



Schweizer E-Health

Verschlüsselte E-Mails zwischen Arzt und Patient

von Hartmut Wiehr

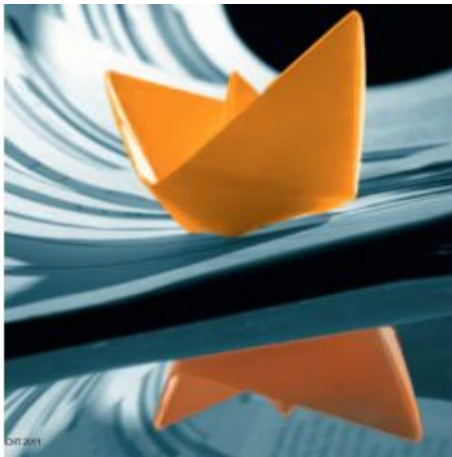
Inhalt

E-Mail-Verschlüsselung.....	4
Ziele: Behandlungserfolg steigern, Kosten senken.....	4
E-Mail-Missbrauch explodiert.....	5

Verschlüsselte E-Mails zwischen Arzt und Patient

von Hartmut Wiehr

Über die Plattform Health Info Net können Ärzte und Patienten in der Schweiz neuerdings Dokumente wie Laborberichte und Befunde verschlüsselt austauschen.



Das Schweizer Netzwerk HIN (Health Info Net) verspricht eine sichere E-Mail-Kommunikation zwischen Ärzten und Patienten. Gegen alle Gefahren von außen.
Foto: HIN

Technologie spielt in der kleinen Schweiz vielleicht eine größere Rolle als in den europäischen Nachbarländern. Dies zeigt auch ein Beispiel aus dem **Gesundheitswesen**¹. So verfügt man mit HIN (Health Info Net) über eine moderne eHealth-Plattform im Schweizer Gesundheitswesen. Sie ermöglicht den Teilnehmern eine sichere und datenschutzkonforme Kommunikation, entsprechend den landesüblichen Standards und Gesetzen.

Die **HIN (Health Info Net AG)**² wurde 1996 von der FMH, dem Berufsverband der Schweizer Ärztinnen und Ärzte, und weiteren Partnern gegründet. Sie ist bis heute in Ärztehand. Laut Angabe von HIN hat man aktuell rund 14.500 Abonnenten aus dem Gesundheitswesen. Außerdem sind über 350 Institutionen wie zum Beispiel Krankenhäuser, Labors, Apotheken und Krankenkassen ebenfalls mit der HIN-Plattform verbunden.

Neben dem brancheninternen Austausch von E-Mails ermöglicht HIN "dank der aufgebauten **PKI**³ (Public Key Infrastructure) auch einen sicheren und kontrollierten Zugriff auf eine Vielzahl geschützter Internet-Applikationen (Secure Web Access oder Single Sign-on) im Gesundheitsbereich", heißt es bei den Betreibern.

¹ <http://www.cio.de/healthcareit/analysen/2905806/>

² <http://www.hin.ch/>

³ <http://www.cio.de/strategien/808217/>

E-Mail-Verschlüsselung

Neu hinzugekommen zum Portfolio ist jetzt die verschlüsselte Versendung von E-Mails auch an Patienten. Mit der von SEPPmail und HIN entwickelten Plattform "Secure Mail GLOBAL" kann man das Dienstleistungsangebot im Bereich Secure E-Mail deutlich erweitern. Die Lösung ermögliche es den HIN-Teilnehmern, "E-Mails auch an Empfänger außerhalb des HIN-Netzwerkes – zum Beispiel an Patienten – verschlüsselt zu verschicken". Die Empfänger ihrerseits könnten dann eingegangene Secure E-Mails ebenfalls wieder verschlüsselt beantworten. Dazu müssen sie nicht über die im HIN-Netzwerk benutzte Software verfügen.

Für diese Lösung wird ein Push-Verfahren eingesetzt, das die verschlüsselte Nachricht als Attachment an den Empfänger überträgt: "Um die **E-Mail-Nachricht**⁴ zu lesen, benötigt der Empfänger ein Passwort, das ihm bei der erstmaligen Nutzung via SMS, Telefon oder Fax zugestellt wird." Die weitere Nutzung danach sei dann ohne ein zusätzliches Passwort möglich.

Ziele: Behandlungserfolg steigern, Kosten senken



Das HIN-Netzwerk integriert verschiedene Komponenten und sorgt für eine abgesicherte Kommunikation.
Foto: HIN

Für den HIN-Geschäftsführer Christian Greuter ist mit dieser Lösung bereits ein Schritt in die Zukunft des Gesundheitswesens getan worden: "Dank Secure Mail GLOBAL kommunizieren Ärzte und Patienten direkt und sicher miteinander. Das eröffnet ganz neue Möglichkeiten für die Patientenninformation. Auch der sichere Informationsaustausch mit ausländischen Partnern ist jetzt möglich."

Mit dieser neuen Form des elektronischen Datenaustauschs könnte die Wirksamkeit medizinischer Behandlungen gesteigert werden. Bei HIN ist man überzeugt, dass sich so auch die Kosten des Gesundheitswesens senken ließen. Beschleunigt werde die Entwicklung dadurch, dass immer mehr Patienten Erfahrung im Umgang mit elektronischen Medien hätten. Von daher erwarten sie auch, ihre Befunde, Laborberichte und andere gesundheitspezifische Dokumente via E-Mail zu erhalten oder über das Web einzusehen.

⁴ <http://www.cio.de/email/2884805/>

E-Mail-Missbrauch explodiert

Dabei müssen natürlich die **Risiken**⁵ des E-Mail-Verkehrs ausgeschaltet werden. Zumal der kriminelle Missbrauch von E-Mails immer mehr zunimmt. Laut HIN stehen Programme für Sniffing (Abfangen von E-Mails), Spoofing (Vortäuschung eines falschen Absenders), Passwort-Cracking und andere Werkzeuge frei im Internet zum Download bereit. Installierte Antiviren-Software und Firewalls täuschen dagegen nur eine scheinbare Sicherheit vor.

Das Schweizer Modell sollte deshalb auch in Deutschland Schule machen. Die e-Health-Plattform umfasst mit ihren 14.500 Mitgliedern mehr als 80 Prozent aller Schweizer Hausärzte. Sie stellt das größte medizinische Netzwerk im Nachbarland dar. Neben Secure Mail GLOBAL von SEPPmail setzt man bei HIN folgende Security-Komponenten ein: Identity- und Access-Management von Oracle, Public-Key-Infrastruktur (PKI) von QuoVadis sowie java-basierter HIN-Client von Zühlke Engineering.

21.03.2013

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in CIO unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von CIO aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.



<http://www.cio.de/healthcareit/strategien/2909552/>

⁵ <http://www.cio.de/knowledgecenter/security/2907602/>