stomatologi[e]

der e-newsletter der österreichischen gesellschaft für zahn-, mund- und kieferheilkunde

SICHERER UMGANG MIT DATEN IN DER TÄGLICHEN PRAXIS

© OÖG

ÖGZMK

Ing. DI (FH) Rainer Kloimstein
Donaublick 6
4074 Stroheim

PRAKTIKERSAMSTAG 2022 „WISSENSPOWER FÜR ZAHNÄRZTINNEN“ LINZ 30.4.2022

Der richtige Umgang mit Informationen ist von großer Bedeutung. Die Verfälschung oder die Nichtverfügbarkeit von Informationen bzw. Daten kann u. a. die Sicherheit der PatientInnenbehandlung massiv gefährden.

Die Offenlegung von personenbezogenen Daten (insbesondere Gesundheitsdaten) kann neben einem großen Imageschaden auch sehr hohe Geldstrafen zur Folge haben..

BEISPIELE AUS DEM GESUNDHEITSBEREICH

vom 30. März 2022

Über 43‘000 medizinische Dateien von zwei Neuenburger Arztpraxen wurden geleakt. Darunter scheinen sensible Daten wie Krankheitsgeschichten und medizinische Behandlungen zu sein.

Aus
<https://www.inside-it.ch/tausende-schweizer-gesundheitsdaten-landen-nach-hackeran-griff-im-darknet-20220330>

Die Einhaltung der nachfolgenden fünf Grundregeln zum Umgang mit Informationen sollten dabei helfen, dass es zu keinen Vorfällen kommt.

INFORMATIONEN RICHTIG ERSTELLEN

Bei der Erstellung und Bearbeitung von Informationen muss darauf geachtet werden, dass man dabei nicht beobachtet wird.

INFORMATIONEN RICHTIG AUFBEWAHREN/VERWENDEN

Vertrauliche Informationsträger (z. B. Papierdokumente, mobile Endgeräte und Datenträger) müssen gesichert aufbewahrt werden, damit keine unbefugten Personen die Informationen einsehen oder verändern können (z. B. PatientInnenakten nicht unbeaufsichtigt lassen.) Verwenden Sie sichere Passwörter mit Zahlen, Buchstaben und Sonderzeichen. Geben Sie diese nicht weiter und notieren Sie diese nicht. Klicken Sie im Internet nie auf „Passwort merken“.

EXKURS DATENSICHERUNG UND DEREN ZUKUNFT

Für den Schutz gegen Schadsoftware wie z.B. Ransomware ist es essentiell eine Datensicherung zu haben. Dabei wird empfohlen mehrere Backups vorzuhalten. Die Erfahrung hat dabei gezeigt dass es vorteilhaft ist eines davon offline aufzubewahren, um dieses von einem Schadsoftwarebefall zu schützen. Weiters sollten sogenannte Restore Test, also eine Prüfung ob das Wiederherstellen aus Backups auch funktioniert, regelmäßig durchgeführt werden. Wenn man sich Dienstleister bedient ist es empfehlenswert diese vertraglich zu verpflichten. Wenn personenbezogene Daten verarbeitet werden muss auch eine Auftragsverarbeitungsvereinbarung nach Art 28 DSGVO abschließen.

Zukünftig ist Cloud Computing u.a. für Datensicherung ein möglicher Lösungsansatz. Hierbei ist im Gesundheitsbereich das Gesundheitstelematikgesetz anzuwenden:
Bei „Cloud Computing“ regelt es eine zwingend vollständige Verschlüsselung der Gesundheitsdaten auf Basis zulässiger kryptografischer Algorithmen iSd GTelV iVm SigV
Dies bedeutet eine Verschlüsselung nicht nur des Transports sondern auch der Daten selbst!

INFORMATIONEN RICHTIG VERTEILEN/VERSENDEN

Bei der Weitergabe von Informationen wird das „Need-to-Know“-Prinzip angewendet. Vermeiden Sie unbedachte mündliche Informationsweitergabe und Situationen, in denen Sie belauscht werden können. Achten Sie auf den richtigen EmpfängerInnenkreis bei E-Mails. Beim externen Versand von vertraulichen oder geheimen Informationen ist eine Verschlüsselung jedenfalls notwendig. Seien Sie vorsichtig und zurückhaltend mit der Weitergabe von Informationen in sozialen Netzwerken.

stomatologi[e]

der e-newsletter der österreichischen gesellschaft für zahn-, mund- und kieferheilkunde

EXKURS DATENWEITERLEITUNG AN KOLLEGEN, PATIENTEN, ZAHNTECHNIKER ...

Grundsätzlich ist im Gesundheitssektor die EU Datenschutz-Grundverordnung (DSGVO) & Gesundheitstelematikgesetz 2012 (GTelG) einzuhalten.

Gem. DSGVO: ist eine Verarbeitung und Übermittlung von Daten nur dann zulässig, wenn entweder eine Zustimmung eine Vertragserfüllung oder rechtliche Grundlage dazu legitimiert.

Das GTelG regelt die Übermittlung der Gesundheitsdaten. Es regelt u.a. den zwingend verschlüsselten Versand (u.a. DaMe, Medicalnet) und die Identitätsfeststellung bei elektronischer Übermittlung.

Ggf. Bestätigung von Kollegen einholen: Hiermit bestätige ich, dass der/die genannte PatientIn sich in meiner Praxis / meinem Institut in Behandlung befindet.

INFORMATIONEN RICHTIG ANNEHMEN

Prüfen Sie die Absenderin/den Absender von Informationen.

Öffnen Sie nur E-Mails (insbesondere darin enthaltene Links und Anhänge) von AbsenderInnen, denen Sie vertrauen zum Schutz vor Computerviren und „Phishing“-Angriffen.

INFORMATIONEN RICHTIG VERNICHTEN/ENTSORGEN

Nicht mehr benötigte Informationen müssen sachgemäß entsorgt werden. Elektronische Datenträger (USB-Sticks etc.) müssen sicher gelöscht und entsorgt werden.

Wir alle tragen einen wichtigen Beitrag zur Informationssicherheit und zum Datenschutz.