13 EDV UND ORGANISATION

In der optimal strukturierten Ordination sollten Sie Zeit für den Verwaltungsaufwand (bei guter Dokumentationsqualität!) minimieren, die Zeit für Ihre Patienten maximieren, über gutes Zeitmanagement verfügen und Serviceleistungen anbieten (Arztbrief, Patientenbrief, ...). Weiters sollte die patientenbezogene Arbeit abgeschlossen sein, wenn der Patient die Ordination verlässt, und keine „Nach(t)arbeit" erforderlich machen. Ohne entsprechende softwaregestützte Patientenverwaltung (mit zusätzlichen Modulen wie z.B. Honorarabrechnung usw.) ist es unserer Ansicht nach nicht möglich, diesen Standard zu erfüllen.

13.1 Hardware, Software, …

13.1.1 Verkabelung, Strom, Serverstandorte

Bei der Elektroinstallation sind ausreichend Rohre für die Verbindung der Arbeitsplätze und deren Versorgung (eigener Stromkreis für die EDV) vorzusehen. Auch wenn Sie mit einem Einplatzsystem beginnen wollen: Bereiten Sie zumindest eine Leerverrohrung für eine EDV Vernetzung vor, das erspart Ihnen spätere Stemmarbeiten und somit Mehrkosten.
Denken Sie auch daran, eine Blitzschutzeinrichtung (an der Hauptleitung im Zählerkasten) zu installieren.
Achten Sie auf genügend Platz für die Geräte, die Luft zur Kühlung benötigen. Sollten Sie Ihren PC in Möbelstücke einbauen lassen, müssen Sie genügend Platz lassen, um den PC im Bedarfsfall auch tauschen zu können. Bedenken Sie: Ein neuer PC kann andere Maße haben.
Bei der Positionierung des Bildschirms ist auf augenermüdende Lichtreflexionen auf der Display-Oberfläche zu achten. Eine indirekte ausgewogene Beleuchtung kann hier Abhilfe schaffen.
Vermeiden Sie (im Winter und im Sommer – wenn möglich) extreme Temperaturen bzw. Temperaturschwankungen. Die Umgebungstemperatur sollte sich zwischen 21° C und 26° C bewegen, das ist speziell beim Einbau von Geräten in Schränke, oder beim Betrieb von Servern zu beachten. Tiefere Temperaturen führen lediglich zu einem erhöhten Stromaufkommen. Es kann auch der Einsatz von klimatisierten Serverschränken erwogen werden (Platz, Abluft, …).
Überlegungen zu Umwelteinflüssen (wie Wasserschaden, Brand, Ausfall Klimaanlage, Blitzschlag) sollten nach Möglichkeit berücksichtigt werden.

13.1.2 Einplatz- oder Mehrplatzsystem

Je nach Größe der Ordination und Patientenfrequenz sind Ein-, Zwei- oder Mehrplatzlösungen möglich. Die Anzahl der Arbeitsplätze ist auch mitentscheidend, ob ein Server installiert werden soll.

<u>Einzelplatzsystem (1 PC oder Notebook mit Drucker, usw.)</u>
Diese Lösung ist vor allem empfehlenswert, wenn man ohne Ordinationshilfe arbeitet. Der Vorteil liegt in den geringen Hardwarekosten, der Nachteil darin, dass der Arzt die Stammdaten (Name, Adresse, Versicherung, ...) erfassen muss und so Zeit für nicht ärztliche Tätigkeiten „verliert".

<u>Mehrplatzsysteme (2 od. mehrere PCs bzw. Notebooks mit Drucker, ev. Server, usw.)</u>
In der Anmeldung erfolgt die Aufnahme der Patientendaten, danach erfolgt die Reihung auf einer Warteliste. Während der eigentlichen Untersuchung werden dann vom Arzt nur noch die medizinisch relevanten Ereignisse protokolliert.

13.1.3 PC (mind. Empfehlung für einen Standard-Arbeitsplatz)

Ein Arbeitsplatz setzt sich mindestens aus einem PC, Monitor, Tastatur und Maus sowie einem Drucker zusammen.

- Prozessor: z.B. Intel Core i5 -i7; mind. 3,2 GHz
- Speicher (RAM) 16 GB
- Festplatte (250 - 500 GB SSD)
- Grafikkarte integriert
- Netzwerkkarte 1 Gbit/s, RJ45-Anschluß; mehrere USB 3.x Schnittstellen, WLAN-fähig, Bluetooth, …
- zusätzliche Sicherungslaufwerke (siehe Sicherung)
- Garantie bzw. Vorortservice

13.1.4 Notebook

Alternativ zu einem stationären PC bietet ein Notebook mehr Flexibilität (Mobilität) und einen geringeren Platzbedarf. Auf allenfalls benötigtes Zubehör (zweiter Bildschirm, zusätzliche Tastatur, usw.) sollte jedoch nicht vergessen werden. Bei einer Reparatur bzw. einem Komponententausch sind hier meist höhere Kosten zu veranschlagen.

13.1.5 Tablet

Immer mehr kommen Tablets z.B. für den Zugriff „von außen“ auf die Ordinationsdaten (etwa bei Hausbesuchen), oder zur Abfrage von z.B. E-Mails über das Ordinations-WLAN zum Einsatz. Dies erfordert insbesondere eine sichere Verbindung zur Ordination und entsprechend kompatible Arztsoftware bzw. eine entsprechend sichere WLAN-Konfiguration. Sollten Sie ein Tablet im Ordinationsumfeld einsetzen wollen, empfiehlt es sich unbedingt, das mit Ihrem EDV-Anbieter abzusprechen.

13.1.6 Server

Ein Server dient als zentraler Rechner und Datenspeicher. Der Vorteil einer Client/Server-Landschaft ist das gleichzeitige Bereitstellen von Daten und Programmen für mehrere Arbeitsplätze. Der Ausfall eines einzelnen Arbeitsplatzes hat keine Auswirkung auf die restlichen noch funktionierenden Arbeitsplätze.

13.1.7 Drucker

Einzelplatzdrucker können üblicherweise nur von einem PC angesteuert werden, Netzwerkdrucker von jedem PC im Netzwerk.

Nachdem mittlerweile die häufigsten Formulare (mit Einführung des e-Rezeptes 2022 inkl. des Rezeptdruckes) auf „Standard A4-weiß“ gedruckt werden können (*siehe Kapitel 5. Planung der Arztpraxis - Formularwesen*), ist ein eigener Schacht (oder die Einzelblattzufuhr) meist nicht mehr bzw. nur für einzelne spezielle Formulare erforderlich. Besprechen Sie mit Ihrem EDV-Betreuer ob ein Einschacht-Drucker ausreichend ist, oder ob mehrere Schächte notwendig sind.

Tintenstrahldrucker haben den Vorteil, dass Farbdruck relativ günstig möglich ist, in der Geschwindigkeit und der Druckauflösung sind sie jedoch Laserdruckern meist unterlegen.

Laserdrucker (Schwarz/Weiß, Farbe) sind schnell und haben den Vorteil, dass keine Tinte Eintrocknen kann. Farblaserdrucker sind etwas teurer in Anschaffung und Betrieb.

13.1.8 Router, Firewall, Virenschutz, Internetanbindung

Verbindungen zu Außenwelt werden meist per Router (Mail, Internetanbindung) hergestellt. Idealerweise sollten, aus Sicherheitsgründen, PC's mit einer Internetanbindung keinen Zugriff auf Patientendaten haben.

Sollte eine Trennung nicht möglich sein, oder sie Mailprogramm und Internetzugang auf dem Ordinationsrechner benötigen, verwenden Sie unbedingt eine Firewall und ein Virenschutzprogramm mit automatischer Aktualisierung. Damit erhöhen Sie die Sicherheit in Ihrem Netzwerk vor Zugriffen oder Angriffen aus dem Internet, und verringern das Risiko einer Infizierung durch Malware.

Wichtig ist zu wissen, dass selbst das beste Schutzsystem Ihnen keine 100%ige IT-Sicherheit gewährleisten kann. Das Verhalten des Anwenders (Surfen im Internet, öffnen von Spam-/Virenmails, Passwortschutz, …) entscheidet maßgeblich über das Einschleusen von Viren od. Malware. Eine gezielte Schulung der Anwender gilt als wichtige Prävention, und ist auch lt. DSG dringend erforderlich.

Innerhalb des GIN (Gesundheits-Informations-Netz, e-card-Leitung) können als „Sichere Mail- und Internetanbindung" die Dienste „gesichertes Internet/e-mail über das GIN" - z.B. von A1 (DaMe secure Internet), Drei Business(e-card Mehrwertdienst Internet), Magenta Business (e-card&Internet) - empfohlen werden. Hier wird der GIN-Mehrwertdienstkanal für die Datenübermittlung verwendet. Informationen dazu finden Sie zB unter www.peeringpoint.at (unter MEHRWERTDIENSTE – Dienste & Angebote) bzw. beim entsprechenden Provider.

Wir empfehlen Ihnen, in jedem Fall nur entsprechend „sichere" Produkte des gewählten Providers in Ihrer Arztordination zu verwenden (gesichertes Internet/E-Mail über das GIN, Business-Produkte mit zusätzlichem Virenschutz, Firewall).

Im GNV-Vertrag ist vereinbart, dass zu Ihrem eigenen Schutz, aber auch zum Zwecke des Daten- und Virenschutzes der anderen Teilnehmer des GNV, auf dem Computer, auf welchem das GNV installiert ist, keine gleichzeitige und ungeschützte direkte oder indirekte Verbindung zu anderen Netzwerken insbesondere zum Internet zuzulassen ist.
Darüber hinaus sind sie lt. § 14 (1) Datenschutzgesetz (DSG) verpflichtet
… unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

Nachdem die Faxübermittlung lt. Gesundheitstelematikgesetz für die Übermittlung von sensiblen Daten (Gesundheitsdaten) nur mehr sehr eingeschränkt möglich ist, und ab Mitte 2026 generell nicht mehr erlaubt sein soll, gilt es hier Alternativen zu suchen.

Nähere Auskünfte darüber erhalten Sie in der Ärztekammer für Vorarlberg - EDV-Abteilung (edv@aekvbg.at, Herr Rauch DW 28, Herr Schelling DW 39).

13.1.9 USV Anlage

Ein Stromausfall kann irreparable Schäden in einer Datenbank bzw. auf einem Server verursachen. Bereits ein kurzer Stromausfall >5ms kann das Betriebssystem Ihres Computers zum Absturz bringen.
Die USV-Anlage ist KEINE Notstromversorgung, sondern sorgt dafür, dass bei kurzen Stromausfällen od. größeren Stromschwankungen Ihre EDV nicht unkontrolliert abstürzt. Sollte Ihre Ordinationstätigkeit eine Notstromversorgung erfordern (z.B. bei Durchführung von Operationen), ist diese entsprechend zu planen.

☑ **TIPP:** Planen Sie die Leistung der USV Anlage so, dass auch Ihre Telefonanlage damit versorgt wird. Sollte eine Notstromversorgung angedacht werden, dann stimmen Sie das mit Ihrem Elektriker ab, ev. kann er Sie diesbezüglich beraten.

13.1.10 Tastatur, Maus, Monitor

Tastatur
Kabelgebundene oder kabellose Tastaturen (Funktastaturen) werden angeboten. Zur Gelenkschonung werden besonders ergonomische Modelle angeboten.

Maus
Kabelgebundene oder kabellose Mäuse (Funkmäuse) sind verfügbar. Zur Gelenkschonung werden besonders ergonomische Modelle angeboten.

Monitor
Bildschirme mit 24 bis 32 Zoll Bildschirmdiagonale sind marktüblich (je nach Erfordernis und Platzbedarf). Sollte eine Bildbearbeitung (z.B. Röntgenbilder) vorgesehen sein, ist auf entsprechende Mindestanforderungen (Bildqualität, Auflösung, …) zu achten.

Lebensdauer/Abschreibung
Hardware ist im Regelfall mindestens über 3 – 5 Jahre nutzbar.
Bezüglich steuerlicher Abschreibungsmöglichkeiten (im Jahr der Anschaffung, auf 3 Jahre, …) informieren Sie sich bitte bei Ihrem Steuerberater.

13.1.11 Kosten

Prinzipiell ist zu sagen, dass bei einem PC nicht nur der Prozessor die Leistung definiert, sondern dass die Gesamtkonfiguration entscheidend ist (Arbeitsspeicher, Mainboard, Grafikkarte, ...). Wir raten daher von „Superbilligangeboten“ dringend ab!
Für etwaige Hardware-Ausfälle ist es ratsam einen Servicepartner an seiner Seite zu haben, der einem die Störung rasch beheben kann. Ein Kauf in Großmärkten kann dieser Anforderung meist nicht gerecht werden.

☑ **TIPP:** *Ärgern Sie sich nicht, wenn Ihre EDV-Anlage innerhalb von einigen Monaten stark an Wert verliert. Durch die rasche Entwicklung im Hardwarebereich steigt die Leistung der Geräte ständig, sodass „alte“ Bauteile rasch im Preis sinken.*

13.1.12 Betriebssystem

Das Betriebssystem ist die Kommunikations-Schnittstelle zwischen der eigentlichen Hardware (Festplatte, Drucker, …) und den darauf installierten Anwendungen (Arztprogramm, Word, Excel, …). Es ist die Basis um den Computer überhaupt praktisch nutzen zu können.
Manchmal ergibt sich durch die Verwendung einer bestimmten Anwendung eine Mindestanforderung an das Betriebssystem!

Es wird ganz allgemein zwischen Microsoft Windows-, Unix/Linux- und Applebasierten Betriebssystemen unterschieden.

13.1.13 Arzt-Softwareanforderungen

Die Software sollte einfach und intuitiv zu handhaben sein, ein Maß dafür ist die nötige Einschulungszeit. Bedenken Sie, dass viele Möglichkeiten die Verwendung oft erschweren. Beachten Sie auch, dass ein gutes EDV System für Kassenärzte nicht in gleichem Maß für Wahlärzte geeignet sein muss.

Simulieren Sie beim Testen eines Programms einen Ordinationsablauf und bedienen Sie dabei den PC selbst, nur so können Sie herausfinden, ob Ihnen die Anwendung zusagt. Besuchen Sie Ordinationen von Kollegen in denen das EDV System bereits installiert ist, falls dies möglich ist.

Überlegen Sie einen „Notbetrieb" für den Fall, dass Ihre EDV komplett ausfällt!

Für Vertragsärzte (ÖGK) gibt es in der ÄK:

- eine Liste der in Vorarlberg im Einsatz befindlichen **Programmpakete**
- eine **Referenzliste der Ärzte**, welche elektronisch abrechnen und es erlauben, diese Information weiter zu geben.

Diese Informationen können bei der ÄK für Vorarlberg - EDV-Abteilung - angefordert werden.

13.2 WLAN

Drahtlose Netzwerke, sogenannte WLAN-Lösungen ergänzen zunehmend traditionelle LANs, bei denen der Netzwerkanschluss über Kabelverbindungen realisiert wird. Zum einen bieten sie Flexibilität bei der Arbeitsplatzgestaltung, zum anderen sind für ihren Aufbau keine aufwändigen Verkabelungsarbeiten notwendig. Die steigende Zahl von mobilen Geräten (Notebooks, Smartphones, etc.) fördert die Verbreitung von WLAN zusätzlich. Sicherheitstechnisch entstehen durch WLANs neue Gefährdungen und es sind einige Maßnahmen zu beachten, um nicht durch ihre Einführung die Sicherheit des gesamten Netzwerks zu gefährden.

Die Bedrohung durch WLAN-Angriffe darf nicht unterschätzt werden; das Aufspüren und der unbefugte Gebrauch von Drahtlosnetzen kann für Angreifer sehr einfach sein. Die Nutzung eines solchen ungeschützten Netzes als kostenloser drahtloser Internetzugang ist noch die harmloseste Art des Missbrauchs, das Ausspionieren von z.B. Patientendaten die weitaus bedenklichere Variante.

Es besteht auch die Gefahr, dass Eindringlinge illegale Aktivitäten über das offene WLAN durchführen, für die dann der Betreiber verantwortlich gemacht wird. Ein ungesichertes WLAN kann daher auch zu rechtlichen Problemen führen.

Bei Bereitstellung von WLAN-Zugang für Patienten (z.B. im Wartezimmer) ist auf eine strikte Trennung zum internen Netz (LAN, WLAN) zu achten.

☑ **TIPP:** Wenden Sie sich für die WLAN-Installation/Konfiguration immer an Ihren EDV-Betreuer.

13.3 Datensicherung

Der Datensicherung kommt eine zentrale Bedeutung zu. Es werden Daten unterschiedlichster Art (Befunde, Bilder, Daten für die Abrechnung, usw.) gespeichert. Ohne diese Daten ist ein „regulärer Ordinationsbetrieb“ kaum vorstellbar.
Wir möchten Sie daher im Besonderen auf die folgenden Punkte hinweisen:

Datensicherungskonzept
Es muss definiert und festgehalten werden, WELCHE DATEN (Server, Datenbank, PCs, usw.) WANN (Tagessicherung, Wochensicherung, Monatssicherung, usw.) WOHIN (LTO-Band, usw.) gesichert werden!
Grundsatz: Nach jedem Ordinations-Schluss MUSS gesichert werden.
Wochen-, Monats- oder Jahressicherungen sind absolut wichtig (es gibt somit mehrere Generationen von Sicherungen)! Was passiert, wenn Sie „versehentlich“ Daten löschen, welche sie über Wochen nicht benötigen. Dann werden zwar Sicherungen gemacht, aber immer ohne diese Daten. Stellen Sie zu einem späteren Zeitpunkt fest, dass Daten fehlen, können diese ev. von einer älteren Monatssicherung od. Jahressicherung zurückgeholt werden.

Grundsatz: Eine Sicherung (z.B. Wochensicherung vom Freitag od. Samstag) muss an einem anderen Ort aufbewahrt werden (z.B. Bankschließfach).
Im Falle eines Brandes od. von Naturkatastrophen (Überschwemmungen) sind Sicherungen im Ordinationstresor ev. beschädigt. Die Aufbewahrung einer Sicherung an einem 2. Standort ist unumgänglich!

Daten-Rücksicherungskonzept
Es ist festzuhalten, wie die Datenrücksicherung erfolgen muss.
Sporadisch muss die Wiederherstellbarkeit von Datenträgern überprüft werden (so dass deren Funktionstüchtigkeit gewährleistet ist)!

Verwendung einer professionellen Sicherungssoftware
Wir empfehlen dringend den Einsatz einer professionellen Sicherungssoftware! Es muss z.B. gewährleistet sein, dass die Sicherungssoftware den Anwender automatisch über den aktuellen Status der Sicherung informiert („Sicherung erfolgreich durchgeführt“ od. „Sicherung fehlerhaft“).

Schriftliche Aufzeichnungen der Konfigurationsdaten
Zusätzlich zur eigentlichen Datensicherung ist es sinnvoll, schriftliche Aufzeichnungen über die verwendeten Passwörter und verschiedene Konfigurationsdetails (Internet-Provider, Mail-Accounts, Netzwerkdrucker, ...) anzulegen. Auf diese soll im Notfall rasch zugegriffen werden können!
Bei Änderung der Konfigurationseinstellungen oder der Passwörter müssen die schriftlichen Aufzeichnungen unbedingt aktualisiert werden.

Sicherung über das e-card-Netz
Es wird auch eine Sicherung über das e-card-Netz angeboten. Die Sicherung erfolgt verschlüsselt, kann automatisch ablaufen und ist somit sehr sicher und immer an einem anderen gesicherten Ort.
Für die Wiederherstellung der Daten wird dann der Schlüssel benötigt (und natürlich das e-card-Netz).

Es gibt keine 100%ige Sicherheit (Stromausfall, Brand, usw.)! Durch den Rückgriff auf aktuelle Sicherungen kann jedoch der Datenverlust nahezu ausgeschlossen werden.

☑ **TIPP:** *Besprechen Sie Ihr persönliches Datensicherungskonzept mit ihrem Softwareanbieter, je nach Größe der Datenbank wird er entsprechende Vorschläge machen.*

13.4 Notfallvorsorge-Konzept

Wichtig ist es, schon frühzeitig – also vor einem echten Notfall – Überlegungen anzustellen, wie die Ordinationsabwicklung im Falle eines teilweisen od. totalen EDV-Ausfalles erfolgen kann!
Stellen sie Überlegungen an, was z.B. zu tun ist bei:

- Ausfall der Telefonanlage
- Ausfall der e-card-Leitung (GIN)
- Fehlerhafter Datensicherung (Rückmeldung Sicherung fehlerhaft)
- Einzelne Drucker funktionieren nicht
- Totalausfall der EDV-Anlage
- usw.

13.5 Datenschutz in der Arztpraxis

Basis sind die EU-Datenschutz-Grundverordnung (EU-DSGVO 2016/679 und das Datenschutz-Anpassungsgesetz 2018 (DSG, BGBL 2017/120).

Das Datenschutzgesetz regelt den Umgang mit personenbezogenen, schutzwürdigen Daten. Zu „Personen" sind nur natürliche Personen zu zählen; bei den Daten wird u.a. zwischen besonderen Kategorien (z. B. Gesundheitsdaten, religiöse oder politische Überzeugung) und personenbezogenen Daten (Adressen, Geburtsdatum, Kundendaten) unterschieden.

Aus den Vorschriften der EU-DSGVO und den DSG ergeben sich einige typische Anforderungen für den Umgang mit personenbezogenen Daten:

- Alle Datenanwendungen, mit denen diese Daten verarbeitet werden, müssen ab dem 25.05.2018 intern im Verzeichnis der Verarbeitungstätigkeiten dokumentiert werden (Artikel 30 EU-DSGVO).
- Ärzte müssen also ein entsprechendes Verarbeitungsverzeichnis erstellen und aktuell halten.
- Den Personen, deren Daten verwendet werden, stehen besondere Betroffenenrechte (z.B. Auskunftsrecht) zu (Artikel 12-23 EU-DSGVO, § 3b Ärztegesetz).
- Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke verwendet werden.
- Die Daten müssen vor Zerstörung und Verlust und vor ordnungswidriger oder unrechtmäßiger Verwendung geschützt werden (Zutritts- und Zugriffsschutzmaßnahmen, Protokollierung).
- Ärzte müssen ein IT-Sicherheitskonzept erstellen und aktuell halten.
- Mitarbeiterinnen und Mitarbeiter
  - sind in Form einer Geheimhaltungsverpflichtung auf das Datengeheimnis zu verpflichten
  - müssen bezüglich IT-Sicherheit (z.B. sichere Nutzung E-Mail und Internet) geschult werden
  - usw.
- Details siehe *Kapitel 40. Datenschutz-Grundverordnung*

Für weitere Auskünfte steht Ihnen Herr Mag. Nitz gerne zur Verfügung.
Info: Mag. Stefan Nitz, Tel. 05572 / 21900 – 46
E-Mail: stefan.nitz@aekvbg.at

Die Bundeskurie Niedergelassene Ärzte stellt Ihnen eine Möglichkeit zur Verfügung, ein „IT Sicherheitskonzept" für Ihre Ordination/en zu erstellen. Dies erfolgt mittels einer Online-Selbstevaluierung, die Sie auf dieser Webseite durchführen können.
https://itsicherheitskonzept.aerztekammer.at/

13.6 Cloud-Lösungen

Auch für die komplette Arztsoftware gibt es mittlerweile Cloud-Lösungen. Wichtig ist aber hier insbesondere abzuklären, welche Services (Anbindung Geräte, Anbindung e-Card, Befundübermittlung per GNV, usw.) tatsächlich alle über die Cloud verfügbar sind.

Lt. der aktuellen Fassung des Datenschutzgesetzes DSG bzw. der Datenschutzgrundverordnung (EU-DSGVO handelt es sich bei Gesundheitsdaten um besondere Kategorien personenbezogener Daten (Artikel 9 DSGVO).
Hier sind insbesondere zu beachten:

Artikel 28 - Auftragsverarbeiter

- *… Garantie dafür, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der EU-DSGVO erfolgt …*
- *… der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch …*
- *... die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags (Gegenstand und Dauer der Verarbeitung, Arzt und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen, Pflichten und Rechte des Verantwortlichen, …) …*
  - *Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen*
  - *zur Verarbeitung befugte Personen müssen sich zur Vertraulichkeit verpflichtet haben*
  - *der Auftragsverarbeiter ergreift alle gemäß Artikel 32 erforderlichen Maßnahmen*
  - *der Auftragsverarbeiter unterstützt den Verantwortlichen seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte von betroffenen Personen*
  - *alle personenbezogenen Daten sind nach Abschluss der Verarbeitungsleistungen zu löschen oder zurück zu geben*
  - *dem Verantwortlichen sind alle erforderlichen Informationen zum Nachweis der Einhaltung der im Artikel 28 genannten Pflichten zur Verfügung zu stellen*
  - *usw.*

Artikel 32 - Sicherheit der Verarbeitung

- *... unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos … treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten …*

Unter den folgenden Voraussetzungen sind Cloud-Lösungen (z.B. Office 365) für Daten besonderer Kategorien denkbar

- Server ausschließlich in der EU (europäisches Datenschutzrecht) oder einem Drittland mit angemessenem Schutzniveau
- vertraglich garantiert, dass die Firma keine Beziehungen mit der USA hat (patriot act)
- verschlüsselte Datenübermittlung und verschlüsselte Datenablage
  (bzw. im besten Fall nur bereits lokal verschlüsselte Daten übermitteln wenn das möglich ist)
- vertraglich garantiert die EU-DSGVO bzw. das jeweils gültige DSG einzuhalten (siehe oben insbesondere Artikel 28 und 32).

Von „großen“ weltweit tätigen Anbietern können diese Voraussetzungen meist nicht erfüllt werden bzw. ist darauf zu achten, dass entsprechende Zusagen/Garantien dazu gibt.

Für weitere Auskünfte steht Ihnen Herr Mag. Nitz gerne zur Verfügung.

Info: Mag. Stefan Nitz, Tel. 05572 / 21900 – 46
E-Mail: stefan.nitz@aekvbg.at

13.7 IT-Sicherheit

Zudem möchten wir diesbezüglich auf die Kampagne der Bundeskurie der niedergelassenen Ärzte zur IT-Sicherheit verweisen (https://www.arztinvorarlberg.at/aek/public/edv).

13.7.1 Sicherer Umgang mit Passwörtern

Wir möchten Sie hiermit zum sorgsamen Umgang mit Benutzernamen und Passwörtern, insbesondere in Verbindung mit Internetportalen, auffordern.

Folgende Regeln sind hier unbedingt zu beachten:

- Bei privat genutzten Diensten im Internet (z.B. Amazon, Google, eBay, iTunes, Newsletter, Internetportale, ...) dürfen keine Ordinations-Mailadressen verwendet werden (weder als Benutzername, noch als Mail-Empfänger). Hier ist nach Möglichkeit eine private Mailadresse von öffentlichen Diensten wie GMX, Outlook.com, … vor zu ziehen.
- Für Dienste im Internet, egal ob privat oder im Rahmen Ihrer ärztlichen Tätigkeit, sollten sie stets unterschiedliche Kennwörter verwenden.
  Es stellt ein hohes Sicherheitsrisiko dar, wenn für verschiedene Dienste die gleichen Anmeldedaten verwendet werden, da ein Angreifer durch das Erlangen einer einzelnen Passwort/Benutzer-Kombination Zugriff auf weitere Dienste hätte.
- Des Weiteren ist die Verwendung von Kennwörtern aus der eigenen Ordination wie z.B. das Anmelde-Kennwort restriktiv zu unterlassen.

Durch die strikte Trennung von Privat und Ordination kann - auch bei Identitätsdiebstahl - der Übergriff von einem in den anderen Bereich weitestgehend vermieden werden.

- Folgende Regeln zum Passwortgebrauch sollten insbesondere beachtet werden:
  - Das Passwort soll nicht leicht zu erraten sein wie z.B. Namen, Kfz-Kennzeichen, Geburtsdaten.
  - Trivial-Passwörter (qwertzui, aaaaaaaa, 08/15, 4711 usw.) sind ebenfalls nicht zu empfehlen. Sie sind oft schon zu erkennen, wenn Sie jemand beim Eingeben Ihres Passworts beobachtet.
  - Innerhalb des Passwortes sollte mindestens ein Groß-, ein Kleinbuchstabe, eine Ziffer und wenn möglich ein Sonderzeichen verwendet werden.
  - Es sollen „lange“ Passwörter verwendet werden - Empfehlung liegt derzeit bei 12-16 Zeichen.

☑ TIPP: Passwörter sollen komplex sein, um nicht erraten zu werden - aber auch einfach, damit sie nicht schriftlich notiert werden müssen.

Bilden Sie Ihr Passwort z.B. aus den Wortanfängen und Satzzeichen einfacher Merksätze.

z.B.:

Heute 23.04. beschloss ich mein Passwort zu ändern.	=>	H23.04.bimPzä
Der Mai ist schön. Es wird warm. Ich freue mich.	=>	DMi$.Eww.1fm

Alternativ könnte auch ein langes, aber leichter zu merkendes Passwort gewählt werden.
Also einfach ein paar Worte aneinander gereiht: => hundhausvogelentegrabRom-4

Einen kleinen Überblick gibt es hier: http://de.wikipedia.org/wiki/Passwort
Sehr interessant ist die Tabelle, wie schnell ein Passwort geknackt werden kann.

☑ **TIPP:** *Passwortmanager: Weil die Anzahl der schwierig zu merkenden Kennwörter mitunter zu groß und nicht mehr zuordnungsfähig wird, empfehlen wir die Verwendung einer Kennwortverwaltung (Passwortmanager). Es handelt sich hierbei um ein Computerprogramm, mit dessen Hilfe Benutzernamen und Kennwörter verschlüsselt gespeichert und verwaltet werden können.*

13.7.2 IT-Sicherheitskonzept

Die Datenschutzgrundverordnung verlangt, dass sich jeder, der personenbezogene Daten verarbeitet, mit den datenschutzrechtlichen Vorgaben in seinem Verantwortungsbereich auseinanderzusetzen hat. Die ordinationsführende Ärztin bzw. der ordinationsführende Arzt als datenschutzrechtlich Verantwortliche bzw. Verantwortlicher hat dabei insbesondere geeignete technische und organisatorische Datensicherheitsmaßnahmen zu ergreifen. Art 32 der EU-Datenschutzgrundverordnung normiert folgendes: Datenschutzrechtlich Verantwortliche müssen bei der Datenverarbeitung

- unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung,
- sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Höhe des Risikos für die Rechte und Freiheiten natürlicher Personen

geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Unter dem Titel „IT-Sicherheitskonzept“ normiert § 8 Abs 1 Gesundheitstelematikgesetz idF BGBl I 2018/37, dass Gesundheitsdiensteanbieter, wie insbesondere Ärztinnen und Ärzte, alle gemäß Art 32 DSGVO und gemäß Gesundheitstelematikgesetz getroffenen Datensicherheitsmaßnahmen auf Basis eines IT-Sicherheitskonzeptes zu dokumentieren haben. Aus dieser Dokumentation muss insbesondere hervorgehen, dass sowohl der Zugriff als auch die Übermittlung der Daten ordnungsgemäß erfolgt und die Daten Unbefugten nicht zugänglich sind.

Das IT Sicherheitskonzept ist die Dokumentation der ergriffenen organisatorischen und technischen Maßnahmen. Die Dokumentation setzt voraus, dass die im IT Sicherheitskonzept beschriebenen Maßnahmen auch im Ordinationsbetrieb faktisch umgesetzt sind. Da IT-Sicherheit insbesondere von Technologie bestimmt ist, die einer stetigen technischen Weiterentwicklung unterliegt, müssen die gesetzten Maßnahmen in den Ordinationen regelmäßig evaluiert und das IT-Sicherheitskonzept aktualisiert werden.

Dass die entsprechenden Angaben und Dokumentationen mit der Zeit immer aufwändiger und komplexer werden, ist evident, wenn man beispielsweise an die Zunahme von smarten, also WLAN-fähigen Geräten denkt. Um hier eine große Erleichterung zu schaffen, hat die Bundeskurie niedergelassene Ärzte ein Servicetool entwickelt.

Dabei handelt es sich um einen Online-Fragenkatalog mit über 300 Elementen, mit dem Kapitel für Kapitel die Dokumentation so präzise, zeitsparend und einfach wie möglich abgearbeitet werden kann. Der Login funktioniert über SSO über die URL:
https://itsicherheitskonzept.aerztekammer.at/

☑ **TIPP:** *Informieren Sie sich über das von der Bundeskurie niedergelassene Ärzte entwickelte Servicetool zur Ausarbeitung/Erstellung Ihres IT-Sicherheitskonzeptes (https://itsicherheitskonzept.aerztekammer.at/). Das erfolgt mittels einer Online-Selbstevaluierung, die Sie auf dieser Website durchführen können. Sie können Teile des Fragebogens auch von Ihrem/n externen IT Dienstleister/n beantworten lassen. Die Auswertung der Antworten, die Sie abschließend erhalten, zeigt Ihnen, wie ausgereift Ihre Vorsichtsmaßnahmen in Sachen IT-Sicherheit zum gegenwärtigen Stand sind, und welche konkreten Maßnahmen Sie ergreifen können, um diesen Status weiter zu verbessern.*

13.8 Informationen zur e-card

Nachdem mit Einführung des e-Rezeptes auch Wahlärzte mit Rezepturrecht zur Verwendung des e-Rezeptes verpflichtet wurden, müssen eben auch Wahlärzte künftig sich um eine e-card-Ausstattung kümmern.

13.8.1 Ablauf e-card anfordern

1. Arztsoftware-Firma auswählen (Details siehe eigener Punkt)
   Vorab mit der Arztsoftware-Firma klären ob bzw. welche e-card-Services über die Arztsoftware abgedeckt werden können.

2. Informationen über die vorhandenen e-card-Provider einholen (ÖGK Vertragspartnerabteilung kontaktieren).

3. Angebote der e-card Provider (A1-Telekom, Hutchison Drei, Magenta, Infotech EDV, spusu) einholen bzw. prüfen welche Provider in meiner Region überhaupt tätig sind.

4. Ausstattungsauftrag (Zeitpunkt usw.) in Abstimmung mit der gewählten Arztsoftware-Firma erteilen.

5. Hierzu muss die genaue Ordinationsadresse bekannt sein, damit der Provider überprüfen kann ob eine e-card-Leitungsanbindung möglich ist!

6. Informationen zu den Mehrwertdiensten einholen

7. Mehrwertdienste sind zB: Befundübermittlung, gesicherter Internetzugang, e-Mail, etc. Damit steht dem Arzt über das GIN (die e-card-Leitung) faktisch eine weitere Datenleitung für Zwecke seiner Ordination zur Verfügung. Im Vordergrund steht dabei die Einhaltung der Sicherheitsrichtlinien, die hohe Verfügbarkeit und eine sehr hohe Qualität des GIN. Damit sind auch z.B. Fernwartung der Arztsoftware und Teleworking möglich. Achtung! Es kann auch MEHR GIN-BANDBREITE über die Provider erworben werden.
   In Vorarlberg wird die Befundübermittlung über das Gesundheitsnetz Vorarlberg (GNV) angeboten.

8. Kontaktaufnahme ÖGK (sobald Ordinationsadresse und Niederlassungsbeginn bekannt sind)

Anforderung Vertragspartnernummer, Formulare, …

9. Allenfalls mit dem „Vorgänger“ vereinbaren, dass dieser seinen GIN-Vertrag über die ÖGK nicht kündigt, sondern eine Ordinationsnachfolge deponiert - Vertragsbedingungen können dann übernommen werden!

10. Mit der "Meldung bei der ÖGK" (Vergabe der Vertragspartnernummer) erfolgt auch die Meldung zur Teilnahme am e-card System. D.h. die SV-Chipkarten Betriebs- u. Errichtungsgesellschaft leitet diese Information an die jeweiligen Telekommunikations-Provider weiter, von welchen Sie dann zusätzlich ev. noch kontaktiert werden.

Nähere Auskünfte zur **e-card** erhalten Sie bei

- **im Kapitel 42 des Praxisgründungsleitfadens**

- ÖGK
  Vertragspartnerabteilung
  Frau Martina Troppacher
  E-Mail: martina.troppacher@oegk.at Tel. 050 76619 - 1651

- e-card Serviceline (Hotline bei Störungen)
  Tel. 050 124 – 33 22

- e-card für Patienten
  Tel. 050 124 33 11

- im Internet
  http://www.chipkarte.at
  http://www.sozialversicherung.at

weitere Informationen zum e-card System (Systemanforderungen, Varianten der Anbindung, GIN, GINS, GINO usw.) und zu ELGA-Anwendungen (e-Medikation, e-Impfpass):
www.chipkarte.at → Gesundheitsdiensteanbieter → e-card-System / e-card Services / ELGA-Anwendungen / Support

Provider-Auswahl:
www.chipkarte.at → Gesundheitsdiensteanbieter → e-card System → GIN Zugangsnetz-Provider

Peering Point, Mehrwertdienste, usw.:
http://www.peeringpoint.at/

13.8.2 e-card-Kosten

Hinsichtlich der Zusammensetzung der Kosten für die e-card-Infrastruktur sind drei Bereiche zu unterscheiden:

1. Von der „Rundfunk und Telekom Regulierungs-Behörde“ den Providern vorgeschriebener Kostenanteil
2. Kosten für Geräte-Ausstattung (Router, GINO-Anbindung, LAN-CCR)
3. Kosten für Servicelevel
4. Kosten für Installation, Inbetriebnahme, Wartung, …

Für Vertragsärzte, die vor dem 1.1.2009 in Vertrag genommen wurden, wird ab 1.1.2010 für Pkt. 3. ein Zuschuss gewährt (12,50 - 15,00 € providerabhängig) (ursprünglich wurden diese Kosten aus Pkt. 3. gänzlich vom Dachverband getragen
Vertragsärzte, die nach dem 1.1.2009 in Vertrag genommen wurden, müssen laut e-card-Gesamtvertrag die gesamten Kosten für Pkt. 3. übernehmen.

Achtung: Übernimmt ein „neuer" Vertragsarzt eine Kassenstelle, so kann er auch die e-card-Infrastruktur und den Provider-Vertrag seines Vorgängers übernehmen. Liegt der Vertragsabschluss des Vorgängers vor dem 1.1.2009 gelten für den Nachfolger die identen (etwas günstigeren) vertraglich bevorzugten Bestimmungen.
Wichtig: Voraussetzung ist jedoch, dass der Vorgänger den e-card-Vertrag noch nicht gekündigt hat!

Aktuelle Informationen zu Preisen und Bandbreiten erhalten Sie beim entsprechenden e-card-Provider. Allgemeine Informationen dazu finden Sie auch auf www.peeringpoint.at.

13.8.3 e-card-Services

Beispielhaft sind hier die folgenden Services angeführt (Details siehe https://chipkarte.at/ → Gesundheitsdiensteanbieter → e-card Services).

- Sozialversicherungsnummern-Abfrageservices (SAS)
- Arzneimittelbewilligungsservice (ABS)
- Elektronische Arbeits(un)fähigkeitsmeldung (eAUM)
- Vorsorgeuntersuchung (VU = DBAS Dokumentationsblat-Annahme-Service)
- Infotool für Erstattungskodex (eÖKO-Tool)
- Abfrage Rezeptgebührenbefreiung (Obergrenze für Rezeptgebühren REGO)
- Elektronisches Kommunikationsservice (eKOS)
- Elektronisches Rezept (eRezept)

Achtung: Nicht alle e-card-Services stehen Wahlärzten zur Verfügung.

13.9 Informationen zu ELGA

Informationen zu ELGA finden Sie auf https://www.elga.gv.at/.

Vorab mit der Arztsoftware-Firma klären ob bzw. welche ELGA-Services über die Arztsoftware abgedeckt werden können.

Beispielhaft sind hier die folgenden ELGA-Services angeführt:

- e-Medikation
- e-Befunde
- e-Impfpass

Nähere Auskünfte zu ELGA bzw. im Falle von technischen Problemen erhalten Sie bei

- ELGA Serviceline
  Tel. 050 124 – 44 22
  support@elga-serviceline.at

13.10 GNV - Gesundheitsnetz Vorarlberg

Das GNV dient in erster Linie dem raschen, kostengünstigen und auf höchstem Niveau der Datensicherheit befindlichen elektronischen Austausch von medizinischen Daten insbesondere zwischen den niedergelassenen Ärzten, den Großlabors und den Spitälern.

Die Ärztekammer für Vorarlberg war bereit, dieses Netz aufzubauen, zu betreiben und dafür Vorleistungen zu erbringen. Die teilnehmenden Krankenanstalten waren von Beginn an maßgeblich in dieses Projekt eingebunden.

Die entsprechende Infrastruktur (Hardware und Software) wird im Auftrag der Ärztekammer von der VTG (Vorarlberger Informatik- und Telekommunikationsdienstleistungsgesellschaft mbH) betrieben. Die VTG befindet sich zu 95% im Besitz des Landes Vorarlberg und zu 5% im Besitz der Gemeindeinformatik GmbH. Sie betreibt auch die Datennetze des Landes und der Gemeinden.

Über welche Verbindungen werden die Befunde übertragen?
Die zur Übertragung notwendigen Datenverbindungen, Programme zur Bereitstellung der Daten für die Übertragung und zur Darstellung der empfangenen Daten etc. sind nicht Teil des GNV-Dienstes sondern vom Teilnehmer auf eigene Kosten und Gefahr bereit zu stellen. Bei jenen Ärzten, welche den GIN-ADSL-Zugang für die e-card installiert haben, ist dieser Zugang auch für die GNV-Dienste verwendbar.

Auch über einen externen DSL-Zugang (Internet) kann die Befundübermittlung erfolgen.

Übertragung von Bilddaten im GNV
Seit 2010 ist auch die Übertragung von elektronischen Bildern (von Radiologen und MR-Instituten) über das GNV möglich.

Übertragung von PDF-Dokumenten
GNV-Teilnehmer haben die Möglichkeit, PDF-Dokumente (mit/ohne Patientenbezug) rasch, komfortabel, sicher und allen gesetzlichen Vorgaben entsprechend, zu übermitteln. Bei entsprechender Einbindung ins Programmpaket (Arzt, Krankenhaus) erfolgt die Übermittlung direkt aus der Anwendung heraus (ähnlich dem Befundversand).

Weitere Informationen
- zur Teilnahme (Voraussetzungen, Vertrag mit der Ärztekammer, usw.)
- zur Installation (wer installiert, Kosten, usw.)
- zu den Kosten (der verschiedenen Varianten - Senden/Empfangen/DICOM-Bilddatenübermittlung - usw.)
- zur Zertifizierung (zur Verschlüsselung der Befunde, usw.)
- zum sicheren Internetzugang (Empfehlung)

Nähere Auskünfte darüber erhalten Sie in der Ärztekammer für Vorarlberg - EDV-Abteilung (edv@aekvbg.at, Herr Rauch DW 28, Herr Schelling DW 39) oder im Internet https://www.arztinvorarlberg.at/aek/public/edv.

13.11 Elektronische Abrechnung (Vertragsärzte)

Vertragsärzte sind zur elektronischen Abrechnung verpflichtet.
Die Abrechnung für die ÖGK wird - im Auftrag der ÖGK - in der Ärztekammer für Vorarlberg durchgeführt. Dazu **muss sich der Arzt mittels eines Formblattes schriftlich bei der Ärztekammer für Vorarlberg anmelden.**

Die Übermittlung dieser Abrechnungsdaten muss in elektronischer Form (per GNV) erfolgen.
Nähere Informationen (Anmeldung, Satzaufbau usw.) können bei der Ärztekammer für Vorarlberg – Kassenärztliche Verrechnungsstelle - angefordert werden.

Info: Klaus Hausmann, Tel. 05572 / 21900 – 36
E-Mail: klaus.hausmann@aekvbg.at

13.11.1 ÖGK-Honorartarif / Ärzte + Zuweisungsstellen

Der ÖGK-Honorartarif wird von der Ärztekammer für Vorarlberg in elektronischer Form zur Verfügung gestellt, oder kann als Druckversion angefordert werden.
Die Daten der Ärzte und Zuweisungsstellen (Spitäler) werden von der Ärztekammer für Vorarlberg in elektronischer Form zur Verfügung gestellt.
Nähere Informationen können bei der Ärztekammer für Vorarlberg - EDV-Abteilung (Herren Rauch und Schelling) - angefordert werden.

13.12 Registrierkassenpflicht

Details dazu finden Sie in Kapitel 7 (Honorierung der ärztlichen Tätigkeit) unter Pkt „Registrierkassen- und Belegerteilungspflicht“.

☑ **TIPP:** *Informieren Sie sich bei Ihrem Steuerberater, ob die generelle Verpflichtung für Sie zum Tragen kommt. Klären Sie mit Ihrem Arztsoftware-Hersteller die möglichen Umsetzungsvarianten.*

13.13 Weitere Auskünfte

Für weitere Auskünfte stehen die EDV-Mitarbeiter der ÄK für Vorarlberg gerne zur Verfügung.

Info: Hans-Peter Rauch, Tel. 05572 / 21900 – 28
E-Mail: edv@aekvbg.at

Info: Günter Schelling, Tel. 05572 / 21900 – 39
E-Mail: edv@aekvbg.at