La prise en charge confidentielle et sûre des patients est un devoir fondamental

Infrastructures critiques: connaissez-vous les faiblesses de votre organisation?

La technologie d'information et de communication est LA technologie clé du 21e siècle. Elle devient également incontournable dans le secteur de la santé. Citons notamment les apps destinées au personnel qui simplifient la communication interne. Néanmoins, il est indispensable d'utiliser des outils particulièrement sûrs. En effet, les autorités compétentes classent les paysages informatiques dans le secteur de la santé parmi les «infrastructures critiques (IC)». Qu'est-ce que cela signifie et à quoi faut-il faire attention?

Dans le secteur de la santé, la prise en charge sûre des patients est une priorité absolue. Les centres de santé et hôpitaux dont le paysage informatique n'offre pas une sécurité des données suffisante s'exposent à de graves conséquences, pour toutes les parties concernées. Ils courent notamment le risque d'un espionnage des données de patients. Cette pratique a souvent pour objectif de revendre les informations au prix fort. Ces données ne sont pas seulement importantes pour les entreprises pharmaceutiques ou les assurances. Elles suscitent également l'intérêt de certains employeurs pour vérifier l'état de santé de leurs employés.

Important: niveau de protection des données maximal dans le secteur de la santé

Les normes de protection des données les plus strictes sont indispensables dans le secteur de la santé pour empêcher l'utilisation frauduleuse d'informations sensibles sur les patients. Dans chaque hôpital, chaque établissement de soins et chaque cabinet médical. C'est également l'avis du législateur allemand. L'Office fédéral allemand de la sécurité dans la technologie de l'information (BSI) classe le paysage des communications dans le secteur de la santé parmi les infrastructures dites critiques (IC). Ce type d'infrastructures revêt une importance capitale pour la communauté.

Le Conseil fédéral suisse partage cette opinion et a adopté à travers une loi, au même titre que son voisin allemand, une stratégie nationale de protection des infrastructures critiques. Cette démarché vise elle aussi à les protéger le plus efficacement possible. En Allemagne, la loi fixe des conditions particulières aux opérateurs de données. Ils doivent notamment désigner un responsable de la sécurité informatique et apporter la preuve d'une protection minimale certifiée de protection informatique.

Failles dans la protection des données interne

Néanmoins, beaucoup d'employeurs ne tiennent souvent pas compte du fait que de nombreuses informations utilisées dans le domaine de la santé ne sont pas conservées uniquement dans l'infrastructure informatique interne. Elles circulent également par d'autres canaux. Les services de messagerie tels que WhatsApp sont par exemple devenus un moyen pratique de communication interne.

En effet, de nombreux collègues se déplacent constamment dans l'établissement et ne sont donc pas toujours joignables par ordinateur. L'utilisation du téléphone est possible mais également restreinte. Les personnels soignants et médecins ne peuvent évidemment pas répondre lorsqu'ils sont en consultation. Et il leur arrive parfois d'oublier de rappeler après coup. Ainsi, il peut se passer du temps avant d'être en

mesure de discuter d'une constatation cruciale. Les messageries instantanées permettent de gérer plus facilement la communication. Les collègues répondent lorsqu'ils ont le temps et rien ne tombe dans l'oubli.

Les avantages d'une app pour entreprises destinée aux collaborateurs

Claudio Badertscher, Business Development Manager Healthcare DACH chez Connect Solutions AG, explique à ce sujet : «Les personnes qui échangent des informations et données dans le cadre d'infrastructures critiques (IC) ne doivent en aucun cas utiliser de messageries gratuites à cet effet. Des règles de protections des données particulièrement strictes auxquelles ces apps ne satisfont pas s'appliquent en effet à ces infrastructures. Les apps sûres et certifiées destinées aux collaborateurs sont l'alternative à WhatsApp & co et permettent de gérer la communication interne de manière simple et, surtout, en toute sécurité.»

Pour les raisons suivantes, les collaborateurs évoluant dans des infrastructures critiques ne devraient échanger que par le biais d'apps spécialement conçues à cet effet:

- Les données ne sont pas enregistrées sur des serveurs américains, au contraire de WhatsApp.
- Elles sont enregistrées au niveau local ou sur place, conformément à la norme mondialement reconnue ISO 27001.

Danger: médecins, personnels soignants et assistants partagent des informations avec WhatsApp

Pour ces motifs, 98% des médecins hospitaliers utilisent WhatsApp & co chaque jour au travail. Ils envoient des photos de leurs constatations ici et là, échangent sur la progression de la maladie de patients et envoient des diagnostiques sur le groupe de discussion commun. C'est la conclusion à laquelle est parvenue une étude de l'institut allemand de protection des données (DDI).

Ce qui simplifie le travail du point de vue des médecins s'avère hautement risqué sur le plan de la protection des données. En tout cas lorsque la communication se fait par des messageries instantanées gratuites telles que

WhatsApp car elles ne respectent aucunement les exigences strictes que fixent les législateurs envers les infrastructures critiques.

Expertise de l'infrastructure informatique interne

La situation peut notamment devenir critique car le réglage par défaut de WhatsApp prévoit que les photos transmises sont automatiquement enregistrées sur le disque dur du téléphone du destinataire. De là, elles se retrouvent facilement dans le Cloud. S'il s'agit d'un appareil privé utilisé pour la communication interne, il peut arriver que des tiers non autorisés aient automatiquement accès à ces données.

En outre, les collaborateurs qui se consacrent à un nouveau défi professionnel ne sont pas toujours supprimés des groupes de discussion. Ils sont alors amenés à voir des données sensibles de patients sans y être autorisés.

Dans les deux cas, il s'agit de violations par négligence grave de la protection des données. Par conséquent, les employeurs dans le secteur de

la santé ne doivent pas examiner uniquement les serveurs internes et les systèmes directement reliés lorsqu'ils évaluent leur infrastructure informatique. Il faut aussi qu'ils se demandent de quelle façon communiquent leurs employés.

Communication via messagerie instantanée: est-il conseillé de l'interdire?

Cela ne signifie pas que les responsables dans les hôpitaux et les autres institutions de santé doivent interdire à leurs collaborateurs de communiquer par messagerie instantanée. Force est de constater que la communication n'importe où n'importe quand offre par ailleurs beaucoup d'avantages:

- Amélioration de la collaboration et du sentiment d'appartenance grâce au lien direct et permanent avec les collègues.
- Augmentation sensible de la qualité du suivi des patients grâce aux échanges plus fiables.

La solution consiste à mettre en place une app professionnelle destinée aux collaborateurs pour la communication interne. Elle permet par exemple d'échanger sans risque des radiographies ou des dossiers médicaux.

- Ce certificat est synonyme de sécurité maximale des informations, données et systèmes et il respecte les lois de sécurité informatique allemandes et suisses.
- L'entreprise qui utilise l'app destinée au personnel demeure propriétaire des données transmises. Cela permet d'éviter le partage non autorisé, l'enregistrement ou la duplication des données.
- Les autorisations d'accès à l'app d'entreprise bénéficient d'une gestion centralisée et sont actualisées en permanence.
- Si un collaborateur quitte son emploi, son compte expire automatiquement.

Pour résumer: Avec une app spécialement conçue pour le personnel, les employeurs du secteur de la santé ne résoudront pas tous leurs problèmes de communication interne comme par magie, mais presque!

1. Ils satisfont aux préférences de communication de leurs collaborateurs et renforcent leur attachement.
2. Ils assurent la protection de la sphère privée de leurs patients.
3. Ils peuvent compter sur un partenaire fiable qui garantit un niveau maximal de sécurité. En effet, l'app est régulièrement contrôlée par des experts externes.

De cette manière, les employés n'ont plus à se faire aucun souci en matière de protection des données. N'est-ce pas merveilleux?

Auteure

Sonja Dietz

Informations complémentaires

Connect Solutions AG
Téléphone +41 44 500 22 15
www.qnnect.com