MEDIENDIENST DER ÖSTERREICHISCHEN ÄRZTEKAMMER

Inhaber, Herausgeber,
Hersteller und Redaktion:
Österreichische Ärztekammer
Öffentlichkeitsarbeit
A-1010 Wien, Weihburggasse 10-12
Telefon 01/51406–3312 DW
pressestelle@aerztekammer.at

PRESSEKONFERENZ

Thema:

Daten können Leben retten

Teilnehmer:

a.o. Univ.-Prof. Dr. Thomas Szekeres
Präsident der Österreichischen Ärztekammer

Dr. Cornelius Granig
Leiter des Bereichs Cyber Security und Krisenmanagement beim Beratungsunternehmen Grant Thornton Austria

Zeit:

Dienstag, 22. Juni 2021, 9.30 Uhr

Ort:

Virtuelle PK aus dem APA-Pressezentrum

Daten: Schützenswerte Rohstoffe und Lebensretter

Bei der Diskussion um personenbezogene Gesundheitsdaten im Spannungsfeld zwischen Cyber Security, Fake News, Datenschutz und wichtigen Forschungsfragen kommen oft die graduellen Abstufungen zum Umgang mit Daten zu kurz.

Statement a.o. Univ.-Prof. Dr. Thomas Szekeres

Daten sind heute das Rückgrat unserer Welt. Sie sind die Grundlage für politische Entscheidungen von höchster Tragweite, wie wir im aktuellen Pandemieverlauf täglich festgestellt haben. Die Menge an weltweit entstehenden Daten befindet sich jetzt auf einem Allzeithoch und steigt laut Studien jährlich um fast 30 Prozent. Für Unternehmen sind Daten heute so wertvoll wie Bargeld – darunter spielen Gesundheitsdaten durch ihre Einzigartigkeit und ihre Aussagekraft eine ganz besondere Rolle und stellen einen unschätzbaren Wert dar. Entsprechend wichtig ist auf der einen Seite der Schutz dieser Daten – auf der anderen Seite können sie gerade im Gesundheitssystem von riesigem Nutzen sein und bergen großes Potenzial für die medizinische Forschung.

Datenverknüpfungen könnten beispielsweise in einer Pandemie, wie wir sie aktuell noch erleben, ein wichtiges Werkzeug sein. Das Gute ist, dass wir die Daten ja schon haben – es fehlt nur die Verknüpfung. Wenn beispielsweise die Daten der Gesundheitsbehörden mit den Medikationsdaten abgeglichen werden können, selbstverständlich anonymisiert oder pseudonymisiert, können schnell Zusammenhänge zwischen verabreichten Medikamenten und Krankheitsverläufen hergestellt werden. Im Idealfall finden wir dann Medikamente, die vor schweren Verläufen schützen – so können Spitäler und damit das Gesundheitssystem entlastet und Patientinnen und Patienten vor Aufenthalten auf Intensivstationen oder Schlimmerem geschützt werden.

Äußerst hilfreich wäre auch die Verknüpfung der Impfdatenbank mit der Infektionsdatenbank. Das Coronavirus ist leider sehr heimtückisch, und seine Mutationen sind durchaus aufmerksam zu beobachten, wie uns aktuell die sogenannte Delta-Variante zeigt. Diese ist anscheinend deutlich ansteckender, und es ist mit den aktuell zugelassenen Impfstoffen ein vollständiger Impfschutz nötig, um effektiv vor einem schweren Verlauf geschützt zu sein. Wenn wir nun die Impfdatenbank mit der Infektionsdatenbank verknüpfen, sind wir schnell informiert, sollten die Infektionszahlen unter den geimpften Menschen steigen. Das könnte auf neue Varianten hinweisen, die sogenannte Impfdurchbrüche verursachen. Selbstverständlich würde die Verknüpfung anonymisiert stattfinden. Es geht nicht darum, Daten von einzelnen Personen abzufragen, sondern um generelle Aussagen über die Wirksamkeit beim Impfschutz. Im Optimalfall gibt es eine regionale Unterscheidungsmöglichkeit, um schnell lokale Ausbrüche von etwaigen Mutationsvarianten feststellen zu können. Hier ist eine schnelle Information doppelt sinnvoll, denn mit raschen Gegenmaßnahmen kann die Ausbreitung eventuell noch eingedämmt werden.

Datenschutzrechtlich wären beide Datenverknüpfungen sicher unbedenklich und, wie ausgeführt, eine eminent wichtige Informationsquelle. Dass wir Ärztinnen und Ärzte, die ja zum einem großen Teil in die Erstellung von Gesundheitsdaten involviert sind, den Datenschutz sehr ernst nehmen, haben wir erst kürzlich wieder unter Beweis gestellt. Wir haben uns ganz klar gegen die geplante Datensammlung im Zusammenhang mit dem Grünen Pass ausgesprochen, wo etwa die Verknüpfung mit aktuellen und historischen Daten über das Erwerbsleben, das Einkommensniveau, etwaige Arbeitslosigkeit, den Bildungsweg und

Krankenstände aller geimpften und genesenen Personen geplant war. Das ging für uns als Österreichische Ärztekammer deutlich zu weit.

Eine bessere Nutzbarkeit von Daten haben zudem zuletzt sowohl der Forschungsrat als auch der Complexity Science Hub Vienna gefordert. Letzterer hat eine Initiative zur Schaffung einer unabhängigen nationalen Medizindatenstelle ins Leben gerufen und auch die Probleme identifiziert, warum die Datenlage in Österreich derzeit so schwierig ist. Daten seien auf viele Institutionen verteilt und würden dort in unterschiedlicher Qualität vorliegen, die Institutionen hätten weder Anreize, Daten zu teilen, noch gäbe es Personalressourcen für eine optimale vernetzte Nutzung der Daten. Zudem würden oft datenschutzrechtliche Bedenken als Vorwand genutzt: Die durchaus strenge europäische DSGVO würde vielfach wesentlich mehr Möglichkeiten zur sinnvollen und sicheren Datennutzung zulassen, meinen die Experten. Aber selbstverständlich muss der Schutz dieser wertvollen Daten jederzeit gewährleistet sein.

Statement Dr. Cornelius Granig

Die Diskussion um die Sicherheit von personenbezogenen Gesundheitsdaten bewegt sich in Österreich grundsätzlich im Spannungsfeld zwischen der Notwendigkeit, mit diesen Daten sicher und sorgfältig umzugehen, und der Sorge, dass sie in die falschen Hände kommen. Die häufigste Meldung von Problemen mit der Sicherheit von Gesundheitsdaten basiert auf der Grundlage von Cyber-Angriffen: Betroffene Krankenhäuser und andere Gesundheitsdiensteanbieter müssen eine Meldung bei der Datenschutzbehörde machen.

Hatte man ursprünglich geglaubt, dass Krankenhäuser von Kriminellen gerade während der Corona-Pandemie verschont würden, hat sich inzwischen das Gegenteil herausgestellt: Da das Personal wegen der vielen neuen Herausforderungen während der Corona-Pandemie vielerorts überlastet war, glaubten Kriminelle, dass Kliniken es mit der IT-Sicherheit nicht so genau nähmen und leichte Opfer seien.

In Deutschland gab es letztes Jahr mehr als 50 erfolgreiche Ransomwareangriffe auf Spitäler, und auch in Österreich kam es zu Verschlüsselungsattacken auf Krankenhausbetreiber, die bei nationalen Stellen gemeldet wurden.

Wie sehen solche Attacken typischerweise aus? Über Phishing-E-Mails wird Schadsoftware in einer Organisation installiert. In vielen Fällen kommt es in der Anfangsphase dazu, dass Daten an die Angreifer übertragen werden. Danach startet die Verschlüsselung der Systeme des Opfers, und die Kriminellen übersenden eine Lösegeldforderung. Wenn der Betroffene bezahlt, versprechen die Kriminellen, die Systeme zu entschlüsseln. Wenn nicht bezahlt wird, droht häufig auch die Erpressung mit dem Missbrauch der gestohlenen Daten.

Viele Angriffe im Gesundheitsbereich kommen allerdings nicht extern, sondern von intern. Meist werden dabei personenbezogene Gesundheitsdaten unrechtmäßig ausgedruckt oder auf einen Memory Stick kopiert, um die betroffene Einrichtung oder sogar die Patientinnen und Patienten zu erpressen. Beide Angriffsmuster illustrieren, dass Gesundheitsdaten ein sehr wertvolles Gut darstellen, dessen Verschlüsselung oder Diebstahl zu großen Problemen führen. Aus diesem Grund ist es wichtig, umfangreiche Maßnahmen für die Computersicherheit zu ergreifen. Neben der physischen Hygiene, die gerade bei Gesundheitsdiensteanbietern eine herausragende Rolle spielt, ist die „Cyberhygiene“ von enormer Wichtigkeit.

Die Devise sollte lauten: Wir verschlüsseln unsere Daten, um sie sicher zu speichern und zu übertragen, und nicht unsere Angreifer!

Sichere Speicherung und Verarbeitung von Gesundheitsdaten

„Cyberhygiene“ ist ein moderner Sammelbegriff für Schutzvorkehrungen geworden, mit denen man Computer und Netzwerke „sauber hält“ und damit Schaden abwendet, den elektronische Eindringlinge und Angriffe verursachen können. In Anlehnung an Hygienekonzepte im Gesundheitsbereich geht es um drei wichtige Themenkreise:

1. Welche Hilfswerkzeuge und Prozeduren stehen zur Verfügung?

Als Analogie zu Desinfektionsverfahren stehen im elektronischen Bereich Programme zur Verfügung (wie Firewalls, Schadsoftwarescanner), die kombiniert mit den richtigen Verfahren (beispielsweise Mehr-Faktor-Authentifizierung, Verschlüsselung) Schädlinge abwehren.

2. Wie kann man Sicherheitsmaßnahmen in die Routine des Arbeitsalltags integrieren?

Die Betreiber von Computern und Netzwerken – seien das Einzelpersonen, Firmen oder Organisationen – müssen Strategien entwickeln, dass ohne spezielles Zutun der Benutzer automatisch bestimmte Verfahren und Prozeduren ablaufen – zum Beispiel die periodische Datensicherung, das Update von Softwarekomponenten, das Auswerten von Zugriffsprotokollen von Computern und Firewalls, das Prüfen von Datenabflüssen sowie das verschlüsselte Speichern und Übertragen von Daten.

3. Wie kann man die Effizienz der Werkzeuge laufend sicherstellen?

Wie bei vorgeschriebenen Hygiene-Prozeduren in Gesundheitseinrichtungen ist es notwendig, dass die Anwender laufend mit der Cyberhygiene konfrontiert werden, indem sie beispielsweise ihr Passwort ändern müssen, ihren Fingerabdruck eingeben müssen oder bestimmte Daten nach einer gewissen Zeit unwiderruflich gelöscht werden.

Laufende Aufklärung und regelmäßiger Kehraus

Damit all diese Schutzwerkzeuge, Prozeduren und Abläufe greifen, ist es notwendig, ganz grundsätzliche Fragestellungen zu klären und gegebenenfalls im IT-Bereich richtiggehend „aufzuräumen“. Zuallererst betrifft das die Datenhygiene: Welche sensiblen Daten befinden sich in welchen Systemen und wie sind sie geschützt? Welche Daten werden wirklich benötigt, wer hat darauf Zugriff darauf und wie können nicht benötigte oder alte Daten sicher gelöscht werden? Ähnliches gilt für Programme und installierte Software: Was ist installiert und was wirklich davon in Verwendung – und welche internen oder externen Benutzer haben die Rechte, diese Programme auszuführen? Das Deinstallieren oder Deaktivieren unbenutzter Programme oder Services führen zu verbesserter Ablaufgeschwindigkeit und Speichernutzung. Der Widerruf von Benutzerrechten gehört regelmäßig nach dem Prinzip durchgeführt, dass die Anwender nur die minimal notwendigen Zugriffsrechte haben sollten.

Überdies muss die gesamte stationäre und mobile Hardware elektronisch erfasst und beobachtet werden. Dazu gehören auch Geräte, die nicht gleich als Computer erkennbar sind, weil sie am „Internet der Dinge“ hängen (z.B. Kameras, Türöffner, Netzwerkkomponenten). Alte Hardware muss ausgetauscht oder auf den neuesten Stand gebracht werden, und unsichere Geräte müssen überhaupt vom Netz.

Die Mitarbeiter sollten laufend in Aufklärungs- und Fortbildungsmaßnahmen über Angriffsmethoden informiert werden, die über soziale Wege vorgenommen werden (z.B. Phishing-E-Mails, CEO-Betrug). Einmal im Jahr sollten solche Angriffe simuliert werden, damit klar ist, ob die Organisation die Risiken ernst nimmt.

Vorbeugung vor Infektionen und Quarantäne für befallene Systeme

Kommt es zu Angriffen, deren Gründe oder Ausmaß unklar sind, oder zu einem Befall mit Schadsoftware, sollten die betroffenen Systeme vom Netz genommen werden, bis sie gründlich untersucht werden konnten. Dies ähnelt den Quarantäne-Stationen im Gesundheitsbereich, in denen Patientinnen und Patienten mit resistenten Keimen oder mit gefährlichen Infektionen isoliert untergebracht werden, um andere nicht zu gefährden.

Damit es nicht dazu kommt, müssen die Einfallstore geschlossen werden. Besondere Vorsicht gilt bei der Verwendung von Memory-Sticks, da diese mit Schadsoftware verseucht sein können, die einen Computervirenbefall oder die Installation eines geheimen Kanals zu virtuellen Angreifern ermöglichen.

Wenn es schmutzig wird: Pläne für den Notfall

Das Um und Auf des Funktionierens unserer elektronischen Welt liegt in der Hand jeder Organisation und jedes Unternehmens: Zumindest einmal im Jahr sollte durch externe Spezialisten eine gründliche Durchuntersuchung der Computersicherheit und Datenintegrität vorgenommen werden. Die gefundenen Schwachstellen sollten in einer Zusammenschau mit den für die Organisation wichtigen Prozessen und Bereichen analysiert werden. Auf dieser Basis kann eine Liste von Verbesserungsnotwendigkeiten erstellt und geführt werden, die mit der Gesamtrisikobewertung einhergeht.

Auch bei sehr sorgfältiger Vorgehensweise kann man niemals totalen Schutz vor Angriffen erreichen, diese aber deutlich dezimieren oder schneller feststellen. Mit spezieller Software zur Prävention von Datenlecks kann beispielsweise der gestiegene Abfluss von Daten entdeckt werden, bevor Hacker große Mengen stehlen können.

Für Notfälle muss man aber immer gerüstet sein: Neben der schnellen Abschaltung und Abschottung betroffener Systeme kann es notwendig sein, ein elektronisches Notsystem in Betrieb zu nehmen, oder für eine gewisse Zeit sogar ohne die Verwendung von elektronischen Hilfsmitteln auszukommen. Die aktive und schnelle Kommunikation an die Mitarbeiter und Patientinnen und Patienten – auch über papierbasierte Kanäle – sowie die schnelle Reaktion machen aus Opfern von Cyberkrisen respektierte und krisengestählte Organisationen, die gelernt haben, nicht nur mit den neuen Informations- und Kommunikationstechnologien, sondern auch mit den mit ihnen einhergehenden digitalen Problemen professionell umzugehen.

Sichere Verwendung von Gesundheitsdaten in der Forschung

Während in tendenziösen Fake-News häufig von „Datenkraken“, „Menschenversuchen“ und unverantwortlichen „Big-Data“-Maßnahmen gesprochen wird, geht häufig die Frage der für die Gesellschaft positiven Verwendung von Gesundheitsdaten für die Forschung unter. Wenn man personenbezogene Gesundheitsdaten sicher verarbeitet und speichert, stellen sie, wie schon erwähnt, einen großen Datenschatz dar, aus dem wichtige Erkenntnisse gewonnen werden können. Die Verwendung von Gesundheitsdaten für die Forschung ist in Österreich durch das Forschungsorganisationsgesetz (FOG) geregelt, konnte aber bisher nicht wirklich beginnen, da bisher eine gemeinsame, vom Gesundheits- und Wissenschaftsminister unterschriebene Verordnung fehlt. Hier sollte pragmatisch vorgegangen werden, indem die Verfahren der Anonymisierung und Pseudonymisierung von Daten durchgeführt werden.

Als **Anonymisierung** bezeichnet man die Entfernung von Elementen von Datensätzen, die eine Zuordnung zu einer Person möglich machen. Anonymisierte Daten können verwendet

werden, wenn die Forschungsergebnisse nicht in die laufende Behandlung der Datenspender einfließen sollen und auch keine Zusatzfragen an diese notwendig sind.

Die **Pseudonymisierung** von Daten ist die richtige Vorgehensweise für viele sinnvolle Anwendungen in der Forschung, wenn die Ergebnisse in die Behandlung von Patientinnen und Patienten einfließen sollen, von denen Daten stammen. Dabei wird an der Stelle, von der die Daten stammen, eine Trennung zwischen den Daten, die eine Zuordnung zu einer Person möglich machen, und den Forschungsdaten gemacht. Über eine strikt separat geführte Tabelle können diese wieder zusammengeführt werden.

Wenn diese Technik korrekt angewandt wird, können beispielsweise eine Verbindung zwischen der Medikation und den Krankheitsverläufen von Patientinnen und Patienten hergestellt und in Österreich an der Erforschung neuer Wege zur Bekämpfung von Krankheiten – allen voran COVID-19 – mit modernen Technologien und sogar künstlicher Intelligenz gearbeitet werden. Die Forschungsergebnisse können in die laufende und zukünftige Behandlung der Patientinnen und Patienten einfließen.

In jedem Fall muss vor dem Beginn eines jeden Forschungsvorhabens eine **Datenschutzfolgeabschätzung** von Spezialisten durchgeführt werden, die Risiken und deren Verhältnismäßigkeit zum erreichbaren Forschungsziel aufzeigt.

Die wahrgenommene Frontalopposition einzelner Datenschützer und teilweise völlig faktenfremde Desinformation von Verschwörungstheoretikern im Internet, denen Modernisierung ein Dorn im Auge ist, sollten nicht den Blick auf das Wesentliche verstellen: Ein verantwortlicher, pragmatischer Umgang mit personenbezogenen Gesundheitsdaten ist nicht nur möglich, sondern sehr wichtig, da er uns als Gesellschaft weiterbringen wird.

Annex

Begriffserklärung Pseudonymisierung

Im Rahmen der Pseudonymisierung werden der Name und andere Identifikationsmerkmale von Menschen durch ein Kennzeichen ersetzt. Damit soll die Bestimmung des Betroffenen durch die forschende Einrichtung ausgeschlossen oder wesentlich erschwert werden (Art. 4, Abs. 5, DSGVO).

Beispiel: Personenbezogene Gesundheitsdaten von Cornelius Granig und Cornelia Granig

Vorname	Nachname	Krankheit	Behandlung
Cornelius	Granig	Uveitis	Cortisontabletten
Cornelia	Granig	Iritis	Augentropfen

Erstellung einer ersten Tabelle, in der Informationen über die Personen mit einer ID verknüpft werden

Tabelle I

ID	Vorname	Nachname
0001	Cornelius	Granig
0002	Cornelia	Granig

Erstellung einer zweiten Tabelle, in der die IDs mit den forschungsrelevanten Daten verknüpft ist:

Tabelle II

ID	Krankheit	Behandlung
0001	Uveitis	Cortisontabletten
0002	Iritis	Augentropfen

Die Tabellen müssen an unterschiedlichen Stellen gespeichert sein, sodass die forschende Stelle den Personenbezug nicht wiederherstellen kann. Die Tabelle mit den ID muss dabei gesondert aufbewahrt werden. Es bedarf dafür technischer und organisatorischer Maßnahmen, damit diese ID keinen dritten Personen zugänglich sind.

Depseudonymisierung

Liegen Forschungsergebnisse vor, die in die laufende Therapie von Personen einfließen sollen, kann die Depseudonymisierung im Interesse der Patientinnen und Patienten vorteilhaft sein (um diese Personen auf neue Ergebnisse hinzuweisen oder neue Behandlungsmöglichkeiten zu testen). Auch für Rückfragen oder die Einholung weiterer Informationen ist dieser Weg zu beschreiten.

In jedem Fall müssen in das Forschungskonzept Mechanismen integriert werden, die eine Reidentifizierung pseudonymisierter Daten vorsehen, da schon zum Zeitpunkt der Pseudonymisierung darauf Rücksicht genommen werden muss. Es müssen klare organisatorische Abläufe für diesen Vorgang festgelegt werden, die verbindliche Genehmigungsschritte und eine nachhaltige Dokumentation vorsehen.

Begriffserklärung Anomysierung

Im Rahmen der Anonymisierung werden personenbezogene Daten derart verändert, dass nicht mehr oder nur mit unverhältnismäßig großem Aufwand Rückschlüsse auf die Person gezogen werden können.

Beispiel:

Personenbezogene Gesundheitsdaten von Cornelius Granig und Cornelia Granig

Vorname	**Nachname**	**Krankheit**	**Behandlung**
Cornelius	Granig	Uveitis	Cortisontabletten
Cornelia	Granig	Iritis	Augentropfen

Vorgang der Anonymisierung:

Erstellung einer Tabelle, in der personenbezogene Informationen gelöscht werden.

Tabelle

Fortlaufende Nummer	**Krankheit**	**Behandlung**
1	Uveitis	Cortisontabletten
2	Iritis	Augentropfen

Anonymisierte Daten werden nicht mehr als personenbezogene Daten behandelt, da keine Rückschlüsse auf die Person gezogen werden können.