Lorsque les médecins et le personnel soignant échangent des données de patients sensibles, le risque est immense

L'app Qnnect: communication interne avec protection intégrale des données

Le manque de temps se fait énormément sentir mais le besoin de travailler en toute sécurité reste légitime. En Suisse, des centaines de milliers de demandes, d'informations et d'images sont échangées par le biais de messageries privées au sein des hôpitaux, établissements de soins et organisations d'aide et de soins à domicile. C'est rapide, efficace et très courant dans de nombreux domaines de la vie. Ce qui paraît anodin revêt en fait une importance cruciale. Les systèmes utilisés fonctionnent sur les serveurs d'entreprises tierces étrangères, raison pour laquelle la protection des données repose sur des bases fragiles. «La crainte d'une catastrophe touchant les données est omniprésente», selon Claudio Badertscher, Business Development Manager Healthcare chez Qnnect Solutions AG, Zurich.

Récemment, le niveau de risque global dans le domaine eHealth a été étudié dans une enquête de l'Université des Sciences Appliquées de Zurich (ZHAW) sur le thème Digital Health. Conclusion: un tiers des 25 experts hospitaliers interrogés au sein d'un réseau jugent réaliste qu'une catastrophe relative aux données touche les systèmes du secteur suisse de la santé dans les dix prochaines années. On identifie surtout un potentiel de risques important dans le piratage des données de patients ou la paralysie de systèmes informatiques. Plus d'un tiers des experts prévoient une probabilité de survenance d'au moins 90 %.

Claudio Badertscher, Business Development Manager Healthcare chez Qnnect Solutions AG, Zurich

En parallèle, les scientifiques de l'Institut pour l'économie de la santé de Winterthour (WIG) mettent en garde dans leur étude «Digital Health – l'avenir du système de santé suisse» contre le trafic d'informations non protégé via des services de messagerie privés car il n'est pas garanti que les exploitants de ces systèmes ne réutilisent pas ou ne transmettent pas des données.

(Pas) une guerre des mondes

Dans les hôpitaux, les cabinets médicaux et les soins quotidiens, l'ancien et le nouveau monde se télescopent. Chacun a son smartphone dans la poche de sa blouse mais les notes sont encore généralement écrites à la main. D'autre part, la nouvelle génération se montre déconcertée devant un télécopieur. Sur les tableaux en liège, les plans de service sont punaisés sous forme papier. Mais une chose semble inévitable et plus qu'une question de temps. La communication sur les réseaux sociaux est un processus solidement engagé. Ce qui parait de plus en plus évident pour bon nombre de gens, en tout état de cause chez les jeunes, se propage à la vitesse de l'éclair dans le milieu professionnel.

Il faut assurément être bien courageux pour passer aux formes de communication numériques. Mais l'heure est venue car une multitude de collaboratrices/teurs le fait de toute façon également au travail: par conséquent, les échanges de réflexions et d'idées au sein d'une équipe se conformeront tôt ou tard à la communication via les réseaux sociaux dans la vie privée – directe, rapide et informelle.

Il faut un programme de Chat

Dans la sphère privée, la mutation a eu lieu depuis longtemps. WhatsApp par exemple compte plus d'un milliard d'utilisateurs à travers le monde et sert surtout pour la communication privée. Mais ce type de programmes de Chat tend également à être de plus en plus utilisé au travail, notamment pour échanger des informations scientifiques entre collègues, discuter des propositions de thérapie, transmettre rapidement des infos importantes, échanger des images, etc.

Cela ne surprend personne que les appareils mobiles soient très répandus précisément dans le domaine hospitalier. On les trouve dans toutes les blouses de travail et poches de pantalon. Une

Pêcher dans la gestion des données sensibles peut coûter cher, au civil comme au pénal. Qui prend au sérieux la protection des données choisira de renoncer aux services de messagerie peu sûrs hébergés sur des Clouds à l'étranger.

enquête effectuée auprès de médecins et d'infirmières et infirmiers dans cinq cliniques du National Health Service (NHS) en Grande-Bretagne a ainsi montré que 90% des médecins jugeaient leurs appareils mobiles utiles voire très utiles.

Près de la moitié utilisent le smartphone pour des services de messagerie basées app. Beaucoup ont indiqué avoir pris des photos de plaies avec leur appareil pour ensuite les envoyer, ainsi que des radiographies, de manière non cryptée.

Une app sûre est indispensable

Une sorte de routine professionnelle comportant des risques semble déjà installée et la Suisse n'échappe pas à ce phénomène. Le souhait d'une app sûre apparaît donc prioritaire. Les personnes interrogées de l'étude britannique sont tout à fait conscientes que les échanges d'informations relatives aux patients via des services non sécurisés sont délicats. Plus de deux tiers des médecins et un tiers du personnel soignant souhaitent en effet avoir une app sûre permettant un échange efficace et juridiquement autorisé de données de patients.

«C'est indispensable du point de vue de la protection des données», souligne Claudio Badertscher, «naturellement, en cas de crise, la direction d'un hôpital pourrait éventuellement argumenter qu'un médecin imprudent a agi de sa propre initiative et sous sa propre responsabilité. Mais cette stratégie résisterait mal à l'épreuve du temps. Je vois déjà les gros titres dans le 20 Minutes, un hôpital néglige la protection de données sensibles de patients. Le préjudice en termes de réputation serait immense car plusieurs milliers de lecteurs auraient déjà digéré le message négatif avant même d'être sorti du train sur le chemin entre le travail et la maison.»

Par conséquent, le souhait d'un canal de données fiable semble plus que légitime car selon notre interlocuteur, «il s'agit en fin de compte de données sanitaires hautement sensibles. Un Cloud quelque part sur la planète ne suffit pas à garantir ni la protection des données ni le secret professionnel.»

A cela s'ajoute le fait que d'autres nuages d'orage s'amoncellent. En Allemagne à l'avenir, il sera permis de surveiller des services de messagerie tels que WhatsApp en cas d'enquête pénale. Ce développement dans le cadre de la lutte antiterroriste montre qu'il est possible de lire une communication avant qu'elle ne soit cryptée. – Badertscher: «La proximité de WhatsApp avec Facebook n'inspire également pas vraiment confiance: La crainte réside dans le fait que des données pourraient être échangées. Naturellement, la communication mobile ne s'arrête pas aux portes de l'hôpital ou du cabinet médical. Les services de messagerie peuvent ainsi améliorer et rendre plus efficaces les échanges dans le milieu médical et au sein des équipes de soins. Mais ils doivent pour cela être sûrs.»

Nouvelles directives, nouvelles exigences

Mieux vaut prévenir que guérir. C'est d'autant plus évident lorsqu'on regarde la révision du règlement général européen sur la protection des données. En tant que nouvelle loi sur la protection des données, il concerne toutes les entreprises actives en Europe. Les entreprises doivent adapter leurs pratiques en matière de protection des données afin de se conformer à la nouvelle loi et d'éviter de fortes amendes. Les services de messagerie tels que WhatsApp qui font partie du Shadow-IT vont donc devenir un problème particulièrement grave pour beaucoup d'entreprises. Dans le cadre des nouvelles directives, elles doivent garantir une messagerie d'entreprise conforme aux règles sur la protection des données.

Le règlement général européen sur la protection des données (RGPD) entrera en vigueur le 25 mai 2018 dans tous les états membres. Le RGPD a été développé dans le but d'harmoniser à travers l'Europe les droits et devoirs correspondants en matière de protection des données. L'objectif consiste à garantir la protection des données des citoyens européens et à améliorer la manière dont les entreprises gèrent les données personnelles et autres données sensibles et les protègent. Dans ce contexte, il est intéressant que la nouvelle loi concerne toutes les entreprises qui traitent ou enregistrent des données de citoyens européens, et ce indépendam-

Près de la moitié des médecins et soignants en hôpital utilisent le smartphone pour des services de messagerie basés sur app. Lorsqu'ils servent à prendre avec l'appareil des photos de plaies pour ensuite les envoyer, ou encore des radiographies, un cryptage devient indispensable.

ment du site d'une entreprise. Cela signifie: Le RGPD ne doit pas être uniquement respecté par les entreprises au sein de l'UE mais également par celles en-dehors, notamment les cliniques qui traitent des patients de l'espace européen.

Le moment est propice pour une solution de Chat sûre

Au regard des nouvelles règles, des risques globaux et de l'utilisation largement répandue de services de messagerie privée, il est d'autant plus étonnant que la plupart des directeurs d'hôpital ou responsables dans le domaine des soins et des services d'aide et de soins à domicile ne mettent toujours pas de solution de Chat sécurisée à la disposition des collaborateurs. En effet, c'est un secret de polichinelle que les professionnels de la médecine, des thérapies et des soins échangent via des services peu sûrs où ils envoient également des données de patients. Par ailleurs, les annonces se multiplient dans les médias à propos de pertes de données dans des hôpitaux et établissements de soins. Si des données de patients tombent en de mauvaises mains, les employés et les cliniques seront exposés à de fortes amendes et les patients en attente d'interventions non urgentes réfléchiront à deux fois avant de choisir une clinique qui a fait les gros titres.

L'issue réside dans une app qui offre tous les avantages d'une solution de Chat moderne et garantit cependant à la fois une protection intégrale des données et une sécurité technique élevée. L'app Qnnect couvre tout cela, tant en ce qui concerne les terminaux mobiles mis à la disposition par l'hôpital que les smartphones ou tablettes privées utilisés chaque jour au travail. Qnnect trouve donc un moyen de résoudre le problème lié aux services de messagerie peu sûrs.

L'app Qnnect, développée par des professionnels qui connaissent depuis longtemps le secteur de la santé. Afin d'exploiter la solution de branche en toute sécurité, elle est proposée sur le centre informatique du client ou un Cloud hautement sécurisé. Cette flexibilité relative aux types d'exploitation (sur place ou Secure Cloud) permet à un hôpital, un établissement de soins ou une organisation spitex de créer un réseau sûr.

Communiquer encore plus intensivement

Dans les institutions de santé, une communication interne sûre vaut naturellement de l'or. Là où règnent le manque de main d'œuvre et de temps, il est absolument judicieux d'échanger des informations de manière rapide et ciblée. Peu importe qu'il s'agisse de contributions importantes ou plus modestes – histoire sur une personne, innovations, évènement en équipe, conseils ou simplement une déclaration constructive. A une époque où les entreprises cherchent désespérément du personnel, cela encourage l'identification et l'engagement des collaborateurs. Les supérieurs malins saisissent leur chance et entrent régulièrement en contact via l'app Qnnect avec le groupe de collaborateurs dont ils ont la responsabilité.

Il y a suffisamment de matière. L'expérience montre que les informations dans l'intranet sont soit découvertes soit par hasard soit ignorées. Les newsletters sont souvent supprimées. Et la plupart des gens passent devant le tableau sans y prêter attention.

En revanche, les collaborateurs sont habitués à s'informer sur plusieurs plans, à diffuser active-

Au sein du Cluster

Les spécialistes de Qnnect Solutions AG travaillent dans un bâtiment avec l'EPF de Zurich et se trouvent à un jet de pierre de l'Université et de l'Hôpital universitaire – un environnement fécond et motivant. Grâce à la solution de chat Qnnect, les utilisateurs communiquent de manière efficace et sûre avec leurs équipes et leurs collaborateurs. Vous avez la maîtrise de vos données grâce à des normes de sécurité très rigoureuses. De plus, vous modernisez et simplifiez la communication interne grâce à une utilisation intuitive. Outre une satisfaction supérieure et davantage d'engagement de la part des collaborateurs, il en résulte aussi de meilleurs processus de travail et une productivité maximisée.

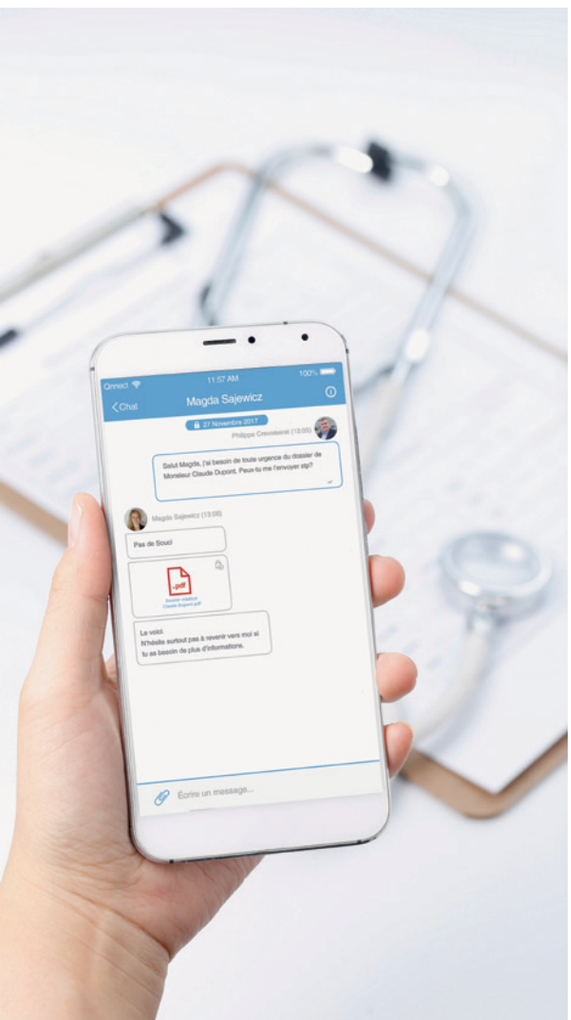
ment des nouvelles et à constamment échanger entre eux. C'est aussi de cette manière qu'ils veulent être tenus au courant et impliqués par leurs supérieurs. Voilà la seule façon pour qu'ils se sentent reconnus et contribuent à la réussite économique. Un programme de Chat sûr et spécialement adapté à l'univers professionnel comme Qnnect facilite la communication interne, en particulier parce qu'il est à la fois sûr et très rapide.

Déjà éprouvé dans le travail quotidien

La communication interne favorise le succès de l'entreprise. C'est la conclusion à laquelle parvient le Enterprise Mobile Apps Report. D'après cette étude, les applications mobiles sont déjà utilisées dans deux tiers des entreprises. Plus de la moitié des 1500 cadres interrogés aux USA, en Chine, en Inde, en Angleterre et en Allemagne trouvent qu'elles sont un facteur de réussite important et offrent par conséquent un avantage concurrentiel.

Cet avis est aussi largement partagé à Zurich où on utilise déjà l'app Qnnect à l'hôpital cantonal de Zoug ou à l'UKBB ou encore parmi les collaborateurs en déplacement au sein de Spitex Zürich Limmat. Dans ce dernier cas, la CEO Christina Brunnschweiler doit assurer jour après jour la communication entre près de 1000 collaborateurs. Depuis qu'elle mise sur l'app de Qnnect, tout est plus simple et plus efficace. Brunnschweiler parle d'une «étape-clé» de la communication interne, une partie essentielle de son travail, justement parce que les collaborateurs travaillent de manière décentralisée chez les clients et ne peuvent donc pas être joints personnellement.

L'ensemble des collaborateurs du Spitex Zürich Limmat disposent donc d'une Phablet, un mélange de téléphone et de tablette sur laquelle ils saisissent leurs prestations et peuvent aussi consulter la planification et la documentation. Il paraît logique d'utiliser les appareils également aux fins de communication interne. La CEO de l'organisation Spitex explique: «Nous avons fait des essais avec WhatsApp mais cela s'est avéré problématique pour des raisons de protection et de sécurité des données. Pour cette raison, nous communiquons principalement par deux canaux en interne: l'app de Qnnect et dans le futur aussi via notre propre système d'entreprise. Avec Qnnect, nous envoyons toutes les informations qui concernent l'entreprise telles que les messages de la direction, les changements de personnel ou les invitations à des évènements. Nous pouvons ainsi atteindre 700 employés qui sont actifs sur la plateforme.»



L'esprit d'équipe se développe chez les collaborateurs travaillant seuls

«Aujourd'hui, nous nous réjouissons que le programme de Chat encourage l'esprit d'équipe chez les collaborateurs qui évoluent en fait en électrons libres. Les chefs des équipes qui rassemblent entre 12 et 30 collaborateurs utilisent par exemple les Chats pour diffuser les comptes-rendus des réunions d'équipe afin que chacun soit au courant. Des groupes dont les membres échangent en temps réel peuvent également se constituer au sein des équipes. Moi-même en tant que supérieure, je reçois un retour direct via les fonctions de «like» et de communication. Et à partir de cela, j'ai réfléchi par exemple à étendre nos directives sur le thème du harcèlement sexuel. Grâce à ces fonctions, je peux savoir de manière simple ce qu'en pensent les employés. Nous concrétisons également les messages importants sous forme de films. Il existe ainsi une vidéo sur notre nouvelle stratégie.

Toutefois, nous ne voulons pas que nos cadres soient joignables en permanence. La Phablet est un instrument de travail que l'on peut simplement éteindre durant le temps libre. En cas d'urgence, nous envoyons de toute façon un SMS. A l'inverse, les collaborateurs ne peuvent pas utiliser la Phablet en privé. Les soignants font généralement bien la part des choses, ils apprennent cela dans leur formation.»

Christina Brunnschweiler salue le programme de Chat introduit car il encourage le sentiment de communauté. «Il me reste à savoir de quelle manière précisément. Nous effectuons actuellement un changement d'organisation que nous présentons d'abord via le programme de Chat que j'expliquerai ensuite de vive voix dans les centres Spitex. Les collaborateurs sont donc d'abord informés par voix numérique puis ils ont l'occasion d'en discuter avec moi. Outre la communication numérique, j'accorde une grande importance au dialogue direct.»

Informations complémentaires

Aurélien Giraud-Rauch
Manager French speaking markets
Qnnect Solutions AG
Clausiusstrasse 50 8006 Zürich
Téléphone 078 628 54 00
www.qnnect.com

Amendes draconiennes et énormes risques de réputation

Pécher dans la gestion de données particulièrement sensibles telles que celles sur la santé peut coûter cher en Suisse. La situation a deux faces: une pénale (système de sanction dans le cadre de la loi sur la protection des données) et une civile. Dans le premier cas, il est question d'amendes parfois considérables, dans le second cas de demandes de dommages-intérêts pouvant également s'avérer très importantes.

Le projet révisé de révision totale de la loi suisse sur la protection des données prévoit une hausse de la limite supérieure des amendes de 10 000 à 250 000 francs au maximum.

Avec l'enregistrement de données en interne (sur le propre serveur) ou sur un Cloud situé en Suisse, hébergé par un fournisseur de Cloud suisse, lequel dispose de toutes les certifications nécessaires, vous faîtes un pas important vers le respect des dispositions relatives à la protection des données et contribuez à éviter que votre entreprise ne subisse une procédure coûteuse et préjudiciable en termes de réputation avec les autorités de surveillance (PFPDT) ainsi que des amendes élevées.