**Rechtliche Vorschriften**

Die zunehmende Digitalisierung im Arzt - Patientenverhältnis hat auch großen Einfluss auf die berufsrechtlichen Dokumentationspflichten. Gemäß ÄrzteG 1998 (sowie auch KAKuG) ist jeder Arzt bzw. jede Ärztin verpflichtet, beratende, diagnostische oder therapeutische Leistungen zu dokumentieren bzw. hat auch jeder Patient/ jede Patientin das Recht, Einsicht in diese Aufzeichnungen zu nehmen. Die im Ärztegesetz (ÄrzteG) und dem Krankenanstalten- und Kuranstaltengesetz (KAKuG) vorgeschriebene Dokumentation ärztlicher Leistungen gilt rechtlich als Datenverwendung.

Für Ordinationen gilt, neben diesen gesetzlichen Regelungen, jedoch zusätzlich sowohl das Datenschutzgesetz (DSG 2000), das allgemein die Verwendung von Daten regelt, als auch das Gesundheitstelematikgesetz (GTelG), das die Übermittlung sensibler Daten regelt. Personenbezogene Daten können gemäß DSG in der Ordination zur medizinischen Behandlung, zur Abrechnung mit der Sozialversicherung verwendet werden. In allen anderen Fällen ist das Einverständnis der Betroffenen einzuholen. Nicht personenbezogene, anonyme Daten kann der Dateninhaber (Arzt) weitergeben. Als niedergelassener Arzt sind Sie Auftraggeber der Datenverwendung. Wenn Sie von IT-Dienstleistern unterstützt werden, lassen Sie sich die datenschutzkonforme Abwicklung schriftlich zusichern. Unter Berücksichtigung des aktuellen Stands der Technik und der wirtschaftlichen Vertretbarkeit haben Ärzte sicherzustellen, dass Daten ordnungsgemäß verwendet werden, vor Zerstörung und Verlust geschützt und für Unbefugte nicht zugänglich sind. Bei Hardware- Gebrechen, Sabotage oder Fehleingaben ist sofort zu reagieren. Gegen Stromausfall, Wasserschaden, Feuer etc. ist Vorsorge zu treffen. Datenbezogene Aufträge an Mitarbeiter sind schriftlich festzuhalten. Der Arzt hat alle in der Ordination Tätigen über Datenschutzvorschriften zu belehren sowie den Zutritt zu den Räumen und die Zugriffsberechtigungen zu regeln (u.a. personengebundenes Login für alle Softwareprodukte). Die Datenverwendung ist zu protokollieren.

**Datensicherheit – konkrete Umsetzung**

Die Datensicherheit kann nur dann gewährleistet werden, wenn Sie sicherstellen, dass betriebsfremde Personen (Patienten, Dienstleister, Reinigungskräfte, etc.) nicht versehentlich oder absichtlich sensible Daten einsehen können:

- PC Monitore so drehen, dass nur Sie und Ihre Mitarbeiter Einsicht haben
- Nutzen Sie Bildschirmschoner (Einschalten nach 30 sec.)
- Kleben Sie Passwörter nicht an den Bildschirm!
- Lassen Sie Daten in Papierform wie Briefe, Faxe, Befunde oder Formulare nicht unbeaufsichtigt liegen
- Gestalten Sie den Anmeldebereich so, dass Gespräche vertraulich bleiben
- Versperren Sie Ihre Karteikästen

**Verträge mit Mitarbeitern und Dienstleistern**

Der Arzt7 die Ärztin als datenschutzrechtlicher AuftraggeberIn, aber auch seine IT-DienstleisterIn und OrdinationsmitarbeiterIn haben ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung Zugang zu Gesundheitsdaten und sind gesetzlich verpflichtet, diese geheim zu halten. Darüber hinaus müssen Sie als OrdinationsinhaberIn festlegen, wer auf welche Daten und in welchem Umfang zugreifen darf. Es empfiehlt sich, nur den unbedingt notwendigen Datenzugriff zu gestatten.

Lassen Sie sich von Mitarbeitern und Dienstleistern die Vorlage der gesetzlichen Bestimmungen unterfertigen. Damit dokumentieren Sie, dass Sie Ihren Pflichten nachgekommen sind und Vereinbarungen über den Zugriff auf Daten getroffen sowie Belehrungen über die Verschwiegenheitspflicht und über andere Pflichten vorgenommen haben. Entsprechende Vorlagen entnehmen Sie bitte dem Evaluationsteil dieses Handbuchs bzw. der Homepage der ÖQMed.

**Dokumentation und Administration**

Als Datenzugriff von außen gilt z.B. der Zugriff von einer Zweitordination aus, aber auch die Fernwartung durch IT-Dienstleister. Der Zugriff ordinationsfremder Personen ist vertraglich zu regeln, Dritte müssen schriftlich die Einhaltung des Datenschutzes garantieren. Für alle Fernzugriffe sind die technische Sicherheit und der Schutz vor unbefugtem Zugriff zu garantieren, alle Maßnahmen sind zu dokumentieren. Jeder Benutzer der Arztsoftware in oder außerhalb der Ordination hat ein „personalisiertes Login" zu verwenden, das ausreichend sicher sein muss (Länge, Klein-/Großbuchstaben, Ziffern, Sonderzeichen). Dokumentation für den Ernstfall Die Arztsoftware hat alle Verwendungsvorgänge zu protokollieren. Es muss für den Datenverantwortlichen (in der Regel der Inhaber der Ordination) jederzeit ersichtlich sein, welcher Mitarbeiter welche Daten geschrieben, gelesen oder geändert hat, da diese Aufzeichnungen im Falle eines Gerichtsverfahrens vorzulegen sind.

**Datensicherung**

Speichern Sie täglich alle Daten, die für einen reibungslosen Betrieb notwendig sind, auf externen Medien (z.B. Festplatte, USB-Stick) – auch Konfigurationsdateien, Zusatzprogramme für EKG, Medizintechnik, Mail und notwendige Software. Prüfen Sie, ob alle gesicherten Daten wiederherstellbar sind. Wenn Sie damit Ihren IT-Dienstleister beauftragen, lassen Sie sich das Ergebnis schriftlich bestätigen. So haftet der Dienstleister auch für die Korrektheit der Sicherung. Sollten Softwarehersteller und IT-Dienstleister unterschiedliche Firmen sein, legen Sie die eindeutige Verantwortung für Sicherung und Wiederherstellung fest. Durch Datenverschlüsselung oder sichere physische Verwahrung (Safe) verwehren Sie Unbefugten den Zugriff auf die Sicherungen. Verteilen Sie die Datenträger mit den gesicherten Daten auf mehrere Orte.

**Notfallplan**

Legen Sie im Vorhinein fest:

- Wie und wo bekomme ich rasch Ersatz-Hardware?
- Wo sind Garantien, Wartungsverträge hinterlegt?
- Wer installiert die Software auf der neuen Hardware?
- Wie schnell kann der IT-Dienstleister im Ernstfall geregelte
- Abläufe wiederherstellen? (Dies sollte vertraglich geregelt sein.)
- Wo sind die Notrufnummern der IT-Dienstleister hinterlegt?
- Wo sind Passwörter, Codes und Lizenzen hinterlegt

**Richtige Entsorgung oder Rückgabe von Datenträgern**

Vertrauliche Patientendaten oder sensible Daten sind alle jene patientenbezogenen Daten und Informationen, die den Kontakt, Auskünfte über den Gesundheitszustand, zur Krankengeschichte oder vergangenen bzw. zukünftigen Behandlungen, zum Inhalt haben.

Werden diese Unterlagen – i.d.R. nach Ablauf der Aufbewahrungsfristen nicht mehr benötigt, können diese vernichtet und entsorgt werden. Aus Gründen des Datenschutzes müssen die Unterlagen ordnungsgemäß, auf sichere Art vernichtet werden, d.h., dass die Daten weder wiederherstellbar und nicht mehr lesbar sein dürfen. Auszumusternde oder defekte Datenträger (CD-ROM, DVD, Festplatten) müssen unter Beachtung des Datenschutzes fachgerecht unbrauchbar gemacht werden.

Erfolgt diese Vernichtung durch einen externen Dienstleister, so sollte dieser regelmäßig auf seine Eignung überprüft werden. Ebenso ist stets dafür Sorgen zu tragen, sich die Verschwiegenheit entsprechend bestätigen zu lassen.

Grundsätzlich ist davon auszugehen, dass **alle Medien bzw. Rechner**, die in einer Ordination zum Einsatz gekommen sind, patientenbezogene Daten gespeichert haben, nicht nur am Server!

Was sollten Sie keinesfalls tun?

- Speichermedien oder Festplatten NICHT in den Papierkorb oder über Hausmüll entsorgen
- Übergeben Sie keine Altgeräte ohne entsprechende Sicherheitsmaßnahmen (z.B. Bestätigung des Übernehmers, dass die Daten gesetzeskonform gelöscht werden und keine Weitergabe an Dritte erfolgt!)

Praxistipps:

- Shreddern Sie Papierdokumente selbst oder übergeben Sie diese einem Dienstleister, mit dem sie einen entsprechenden Vertrag geschlossen haben
- Funktionsfähige Festplatten können durch Einsatz einer geeigneten Löschsoftware gelöscht werden. Ein alleiniges „Formatieren“ durch das Betriebssystem selbst wird nicht als sicher angesehen
- Wollen Sie ganz sichergehen, zerstören Sie Sicherungs- und Speichermedien physisch (Zerkleinerung, Shreddern)
- Die Auswahl und der korrekte Einsatz einer Löschsoftware sind für Nichtfachleute nicht trivial, insbesondere falls Festplatten gelöscht werden sollen, auf denen ein Betriebssystem läuft. Daher empfehlen wir für diesen Zweck die Beauftragung eines zertifizierten Dienstleisters, der die korrekte Löschung vertraglich zusichern muss
- Werden Festplatten aus einem Rechner entnommen und weitergegeben, können die Daten bei Einsatz einer Verschlüsselungssoftware (beispielsweise „Bitlocker“ von Microsoft oder die Open-Source Software „Truecrypt“) ohne den ursprünglichen Wirtsrechner nicht mehr gelesen werden. Eine Weitergabe ohne den Rechner (und damit ohne dem Benutzerschlüssel) ist daher datenschutzrechtlich als sicher anzusehen

**Sichere Nutzung des Internet**

Im Zeitalter einer zunehmend vernetzten elektronischen Kommunikation ist es kaum noch realisierbar, einen Praxisrechner ohne Internetanschluss auszustatten. Beim Surfen im Internet oder Versand bzw. Empfang von E-Mails öffnet sich der Rechner nach außen. Somit ist es unumgänglich, den PC vor potentiellen Angriffen zu schützen!

Wie Sie trotzdem einen optimalen Datenschutz erreichen:

- Nutzen Sie das Internet in der Ordination idealerweise nur auf Rechnern, die keine Patientendaten enthalten.
- Zum Schutz vor Viren und Würmern ist die Installation einer Antivirensoftware unumgänglich!
- Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze überwachen und sich täglich auf dem aktuellen Stand halten.
- Um sich vor direkten Angriffen aus dem Internet zu schützen, empfiehlt sich der Einsatz einer Firewall. Eine Firewall sollte den Datenverkehr zwischen verschiedenen Netzsegmenten (z.B.: LAN und Internet) absichern und regulieren.
- Es wird empfohlen, die Konfiguration des Internetbrowsers und der Firewall durch IT Experten durchführen und überprüfen zu lassen.

Nach Möglichkeit sollte der Einsatz eines WLAN (Wireless-Local-Area-Network) in der Ordination vermieden werden, da nicht die gleiche Betriebssicherheit und Betriebszuverlässigkeit garantiert werden kann, wie mit einer direkten Verkabelung. Generell ist der Einsatz einer hochwertigen symmetrischen Verschlüsselung für Patientendaten sinnvoll, mit der alle auf Datenträgern, Notebooks und PC´s vorhandenen Patientendaten verschlüsselt abgelegt werden können.

Sollte der WLAN Einsatz dennoch notwendig sein, muss auf eine ausschließlich verschlüsselte Verwendung geachtet werden, die den aktuellen technischen Anforderungen gerecht wird. (Ihr IT Dienstleister ist hier auf dem aktuellen Stand)

**Vernetzte IT im Gesundheitswesen**

Werden sensible Daten an ordinationsfremde Systeme übertragen, bürgt der „Datenbereitsteller", also in der Regel der Arzt, für die Einhaltung der entsprechenden Gesetze.

**Achtung!** Eine Übertragung per E-Mail oder ein ungesichertes Webformular ist in jedem Fall unzulässig.

**Gerichtete Befundübertragung/ Sichere Netze** bedeuten, dass die Übertragung einer Information an einen bestimmten Empfänger erfolgt, den der Absender bewusst und gezielt kontaktiert hat und basieren auf getrennten Datenströmen, die einen Zugriff aus dem Internet verhindern. Sie gilt idR datensicher. Die Dokumente werden als signierte und verschlüsselte E-Mails übertragen und sind für Dritte nicht einsehbar.

**Wie neu muss die IT sein?**

Die meisten ärztlichen IT-Systeme sind heute vernetzt, entweder lokal (Stationen, Server, GINA) oder global (Internet, GIN, ELGA), und müssen daher laufend aktualisiert werden. Das Betriebssystem ist eine äußerst komplexe Software, die zwischen Hardware und

Anwendungsprogrammen vermittelt. Um Fehlern und Sicherheitslücken vorzubeugen, liefern Hersteller regelmäßig funktionelle Updates (neue Funktionen werden bereitgestellt und Fehler ausgebessert) und Sicherheitsupdates (Schließung von Sicherheitslücken). Fragen Sie im Zweifelsfall Ihren IT-Dienstleister, welche Supportzeiträume für Ihr Betriebssystem gelten. Der Browser ermöglicht die Internet-Kommunikation, aber auch die Arztsoftware u.a. Programme nutzen ihn im Hintergrund. Er muss daher vom Hersteller laufend aktualisiert werden. Software-Update oder neue Hardware? Sollte ein Software-Update (Betriebssystem, Browser, Arztsoftware) finanziell unrentabel sein, sollten Sie eine neue Hardware in Betracht ziehen.

**Supportzeiträume für gängige Betriebssysteme**[1]

| Produkt | Veröffentlichung | Ende Mainstream Support | Ende Extended Support |
|---|---|---|---|
| Windows 2000 | 12.02.2000 | 30.06.2005 | 13.07.2010 |
| Windows XP | 25.10.2001 | 14.04.2009 | 08.04.2014 |
| Windows Server 2003 | 28.05.2003 | 13.07.2010 | 14.07.2015 |
| Windows Vista | 30.11.2006 | 10.04.2012 | 11.04.2017 |
| Windows Server 2008 | 27.02.2008 | 09.07.2013 | 10.07.2018 |
| Windows 7 | 22.10.2009 | 13.01.2015 | 14.01.2020 |
| Windows Server 2008 R2 | 22.10.2009 | 09.07.2013 | 10.07.2018 |
| Windows 8 | 26.10.2012 | 09.01.2018 | 10.01.2023 |
| Windows Server 2012 | 04.09.2012 | 09.01.2018 | 10.01.2023 |
| Windows 8.1 | 18.10.2013 | 09.01.2018 | 10.01.2023 |
| Windows Server 2012 R2 | 25.11.2013 | 09.01.2018 | 10.01.2023 |

**IT Sicherheitskonzept**

ÄrztInnen sind gesetzlich dazu verpflichtet, alle Datensicherheitsmaßnahmen schriftlich zu protokollieren. Dieses „IT-Sicherheitskonzept“ umfasst u.a.:

- Dokumentation der Aufgabenverteilung und der daraus resultierenden Datenverwendung je MitarbeiterIn
- Dokumentation der Zutrittsberechtigung zu den Ordinationsräumen je MitarbeiterIn
- Von MitarbeiterInnenn unterzeichnete Belehrung über Datenschutzvorschriften
- Unterzeichnete Aufteilung der Zugriffsberechtigung auf Daten und Programme je MitarbeiterIn
- Informationen über Datensicherungsmaßnahmen und Datensicherungen

Die Dokumentation muss belegen, dass Zugriff und Weitergabe von Daten ordnungsgemäß erfolgen und die Daten für Unbefugte nicht zugänglich sind. Die entsprechenden Dokumente sind laufend zu aktualisieren.

[1] Abb.: In Anlehnung an „Datensicherheit in Ordinationen“ (2014), Quelle: ÖÄK Bundeskurie NLÄ

ÄRZTEKAMMER FÜR WIEN

**Weitere Informationen:**

Finden Sie auf der Homepage der Ärztekammer für Wien oder der Homepage der Österreichischen Ärztekammer

**Ansprechpartnerin in der Ärztekammer für Wien:**

Mag.a Julia Müller-Rabl, MA
Stabsstelle Gesundheitsplanung und E-Health
Tel: 01/51501-1423
Fax: 01/ 5126023-1423
mueller-rabl@aekwien.at

Österreichische Ärztekammer (2014). *Informationen zur IT-Sicherheit in Ordinationen.* Abgerufen von http://www.aerztekammer.at/arztsoftware

# 12 REGELN ZUR DATEN-SICHERHEIT

1. **RECHTLICHE VORSCHRIFTEN.** Informieren Sie sich über Ihre Rechte und Pflichten. Verschriftlichen Sie alle Vorgänge und sammeln Sie die Unterlagen an einem Ort.

2. **PHYSISCHER SCHUTZ.** Stellen Sie sicher, dass betriebsfremde Personen keine sensiblen Daten einsehen können. Beschränken und kontrollieren Sie den Zutritt, beschränken Sie absichtliche oder versehentliche Einblicke, schützen Sie die Bereiche, in denen mit sensiblen Daten gearbeitet wird. Sehen Sie einen Einbruchs- und Diebstahlschutz vor.

3. **MITARBEITER.** Weisen Sie auf die Geheimhaltungspflicht in den Dienstverträgen hin. Legen Sie in einem Schriftstück für jeden Mitarbeiter fest, welche Dateneinsicht jeder Mitarbeiter benötigt.

4. **RECHNER / BETRIEBSSYSTEM.** Benutzen Sie ein Betriebssystem, das mit Sicherheitsupdates versorgt wird, einen aktuellen Browser sowie einen aktuellen Virenschutz. Überprüfen Sie Ihre Rechner unter www.peeringpoint.at/browsersicherheit. Falls Sie auf das Internet ohne GIN (e-card-Netzwerk) zugreifen, aktivieren Sie eine Software-Firewall.

5. **ORDINATIONSSOFTWARE.** Überprüfen Sie, ob eine Mitarbeiterverwaltung mit persönlichem Login unterstützt wird, fordern Sie eine starke Passwortqualität. Beschränken Sie die Zugriffe Ihrer Mitarbeiter auf die notwendigen Daten und stellen Sie sicher, dass die tatsächlichen Datenzugriffe protokolliert werden.

6. **DATENSICHERUNG.** Sichern Sie regelmäßig alle wesentlichen Daten Ihres IT-Systems. Bewahren Sie die Sicherungsmedien extern oder an einem geschützten Ort (Safe) auf. Kontrollieren Sie periodisch die Qualität der Medien und prüfen Sie die Wiederherstellbarkeit Ihres Systems. Treffen Sie Vorkehrungen für einen Softwarewechsel oder die Beendigung Ihrer ärztlichen Tätigkeit.

7. **DATEN ÜBERTRAGEN.** Übertragen Sie personenbezogene Daten nur mit gesicherter Befundübertragung oder (unter den gesetzlich vorgesehenen Auflagen) per Fax. Verwenden Sie keinesfalls E-Mail!

8. **DIENSTLEISTERVERTRÄGE.** Stellen Sie die Geheimhaltungsverpflichtung schriftlich sicher. Regeln Sie die Möglichkeiten der Fernwartung und den Zugriff auf Daten oder Sicherungsmedien. Erfragen Sie in Ihrer Ärztekammer die entsprechenden Vorlagen. Vermeiden Sie unbeschränkte Fernwartungszugänge.

9. **REPARATUR/ENTSORGUNG.** Geben Sie Datenträger nur ohne Daten an Dritte weiter, zerstören Sie gegebenfalls selbst die Festplatten. Denken Sie an den Inhalt von Sicherungsmedien. Fordern Sie von dem Dienstleister eine schriftliche Bestätigung der Einhaltung des Datenschutzes.

10. **PERSÖNLICHES VERHALTEN.** Gehen Sie mit den neuen Medien und Möglichkeiten kritisch um: Öffnen Sie keine E-Mails von unbekannten Personen, misstrauen Sie Gratisversprechungen, geben Sie keine vertraulichen Daten bekannt – so wird beispielsweise keine Bank oder Kreditkartenfirma Informationen von Ihnen per E-Mail einholen!

11. **NEUE GEFAHREN BEDENKEN.** Sichern Sie ein verwendetes WLAN nach dem Stand der Technik ab. Denken Sie an Daten auf mobilen Geräten (Notebook, Tablet, Smartphone), insbesondere bei Weitergabe und Diebstahl. Externe Zugriffe auf die Ordinationsdaten sind entsprechend zu sichern.

12. **REGELMÄSSIGE ÜBERPRÜFUNGEN.** Die aktuelle Technik und die damit verbundenen Möglichkeiten und Gefahren schreiten rasant voran. Denken Sie bei allen Konfigurationsänderungen auch an die IT-Sicherheit und dokumentieren Sie alle wesentlichen Vorgänge. Aktualisieren Sie in regelmäßigen Abständen Ihr IT-Sicherheitskonzept.

Eine Empfehlung von

BUNDESKURIE NIEDERGELASSENE ÄRZTE

ÖSTERREICHISCHE ÄRZTEKAMMER