

„ePA für alle“ und neue IT-Sicherheitsrichtlinie

Viele Fragen – (fast) alle Antworten



Peter Oleownik

1. stellv. Vorstandsvorsitzender der KZV Schleswig-Holstein

Schleswig-Holsteinischer Zahnärztetag – Neumünster – 14. März 2026

14.03.2026

1

Die wichtigsten Fragen ...

- Welche Voraussetzungen gelten für die Nutzung der ePA?
- Welche Daten **MÜSSEN** in die ePA kopiert werden?
- Welche Daten **KÖNNEN** zusätzlich in die ePA eingestellt werden?
- Was muss **NICHT** in die ePA eingestellt werden?
- Wie müssen Patienten über die ePA informiert werden?
- Wo gibt es Info-Materialien fürs Team und für Patienten?
- Was muss in der Praxis dokumentiert werden?
- Was ist das Besondere an einem PDF/A-Dokument?
- Was sind eigentlich MIOs?
- Wie wird die Befüllung der ePA abgerechnet?

14.03.2026



Voraussetzungen für Befüllung

- Pat. besitzt eine ePA und hat Zugriff nicht unterbunden
- eGK wurde gesteckt → Zugriff für 90 Tage (+/-)
- kein Widerspruch des Patienten gegen das Einstellen
- Die Daten müssen
 - selbst erhoben worden sein,
 - aus der aktuellen Behandlung stammen und
 - in elektronischer Form vorliegen
- es stehen keine erheblichen therapeutischen Gründe oder Rechte Dritter entgegen (im zahnärztlichen Bereich kaum zu erwarten: z. B. Informationen zu sexuell übertragbaren Infektionen, psychischen Erkrankungen, Schwangerschaftsabbrüchen, Ergebnisse genetischer Untersuchungen)

14.03.2026

Welche Daten MÜSSEN in die ePA kopiert werden?

- → elektronische Medikationsliste (eML)
(wird automatisiert im Rahmen des E-Rezepts befüllt)
- **Befundberichte** über selbst erhobene Befunde oder durchgeführte Behandlungen zur Information Dritter, vergleichbar einem Arztbrief oder in Gestalt eines solchen
Achtung! Nur, wenn Sie sowieso einen Befundbericht geschrieben hätten, also nicht extra für die ePA !!!
- Laborbefunde, z. B. histologische Untersuchungen
 - Einstellung durch den **Zahnarzt**, da er die Untersuchung veranlasst hat und das Labor keinen Zugriff auf die ePA des Patienten hat!

14.03.2026

Welche Daten **SOLLEN** zusätzlich in die ePA eingestellt werden?

- auf Verlangen der Patientin/des Patienten bzw. nach Rücksprache
- → **eZahnbonusheft (MIO)**
- unstrukturierte Daten, wenn sie in der konkreten, aktuellen Behandlung elektronisch verarbeitet wurden und es überhaupt technisch möglich ist, sie einzustellen, wie z. B.
 - Röntgenbilder (sofern diese im PVS und als **PDF/A** vorliegen)
 - eAU-Bescheinigung
 - PAR-Behandlungsplan
 - PSI-Formular
 - sonstige zahnmedizinisch relevante Dokumentation

14.03.2026

Was ist eigentlich ein MIO?

- MIOs = **Medizinische InformationsObjekte**
- klar definierte „Informationsbausteine“ in der ePA
- dienen dazu, medizinische Daten in der ePA standardisiert und mit **genau festgelegter Struktur** zu dokumentieren
- unabhängig von Softwaresystem der Praxis (PVS)
- unabhängig von Krankenkassen-App
- erstes MIO: „zahnärztliches Bonusheft“ (seit 2022)

Patientendaten	Datum	<input type="checkbox"/> IP	<input type="checkbox"/> 01	Praxis
----------------	-------	-----------------------------	-----------------------------	--------

- in Zukunft weitere MIOs geplant, z.B. Implantat-Pass, MIO Bildbefund, elektronischer Medikationsplan (eMP), Gelbes Untersuchungsheft (U-Heft)

14.03.2026

PDF/A Portable Document Format / Archivable

- Dateiformat zur Langzeitarchivierung digitaler Dokumente (ISO, 2005)
- Dokumente müssen unabhängig von Bearbeitungs-Tools, Betriebssystemen und technologischen Veränderungen unverändert bleiben
- Lesbarkeit für sehr lange Zeiträumen gewährleistet (revisionssichere Archivierung)
- keine Einbettung von Audio- oder Videodateien
- keine externen Ressourcen, d. h. Grafiken und Schriftarten müssen direkt im Dokument eingebettet sein
- keine Verschlüsselung von Dokumenten
- digitale Signaturen möglich
- unterstützt Einbettung von Metadaten, wodurch Dokumente sich leichter identifizieren und suchen lassen.
- vier Varianten: PDF/A-1, PDF/A-2, PDF/A-3 und PDF/A-4



14.03.2026

Welche Daten **SOLLEN** zusätzlich in die ePA eingestellt werden?

- auf Verlangen der Patientin/des Patienten bzw. nach Rücksprache
- → **eZahnbonusheft (MIO)**
- unstrukturierte Daten, wenn sie in der konkreten, aktuellen Behandlung elektronisch verarbeitet wurden und es überhaupt technisch möglich ist, sie einzustellen, wie z. B.
 - Röntgenbilder (sofern diese im PVS und als **PDF/A** vorliegen)
 - eAU-Bescheinigung
 - PAR-Behandlungsplan
 - PSI-Formular
 - sonstige zahnmedizinisch relevante Dokumentation

14.03.2026

Was muss NICHT in die ePA eingestellt werden?

- Daten, die nur analog vorliegen, wie z. B.
 - Röntgenbilder
 - Dokumente, die nur in Papierform vorliegen
 Diese müssen nicht nachdigitalisiert werden.
- Daten, die auf externen Servern ohne Möglichkeit des Abrufens im PVS liegen, wie z. B.
 - Röntgenbilder
- Daten, die durch andere (Zahn-)Ärztinnen oder (Zahn-)Ärzte erhoben worden sind
 - Ausnahme: Laborbefunde (z.B. Histologie), die selbst beauftragt wurden

14.03.2026

ePA1
BEMA

Erstbefüllung einer elektronischen Patientenakte

4 Punkte

1. Die Leistung nach Nr. ePA1 umfasst
 - die Verarbeitung von versorgungsrelevanten zahnmedizinischen Informationen oder Angaben zum Bonusheft aus der aktuellen Behandlung des Versicherten für eine erstmalige einrichtungs-, fach- und sektorenübergreifende Dokumentation in der elektronischen Patientenakte nach Maßgabe des § 346 Abs. 3 SGB V,
 - die Prüfung, ob **erhebliche therapeutische Gründe oder erhebliche Rechte Dritter** einer Übermittlung in die elektronische Patientenakte entgegenstehen,
 - die Prüfung und ggf. Ergänzung der zu den Dokumenten gehörenden **Metadaten**,
 - die Einholung der **Einwilligung des Versicherten** in den Zugriff auf Daten in dessen elektronischer Patientenakte.
2. Die Leistung nach Nr. ePA1 ist **einrichtungs-, fach- und sektorenübergreifend nur einmal je Versicherten und elektronischer Patientenakte** abrechenbar.
3. Die Leistung nach Nr. ePA1 ist **nicht neben der Leistung nach Nr. ePA2** abrechenbar.

10

14.03.2026

ePA2
BEMA

Aktualisierung einer elektronischen Patientenakte

2 Punkte

1. Die Leistung nach Nr. ePA2 umfasst
 - die Verarbeitung von versorgungsrelevanten zahnmedizinischen Informationen oder Angaben zum Bonusheft aus der aktuellen Behandlung des Versicherten für eine einrichtungs-, fach- und sektorenübergreifende Dokumentation in der elektronischen Patientenakte nach Maßgabe des § 346 Abs. 3 SGB V,
 - die Prüfung, ob **erhebliche therapeutische Gründe oder erhebliche Rechte Dritter** einer Übermittlung in die elektronische Patientenakte entgegenstehen,
 - die Prüfung und ggf. Ergänzung der zu den Dokumenten gehörenden **Metadaten**,
 - die Einholung der **Einwilligung des Versicherten** in den Zugriff auf Daten in dessen elektronischer Patientenakte.
2. Die Leistung nach Nr. ePA2 ist **höchstens einmal je Sitzung** abrechenbar.
3. Die Leistung nach Nr. ePA2 ist **nicht neben** der erstmaligen Befüllung der elektronischen Patientenakte nach **Nr. ePA1** abrechenbar.

11

14.03.2026

Informationspflichten

- Primäre Informationspflicht zur ePA besteht vor allem für die **Krankenkassen**, die ihre Versicherten umfassend über die ePA aufklären müssen (§ 343 SGB V)
- Praxen müssen aber Patientinnen und Patienten darüber informieren, mit welchen Daten ihre ePA **standardmäßig** oder **auf ihren Wunsch** befüllt wird
- **Voraussetzung: Patient/in hat nicht widersprochen**
- Besondere Informationspflichten bestehen für das Einstellen von sensiblen Daten (z. B. sexuell übertragbare Infektionen). Hier müssen die Patientinnen und Patienten vor dem Einstellen explizit auf ihr Widerspruchsrecht hingewiesen werden.

Wie muss informiert werden?

- keine festen Vorgaben
- mündlich im Rahmen eines Gesprächs mit der Patientin oder dem Patienten oder
- mittels eines standardisierten Formulars oder
- in Form eines Aushangs in der Praxis

14.03.2026

Kassenärztliche Bundesvereinigung KZBV

Die „ePA für alle“ im Überblick: Informationspflichten

Die „ePA für alle“ im Überblick: Informationspflichten

Die „ePA für alle“ im Überblick: Widerspruchsrechte

Die „ePA für alle“ im Überblick: Dokumentationspflichten

Die „ePA für alle“ im Überblick: Befüllung

www.kzbv.de

Stand Dezember 2024

14.03.2026

KZBV Kassenärztliche Bundesvereinigung

Wichtige Hinweise zu Ihrer elektronischen Patientenakte

Befüllung der elektronischen Patientenakte (ePA)

Praxisaushang

Zahnarztpraxen können mit diesem Praxisaushang Ihre Patientinnen und Patienten drucken zur Verfügung.

Praxisaushang zur ePA (DIN A4)

Praxisaushang zur ePA (DIN A3)

Mehr Informationen zu Ihrer elektronischen Patientenakte

ePA-Infoservice der Krankenkassen

ePA-Infoseite Bundesministerium für Gesundheit

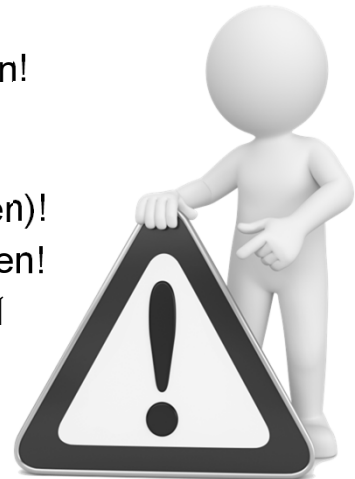
14.03.2026

www.kzv-sh.de

14.03.2026

Fazit

- mit ePA-Funktionen des PVS vertraut machen!
- alle PVS-Updates immer zeitnah einspielen!
- Informationsangebote des PVS-Herstellers nutzen (ggf. Info-Material, Videos, Schulungen)!
- Infos von **KZBV**, KZV S-H und **gematik** nutzen!
- informieren, ob der Patient eine ePA hat! ☒☒
- mit Patienten offen über ePA sprechen!
- Wünsche der Patienten dokumentieren!
- ePA „mit Sinn und Verstand“ befüllen!
- ePA1/ePA2 korrekt abrechnen!



14.03.2026

Die neue IT-Sicherheitsrichtlinie

Viele Fragen – (fast) alle Antworten

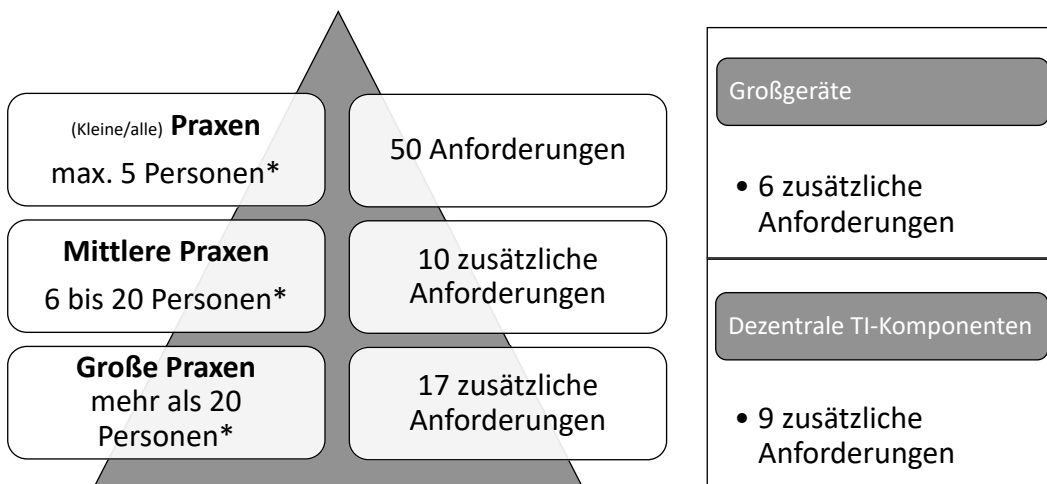


Peter Oleownik
 1. stellv. Vorstandsvorsitzender der KZV Schleswig-Holstein
 Schleswig-Holsteinischer Zahnärztetag – Neumünster – 19. März 2026

14.03.2026

19

IT-Sicherheitsrichtlinie: Umzusetzende Anforderungen im Überblick



*) Personen, die ständig in der Datenverarbeitung tätig sind

20

14.03.2026



IT-Sicherheit ist Chefsache und Teamsache!

- Praxisleitung und Team** müssen für IT-Sicherheit sensibilisiert sein
- Bewusstsein für IT-Sicherheit muss bei allen „in Fleisch und Blut“ übergehen → jeder im Team trägt ein Stück Verantwortung
- Unterweisung bei Neueinstellungen und danach kontinuierlich
- Betrifft **alle, die in der Praxis einen PC bedienen**
- Nehmen Sie IT-Sicherheit (sofern noch nicht geschehen) in Ihr **QM** auf!
- Machen Sie IT-Sicherheit regelmäßig zum Thema auf Ihren **Team-Besprechungen!**

14.03.2026

23

Sichern Sie regelmäßig Ihre Daten!

- regelmäßige (ggf. tägliche) Backups von allen gespeicherten Daten** erstellen insbes. **Behandlungsdaten** und **Röntgen**, aber auch isolierte PCs (CAD, QM usw.) auch Router-Daten, **Konnektor**, mobile Geräte u.a.
- diese offline oder in einer gesicherten Cloud (mit BSI C5-Testat) lagern
- 3-2-1 Regel** (mind. 3 Sicherungen, 2 unterschiedliche Medien, 1 offline)
- 30-2-1 Regel n. Richard Marnau** (30 Tage, 2 verschiedene Medien, 1 offline)
- Datensicherung möglichst **automatisieren!**
- Programme (PVS!)** vor Datensicherung unbedingt **schließen!**
- Prüfen**, ob wirklich alle Daten gesichert wurden
 - regelmäßige Wiederherstellungstests (2-4x im Jahr)
 - evtl. (ausrangierten) Stand-alone-PC nutzen











14.03.2026

24

[A1.23] Art der Datensicherung



Es muss festgelegt werden, **wie** die Daten gesichert werden.

- 💡 **Welche Daten** müssen gesichert werden?
- 💡 **Wie oft** müssen die Daten gesichert werden?
- 💡 **Wie lange** dauert eine Datensicherung?
- 💡 **Wann** sollten die Daten idealerweise gesichert werden? (manuell/automatisch)
- 💡 Wie groß muss das **Speichermedium** sein?          
- 💡 **Wofür/wogegen** sollen Daten gesichert werden?
Einbruch/Diebstahl/Vandalismus, technische Defekte, Fehlbedienung, fehlerhafte Updates, Hacker-/Ransomware-Attacke, Feuer, Wasser ...

25 von 170

14.03.2026

Updates regelmäßig und auf allen Geräten

- Updates beseitigen Fehler, verbessern die Performance, stellen neue oder verbesserte Funktionen zur Verfügung und **erhöhen die Sicherheit** von Systemen
- Aktualisieren Sie zeitnah alle Systeme, die updatefähig sind (Server und alle PCs, ggf. virtuelle Maschinen, **Betriebssystem (Windows!!!)**, PVS, andere Programme (Office!), aber auch Router, Firewall, Konnektor und eHealth-Terminal, mobile Geräte!)
- Automatisieren** Sie Updates überall, wo es geht!
- Beachten Sie, dass Updates oft einen **Neustart des Systems** erfordern!
- Planen Sie Updates so, dass sie nicht Ihren Praxisablauf stören! (evtl. Mittagspause?)
- Legen Sie fest, wer in Ihrer Praxis für Updates zuständig ist!**
- Separieren Sie Systeme, die keine Updates mehr bekommen, vom Netz der Praxis und wechseln Sie möglichst auf updatefähige Systeme!

14.03.2026

26



ChatGPT

Erstelle eine Tabelle, in welche die Zuständigkeiten für die Aufgaben in einer Zahnarztpraxis mit 2 Zahnärzten, 5 ZFAs und 2 Auszubildenden eingetragen werden können!

14.03.2026

27

The screenshot shows an Excel spreadsheet titled 'Zuständigkeiten_Zahnarztpraxis - Excel'. The spreadsheet contains a table with the following structure:

	A	B	C	D	E	F	G	H	I	J	K
1	Bereich / Aufgabe	Zahnarzt 1	Zahnarzt 2	ZFA 1	ZFA 2	ZFA 3	ZFA 4	ZFA 5	Azubi 1	Azubi 2	Bemerkungen
2	Patientenaufnahme & Terminvergabe										
3	Anamnese & Aufklärung										
4	Behandlung (konservierend, chirurgisch)										
5	Assistenz am Behandlungsstuhl										
6	Prophylaxe (PZR, Fissurenversiegelung)										
7	Röntgen (Aufnahme & Dokumentation)										
8	Instrumentenaufbereitung / Steri										
9	Bestellungen & Materialwirtschaft										
10	Abrechnung (BEMA, GOZ, KZV)										
11	Kassenbuch & Finanzen										
12	QM / Hygienepläne										
13	Social Media / Marketing										
14	Kommunikation mit Labor										
15	Aus- & Weiterbildung organisieren										
16											
17											
18											

Benutzerberechtigungen – Wer darf was?

- Aufgabenverteilung im Team
- Unterschiedliche Rechte/Rollen für Personen im PVS
- Unterschiedliche Rechte für PCs im Netzwerk
- Trennung Administrator/Benutzer „ab dem 1. Computer!“ [R. Marnau]
- Tipp: **optische Trennung Admin/Benutzer** durch anderen Desktophintergrund!
- Admin-Zugang ausschließlich für Wartungsarbeiten nutzen, niemals für das „Tagesgeschäft“



„Es bringt ein **unfassbar hohes Schutzniveau**, als Benutzer zu arbeiten und nicht als Administrator.“ [Richard Marnau, 19.11.2025]

14.03.2026

29

Nutzen Sie starke Passwörter und 2FA

- Mindestens 8 Zeichen**
- kleine + große Buchstaben, Zahlen und Zeichen**
- xzU1#5F? → korrekt, aber schlecht zu merken
- Aber trotzdem gut zu merken:
 - Meinkaterhat4Beineeee#
 - Ichhatte2025#6Dates
 - Mein1.FreundHiess#Kevin
- für alle Accounts **unterschiedliche Passwörter**
- Passwort-Manager** verwenden!
- Wo immer möglich **2FA/MFA** nutzen!

Die Zeit, die ein Hacker benötigt, um dein Passwort mittels einer Brute-Force-Angriffe zu ermitteln 2025

12 x RTX 5090 | bcrypt (10)

Passwortlänge (Zeichen)	nur Zahlen	nur Kleinbuchstaben	Klein- & Großbuchstaben	Zahlen und Klein-/Großbuchstaben	Zahlen, Klein-/Großbuchstaben und Symbole
4	Sofort	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	57 Minuten	2 Stunden	4 Stunden
6	Sofort	46 Minuten	2 Tage	6 Tage	2 Wochen
7	Sofort	20 Stunden	4 Monate	1 Jahr	2 Jahre
8	Sofort	3 Wochen	15 Jahre	62 Jahre	184 Jahre
9	2 Stunden	2 Jahre	791 Jahre	3k Jahre	11k Jahre
10	1 Tag	40 Jahre	41k Jahre	238k Jahre	803k Jahre
11	1 Woche	1k Jahre	2 Mio Jahre	14 Mio Jahre	56 Mio Jahre
12	3 Monate	27k Jahre	111 Mio Jahre	917 Mio Jahre	3 Mrd Jahre
13	3 Jahre	705k Jahre	5 Mrd Jahre	56 Mrd Jahre	275 Mrd Jahre
14	28 Jahre	18 Mio Jahre	300 Mrd Jahre	3 Bio Jahre	19 Bio Jahre
15	284 Jahre	477 Mio Jahre	15 Bio Jahre	218 Bio Jahre	1 Brd Jahre
16	2k Jahre	12 Mrd Jahre	812 Bio Jahre	13 Brd Jahre	94 Brd Jahre
17	28k Jahre	322 Mrd Jahre	42 Brd Jahre	840 Brd Jahre	6 Trio Jahre
18	284k Jahre	8 Bio Jahre	2 Trio Jahre	52 Trio Jahre	463 Trio Jahre

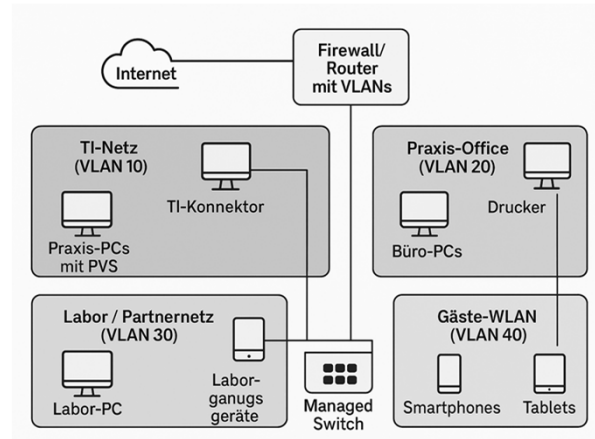
Hive Systems hivesystems.com/password

14.03.2026

30

Separieren Sie Ihr Netzwerk!

- Netzwerke so gut es geht trennen
- WLAN für Patienten** separieren
- WLAN für Team** separieren
- Praxisnetzwerk von privatem Netzwerk trennen
- physische Trennung oder über V-LANS
- Schutz des Übergangs zum Internet durch eine **Firewall!**



14.03.2026

31

Verschlüsseln Sie Ihre Daten(träger)!

- Nur verschlüsselte Daten sind sicher!
- verschlüsselte Daten sind bei Verlust eines Datenträgers oder Datendiebstahl für den Dieb unbrauchbar
- Verschlüsseln Sie alles, was man verschlüsseln kann!**
- Neue Datenträger am besten vor der ersten Verwendung verschlüsseln
- neue Festplatten werden oft mit **Verschlüsselungs-Software** ausgeliefert
- Verschlüsselungs-Software **BitLocker** gehört zur Grundausstattung von Windows 11 Pro



© Feodora – stock.adobe.com

14.03.2026

32

BitLocker Schritt für Schritt

14.03.2026

Vorsicht im Umgang mit E-Mails!

- Zugriffsrechte auf Mailprogramme regeln (QM, IT-Konzept)
- automatische Interpretation von HTML-Code und anderen aktiven Inhalten in E-Mails deaktivieren.
- Dateianhänge nicht arglos öffnen! vor dem Öffnen auf Schadsoftware prüfen!
- Links in Mails nicht arglos anklicken!
- Mails unbekannter Herkunft nicht öffnen!
- bei zweifelhaften Mails Absender anrufen!
- Jede Infektion ist ein unkalkulierbares Risiko!**
- Wachsamkeit und Wissen schulen: **3-Sekunden-Sicherheitscheck** des BSI:
 - **Kenne ich den Absender?**
 - **Ergeben Betreff und Nachricht Sinn (passen sie zueinander)?**
 - **Habe ich einen Anhang von dieser Person erwartet?**



Wenn möglich unterschiedliche, vertrauliche E-Mailadressen nutzen!
z.B. labor@musterzahn.de,
depot@musterzahn.de,

14.03.2026

34

Vorsicht beim Surfen im Internet?

- Reduzieren Sie das „Surfen im Internet“ aus der Praxis heraus auf das absolut Notwendige!
- häufig Infektionen durch aktive Komponenten (z.B. ActiveX, Scriptsprachen, Multimedia-Plugins), ggf. deaktivieren!
- Vorsicht bei unbekanntem Internetseiten! (insbes. Downloads, Software, Musik, Filme, Spiele usw.)
- Wichtige Adressen (z. B. kzv-sh.de ☺) in **Lesezeichen-Symboleiste** ablegen!
- Browser entfernen**, wo sie nicht benötigt werden (**Behandlungszimmer!**)
- Für Recherchen, Bestellungen usw. evtl. separate PCs, möglichst in separatem Netz verwenden!
- Jede Infektion ist unkalkulierbares Risiko!**



14.03.2026

35

Denken Sie auch an physischen Schutz!

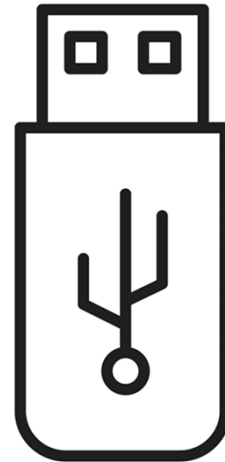
- Schützen Sie Server und IT-Komponenten vor unbefugtem Zugriff
- Halten Sie wichtige IT-Komponenten unter Verschluss
- Bildschirme an der Anmeldung müssen so positioniert sein, dass Patienten keine Daten mitlesen können (Blickschutzfilter)
- Bei Verlassen des Behandlungszimmers abmelden
- externe Datenträger nicht rumliegen lassen
- klare schriftliche Regeln dazu aufstellen, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen
- auch an Feuer, Wasser, Einbruch denken!

14.03.2026

36

Vorsicht vor mitgebrachten Datenträgern!

- Äußerste Vorsicht bei Datenträgern, die von Patienten mitgebracht werden
- „Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.“ [A1-36]
- wenn möglich zum Öffnen Stand-alone-PC oder PC in separiertem Netzwerk verwenden

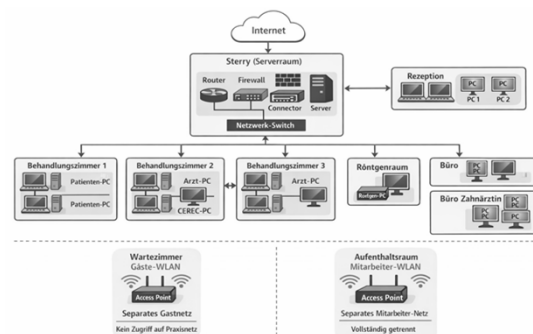


14.03.2026

© Warpiya – stock.adobe.com

Dokumentieren Sie Ihr System lückenlos!


- Netzwerkplan** (selbst zeichnen oder KI machen lassen! ↓)
- Lückenlose Inventarliste (Muster KZBV)
- Vordrucke für Einstellung neuer MA und bei Weggang von MA
- Vordruck für Vertrag mit Fremdpersonal
- Wer macht was? Zuständigkeiten/ Verantwortlichkeiten
- Liste mit allen IP-Adressen** (für IT-ler oft Dreh- und Angelpunkt)
- Liste mit allen **Passwörtern und Zugangsdaten** (auch für Konnektor!)
- Ordner mit allen Unterlagen (Sie müssen alle Daten haben!)
- PIN- und PUK-Briefe für SMC-B, eHBA usw.
- Notfallplan**




14.03.2026


38

VERHALTEN BEI IT-NOTFÄLLEN







Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!




IT-Notfallrufnummer:




Wer meldet?




Welches IT-System ist betroffen?



Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?



Wann ist das Ereignis eingetreten?




Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

<p>Weitere Arbeit am IT-System einstellen</p>	<p>Beobachtungen dokumentieren</p>	<p>Maßnahmen nur nach Anweisung einleiten</p>
---	--	---

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

14.03.2026
39

 Wo befindet sich die
aktuelle Datensicherung?

www.kzv-sh.de/390

Kein Backup - Kein Mitleid!

Linus Neumann (CCC), 30.03.19, Schleswig-Holsteinischer Zahnärztetag, Neumünster

14.03.2026
40