



ARBEITSSCHUTZ UND HYGIENE IM GESUNDHEITSWESEN

RECHTSSICHERHEIT SCHAFFEN • FACHWISSEN ERHALTEN • ARBEITSALLTAG ERLEICHTERN

PROFESSIONELLES KRISENMANAGEMENT

GEZIELTE KRISEN- RESILIENZ IM GESUNDHEITSWESEN

Lesen Sie, wie Einrichtungen im Gesundheitswesen ihre Krisenresilienz gezielt stärken können. **S. 3**

IT-AUSFALL IN DER PRAXIS: SIND SIE VORBEREITET?

Wie Sie mit Datensicherung und Notfallplanung Ausfälle schnell beherrschen. **S. 6**

GEWALT DURCH PATIENTEN RICHTIG BEWÄLTIGEN

So sorgen Sie mit klaren Regeln und Prävention für mehr Sicherheit im Praxisalltag. **S. 10**



SAFETYXPERTS

Ihre Spezialisten für Arbeitssicherheit

DAS EXPERTENTEAM



Renate Tief

Ihre Expertin für das Hygienemanagement im Gesundheitswesen. Renate Tief ist die Geschäftsführerin der Beratungsfirma CPG Tief, externe Auditorin (DGQ), externe Datenschutzbeauftragte und Hygienemanagementbeauftragte. Mit ihrem fundierten Fachwissen unterstützt sie seit über 30 Jahren vor allem Arztpraxen, aber auch Altenheime und Kliniken bei der Optimierung der gesamten Abläufe. Seit 15 Jahren ist sie auch als Chefredakteurin für den VNR tätig.

Krisen meistern, bevor sie entstehen

Liebe Leserin, lieber Leser,

Gefahren, Risiken und Krisen entstehen nicht nur im medizinischen Bereich. Auch bei IT-Ausfällen, Datenpannen, Bränden, Einbrüchen oder gewalttätigen Patienten müssen Sie und Ihre Mitarbeiter schnell, sicher und routiniert handeln können.

Diese Spezialausgabe befasst sich mit dem Thema „Professionelles Krisenmanagement“. Bereiten Sie sich zusammen mit Ihren Kollegen in Ruhe auf den Ernstfall vor – werden Sie krisenresilient. Besprechen Sie kritische Ausnahmesituationen regelmäßig in Teamsitzungen, sensibilisieren Sie Ihre Mitarbeiter für potenzielle Risiken und entwickeln Sie praxisnahe Notfallpläne für den Ernstfall.

Renate Tief

Renate Tief

ALLES INKLUSIVE



Onlinebereich

Nutzen Sie über 500 Checklisten, Muster und Vorlagen unter: [safetyxperts.de/login](https://www.safetyxperts.de/login)



Spezialreports & Facharchiv

Möchten Sie in ein Thema tiefer eintauchen, finden Sie praktische E-Books und Arbeitshilfen.



Fragen an die Xperten

Stellen Sie Ihre individuellen Fragen zum Thema Arbeitsschutz gerne über das Kontaktformular auf [safetyxperts.de/login](https://www.safetyxperts.de/login)



Videos & Webinare

Im Onlinebereich finden Sie unter „Videos“ und „Veranstaltungen“ praktische Inhalte für Ihre Unterweisung.



Krisenresilienz in Einrichtungen des Gesundheitswesens

Um Akutsituationen und Krisen besser zu bewältigen, braucht es psychische Anpassungs- und Widerstandsfähigkeit – die sogenannte Krisenresilienz. Ziel dabei ist es, souverän mit belastenden Situationen umzugehen und nicht unvorbereitet von Krisen überrascht zu werden. Mit den folgenden Tipps schaffen Sie die Voraussetzungen dafür, dass Sie und Ihre Kollegen auch in plötzlich auftretenden Krisensituationen handlungsfähig bleiben.

Identifizieren Sie mögliche Krisen

Besprechen Sie mit Ihren Kollegen in der nächsten Teamsitzung, welche Krisen oder Ausnahmesituationen auftreten könnten und welche präventiven Maßnahmen dafür festgelegt werden sollten.

Beispiele für potenzielle Krisen:

- Einbrüche, Diebstahl
- IT-Ausfall
- Datenschutzpanne
- Personalausfall
- Gewaltübergriffe, mediale Eskalationen
- Lieferengpässe
- usw.

Schaffen Sie (Kommunikations-)Strukturen

In jeder Ihrer folgenden Teamsitzungen nehmen Sie sich gezielt eine mögliche Krisensituation vor, um Präventionsmaßnahmen und Bewältigungsstrategien zu besprechen und festzulegen.

Das heißt, Sie und Ihr Team:

- erkennen die Risiken,
- finden gemeinsam Lösungsstrategien,
- erstellen Handlungs- bzw. Notfallpläne für die ermittelten Krisen,
- legen die Kommunikationswege fest.

Dieser regelmäßige Austausch im Team gibt Sicherheit, ein besonders wichtiger Aspekt im Krisenmanagement. Bieten Sie Ihren Mitarbeitern auch zusätzlich regelmäßig interne und/oder externe Fort- und Weiterbildungen an, die notwendig sind, um auf Krisen vorbereitet zu sein.

Warum Führungskräfte Vorbilder sein sollten

Ein wirksames Krisenmanagement lebt von der Vorbildfunktion der Leitungskräfte. Sie und Ihre Führungskräfte sollten deshalb auch in stressigen Situationen Ruhe, Gelassenheit und einen kühlen Kopf vorleben. Sie sind der Fels in der Brandung. Das wirkt beruhigend auf die Kollegen und Bewohner bzw. Patienten. Das bedeutet natürlich für die Führungskräfte selbst eine konsequente Selbstfürsorge und einen guten Umgang mit den eigenen Emotionen, um das persönliche, psychische sowie physische Wohlergehen sicherzustellen.

Nehmen Sie das eigene aktuelle Befinden und die persönlichen Bedürfnisse wahr, um angemessen darauf zu reagieren. Planen Sie hierfür bewusst Zeiten für Erholung, Reflexion und den kollektiven Austausch ein. Nur wer langfristig handlungsfähig bleibt, kann in Krisensituationen verlässlich Entscheidungen treffen und Mitarbeitende sicher führen.



Krisenresilienz hilft, auch in belastenden Situationen souverän und handlungsfähig zu bleiben.

Selbstfürsorge: Lernen Sie, gut zu sich selbst zu sein!

Emotionale Selbstfürsorge bedeutet:

- sich für sich selbst Zeit zu nehmen,
- die eigenen Gefühle wahrzunehmen,
- allein zu sein und
- Wohltuendes zu genießen.

Kognitive Selbstfürsorge heißt:

- eigene Gedanken, Haltungen und Glaubenssätze bewusst wahrzunehmen,
- sich Zeit zur Reflexion zu nehmen,
- den Fokus auf Veränderbares zu legen und
- Unveränderbares zu akzeptieren.

Soziale Selbstfürsorge bedeutet:

- wertvolle und unterstützende Beziehungen aufzubauen und zu pflegen,
- Konflikte offen anzusprechen und sich mit vertrauten Menschen auszutauschen. Das stärkt innere Gelassenheit und das Gefühl der Selbstwirksamkeit.



Fazit

Mit diesen wichtigen Aspekten zeigen Sie in Krisen- und Notfallsituationen eine souveräne, überzeugende Haltung. Durch Coachings, Teambildungsmaßnahmen und ähnliche Trainings können Bewusstsein, Kenntnisse und Fähigkeiten zur Krisenbewältigung gezielt aufgebaut und gestärkt werden.

Einbruch in der Einrichtung oder Praxis: Wenn Täter gezielt zuschlagen

In den letzten Jahren häufen sich Einbrüche und Diebstähle in Arztpraxen. Dabei werden manchmal nur ein paar hundert Euro entwendet. Erst im April 2026 trieb ein Einbrecher im Regensburger Ostenviertel sein Unwesen und entwendete Bargeld aus einer Arztpraxis. Im Februar 2026 brachen Täter in zwei Arztpraxen in Rosenheim ein und entwendeten technische Geräte im Wert von mehreren hunderttausend Euro. Die Liste der Vorfälle ist lang. Dabei werden neben Bargeld häufig auch Medikamente und teure medizinische Geräte gestohlen. Die durch den Einbruch verursachten Schäden – oft in Höhe von mehreren tausend Euro – kommen zusätzlich hinzu. Da hilft nur eins: rechtzeitig vorbeugen. Wie Sie sich und Ihre Praxis schützen und wie Ihre Mitarbeiter Sie dabei unterstützen können, erfahren Sie in diesem Beitrag.

Lassen Sie sich von der Polizei beraten

Jede Praxis hat individuelle Schwachstellen und benötigt daher passende Schutzmaßnahmen. Die beste Anlaufstelle für eine professionelle Beratung ist Ihre örtliche Polizei. Die kriminalpolizeilichen Beratungsstellen analysieren mögliche Sicherheitslücken und zeigen Ihnen, mit welcher Sicherungs- und Überwachungstechnik Sie Ihre Praxis wirksam vor Einbruch schützen können. Welche Beratungsstelle für Sie zuständig ist, erfahren Sie bei Ihrer Polizeidienststelle vor Ort.

Fotografieren Sie wertvolle Geräte

Eine Liste Ihrer Praxisapparaturen mit den individuellen Geräte-nummern liegt Ihnen sicher bereits vor. Hochwertige Geräte soll-

ten Sie zusätzlich fotografieren. Hat ein Gerät ein besonderes Kennzeichen, fotografieren Sie auch dies. Die Polizei kann den Verbleib der gestohlenen Gegenstände so besser ermitteln. Tragen Sie weitere Wertsachen in eine sogenannte Wertsachenliste ein und machen Sie ggf. auch davon Fotos. Damit steigen Ihre Chancen, das Diebesgut zurückzubekommen. Zudem erleichtert das den Tatnachweis erheblich und macht das Diebesgut für Hehler uninteressant.



Download-Tipp

Ein Wertsachenverwaltungsprogramm zum Download finden Sie im Internet unter: <https://kurzlinks.de/rg0t>

Checkliste „Einbruchsprävention“



Anmerkung	Ja	Nein	Tipp
Verwahren Sie in Ihrer Praxis regelmäßig hohe Bargeldbeträge?	☐	☐	Lassen Sie keine hohen Geldbeträge für längere Zeit in der Kasse; entnehmen Sie sie regelmäßig, bei Bedarf auch mehrmals täglich (schließen Sie das Geld z. B. in einen zertifizierten Safe ein).
Gibt es in Ihrer Praxis einen Safe? Wenn ja, Marke: _____	☐	☐	
Überprüfen Sie oder von Ihnen beauftragte Mitarbeiter die Kasse bzw. die Geldbearbeitung an der Anmeldung?	☐	☐	Geldzählen oder andere Kassenüberprüfungen sollten immer in einem separaten Raum durchgeführt werden oder zumindest zu einem Zeitpunkt, zu dem keine Patienten mehr in der Praxis sind. Stellen Sie sicher, dass Sie oder Ihre Mitarbeiter dabei nicht beobachtet werden können, etwa durch eine transparente Eingangstür.
Können unbefugte Personen Sie oder Ihre Mitarbeiter dabei beobachten?	☐	☐	
Nehmen Sie hohe Geldbeträge mit nach Hause?	☐	☐	Hohe Bargeldbeträge sollten Sie direkt zur Bank bringen – möglichst tagsüber. Ansonsten besteht die Gefahr, dass Diebe Sie beobachten und überfallen oder bei Ihnen zu Hause einbrechen.
Sind die Wertsachen, die sich in Ihrer Praxis befinden, in eine Liste eingetragen und katalogisiert?	☐	☐	siehe Tipp vor dieser Tabelle unter: https://kurzlinks.de/xzeg
Stellen Sie bzw. Ihre Mitarbeiter vor dem Verlassen der Praxis immer sicher, dass alle Fenster und Türen geschlossen sind?	☐	☐	Legen Sie fest, wer am Abend den „Sicherheitsrundgang“ macht. Dabei müssen vor allem auch gekippte Fenster geschlossen werden. (Empfehlung: Auch immer die Rollläden herunterlassen!)
Haben Sie eine Alarmanlage?	☐	☐	Lassen Sie sich hierzu von der Polizei beraten!
Halten Sie einen guten Kontakt zu Ihrer Nachbarschaft? Aufmerksame Nachbarn sind ein guter „Einbruchschutz“; sie achten eher auf ungebetene Gäste, wenn ein gutes Verhältnis besteht.	☐	☐	Schon in vielen Fällen haben aufmerksame Anwohner rechtzeitig „Alarm geschlagen“.



Mit diesen 7 Verhaltensregeln haben Sie die Situation nach einem Einbruch im Griff

Falls Ihre Mitarbeiter morgens vor Ihnen die Praxis betreten und einen nächtlichen Einbruch feststellen, sollten dafür klare Verhaltensregeln festgelegt sein:

1. Wichtigste Regel: Berühren oder verändern Sie nichts am Tatort. Andernfalls können wichtige Spuren zerstört, verwischt oder verunreinigt werden, was die Ermittlungen erheblich erschweren kann.
2. Ihre Mitarbeiter informieren Sie als Ersten, damit Sie Ihre Versicherung verständigen können.
3. Anschließend informieren Ihre Mitarbeiter umgehend die Polizei und schildern den Vorfall.
4. Weisen Sie Ihre Mitarbeiter an, den Tatort sofort zu fotografieren, dabei jedoch nichts zu verändern oder zu berühren.
5. Besprechen Sie mit Ihrem Praxisteam, wie Sie die Patienten, die Sie an dem Tag erwarten, verständigen, wenn Sie eventuell keinen Zugriff mehr auf den Praxiscomputer haben.
6. Stellen Sie zusammen mit Ihrem Team eine Stehlgutliste (Diebstahlschaden) auf, in der Sie die entwendeten und eventuell beschädigten Gegenstände (einschließlich Bargeld) auflisten. Am besten, Sie legen im Vorfeld eine Wertsachenliste an, in der die genaue Bezeichnung, das Alter und der Anschaffungspreis der Wertsachen aufgeführt sind.
7. Sofern Kreditkarten oder Handys aus der Praxis entwendet worden sind, müssen Sie sie sofort sperren lassen (Sperr-Notrufnummer 116 116).

Mit diesen 9 Maßnahmen schützen Sie Ihre Pflegeeinrichtung vor Einbruch und Diebstahl

Einbrecher machen leider auch vor Seniorenheimen, Einrichtungen des betreuten Wohnens oder Tagespflegen keinen Halt. Im Gegenteil: Für sie ist es oft leichte Beute. Immer wieder ist von Diebstählen oder Einbrüchen in Pflegeheimen und Tagespflegestätten zu lesen. Die Einbrecher lassen Schmuck und Geld mitgehen, aber auch Tresore in Tagespflegeheimen wurden schon geknackt. Nutzen Sie deshalb die folgenden neun Tipps, um sich besser zu schützen.

1. Externe, unbekannte Handwerker: Lassen Sie sich stets einen Ausweis zeigen und prüfen Sie bei Heimleitung, Pflegedienstleitung oder Hausmeister nach, ob der Auftrag bekannt ist. Unbekannte Personen sollten möglichst nicht unbeaufsichtigt bleiben.
2. Mitarbeiter sollten ermutigt werden, unbekannte Personen freundlich anzusprechen und nach ihrem Anliegen zu fragen.
3. Seien Sie besonders aufmerksam, wenn sich unbekannte Personen auffällig langsam und beobachtend durch die Einrichtung bewegen – möglicherweise spähen sie gezielt für einen späteren Einbruch aus.
4. Bewohner im betreuten Wohnen sollten regelmäßig daran erinnert werden, ihre Tür beim Verlassen des Zimmers abzuschließen und nicht nur zuzuziehen.
5. Lassen Sie Fenster im Erdgeschoss nicht gekippt. Sie gelten als leicht überwindbare Schwachstelle.
6. Schlüssel sollten niemals an offensichtlichen oder leicht zugänglichen Orten versteckt werden.
7. Stellen Sie direkt am Gebäude keine Mülltonnen oder andere Gegenstände ab, die Einbrechern das Erreichen von Fenstern oder Balkonen erleichtern könnten. Sinnvoll ist außerdem eine individuelle Sicherheitsberatung durch die Polizei vor Ort. Dabei werden unter anderem Beleuchtung, Zugänge und mögliche Schwachstellen der Einrichtung geprüft – in der Regel kostenfrei.
8. Eingänge sind gut einsehbar zu gestalten.
9. Auch wenn es immer wieder gesagt wird: Wertsachen sollten nicht offen im Zimmer aufbewahrt werden. Größere Geldbeträge und wertvoller Schmuck gehören in den Safe – niemals in Schubladen oder leicht zugängliche Verstecke, wo sie leicht auffindbar sind.



Seniorenheime und Tagespflegen geraten zunehmend ins Visier von Einbrechern und Dieben.

Türen und Fenster als mögliche Schwachstellen absichern

Guten Schutz bieten Türen und Fenster nach DIN EN 1627 (mindestens Widerstandsklasse RC 2), da sie keine konstruktiven Schwachstellen aufweisen und auch von der Polizei empfohlen werden. Ohne entsprechende Sicherungen lassen sich Fenster und Türen oft in Sekundenschnelle aufhebeln. Gitterroste und Kellerschächte sollten zudem mit stabilen Abhebesicherungen versehen sein, um einen Einstieg zu verhindern.

Worst Case: IT-Ausfall oder Datenpannen in der Praxis oder Einrichtung

Kennen Sie das? Es ist früh am Morgen, die Sprechstunde hat gerade begonnen, die ersten Patienten sitzen bereits in Ihrem Wartezimmer und plötzlich fällt Ihr IT-System aus. Wenn Sie das noch nie erlebt haben, hatten Sie bisher Glück, denn das ist oft ein Horrorszenario. Aber auf Glück allein sollten Sie sich nicht verlassen. Erstellen Sie zusammen mit Ihren Mitarbeitern und in Absprache mit Ihrem Softwareanbieter vorbeugende Sicherheitskonzepte. Oberste Priorität: die regelmäßige Sicherung aller Daten! Nicht nur, um sich vor Hackerangriffen zu schützen, benötigen Sie eine funktionierende Datensicherung, sondern auch für den Fall eines Systemabsturzes. Liegen Ihnen gute Datensicherungen vor, kann der Praxisbetrieb sehr schnell wieder anlaufen. Wir zeigen Ihnen im Folgenden, wie Sie Ihre Daten professionell sichern und den Praxisbetrieb im Ernstfall schnell wiederherstellen können.

Diese Methoden der Datensicherung stehen Ihnen zur Verfügung

Entweder Sie nutzen eine Datensicherungssoftware (Backup-Software) oder Sie speichern nur Ihre selbst erstellten Daten regelmäßig auf einem externen Speichermedium. Meine Empfehlung: Doppelt hält besser! Nutzen Sie beides.

- 1. Volldatensicherung bzw. Vollbackup: Vorteil:** Es werden alle Daten komplett gesichert. Bei einer Wiederherstellung wird nur die letzte Volldatensicherung benötigt. **Nachteil:** Aufgrund der sehr großen Datenmenge ist die Datensicherung sehr zeitintensiv.
- 2. Stufenweise (inkrementelle) Datensicherung bzw. inkrementelles Back-up:** Es werden die Dateien gesichert, die seit der letzten (inkrementellen) Sicherung verändert oder hinzugefügt worden sind. **Vorteil:** Die tägliche Datensicherung ist nicht so zeitintensiv. **Nachteil:** Bei einer Wiederherstellung benötigen Sie die letzte Vollsicherung und alle seitdem durchgeführten inkrementellen Datensicherungen.
- 3. Differentielle Datensicherung bzw. differentielles Back-up:** Es werden nur die Dateien gesichert, die seit der letzten Vollsicherung verändert oder hinzugefügt worden sind. **Vorteil:** Die tägliche Datensicherung ist nicht so zeitintensiv. **Nachteil:** Bei einer Wiederherstellung benötigen Sie die letzte Vollsicherung und die zuletzt durchgeführte differentielle Datensicherung.

Back-ups werden meist vom Softwarebetreuer eingerichtet und laufen automatisch im Hintergrund oder nachts ab.

Datensicherung nach dem Generationenprinzip

Wenn Sie sich selbst (zusätzlich) um die Datensicherungen kümmern, gehen Sie am besten nach dem Generationenprinzip wie folgt vor, um sicherzustellen, dass auch ältere Datenstände im Notfall verfügbar bleiben:

- **Täglich:** Es wird eine Sicherung auf ein neues Medium angelegt. Diese „Sohn-Medien“ rotieren jede Woche, d. h., nach einer Woche wird wieder das erste Sohn-Medium überschrieben.
- **Wöchentlich:** Die „Vater-Medien“, die jeweils am Ende einer Woche beschrieben werden, rotieren jeden Monat (nach einem Monat wird wieder das erste Vater-Medium überschrieben).
- **Monatlich:** „Großvater-Medien“, die jeweils am Ende eines Monats beschrieben werden, rotieren jedes Jahr (nach einem Jahr wird wieder das erste Großvater-Medium überschrieben).

Das bedeutet, dass Sie bei einer Sicherung im Rahmen einer Fünf-Tage-Woche folgende Medien benötigen:

- Vier Sohn-Medien (Montag–Donnerstag; am Freitag wird auf die Vater-Medien gesichert)
- Vier Vater-Medien (für die ersten vier Freitage eines Monats, am fünften bzw. letzten Freitag speichern Sie auf dem Großvater-Medium)
- Zwölf Großvater-Medien (für den letzten Tag in jedem Monat)

Nach diesem Prinzip könnte man stets auf Sicherungen an

- jedem der letzten vier Werktage (Sohn-Sicherungen)
- jedem der letzten vier Freitage (Vater-Sicherungen)
- jedem der letzten zwölf Monatsenden (Großvater-Sicherungen) zugreifen.



Hinweis

Legen Sie fest, welche Sicherungsart (Vollsicherung, differentielle oder inkrementelle Sicherung) durchgeführt werden soll.

So lagern Sie Datenträger für Ihre Datensicherung richtig

- Die Lagerung muss unter magnetfeld-/staubgeschützten und klimagerechten Bedingungen erfolgen.
- Bewahren Sie Datenträger mit wöchentlichen und monatlichen Sicherungen nicht in der Praxis auf.
- Deponieren Sie tägliche Sicherungen in einem Tresor (Schutz vor unberechtigtem Zugriff sowie vor Feuer und Wasser).



Wichtig

Führen Sie regelmäßig Rücksicherungen selbst durch oder lassen Sie dies von Ihrem Softwarebetreuer regelmäßig durchführen. So stellen Sie sicher, dass im Ernstfall tatsächlich auf die gesicherten Daten zugegriffen werden kann. Denken Sie auch an eine Cloud-Datensicherung (Cloud-Backup).

Sie schützt Ihre Daten, indem Kopien Ihrer Dateien und Ordner oder Ihr gesamtes System automatisch über das Internet auf externe Server übertragen werden.



Die 6 häufigsten Systemausfälle – und wie Sie ihnen vorbeugen

Die folgenden Systemausfälle treten in Einrichtungen des Gesundheitswesens besonders häufig auf. Mit den passenden Maßnahmen können Sie viele dieser Risiken gezielt vermeiden:

- **Überlastung des Systems:** Lassen Sie die Autostart-Einstellung überprüfen. Stellen Sie sicher, dass nur die Programme gestartet werden, die Sie auch wirklich nutzen.
- **Falsche Bedienung:** Bleiben Sie ruhig, wenn das System langsam reagiert oder kurz nicht funktioniert. Vermeiden Sie hektische Eingaben – oft hilft bereits eine kurze Pause, um einen Systemabsturz zu verhindern.
- **Fehlende Updates:** Spielen Sie notwendige Updates unverzüglich – nach den Vorgaben Ihres Softwareherstellers – ein, da auf diese Weise Fehler in der Software behoben und Sicherheitslücken geschlossen werden. (Auch die IT-Sicherheitsrichtlinie der KBV schreibt dies ausdrücklich vor!)
- **Überhitzung:** Gerade bei intensiver Nutzung, etwa durch digitale Aktenführung, können Computer stark beansprucht werden. Achten Sie deshalb darauf, dass Lüftungsschlitze frei bleiben und die Geräte nicht zugestellt oder abgedeckt werden.
- **Fehlende Defragmentierung:** Lassen Sie Ihre Festplatte regelmäßig warten und defragmentieren. Dadurch werden Daten neu geordnet, die Systemstabilität verbessert und die Rechengeschwindigkeit erhöht.
- **Hacker-Angriffe auf das System:** Schadsoftware kann Systeme sperren oder Abstürze verursachen. Informieren Sie bei Verdacht sofort Ihren Vorgesetzten und den Softwarebetreuer. Führen Sie keinesfalls eigenständig eine Rücksicherung durch, da sonst auch Sicherungen infiziert werden könnten.

„Notfallplan Datenpanne“: So gehen Sie vor

Eine Datenpanne passiert schneller als gedacht. Umso wichtiger ist es, dass Sie und Ihre Kollegen wissen, wie im Ernstfall richtig gehandelt wird. Die folgenden Hinweise helfen Ihnen, Ihren organisationspezifischen Notfallplan „Datenpanne“ aufzustellen.

Was ist eine Datenpanne?

Nach der DSGVO liegt eine Datenpanne vor, wenn der Schutz von personenbezogenen Daten nicht mehr gewährleistet ist. Und das ist dann der Fall, wenn diese Daten verlorengegangen sind bzw. vernichtet, verändert oder Unbefugten offengelegt wurden.

Datenpanne melden – ja oder nein?

Der Datenschutzverantwortliche (Geschäftsführer, Heimleitung, Praxisinhaber etc.) ist verpflichtet, der für Sie zuständigen Datenschutzbehörde innerhalb von 72 Stunden zu melden, dass der Schutz personenbezogener Daten verletzt worden ist. Und zwar immer dann, wenn diese Verletzung voraussichtlich oder eventuell zur Folge hat, dass die Rechte und Freiheiten der betroffenen Person(en) dadurch einem hohen Risiko ausgesetzt sind. Werden durch diese Datenpanne voraussichtlich die Rechte und Freiheiten der betroffenen Person(en) einem hohen Risiko ausgesetzt, sind Sie verpflichtet, die Betroffenen davon zu unterrichten (z. B. die Patienten, Mitarbeiter etc.). Die Meldepflicht besteht, unabhängig davon, ob bereits ein Schaden eingetreten ist oder nicht.



Wichtig

Die Datenschutzbehörden der Länder definieren den Begriff „Risiko“ so: „Ein Risiko ist die Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt oder zu einem weiteren Schaden führen kann.“ Denken Sie daran, die Meldepflicht liegt beim Datenschutzverantwortlichen. Der Datenschutzbeauftragte kann ihn dabei unterstützen.

Notfallplan: „Datenpanne“

Schritt 1: Datenpanne feststellen

Sie halten schriftlich fest, wann Sie welche Datenpanne in welchem Umfang festgestellt haben:

- Welche Art von Datenpanne liegt vor: Was genau ist passiert?
- Wie viele Datensätze sind ungefähr betroffen?
- Welcher Personenkreis ist betroffen? (Wie viele Personen, Mitarbeiter, Bewohner oder Patienten)
- Welche Maßnahmen haben Sie bisher ergriffen?

Schritt 2: Führen Sie eine Risikoanalyse durch

- Sie beurteilen den Schaden, der den Betroffenen durch die Datenpanne entstehen wird bzw. schon entstanden ist.

Schritt 3: Kommen Sie umgehend Ihrer Meldepflicht nach

- Stellen Sie ein hohes Risiko für einen Schadenseintritt fest, informieren Sie sofort Ihre zuständige Aufsichtsbehörde über die Datenpanne. Ihrer Meldepflicht müssen Sie innerhalb von 72 Stunden nachkommen.
- Um Ihre Aufsichtsbehörde zu informieren, verwenden Sie ein Meldeformular, das Sie von der Internetseite der Behörde herunterladen können.
- Sind besonders sensible Daten (z. B. Patientendaten) betroffen, informieren Sie die betroffenen Personen unverzüglich und in leicht verständlicher Sprache. Eine schuldhaft verzögerte Mitteilung ist unzulässig.

2 Beispiele für meldepflichtige Datenpannen, bei denen ggf. auch die Betroffenen informiert werden müssen:

1. Ein Mitarbeiter schickt einen Arztbrief mit sensiblen Gesundheitsdaten einer Patientin per Fax an den falschen Empfänger.
2. Bei einem Hacker-Angriff in Ihrer Praxis werden sensible personenbezogene Daten gestohlen.

Achtung, Bußgeld!

Verstöße gegen die Meldepflicht können hohe Bußgelder und Schadenersatzforderungen nach sich ziehen.

Datenschutz beginnt mit Prävention

Tun Sie alles dafür, Datenpannen von vornherein zu vermeiden. Sprechen Sie das Thema regelmäßig in Teambesprechungen an, um Ihre Mitarbeiter dauerhaft für den Datenschutz zu sensibilisieren. Schon kleine Unachtsamkeiten können zu erheblichen Datenschutzverstößen und rechtlichen Konsequenzen führen. So bleibt das Bewusstsein für einen verantwortungsvollen Umgang mit personenbezogenen Daten dauerhaft erhalten.



Blackout in der Arztpraxis: Mit einem Notfallplan sind Sie gut gewappnet!

Irgendwann passiert es in jeder Praxis: Das Wartezimmer ist voll, die Patienten stehen bis zur Eingangstür – und plötzlich passiert es: Das Licht erlischt, alle Bildschirme sind schwarz, kein Ultraschall, kein Röntgen – nichts geht mehr. STROMAUSFALL – ein Horrorszenario. Womöglich sitzt auch noch ein Patient im Fahrstuhl fest. Haben Sie das schon einmal erlebt? Dann heißt es: Ruhe bewahren. Denn nicht immer fließt der Strom nach wenigen Minuten wieder. Mit unserer Hilfe erstellen Sie einen praxisnahen Notfallplan für Stromausfälle, damit im Ernstfall jeder weiß, was zu tun ist.

9 Tipps, mit denen Sie und Ihr Team bei Stromausfall alles im Griff behalten

Bewahren Sie Ruhe!



1.	Praxis komplett dunkel: Für diesen Notfall müssen Sie mindestens eine Taschenlampe an der Anmeldung deponiert haben, die Sie bzw. Ihre Mitarbeiter notfalls auch im Dunkeln finden. Bewahren Sie weitere Taschenlampen in einem auch im Dunkeln leicht zugänglichen Schrank auf, damit weitere Lampen bei Bedarf verteilt werden können.
2.	Jetzt überprüfen Sie den Sicherungskasten.
3.	In der Zwischenzeit überprüft ein Mitarbeiter, ob im Fahrstuhl Personen feststecken. Wenn ja, wird umgehend die für den Fahrstuhl zuständige Firma verständigt. Notfall-Rufnummer: _____. Die eingeschlossenen Personen werden darüber informiert, dass Hilfe unterwegs ist.
4.	Gleichzeitig kann sich ein weiterer Mitarbeiter erkundigen, ob auch bei Nachbarn oder vielleicht sogar im ganzen Stadtteil der Strom ausgefallen ist.
5.	Sie werden jetzt einige Anrufe tätigen müssen. Denken Sie daran, dass auch Ihre Telefonanlage bei einem Stromausfall nicht funktioniert. Anrufe erledigen Sie mit Ihrem Handy! Lassen Sie sich dabei ggf. von Ihren Mitarbeitern unterstützen.
6.	Rufen Sie beim Stromversorger an. Tel.: _____
7.	Legen Sie fest, welcher Mitarbeiter die Patienten in der Praxis bittet, Ruhe zu bewahren. Falls mit einem längeren Stromausfall zu rechnen ist, werden die Patienten gebeten – soweit dies möglich ist –, nach Hause zu gehen (Fluchtwege sind beschildert und gut sichtbar. Vorgeschrieben sind beleuchtete Fluchtwege).
8.	Bei längerem Stromausfall kann der Kühlschrank die Temperatur nicht mehr halten. Sie und Ihre Mitarbeiter wissen, wie lange Sie Zeit haben, die Inhalte umzulagern. Tipp: Vereinbaren Sie bereits im Vorfeld mit Ihrer Apotheke, dass Sie im Fall eines längeren Stromausfalls Impfstoffe und eventuell auch andere Medikamente und Materialien in der Apotheke lagern dürfen. Apotheken haben meist ein Notstromaggregat.
9.	Falls durch den Stromausfall Daten verlorengegangen sind, setzen Sie sich zu gegebener Zeit mit Ihrer Softwarefirma in Verbindung.



Ein Stromausfall kann den gesamten Praxisbetrieb lahmlegen – klare Notfallpläne helfen, im Ernstfall ruhig und sicher zu handeln.



Mein Tipp

Bei einem plötzlichen Stromausfall gehen alle Daten verloren, die noch nicht gespeichert wurden. Darüber hinaus können Computer, Server oder Festplatten durch Spannungsschwankungen, Kurzschlüsse oder Überspannungen beschädigt werden. Die Folgen reichen von Datenverlusten und Systemausfällen bis hin zu kostspieligen Reparaturen und längeren Betriebsunterbrechungen.

Schutz bietet eine sogenannte unterbrechungsfreie Stromversorgung (USV). Sie überwacht die Stromversorgung permanent und übernimmt bei einem Stromausfall oder einer Netzstörung innerhalb weniger Millisekunden die Energieversorgung der angeschlossenen Geräte. Ein Warnton oder eine optische Anzeige signalisiert den Ausfall der Netzspannung. Die integrierte Batterie versorgt dann beispielsweise Server, Computer, Netzwerkkomponenten oder Telefonanlagen für einen begrenzten Zeitraum weiter mit Strom.

Diese Überbrückungszeit verschafft Ihnen wertvolle Minuten, um offene Dateien zu speichern, wichtige Daten zu sichern und die Systeme kontrolliert herunterzufahren. Moderne USV-Anlagen können diesen Vorgang sogar automatisch auslösen und so das Risiko menschlicher Fehler reduzieren. Dadurch lassen sich Datenverluste vermeiden und Schäden an Hard- und Software minimieren.

Besonders für Pflegeeinrichtungen, Arztpraxen und andere Einrichtungen mit digitaler Dokumentation ist eine USV ein wichtiger Bestandteil der Notfallvorsorge. Nach Wiederherstellung der Stromversorgung schaltet die USV automatisch in den Normalbetrieb zurück und lädt ihre Batterien selbstständig wieder auf. So steht der Schutz auch beim nächsten Stromausfall sofort zur Verfügung.



Stromausfall im Pflegeheim: Sind Sie auf den Ernstfall vorbereitet?

Ein Stromausfall in einem Seniorenheim hat weitreichende Folgen, da die Versorgung der Bewohner sichergestellt bleiben muss. Umso wichtiger ist ein gut vorbereiteter Notfallplan. Die folgenden Tipps unterstützen Sie bei dessen Erstellung.

Legen Sie fest, wie Sie bei einem Blackout weiterhin wichtige Informationen erhalten können

- Funktionieren Handys/Laptops noch? Denken Sie daran: Bei Stromausfall können die Handys nicht nachgeladen werden! Legen Sie fest, wie dann vorzugehen ist.
- Sind batteriebetriebene Radios vorhanden?
- Kennen Sie die Anlaufstelle, von der Sie im Katastrophenfall Informationen und eventuell Hilfe erhalten können?
- Gibt es in Ihrem Haus ein Notstromaggregat?

Versorgung der Bewohner

- Erfassen Sie Bewohner mit lebenswichtigen strombetriebenen Geräten und planen Sie bei längeren Stromausfällen frühzeitig einen Transport ins Krankenhaus.
- Vereinbaren Sie mit anderen Pflegeheimen Notfallaufnahmen und halten Sie die Kontaktdaten in einer ausgedruckten Liste fest.
- Erfassen Sie die Bewohner, die bei längerem Stromausfall von Angehörigen betreut werden können.

So gehen Sie bei Stromausfall bis zu 8 Stunden vor

- Aktivierung der Notstromversorgung (wenn vorhanden)
- Wasservorräte anlegen (z. B. Eimer, Kanister), da die Wasserversorgung nach 8–24 Stunden ausfallen kann
- Ausfall der Sicherheitssysteme, Schließtüren:
 - Sicherung der Türen (z. B. mit Fahrradschlössern)
 - Wissen Mitarbeitende, wie sie Brandschutz-/Sicherungstüren manuell öffnen können?
- Ausfall der Aufzüge:
 - Müssen Personen befreit werden?
 - Wissen Mitarbeitende, wie sie Aufzüge manuell bedienen können?
- Ausfall von Patientennotrufsystemen: regelmäßige Kontrollgänge durch Mitarbeitende
- Bei Ausfall der Küche oder Fremdversorgung Essen aus vorhandenen Vorräten zubereiten
- Eventuell Verunsicherung, Ängste, vermehrte Stürze der Bewohner: Beruhigung durch Mitarbeitende



Mein Tipp

- Halten Sie Glocken oder Trillerpfeifen vor, die Sie im Notfall an die Bewohner verteilen, damit diese sich bemerkbar machen können.
- Ausfall der Beleuchtungen bei Nacht: Verteilung von Leuchtgeräten, z. B. Raumlampen, Campingleuchten etc. an Bewohner

- Stellen Sie Stirnleuchten für Mitarbeitende bereit, damit sie bei der Versorgung von Bewohnern beide Hände frei haben.

Vorgehen bei Stromausfall von 8 bis 24 Stunden

- Bei möglichem Ausfall der Toiletten: Toilettenstühle und große reißfeste Müllbeutel nutzen
- Bei möglichem Ausfall der Heizung:
 - Heizstrahler bereithalten, die an ein Notstromaggregat angeschlossen werden können
 - Decken verteilen, Temperaturkontrolle in den Schlafräumen, ggf. Menschen zusammenlegen (mehr Wärmeentwicklung)
- Bei möglichem Ausfall der Wasserversorgung: Wasservorräte nutzen (Hygiene, Küche)
- Ausfall der Wäscherei: Sind ausreichend eigene Wäschevorräte vorhanden?
- Engpässe Geschirr: Einweggeschirr nutzen
- Ermüdungserscheinungen beim Personal: Personalwechsel möglich?

Bei Stromausfall von mehr als 24 Stunden gehen Sie so vor

- Krisenstab gemeinsam mit der Einsatzleitung des Katastrophenschutzes abstimmen
- Prüfen, ab wann die Versorgung nicht mehr aufrechterhalten werden kann
- Entscheiden, ob eine Evakuierung notwendig ist
- Bei Ausfall der Brandmeldeanlage Mitarbeitende als Brandwachen pro Etage einsetzen
- Medikamentenengpässe prüfen (z. B. Insulin)
- Versorgung über Krankenhausapotheken oder Hilfsorganisationen organisieren
- Lebensmittelvorräte kontrollieren und Unterstützung durch Dienstleister prüfen
- Engpässe bei Verbrauchsmitteln frühzeitig abklären
- Versorgung mit Hygiene-, Inkontinenz- und Verbandmaterial sicherstellen
- Verlegung und Kühlung Verstorbener organisieren (Abstimmen, ob Bestatter Verstorbene abholen können)



Fazit

Ein längerer Stromausfall kann die Versorgung von Pflegebedürftigen stark gefährden. Erstellen Sie daher einen Notfallplan und schulen Sie Ihre Mitarbeitenden entsprechend.

Nie mehr Angst vor gewalttätigen Patienten: So schützen Sie sich und Ihre Mitarbeiter

Immer häufiger und leider nicht ausgeschlossen: Patienten werden gegenüber Ihnen oder Ihren Mitarbeitern gewalttätig. Dazu zählen nicht nur verbale Übergriffe, sondern auch tätliche Angriffe. Wichtig ist, sofort und konsequent zu reagieren und zugleich zu hinterfragen, wie es überhaupt zu der Eskalation kommen konnte. Setzen Sie dieses Thema auf die Tagesordnung der nächsten Teamsitzung. Sie und Ihre Mitarbeiter sollten den Ursachen der Übergriffe auf den Grund gehen. Überlegen Sie, ob eventuell das eigene Verhalten die Aggression beim Patienten ausgelöst hat. Legen Sie Verhaltensregeln fest, damit vor allem Ihre Mitarbeiter sich in einer Gewaltsituation richtig verhalten, und geben Sie – soweit möglich – Präventionsmaßnahmen vor.

Warum ist ein Mensch aggressiv?

Ein aggressiver Patient ist ein Mensch in Not, er ist innerlich zerissen, wütend und fühlt sich der Situation hilflos ausgeliefert. Er versucht, dieser Notsituation durch Gewalt zu entkommen und die Anspannung so abzubauen. Meist sind es nichtige Anlässe – eine Berührung, eine falsch verstandene Geste, ein unerfüllter Wunsch –, die das gewalttätige Handeln des Patienten auslösen. Wenn Sie und Ihre Mitarbeiter sich dessen bewusst sind, haben Sie bereits den ersten wichtigen Schritt getan, um solchen Situationen vorzubeugen.

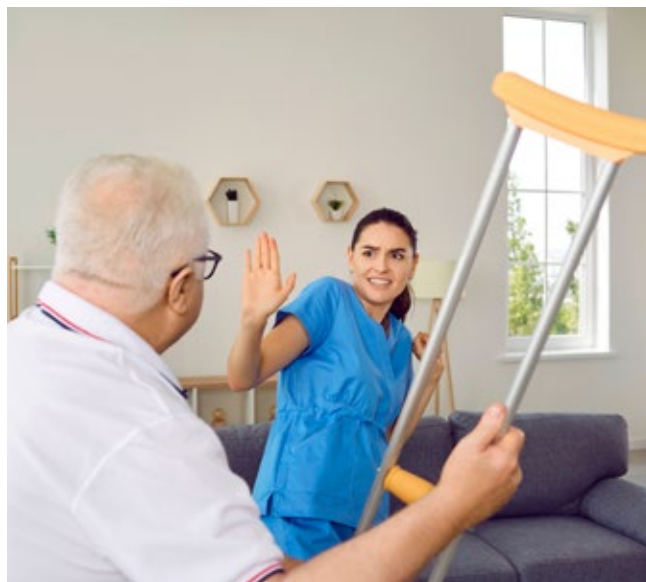
Halten Sie die notwendigen Verhaltensregeln in einer Arbeitsanweisung fest. Nutzen Sie dazu das folgende Muster.



Arbeitsanweisung: Verhalten bei Gewaltübergriffen

- **Ziel:** Mit diesen Verhaltensregeln möchten wir Gewalt und Aggression in unserer Praxis oder bei Hausbesuchen verhindern oder im Keim ersticken.
- **Bestehendes Risiko:** Mitarbeiter, Praxisinhaber und anwesende Patienten können verletzt werden.
- Lassen Sie bei auffälligen Patienten immer die Zimmertür offen!
- Geben Sie bei Hausbesuchen oder Tätigkeiten in Pflegeheimen stets einem Kollegen bzw. den Pflegekräften im Heim Bescheid. Teilen Sie ihnen den Grund mit.
- Nicht den Mutigen spielen! Schon beim kleinsten Anzeichen einer Gewaltbereitschaft holen Sie einen Kollegen oder den Arzt bzw. die Ärztin zu Hilfe.
- Im Umgang mit schwierigen Menschen sollten Sie Gelassenheit ausstrahlen. Dazu tragen eine gleichmäßige Atmung und ein entspannter Gesichtsausdruck bei.
- Vermeiden Sie jede Art von Drohgebärden, zeigen Sie nicht mit dem Finger auf eine Person, ballen Sie keinesfalls die Hand zur Faust – so etwas wird in der Regel als Aggressivität gedeutet.
- Bewegen Sie sich ruhig und koordiniert. Hektische, plötzliche Bewegungen können als Drohgebärden aufgefasst werden.
- Beobachten Sie unauffällig, das heißt, fixieren Sie Ihr Gegenüber nicht mit Blicken. Achten Sie auf Zeichen, die einen Angriff ankündigen (trockener Mund, weit geöffnete Augen, schneller Atemrhythmus, hastiger Puls (mitunter an den pochenden Schläfen zu erkennen), Schweißbildung, starrer Gesichtsausdruck).

- Sprechen Sie ruhig und in angemessener Lautstärke. Schreien bewirkt meist das Gegenteil dessen, was man erreichen möchte.
- Fallen Sie einem aggressiven Patienten nicht ins Wort. Zeigen Sie stattdessen Verständnis für seine Äußerung.
- Sprechen Sie den Angreifer mit Namen an und beschimpfen Sie ihn niemals!
- Anweisungen müssen kurz, verständlich und prägnant sein. Wiederholen Sie notfalls die Aussagen.
- Ironie, Zynismus und Sarkasmus sind fehl am Platz. Ebenso ungeeignet sind Androhungen von Strafen und Sanktionen. Bieten Sie stattdessen Lösungen an.
- Korrekter Arbeitsschutz (kein Schmuck, festes Schuhwerk) erleichtert die Abwehr von gewalttätigen Übergriffen.
- Dokumentieren Sie jeden Zwischenfall. Informieren Sie den Vorgesetzten und ggf. die Berufsgenossenschaft.



Klare Verhaltensregeln und Präventionsmaßnahmen helfen, angemessen auf Gewalt durch Patienten zu reagieren.

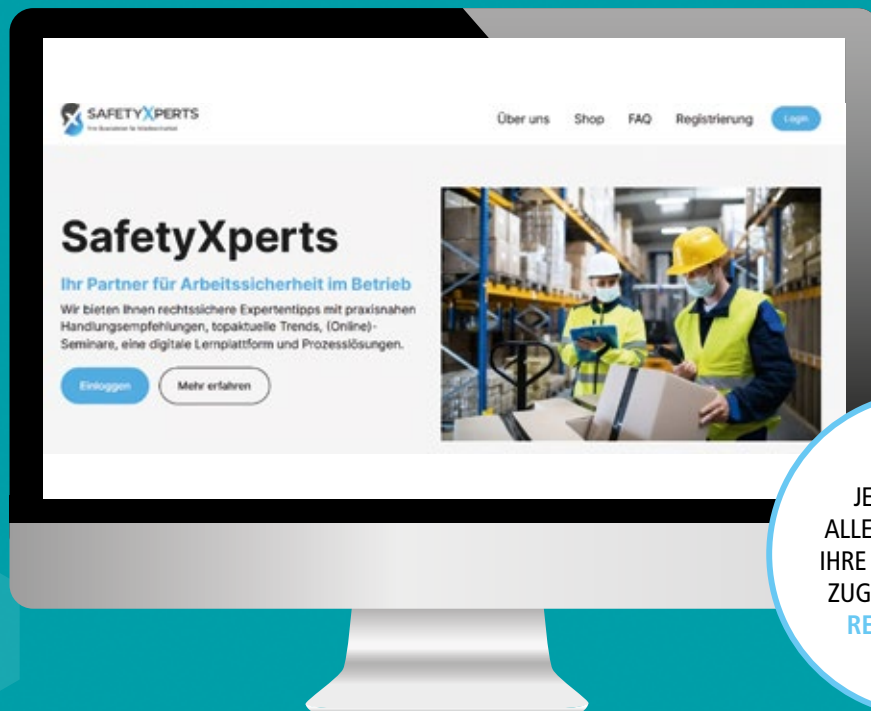


Mein Tipp

Werden Sie oder Ihre Mitarbeitenden durch einen Gewaltübergriff verletzt, ist dies ein Arbeitsunfall. Melden Sie ihn umgehend Ihrer Berufsgenossenschaft.



NUTZEN SIE IHREN EXKLUSIVEN ONLINEBEREICH



JEDERZEIT VON
ALLEN GERÄTEN AUF
IHRE ARBEITSHILFEN
ZUGREIFEN. GLEICH
REINSCHAUEN!



**Nutzen Sie den
Onlinebereich auch
mobil und stöbern
Sie durch die Updates:
safetyxperts.de/login**



Arbeitshilfen: Muster, Vorlagen, Checklisten

Bequemer als Google und verlässlicher als KI: Sie finden über die Schlagwortsuche alle Arbeitshilfen zum Herunterladen und Bearbeiten.



Archiv: Ihre Ausgaben

Digital und auf allen Geräten können Sie auf die bisher erschienenen Ausgaben bequem zugreifen – nichts geht verloren!



Newsfeed: Aktuelle Beiträge

Bleiben Sie stets über aktuelle Themen und wichtige Änderungen im Arbeitsschutz informiert.

Impressum

SafetyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG • Theodor-Heuss-Str. 2–4, 53095 Bonn • Telefon: 02 28 / 95 50 120 • Fax: 02 28 / 36 96 486 • Internet: www.safetyxperts.de • E-Mail: kundendienst@safetyxperts.de • E-Mail für Leserfragen: gesundheitswesen@safetyxperts.de • Vorstand: Richard Rentrop • ISSN: 2365-7723 • Erscheinungsweise: 26-mal pro Jahr • Redaktionell Verantwortlicher: Martin Grashoff, VNR Verlag für die Deutsche Wirtschaft AG; Adresse s. o. • Redaktion: Renate Tief, Estenfeld (RT) • Produktmanagement: Chanaya Schönborn, Bonn • Satz: Schmelzer Medien GmbH, Siegen • Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim • Titelbild: © SneakyPeakPointspeopleimages.com – stock.adobe.com • Alle Angaben in „Arbeitsschutz und Hygiene im Gesundheitswesen“ wurden mit äußerster Sorgfalt

ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden. Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. © 2026 by SafetyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau.

Bildnachweise: Seite 3: AdobeStockRobert Kneschke; Seite 5: AdobeStock Aleksandr; Seite 8: AdobeStock stgrafix; Seite 10: AdobeStock Studio Romantic

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

Dieser Fachnewsletter richtet sich gleichermaßen an weibliche und männliche Leser. Aus Gründen der Lesbarkeit wird die männliche Schreibweise (z. B. Unternehmer, Mitarbeiter) gewählt. Diese schließt stets alle Geschlechterformen mit ein.





Datenschutzvorfälle in Gesundheitseinrichtungen

Die Studie „Eine entscheidende Investition: Am Puls der Technologie im Gesundheitswesen“ aus dem Jahr 2022 zeigt, dass 91 % der Gesundheitseinrichtungen in Deutschland in den letzten zwei Jahren mindestens einen Datenschutzvorfall erlitten hatten. Die Hauptursachen waren:

- Datenverlust durch vorsätzliches oder fahrlässiges Fehlverhalten der Mitarbeiter: 63 % in Deutschland (49 % weltweit)
- Datenschutzverletzungen aufgrund externer Ursachen, z. B. durch DDoS-Attacken: 59 % in Deutschland (48 % weltweit)

Quelle: Arzt und Wirtschaft, 28.10.2022



SAFETYXPERTS

Ihre Spezialisten für Arbeitssicherheit