FSDZ RECHTSANWÄLTE & NOTARIAT AG
ZUGERSTRASSE 76b
CH-6340 BAAR
Tel. ++ 41 41 727 60 80
ameti@fsdz.ch

Warum die Ärzteschaft Gesundheitsdaten konsequent verschlüsselt per E-Mail versenden soll

25.4.2022

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Milica Stefanovic
MLaw Rechtsanwältin[2]
stefanovic@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Carmen De la Cruz
Rechtsanwältin und Notarin 1,2
Eidg. dipl. Wirtschaftsinformatikerin
Industriestrasse 7
6300 Zug
delacruz@lexcellence.swiss

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt[1,2]
BSc Wirtschaftsinformatik

Zugerstrasse 76b
CH-6340 Baar
Tel.: ++41 41 541 79 60
info@boehnilaw.ch
www.boehnilaw.ch
.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug

Interne Verfasserin: MLaw Argonita Ameti

E-Mails sind heutzutage im Geschäftsverkehr als Kommunikationsmittel kaum noch wegzudenken. Für das medizinische Umfeld gelten für den Versand von E-Mails verschärfte Sicherheitsanforderungen. Vertrauliche Patientendaten dürfen daher nur per E-Mail versendet werden, wenn Massnahmen zum Schutz vor unbefugter Kenntnisnahme ergriffen werden. Hier leistet die Verschlüsselung der E-Mail-Nachrichten einen wesentlichen Beitrag.

Beim Versenden von unverschlüsselten Nachrichten besteht die Möglichkeit, dass der Inhalt der Nachrichten gelesen, kopiert oder manipuliert wird. Sensible Daten sind daher zum Schutz vor Zugriff durch Unbefugte zu verschlüsseln. Praxisinhaber gelten nach Art. 24 Abs. 1 und Art. 32 DSGVO als datenschutzrechtlich Verantwortliche und sind verpflichtet, technische und organisatorische Massnahmen für eine verordnungskonforme Verarbeitung von Patientendaten zu treffen. Dabei ist der aktuelle Stand der Technik zu berücksichtigen, d.h. technische Massnahmen, deren Geeignetheit und Effektivität erwiesen ist (Art. 32 DSGVO). Bei Gesundheitsdaten ist eine Verschlüsselung als geeignet, erforderlich und angemessen im Sinne von Art. 32 DSGVO anzusehen. Das Versenden von unverschlüsselten E-Mail-Nachrichten mit Patientendaten widerspricht insofern den Vorgaben des DSGVO und ist deshalb immer sanktionsbewährt.

Das revidierte Datenschutzgesetz (revDSG) sieht neu Bussen in der Höhe von bis zu CHF 250'000.-- für Datenschutzverstösse vor (Art. 61 – 63 revDSG). Die revDSG-Bussen richten sich gegen die verantwortliche natürliche Person. Für die vorsätzliche Verletzung von Sorgfaltspflichten sowie der beruflichen Schweigepflicht aufgrund einer schlecht geführten Informatik trägt jeder Arzt persönlich die volle Verantwortung und wird auf Antrag mit einer entsprechenden Busse bestraft.

Der Berufsverband der Schweizer Ärztinnen und Ärzte FMH empfiehlt Patientendaten, die via E-Mail ausgetauscht werden, stets zu verschlüsseln. Durch die Kommunikation über die Plattform Health Info Net (HIN) kann auf eine einfache Art und Weise eine sichere und datenschutzkonforme Kommunikation, entsprechend den landesüblichen

Standards und Gesetzen hergestellt werden. Um die Dienste der Plattform zu nutzen, ist eine HIN-Identität notwendig. Die HIN vergibt eine elektronische Identität, nachdem ein mehrstufiger Verifikationsprozess die Ausweispapiere sowie berufsspezifischen Attribute geprüft hat. Zudem ist mit der von der HIN entwickelten und im Abonnement enthaltenen Plattform „HIN Secure Mail GLOBAL“ jeder Arzt ohne Aufwand in der Lage, jedem Patienten direkt und automatisch eine verschlüsselte E-Mail zu versenden. Die Empfänger können die eingegangenen Secure E-Mails ebenfalls wieder verschlüsselt beantworten, ohne über die im HIN-Netzwerk benützte Software zu verfügen. Ferner bietet die HIN Plattform auch den „HIN TALK VIDEO“ Service an, die End-to-End verschlüsselte Audio- und Videokonferenzen mit anderen Mitarbeitenden oder Patienten ermöglicht und ebenfalls im Abonnement enthalten ist.

Ob die Patienten ausnahmsweise von Verschlüsselungslösungen rechtswirksam verzichten können, ist rechtlich umstritten. Die DSGVO sieht jedenfalls keine Rechtsgrundlage hierfür vor. Die Patienten müssen in einem solchen Fall mindestens über die Risiken von unverschlüsselten E-Mail-Nachrichten orientiert und Ihnen alternative und sichere Kommunikationsmöglichkeiten angeboten werden (z.B. Verschlüsselung der E-Mail, telefonisch, postalisch). Ein Restrisiko bleibt jedoch bestehen. Die Aufsichts- und Zulassungsbehörde kann solche Einwilligungserklärungen im Einzelfall als unzulässig erklären, wodurch sich der verantwortliche Arzt einer Datenschutzverletzung aussetzt, die für ihn strafrechtliche sowie aufsichtsrechtliche Konsequenzen haben kann.

Der unverschlüsselte E-Mailverkehr im Gesundheitswesen kann die Vertraulichkeit und die Einhaltung der ärztlichen Schweigepflicht nicht gewährleisten. Insofern ist eine Verschlüsselung von sensiblen Patientendaten zwingend notwendig, womit das Einsehen der E-Mails auf dem Weg zum Empfänger verunmöglicht wird. Ferner führt bei Berufsgeheimnisträgern wie Ärzten eine Verletzung der Geheimhaltungspflicht entsprechend den Strafbestimmungen zu einer Geld- oder Freiheitsstrafe oder einer hohen revDSG-Busse und kann zudem aufsichtsrechtliche Konsequenzen zur Folge haben. Ärzte kommen dementsprechend nicht darum herum, beim digitalen Versenden von Gesundheitsdaten mit allen Dritten (Patienten, Spitälern oder anderen Gesundheitsfachpersonen) konsequent auf Verschlüsselung zu setzen.