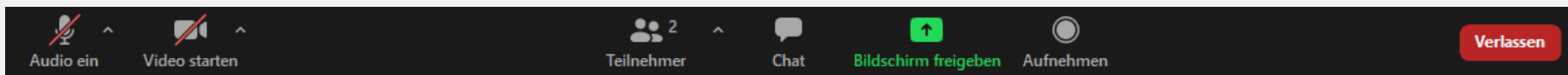
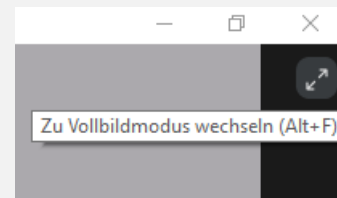


Digitalisierung in der Arztpraxis – Teil 3

Herzlich
willkommen!

Interaktion mit Zoom

- alle Teilnehmer*innen sind zu Beginn stumm geschaltet
- für die bessere Ansicht: Vollbildmodus oben rechts anschalten
- Erklärung der Symbole der unteren Leiste



↑
Funktionen können für Fragen aktiviert werden; Video ist nicht nötig, kann aber genutzt werden

↑
Anzahl der aktuellen Teilnehmer*innen; Klick auf den Button = Anzeige der Teilnehmerliste.

↑
Chatfunktion: Rückfragen gerne bevorzugt via Mikrofon stellen oder aber via Chatfunktion direkt an den **Host**. Die Teilnehmer*innen sehen Ihre Fragen nicht.

↑
Nicht für die Teilnehmer*innen möglich.

↑
Die Präsentation wird für interne Zwecke aufgezeichnet. Sie erhalten später die Präsentation als PDF.

↑
Hier verlassen Sie das Meeting.

Vorstellung der Referenten

- **Frank Winsel**
Geschäftsführer der W&B GmbH
- **Kai-Uwe Quast**
Vertriebsleiter der W&B GmbH
- **Stephanie Schöllermann**
Staatl. gepr. Betriebswirtin Marketing



Vorstellung der W&B GmbH

- seit 1995 Spezialisten im Bereich Digitalisierung, IT-Sicherheit und Datenschutz
- unterschiedliche Geschäftsbereiche: Medical, Industrie, Handel usw.
- langjähriger Technologiepartner der Ärzten Genossenschaft Nord eG in den Bereichen IT-Sicherheit und Praxisdigitalisierung



AGENDA.

Teil 1: Digitale-Versorgung-Gesetz (DVG)

- Was ist das DVG und was bedeutet es?
- Wie ist die momentane IT-Situation?
Warum wurde das DVG beschlossen?
- IT-Sicherheitsmaßnahmen im Zuge des DVG

Bedeutung des Digitale-Versorgung-Gesetz (DVG)

- § 75b SGB V – regelt die IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung
- Zeitschiene
 - verabschiedet am 19.12.2019
 - tritt zum 01.01.2021 in Kraft
 - einzelne Maßnahmen treten in Stufen in Kraft:
01.04.21 / 01.07.21 /
01.01.22 / 01.07.21 / 10.07.22



Bedeutung des Digitale-Versorgung-Gesetz (DVG)

- maßgeblich beteiligt ist hier das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- die Maßnahmen richten sich nach dem Modell des „BSI Grundschutz“



Bedeutung des Digitale-Versorgung-Gesetz (DVG)

- Link zum Dokument „Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ der KBV:

https://www.kbv.de/media/sp/RiLi_75b_SGB_V_Anforderungen_Gewae_hrleistung_IT-Sicherheit.pdf



Wie ist die momentane IT-Situation?

Warum wurde das DVG beschlossen?

- hohe IT-Sicherheit wird vorausgesetzt für Dienste und Anwendungen im medizinischen Umfeld (wie z. B. die Telematikinfrastruktur) - daher auf die DSGVO achten bevor das DVG umgesetzt wird
- trotz der Richtlinien der DSGVO keine homogene, sichere IT-Landschaft – IT-Sicherheitsvorfälle treten immer häufiger auf und sind gravierend



Wie ist die momentane IT-Situation?

1. Datenschutz-Grundverordnung (DSGVO)

- https://www.datenschutz-bayern.de/technik/best_practices/medizin.pdf

und

2. Digitale-Versorgung-Gesetz (DVG)

- https://www.kbv.de/media/sp/RiLi_75b_SGB_V_Anforderungen_Gew_aehrleistung_IT-Sicherheit.pdf

A. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

I. PRÄAMBEL

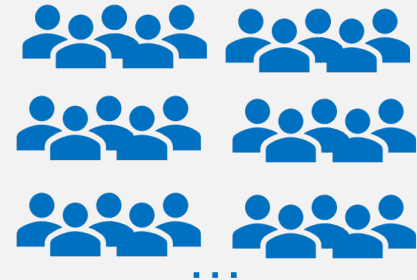
Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der **technisch-organisatorische Maßnahmen im Sinne von Artikel 32 Datenschutz-Grundverordnung** zu standardisieren. Die hier getroffenen Richtlinien erfüllen diesen Auftrag und dienen damit dem Zweck, die Handhabung der **Vorgaben der Datenschutz-Grundverordnung** im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen –psychotherapeutischen Praxis. Die Richtlinie legt technischen Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.

IT-Sicherheitsmaßnahmen im Zuge des DVG

Die umzusetzenden Anforderungen richten sich nach der Größe der Praxis.

- **Praxis:** Eine vertragsärztliche Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen.
- **Mittlere Praxis:** Eine vertragsärztliche Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betrauten Personen.
- **Großpraxis:** Eine Praxis mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder eine Praxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Labore).



IT-Sicherheitsmaßnahmen im Zuge des DVG

- Mitarbeiterunterweisung
(Awareness-Schulung)

4 Passwort-Schutz

Der Zugang zu personenbezogenen Daten jeglicher Art ist Unbefugten, insbesondere Cyberkriminellen, durch geeignete Maßnahmen zu erschweren. Starke Passwörter helfen dabei im Alltag, die Logins von Beschäftigten wirksam abzusichern.

- ☐ Bewusstsein bei Beschäftigten, was starke Passwörter sind und wie mit diesen umzugehen ist (z. B. keine Haftnotizen am Arbeitsplatz, niemals weitergeben, ...)
- ☐ Empfehlung zur Vermeidung leicht zu erratender Passwörter oder Passwortbestandteile

DSGVO nach https://www.datenschutz-bayern.de/technik/best_practices/medizin.pdf



IT-Sicherheitsmaßnahmen im Zuge des DVG

- Mitarbeiterunterweisung
(Awareness-Schulung)
- Monitoring, EventLock, Überwachung
der PC- und Serversysteme



IT-Sicherheitsmaßnahmen im Zuge des DVG

- Mitarbeiterunterweisung (Awareness-Schulung)
- Monitoring, EventLog, Überwachung der PC- und Serversysteme
- Patch-Management aller Server und PC-Systeme (auch an Third-Party-Produkte denken)

1 Patch Management

Veraltete Softwarestände bergen ein erhöhtes Angriffsrisiko wegen potentieller Schwachstellen. Die eingesetzte Software muss daher durch regelmäßige Sicherheitsupdates aktuell gehalten werden.

- ☐ Konzept zum Patch Management vorhanden (u. a. Update-Plan mit Übersicht der eingesetzten Software)
- ☐ Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software, Fachanwendungen und medizinische Geräteumgebung (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)
- ☐ Ausschließlicher Einsatz von Desktop-Betriebssystemen, für die der Hersteller/Maintainer beim Bekanntwerden von Schwachstellen Sicherheitsupdates zur Verfügung stellt
- ☐ Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server
- ☐ Automatische Updates der Desktop-Betriebssysteme (direkt vom Hersteller oder durch zentrale Verteilung)

IT-Sicherheitsmaßnahmen im Zuge des DVG

- Mobile-Device Management (MDM):
 - Schutz vor Schadsoftware
 - nur vertrauenswürdige Apps
 - kein Mischbetrieb (Privat/Praxis)
 - Verschlüsselung und automatisches Löschen bei Missbrauch/Verlust



IT-Sicherheitsmaßnahmen im Zuge des DVG

- Mobile-Device Management (MDM):
 - Schutz vor Schadsoftware
 - nur vertrauenswürdige Apps
 - kein Mischbetrieb (Privat/Praxis)
 - Verschlüsselung und automatisches Löschen bei Missbrauch/Verlust
- Antivirus-Software

2 Malware-Schutz

Ein Befall mit Schadcode führt oft zu einer erheblichen IT-Störung. Durch Antiviren-Programme werden zwar nicht alle Schadcode-Varianten erkannt, aber viele Standardangriffe abgefangen. Ein wirksamer Anti-Malware-Schutz ist folglich einzusetzen.

- ☐ Endpoint Protection auf jedem Arbeitsplatzrechner
- ☐ Tägliche automatische Aktualisierung der Antivirensignaturen
- ☐ Zentrale Erfassung von Alarmmeldungen durch die IT-Administration
- ☐ Klare Anweisungen an Beschäftigte zum Umgang mit Alarmmeldungen

DSGVO nach https://www.datenschutz-bayern.de/technik/best_practices/medizin.pdf

IT-Sicherheitsmaßnahmen im Zuge des DVG

- Firewall
 - Total Security (empfohlen)
 - Content Filter
 - HTTPS Überwachung
 - Web-App-Firewall
 - Maskierung ausgewählter Inhalte

14 Firewall

Zugriffsversuche von außen auf den eigenen Betrieb sind nicht zu verhindern. Wichtig ist es, diese bestmöglich durch ein Firewall-Regelwerk zu blockieren und zu protokollieren, um Gefahren zu erkennen und Sicherheitsmaßnahmen bedarfsgerecht zu gestalten.

- ❑ Abschottung aller internen Server, PCs und am internen Netz angebundenen medizinischen Geräte vom Internet durch eine Firewall gegenüber dem Internet; „Air Gap“, also die Trennung vom Netzwerk, sollte bei kritischen Systemen, sofern verhältnismäßig möglich, umgesetzt werden
- ❑ Regelmäßige Überprüfung der ordnungsgemäßen Konfiguration der Firewall (z. B. mittels Portscans auf die eigenen IP-Adressen von extern und periodischer Pentests)

DSGVO nach https://www.datenschutz-bayern.de/technik/best_practices/medizin.pdf

IT-Sicherheitsmaßnahmen im Zuge des DVG

- Firewall
 - Total Security (empfohlen)
 - Content Filter
 - HTTPS Überwachung
 - Web-App-Firewall
 - Maskierung ausgewählter Inhalte
- Verschlüsselung der Datenträger



IT-Sicherheitsmaßnahmen im Zuge des DVG

- Firewall
 - Total Security (empfohlen)
 - Content Filter
 - HTTPS Überwachung
 - Web-App-Firewall
 - Maskierung ausgewählter Inhalte
- Verschlüsselung der Datenträger
- Backup (Wiederherstellungskonzept)

7 Backups

Ausfälle von Datenträgern, sei es durch Störungen oder Cyberattacken, können nachhaltige Schäden bis hin zum Totalausfall eines Betriebs führen. Regelmäßige Sicherungen wichtiger Datenbestände sind daher Voraussetzung, um einen IT-Ausfall möglichst schadlos zu überstehen. Zu beachten bleibt, dass Trojaner je nach Ausgestaltung auch auf Backups übergreifen können.

- ☐ Vorhandensein eines schriftlich fixiertes Backup-Konzepts
- ☐ Regelmäßige Überprüfung, ob mindestens ein Backup täglich durchgeführt wird

DSGVO nach https://www.datenschutz-bayern.de/technik/best_practices/medizin.pdf

IT-Sicherheitsmaßnahmen im Zuge des DVG

- Firewall
 - Total Security (empfohlen)
 - Content Filter
 - HTTPS Überwachung
 - Web-App-Firewall
 - Maskierung ausgewählter Inhalte
- Verschlüsselung der Datenträger
- Backup (Wiederherstellungskonzept)
- Berechtigungskonzept/Gruppenrichtlinien

5 Rollen-/Rechtekonzept

Nutzer sollen nur auf die personenbezogenen Daten zugreifen können, die für ihre Tätigkeit erforderlich sind. Durch Einführung von Benutzerrechten zu bestimmten Rollen (z. B. Buchhaltung, IT-Administration) werden unterschiedliche Rechte an konkrete Personen zugewiesen.

- ☐ Erstellen von Rollenprofilen für die Beschäftigten unter Einbeziehung der Einträge des Verzeichnisses der Verarbeitungstätigkeiten
- ☐ Über das Rollen-/Rechtekonzept den Zugang zu Informationen und Gebäuden/Bereichen gezielt steuern und reglementieren
- ☐ Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug) an die Mitarbeiter etablieren
- ☐ Regelmäßige Überprüfung (z. B. einmal pro Jahr), ob die Zuweisung der Rollen den Vorgaben entspricht sowie, ob die Rollen noch den Anforderungen der Geschäftstätigkeit entspricht
- ☐ Keine Administratorerkennung für Nutzer, die keine administrativen Tätigkeiten ausführen
- ☐ Verschiedene administrative Rollen (z. B. Anlage neuer Benutzer, Durchführung von Backups, Konfiguration der Firewall) für die IT-Administration erstellen

IT-Sicherheitsmaßnahmen im Zuge des DVG

- Dokumentation der IT-Anlage
 - möglichst auch angrenzende Themen wie Telefonie, Internet Web-Dienste usw.

W&B

Dokumentation

Musterpartner GmbH

Musterstraße 25
 12345 Musterhausen
 +49 (451) 123456

Kundennummer: 00000
 Service Rufnummer: +49 (451) 39988-311
 Service E-Mail: servicehotline@wb-net.de

Service-Leistungen:

Helpdesk und Kostengest		Stunde	Backup Management
Prozess		Nein	
Dienstleistungs-Kontingent		Nein	

Server und Netzwerk Management

W&B Managed Free Server (Monitoring, Patch Management und Antivirus pro physischen Server oder VM Host-Server inkl. einem VM Client-Server)		Ja
W&B Managed Virtual Server (Monitoring, Patch Management und Antivirus pro virtualisierten VM Host)		Nein
Server - nur Virenschutz + Monitoring		Nein
Monitoring pro Betriebssystem (Linux, Windows, Unix, etc.)		Nein

Managed Printservice

Drucker- und Servicegarantie		Nein
and. Toner		Nein

W&B

27. Standorte

Es werden alle relevanten Räume für die IT-Sicherheit erfasst.
(Beispiele: Standort des Konzeptions, Aufbewahrungsort der Sicherungsmedien, Firewall, Server usw.)

Sicherungsmedium lokal (Beispiel)

IT-Sicherheit: Sicherungsmedien (RDX)
 Raum: (Beispiel: Büro)
 Aufbewahrungsort: (Beispiel: Tresor, Schreibtisch, Schrank)

Sicherungsmedium Cloud (Beispiel)

Cloud Storage
 IT-Sicherheit: Als Speicherort (Cloud Storage) für die verschlüsselten Backupdaten, wird Speicherplatz in einem deutschen, DIN ISO 27001 zertifizierten Rechenzentrum genutzt.
 Aufbewahrungsort:

Kassabox

(Beispiel: Serverraum)

(Beispiel: unten im Serverschrank)

WatchGuard

(Beispiel: Serverraum)

(Beispiel: unten im Serverschrank)

Server

(Beispiel: Serverraum)

(Beispiel: unten im Serverschrank)

ung Server (Beispiel)

USV

(Beispiel: Serverraum)

(Beispiel: unten im Serverschrank)

erfassen

Dokumentation: Muster-GmbH

W&B

28. Netzwerplan (Musterplan)

Dokumentation: Muster-GmbH

W&B

Netzwerkplan

Dokumentation: Muster-GmbH

IT-Sicherheitsmaßnahmen im Zuge des DVG

- Selbst-Check durchführen:
IT-Sicherheit in Praxen
- Download der Checkliste unter
www.aegnord.de/meldungen

Selbst-Check

IT-Sicherheit in Praxen



Mit unserem Selbst-Check können Sie sich ganz einfach einen Überblick über den Stand der IT-Sicherheit in Ihrer Praxis verschaffen. Sollten Sie auf dieser Liste Punkte mit nein oder gar nicht beantworten können, herrscht Änderungs- und/oder Aufklärungsbedarf.

W&B steht Ihnen zur Seite, wenn es darum geht, die IT und deren Pflege auf den aktuell geforderten Stand zu bringen. Für eine unverbindliche Beratung erreichen Sie uns unter 0451 39988-0 oder per Mail an info@wb-net.de.

Abteilung	Frage	ja	nein	?
Technische Einrichtungen	Ich habe eine vollwertige Firewall (keine Router- oder Softwarefirewall).			
	Ich habe einen Server (bei mehr als 3 Arbeitsplätzen).			
	Der Server ist an einer unterbrechungsfreien Stromversorgung angeschlossen (USV, Notfallbatterie).			
	Mein Server/Hauptrechner hat gespiegelte Festplatten (RAID-System).			
	Ich habe für jeden Wochentag eine eigene Datensicherung auf einem einzelnen Medium.			
	Ich habe zusätzlich zu der tägl. Datensicherung auch eine Monats- und/oder Quartalsdatensicherung.			
	Ich lagere die derzeit nicht verwendeten Datensicherungen nicht in der Praxis, oder habe diese in einem feuer- und wasserfestem Safe.			
Personal	Ich weiß, dass alle Daten gesichert werden (nicht nur die Abrechnungsdaten) und überprüfe, ob die Sicherungen sauber durchgelaufen sind (Röntgenbilder, Steriprotokolle, Mails, Dokumente etc.).			
	Alle meine PCs und der Server sind verschlüsselt.			
	Ich habe jedes Teammitglied in das Thema Datenschutz und Datensicherheit eingewiesen und mir den Kenntnisstand verifizieren lassen.			
	Ich weiß, wer in der Praxis für die Datensicherung verantwortlich ist und auch wer verantwortlich ist, wenn die hauptverantwortliche Person nicht in der Praxis ist (Krankheit, Urlaub etc.).			
	In der Praxis wissen alle, wer die verantwortliche Person ist, wenn Störungen auftreten.			
	In der Praxis wissen alle, wer die verantwortliche Person ist, wenn Anfragen zum Datenschutz auftreten.			
	Jedes Teammitglied hat seinen eigenen und personalisierten Windowszugang, oder hat zumindest eingeschränkten Zugriff auf die systemrelevanten Daten auf Dateiebene (nicht innerhalb der Abrechnungssoftware, sondern auf Ebene des Betriebssystems).			
Software	Ich weiß, dass auch wenn ich keinen Datenschutzbeauftragten benannt habe, ich den Datenschutz genauso einzuhalten habe.			
	Ich habe einen Virenschutz auf jedem PC (auch wenn dort nicht in das Internet gegangen wird).			
	Ich update mein IT-System mit den erforderlichen Sicherheitsupdates für meine Betriebssoftwares (Windows-Updates, Adobe, Flash, Java, Acrobat) ein Mal die Woche.			
	Ich überprüfe vorher, ob diese Updates mit meinen anderen Softwares kompatibel sind (z. B. Abrechnungssoftware, Röntgensoftware, Sterissoftware).			
Dokumentation	Ich weiß, auf welchem Stand meine Softwares sind und ob ein Update notwendig ist, bei einer Änderung der Betriebssoftware.			
	Ich habe eine vollständige und laufende Dokumentation meiner eingesetzten PCs und der Netzwerkgeräte inklusive Seriennummern.			
	Ich habe eine vollständige und laufende Dokumentation meiner eingesetzten Softwares.			
	Ich habe eine vollständige und laufende Dokumentation meiner an die IT angebotenen Geräte (Röntgen, Sterigeräte, CAD/CAM, Einheiten) inklusive Seriennummern und Ansprechpartner des Herstellers.			

Kontakt Daten und weiterführende Informationen

- **Ärztegenossenschaft Nord eG**
Kolja Willems
Bahnhofstraße 1-3
23795 Bad Segeberg
Tel.: 04551-999910
Fax.: 04551-999919
Mail: kolja.willems@aegnord.de
www.aegnord.de

Alle Informationen zur heutigen Veranstaltung unter: www.aegnord.de/meldungen.

- **W&B GmbH**
Frank Winsel / Kai-Uwe Quast
Steinmetzstraße 7
23556 Lübeck
Tel.: 0451 39988-0
Fax: 0451 39988-44
Mail: info@wb-net.de
www.wb-medical.de



W&B

ärzte genossenschaft Nord eG
Medizin verbindet. menschlich | politisch | wirtschaftlich

Fragen immer gerne.

Danke für Ihre
Aufmerksamkeit!