# Cryptage des courriers électroniques contenant des données personnelles à protéger : pour que ce qui est confidentiel le reste

Autor(en): **Seifert, Elisabeth**

Objekttyp: **Article**

Zeitschrift: **Curaviva : revue spécialisée**

Band (Jahr): **9 (2017)**

Heft 3: **Mort annoncée de l'EMS : les modèles d'habitat pour personnes âgées se réinventent**

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-841497

Cryptage des courriers électroniques contenant des données personnelles à protéger

# Pour que ce qui est confidentiel le reste

**Dans les institutions, le cryptage des courriels contenant des données personnelles confidentielles est encore peu usuel. Curaviva Suisse et Health Info Net AG collaborent pour promouvoir une prise de conscience en faveur d'une communication sécurisée.**

Élisabeth Seifert

La communication par e-mails est aujourd'hui incontournable dans notre société. Mais c'est à peine si nous avons conscience que des tiers peuvent aussi les lire dès le moment où notre message électronique, qui ne regarde qu'un seul destinataire particulier, est envoyé. Sur la route vers leur destinataire, les courriels sont mis en mémoire à plusieurs reprises, processus au cours duquel les données peuvent être copiées, modifiées mais aussi supprimées. Peter E. Fischer, président de Swiss Internet Security Alliance (SISA) et professeur en sécurité de l'information et protection des données dans le domaine de la santé à la Haute école de Lucerne, compare les courriels non cryptés à des cartes postales que tout le monde peut lire librement sur le trajet vers leur destinataire.

Et c'est bien pour cette raison qu'on n'envoie pas des données et des informations confidentielles par carte postale. Généralement, on se pose moins de questions quand on envoie des courriels au contenu confidentiel. C'est particulièrement délicat dans les domaines de la santé et du social où les prestataires de services échangent en permanence sur la façon dont se déroule le traitement d'une personne en particulier, y décrivent les symptômes, émettent des diagnostics et prescrivent des médicaments. Quand un dossier médical devient public, cela peut avoir des conséquences indésirables, avertit Peter E. Fischer. «Il peut arriver que quelqu'un soit de ce fait socialement exclu ou perde son emploi.»

**En route vers son destinataire, un e-mail peut être copié, modifié et supprimé.**

La confidentialité doit donc être assurée lorsqu'il s'agit de données personnelles qui doivent être protégées. Le préposé fédéral à la protection des données et à la transparence a édité un «Guide pour le traitement des données personnelles dans le domaine médical». Il y fait notamment remarquer que lors du transport de données personnelles par l'intermédiaire des divers supports informatiques, il convient de recourir à des méthodes de chiffrement des données. À cet effet, il se réfère aux principes ancrés dans la Constitution fédérale et aux dispositions légales. La loi sur la protection des données, exige «des mesures appropriées techniques et organisationnelles» pour empêcher que des tiers non autorisés manipulent des données personnelles. Et l'ordonnance de cette même loi précise qu'en transmettant des données personnelles et en transportant des supports de données, il faut empêcher que les données «puissent être lues, copiées, modifiées ou supprimées sans autorisation».

Dans les hôpitaux et chez les médecins ainsi que dans la grande majorité des organisations d'aide et de soins à domicile, il est aujourd'hui généralement courant de crypter les e-mails contenant des données personnelles sensibles. Selon Peter E. Fischer, les courriels cryptés ressemblent à des lettres fermées et cachetées. Il existe sur le marché une multitude de procédés de cryptage. En Suisse, l'offre la plus étendue est celle de Health Info >>

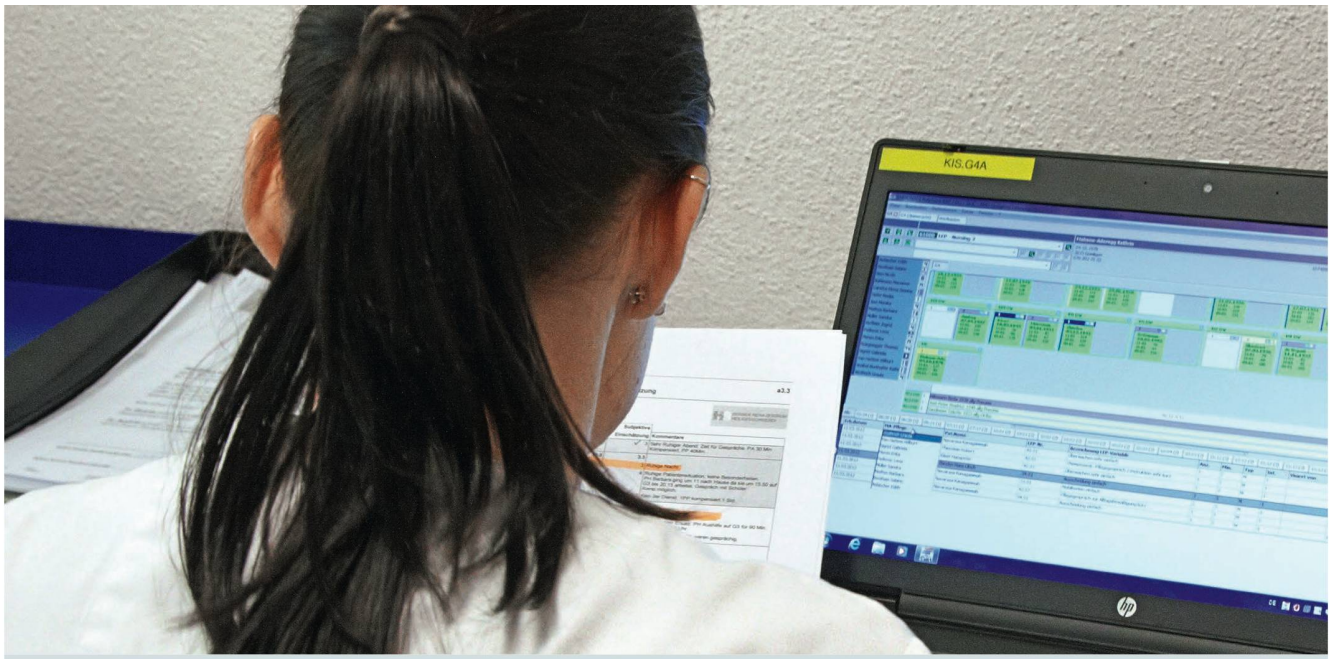
Texte traduit de l'allemand

Net AG (HIN). «D'autres offres sont souvent plus avantageuses, voire gratuites», explique-t-il. «Mais ces solutions, outre une moins bonne pénétration du marché, présentent l'inconvénient de nécessiter de la part de leur utilisateur une certaine compréhension de l'informatique».
Le cryptage de courriels proposé par HIN est, au contraire, facile à gérer, assure ce spécialiste qui, par ailleurs, n'entretient aucune relation commerciale avec Health Info Net AG. L'envoi des messages électroniques se fait via les logiciels de messagerie habituels. Les messages eux-mêmes sont cryptés «en arrière plan» sans même que les utilisateurs s'en aperçoivent, souligne Peer Hostettler, responsable du marché chez Health Info Net AG. En l'occurrence, ce cryptage ne fonctionne pas seulement pour les courriels échangés entre les membres de la communauté HIN mais à tous les autres destinataires.

**Le chiffrement des courriels est encore trop peu répandu dans les EMS.**

**De l'importance des courriels à l'ère de la cybersanté**

Pourtant le chiffrement des courriels est encore trop peu répandu dans les EMS, bien qu'on y envoie de nombreux messages électroniques contenant des informations confidentielles sur l'état de santé des résidents. En collaboration avec Curaviva Suisse, HIN soumet actuellement aux institutions membres une offre spéciale par le biais du portail «HIN Curaviva Gateway». «Diverses institutions membres nous ont interpellés à propos du Mail HIN qui a la plus large diffusion en Suisse et qui est utilisé, notamment, par les services d'aide et de soins à domicile», déclare Markus Leser, responsable du Domaine spécialisé personnes âgées de Curaviva Suisse, pour expliquer la collaboration avec Health Info Net AG.
Nicolai Lütschg, délégué de la région du nord-ouest de la Suisse au sein du groupe de pilotage E-health de Curaviva Suisse et directeur de la communauté de référence E-Health Argovie constate lui aussi un besoin grandissant, dans les EMS, d'information sur la digitalisation galopante dans le domaine de la santé. Au plus tard d'ici 2022, ces établissements devront rejoindre une communauté de référence pour pouvoir gérer les dossiers électroniques des patients. En l'espèce, on accorde une grande attention à la transmission sécurisée des données personnelles et médicales.
Toutefois, à ce stade, on ne connaît pas encore le rôle que joueront les e-mails classiques à l'ère de la cybersanté. La communication sur les plateformes e-health, par lesquelles transitera aussi l'échange vers les dossiers électroniques des patients, n'est pas basée sur les messages électroniques. Mais le trafic des courriels dans les communications des prestataires de services entre eux devrait cependant conserver toute son impor-




Les EMS envoient de nombreux e-mails contenant des informations confidentielles sur l'état de santé des résidents. Le cryptage des courriels est cependant encore peu pratiqué. Photo: Martin Glauser

tance pendant longtemps encore. Déjà parce que chaque résident, respectivement chaque patient peut décider lui-même de l'ouverture d'un dossier électronique du patient le concernant. Ensuite, parce que les prestataires de soins ambulatoires ne sont pas obligés tenir des dossiers électroniques de leurs patients.

**Les communications internes ne sont pas automatiquement sécurisées**

Le cryptage généralisé des courriels concerne surtout les établissements d'une certaine taille, précise Nicolai Lütschg. En partent chaque jour des dizaines d'e-mails avec des données sensibles à destination des hôpitaux, des médecins mais aussi de particuliers, donc hors des murs de leur propre organisation. En revanche, dans les EMS de petite et moyenne taille, l'échange de courriels se fait généralement à l'intérieur de l'institution. Mais ces courriels internes sont gérés par un serveur in-house. «Si ces serveurs sont bien entretenus et correctement configurés, ils sont sûrs», Nicolai Lütschg en est persuadé. Un avis que peut partager le spécialiste de la sécurité des données Peter E. Fischer: «La sécurité des communications internes est garantie, pour autant que le système central ainsi que chaque ordinateur soient toujours techniquement actuels, que toutes les mises à jour aient été installées, surtout pour le firewall et la protection des virus.» Or, il constate que c'est précisément dans les petites et moyennes structures que la maintenance des systèmes laisse le plus souvent à désirer. La Swiss Internet Security Alliance offre des outils gratuits pour contrôler les ordinateurs et, si nécessaire, les nettoyer.

Dans leurs communications externes, surtout celles avec des médecins de premier recours et des spécialistes, de nombreux homes utilisent encore le fax classique. Cette façon de transmettre des données est, selon Nicolai Lütschg, relativement sûre. Néanmoins Peter E. Fischer objecte qu'en principe, une transmission par fax peut aussi être interceptée. La différence tient au fait que dans le cas d'un fax on ne peut capter les données qu'au moment même de la transmission.

**Quand des données sont piratées**

«Dans les communications entre organisations, chaque institution doit juger pour elle-même quelle offre est la plus appropriée pour la sécurité des échanges, par exemple le cryptage des courriels», affirme Nicolai Lütschg. Peer Hostettler, de Health Info Net AG, rappelle les dispositions légales qui obligent les prestataires de services dans les domaines de la santé et du social à prendre des mesures de sécurité pour la transmission de données. De plus, les recommandations de la protection fédérale des données et de la transparence figurant dans le «Guide pour le traitement des données personnelles dans le domaine médical» cité plus haut, ont valeur juridique. La non observation de ces recommandations peut entraîner des conséquences pénales si certaines données sont effectivement volées. Dès le mois de mai 2018, une loi de protection des données plus sévère entrera en vigueur en Suisse avec des exigences nettement plus élevées et des peines plus lourdes en cas de non-respect, rappelle Peter E. Fischer. ●

## «Sécurité traitée à la légère»

Le centre pour seniors d'Uzwil, dans le canton de St-Gall, travaille depuis trois ans avec des courriels cryptés et recourt pour cela aux services de Health Info Net AG. «Dans les EMS, la sécurité des données est souvent traitée à la légère», constate le directeur Kurt Marti. Avec ses 175 lits, le centre pour seniors d'Uzwil fait plutôt partie des grandes institutions. L'ensemble des échanges de courriels des quarante-cinq postes PC est crypté, peu importe qu'il s'agisse de courriels internes ou entre organisations. «En cryptant l'ensemble des communications électroniques, je ne dois plus me préoccuper de leur sécurité», reconnaît Kurt Marti. La décision de recourir à HIN tient surtout à sa large diffusion auprès des médecins. Les résidences Tertianum, notamment, travaillent dans l'ensemble de la Suisse avec HIN Mail. Actuellement, dix à vingt autres institutions s'intéressent à l'offre de HIN. (esf)