Organisation internationale de normalisation

Réf.: 1154

Une nouvelle norme ISO sur la gestion de la sécurité des informations de santé

2008-08-28

La nouvelle norme I**SO 27799:2008, *Informatique de santé – Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002*,** qui vient de paraître, traite d'un domaine éminemment sensible, les informations personnelles de santé, et de la meilleure façon d'en assurer la protection.

L'ISO 27799:2008 s'applique à tous les aspects de l'information de santé, quels qu'en soient la forme, le support utilisé pour les stocker ou les moyens mis en œuvre pour leur transmission. La norme spécifie une série de contrôles détaillés en vue de la gestion de la sécurité de ce type d'informations et fournit des recommandations quant aux bonnes pratiques à suivre dans ce domaine. En mettant en œuvre cette nouvelle Norme internationale, les organismes de santé et autres dépositaires d'informations de santé pourront garantir un niveau de sécurisation minimum requis adapté aux conditions et circonstances.

Dans le secteur de la santé, les systèmes informatiques doivent répondre à des exigences de sécurité particulièrement rigoureuses car ils doivent rester opérationnels en cas de catastrophes naturelles, de pannes de système ou d'attaques par refus de service. En même temps, les données que contiennent ces systèmes sont confidentielles et leur intégrité doit être préservée. Tous les organismes de santé, quels qu'en soient la taille, la situation ou les types de prestations, sont donc tenus de mettre en œuvre des contrôles stricts pour protéger les informations de santé qui leur sont confiées.

Avec l'utilisation croissante des technologies sans fil et de l'Internet dans les prestations de soins et du fait de l'accroissement des échanges électroniques d'informations personnelles de santé entre professionnels de la santé, une gestion efficace de la sécurité des technologies de l'information dans le domaine de la santé est un impératif des plus urgents qui justifie clairement l'utilité de l'adoption d'une référence commune en la matière.

Comme l'indique le titre de la norme, l'ISO 27799:2008 est associée à l'ISO/CEI 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information.* Pour établir les recommandations permettant d'interpréter et d'appliquer l'ISO/CEI 27002 spécifiquement à l'informatique de santé, les compétences de professionnels du secteur de la santé ont été mises à contribution. L'adaptabilité était un critère important car de nombreux professionnels exercent de manière isolée ou dans de petites cliniques qui ne disposent pas des ressources informatiques spécifiques nécessaires pour gérer la sécurité des informations.

Si tous les objectifs de contrôle de la sécurité indiqués dans l'ISO/CEI 27002 concernent aussi l'informatique de santé, certaines mesures nécessitent toutefois des explications plus poussées de façon à en optimiser l'usage pour assurer la protection de la confidentialité, de l'intégrité et de la disponibilité des informations de santé. Le secteur de la santé appelle, par ailleurs, certaines exigences spécifiques supplémentaires. Cette Norme internationale fournit donc ces recommandations supplémentaires spécifiques, dans un format que les personnes responsables de la sécurité des informations de santé peuvent aisément comprendre et adopter.

L'ISO 27799 contient un plan d'action pratique pour mettre en application l'ISO/CEI 27002 dans un environnement de santé. Ainsi, avec ces deux normes, est défini tout ce qui est requis en termes de sécurité de l'information dans les soins de santé. L'ISO 27799 compte trois annexes informatives, couvrant respectivement les menaces générales qui planent sur les informations de santé, les tâches et autres normes qui peuvent s'appliquer aux aspects particuliers de la sécurité des informations de santé, et les avantages des outils d'aide à la mise en place de cette sécurité.

L'ISO 27799:2008, *Informatique de santé – Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002,* a été élaborée par l'ISO/TC 215, *Informatique de santé.* Elle est disponible au prix de 154 francs suisses auprès des instituts nationaux membres de l'ISO (voir la liste complète avec les coordonnées) et du Secrétariat central de l'ISO par l'intermédiaire de l'ISO Store ou en contactant le département Marketing & Communication (voir colonne de droite).