise professionnelle. La confiance des tutelles, et surtout celle des patients et de leurs familles, en sera augmentée ainsi que la notoriété globale du système de santé et de sa qualité.

Références bibliographiques

[1] Groupement pour la Modernisation des Système d'Information Hospitalier (GMSIH), Agence nationale d'appui à la performance des établissements de santé et médico-sociaux (ANAP), www.anap.fr, site consulté le 08/03/11

[2] Menaces informatiques et pratiques de sécurité en France, Ed Club de la Sécurité de l'Information Français (CLUSIF), 17 juin 2010, www.clusif.asso.fr, site consulté le 08/03/11.

[3] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : article 29, disponible sur http://www.legifrance.gouv.fr, site consulté le 08/03/11.

[4] Loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (1), JORF 5 mars 2002, version consolidée au 26 février 2010, www.legifrance.gouv.fr, site consulté le 08/03/11.

[5] Manuel de certification des établissements de santé v2010, Haute Autorité à la Santé, juin 2009, www.has-sante.fr, site consulté le 08/03/11.

[6] NF EN ISO 27799 - Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002, Ed Afnor, septembre 2008, www.afnor.org

[7] Développement d'une grille de positionnement au regard des exigences de l'ISO 27799 Ayoub BOUDMANE, Léa GUIBON, Mei LI, Emilie SILVI, Anisseh ZARJI - Projet d'intégration Master Management de la Qualité, 2010-2011. Université de Technologie de Compiègne, www.utc.fr/master-qualite, rubrique « Travaux » puis "Management Qualité", réf n°168, site consulté le 08/03/11

[8] NF EN ISO/CEI 17050-1, Évaluation de la conformité - Déclaration de conformité du fournisseur - Partie 1 : exigences générales, Ed Afnor, avril 2005, www.afnor.org

[9] NF EN ISO/CEI 17050-2, Évaluation de la conformité - Déclaration de conformité du fournisseur - Partie 2 : documentation d'appui, Ed Afnor, avril 2005, www.afnor.org