HANDLUNGSEMPFEHLUNG

## DIGITALISIERUNG UND PATIENTENSICHERHEIT

# Risikomanagement in der Patientenversorgung

AKTIONSBÜNDNIS PATIENTENSICHERHEIT

patientensicherheit schweiz

Plattform Patientensicherheit

# Inhalt

# Vorwort

Die Digitalisierung hat in nahezu allen Lebensbereichen Einzug gehalten und ist bereits jetzt integraler Bestandteil der Gesundheitsversorgung. Durch die neuen digitalen Technologien und Anwendungsmöglichkeiten ergeben sich in der Medizin neue Chancen, die Gesundheitsversorgung noch wirksamer und effizienter zu gestalten. Spektakuläre Fälle zeigen aber auch die Risiken auf, die mit dem System einhergehen. Unmittelbare Schäden, nicht nur für die Leistungsfähigkeit, sondern auch für die Patientensicherheit, sowohl im Hinblick auf die physische, psychische aber auch soziale Unversehrtheit der Behandelten können die Folge sein.

Die Patientensicherheitsorganisationen in Deutschland, Österreich und der Schweiz erreichen eine Vielzahl von Anfragen zum Thema Digitalisierung. Die durch Digitalisierung erzeugten Veränderungen sind dynamisch, umfassend und in ihren Auswirkungen fallweise durchaus disruptiv. Um diesen Entwicklungen gerecht zu werden, müssen Kräfte gebündelt werden. Zum anderen sind wesentliche Herausforderungen der Digitalisierung nicht an Landesgrenzen gebunden. Das Aktionsbündnis Patientensicherheit (APS), die Plattform Patientensicherheit Österreich und die Stiftung Patientensicherheit Schweiz legen nun gemeinsam zwei Empfehlungen zum Thema Digitalisierung und Patientensicherheit vor:

Eine Handlungsempfehlung gibt Hinweise für Patientinnen und Patienten zum sicheren Umgang mit Apps (http://www.aps-ev.de/patienteninformation/). Die hier vorgelegte Handlungsempfehlung zeigt Herausforderungen und Lösungen der Digitalisierung für das Risikomanagement auf.

Durch die zunehmende Digitalisierung verändern sich relevante Risiken in der Patientenversorgung: Während einige Risiken minimiert werden, kommen neue Risiken hinzu, andere erhöhen sich deutlich.

Diese Handlungsempfehlung richtet sich an Angehörige aller Berufsgruppen und Fachdisziplinen, die in der Gesundheitsversorgung tätig sind und soll

**Sensibilisieren**, für die mit der Digitalisierung des Gesundheitswesens einhergehenden neuen bzw. zunehmenden Risiken.

**Informieren**, über mögliche Ursache-Wirkungsbeziehungen dieser Risiken, um ein Verständnis für diese häufig abstrakt anmutenden Risiken zu ermöglichen.

**Helfen**, eine individuelle Nutzen-Risiko-Abwägung für bestehende und geplante digitale Innovationen durchzuführen, um bestehende oder drohende Risiken zu minimieren, um die Chancen dieser neuen Techniken zum Wohl aller Beteiligten zu nutzen.

Effektives Risikomanagement fokussiert auf die wenigen, wirklich relevanten Risiken, getreu dem Motto: „Weniger ist mehr!“. Daher beschränkt sich diese Handlungsempfehlung auf sechs aus Sicht der Autoren wesentliche Risiken der Patientenversorgung im Zusammenhang mit der Nutzung digitaler Techniken und Systeme. Sie hat damit keinen Anspruch auf Vollständigkeit, ermöglicht aber einen systematischen, sinnvollen Beginn im Umgang mit dieser Thematik.

Diese Handlungsempfehlung ersetzt jedoch weder die Konsultation von IT-Spezialisten noch die individuelle, maßgeschneiderte Risikobewertung unter Beachtung der jeweiligen Gegebenheiten vor Ort. So können weitere Risiken als die hier genannten im Einzelfall von hoher Relevanz für die Patientensicherheit sein. Auch kann das Risiko durch vorbeugende Maßnahmen minimiert werden, eine gänzlich risikofreie Anwendung digitaler Systeme wird jedoch niemals erreicht werden können.

Als methodische Grundlage der Handlungsempfehlung wurde eine modifizierte Form der Szenario-Analyse nach ONR 49002-2:2014 gewählt, die geeignet ist, durch bildhafte Darstellung einer Situation, deren Komplexität zu reduzieren und sie so verständlich für alle Beteiligten werden zu lassen. Zur Verdeutlichung des Sachverhaltes wurden für jedes daraus entstandene Szenario konkrete, praktische Beispiele aufgeführt. Grundsätzlich sind diese spezifischen Beispiele auf alle Sektoren und Fachdisziplinen anwendbar, auch wenn nicht alle Risiken in den Bereichen gleichermaßen ausgeprägt sind.

Die intensive Beschäftigung mit den Risiken der Digitalisierung des Gesundheitswesens zeigt neben den unstrittig vorhandenen hohen Chancen auch gravierende Risiken für die Patientensicherheit auf. Digitale Anwendungen zur Gesundheitsversorgung sollten daher ebenso wie Arzneimittel und Medizinprodukte einer Risikoanalyse und einer entsprechenden Überprüfung unterworfen werden, um die Chancen der Digitalisierung durch Minimierung der Risiken im Sinne guter und sicherer Patientenversorgung zu nutzen.

Diese Handlungsempfehlung wurde vor Drucklegung von zahlreichen Experten und Praktikern aus unterschiedlichen Berufsfeldern gelesen und kommentiert. Für ihre wertvollen Hinweise danken wir allen Kommentatoren und insbesondere allen Mitarbeitenden in der Arbeitsgruppe.

**Hedwig François-Kettner**
Aktionsbündnis
Patientensicherheit e.V.

**Dir$^{in}$ Dr.$^{in}$ Brigitte Ettl**
Plattform
Patientensicherheit
Österreich

**Prof. Dieter Conen**
Stiftung
Patientensicherheit
Schweiz

# Digitalisierung und Patientensicherheit – Wie sind Sie aufgestellt?

Folgende Fragen verdeutlichen zentrale Aspekte der mit zunehmender Digitalisierung einhergehenden Risiken:

Wie stellen Sie sicher, dass bei einem Ausfall oder einer Störung der IT-Infrastruktur weiterhin eine sichere Patientenbehandlung durchgeführt werden kann?

Mit welchen Maßnahmen können Sie eine sichere Patientenversorgung beim Betrieb digitaler, netzwerkangebundener Medizinprodukte gewährleisten?

Sind Ihr IT-Netz und von Ihnen eingesetzte vernetzte Medizinprodukte ausreichend geschützt vor Manipulation und Datendiebstahl durch externe Angriffe?

Sind Ihre digitalen Daten ausreichend vor unberechtigtem Zugriff durch Dritte (z.B.: neugierige Angehörige) geschützt?

Wenn Sie Daten externen Dienstleistern überlassen, mit welchen Maßnahmen können sie sich vor Datenverlust oder Missbrauch schützen?

Verfügen alle Beteiligten über ausreichend digitale Kompetenz, um zur sicheren Patientenbehandlung Störungen und Schwachstellen des IT-Systems zu erkennen?

# Digitalisierung und Patientensicherheit – Darauf kommt es an!

Zusammenfassend lassen sich aus den sechs priorisierten Risiken folgende, grundsätzliche Empfehlungen ableiten.

1. Übernehmen Sie als Leitung die Verantwortung für die digitale Sicherheit.

2. Benennen Sie einen Sicherheitsbeauftragten für Ihr IT-System und damit vernetzte Medizinprodukte und definieren Sie Sicherheitsstufen.

3. Gewährleisten Sie ausreichend zeitliche, personelle und materielle Ressourcen, um dauerhaft eine sichere Infrastruktur und angemessene Kenntnisse in Bezug auf IT-Sicherheit zu gewährleisten.

4. Sorgen Sie bei allen Beteiligten für die erforderlichen Kenntnisse über die Risiken von digitalen Schnittstellen, Passwörtern und Datenträgern. Achten Sie darauf, dass Passwörter dem aktuellen Sicherheitsstandard entsprechen und regelmäßig aktualisiert werden.

5. Sensibilisieren Sie alle Beteiligten über die Risiken von digitalen Anwendungen und praktikablen Maßnahmen zum Schutz vor unberechtigtem Zugriff (z.B. Blickschutz).

6. Sorgen Sie für ein räumliches Umfeld, das einen sicheren digitalen Arbeitsplatz ermöglicht.

7. Führen Sie regelmäßig eine individuelle Risikoanalyse durch, welche IT-Systeme bei Ausfall oder Störung zu welchen Konsequenzen für die Patientenbehandlung führen. Erstellen Sie auf dieser Basis ein Ausfallkonzept für IT und vernetzte Medizinprodukte mit einem Maßnahmen- und Informationsplan.

8. Sensibilisieren Sie Führungskräfte regelmäßig für die Notwendigkeit eines Ausfallkonzeptes für IT und vernetzte Medizinprodukte als Teil des Notfall- und Krisenmanagements und schulen Sie das ggf. betroffene Personal angemessen, damit im Ernstfall theoretische Überlegungen auch praktisch umgesetzt werden.

9. Stellen Sie die redundanten Systeme und Dienstleistungen dauerhaft bereit, die bei Ausfall der IT und/oder vernetzten Medizinprodukte unter Berücksichtigung des Versorgungsauftrages erforderlich sind.

10. Überlassen Sie Daten externen Dienstleistern nur, wenn die Erfüllung gesetzlicher Anforderungen (Europäische Datenschutzgrundverordnung) nachgewiesen wurde.

11. Lassen Sie sich vom externen Dienstleister vertraglich ein Ausfallkonzept zusichern und klären Sie haftungsrechtliche Fragen.

12. Lassen Sie überprüfen, ob die Infrastruktur des externen Dienstleisters mit Ihrer Infrastruktur (Hard- und Software) kompatibel ist.

13. Stellen Sie sicher, dass Hard- und Software kompatibel, validiert und aufeinander abgestimmt sind, insbesondere auch nach Austausch/Ersatz einzelner Komponenten und nach Erweiterung oder Updates des Systems.

14. Achten Sie auf die Kompatibilität der Sicherheits- und Leistungsanforderungen von IT-Systemen und vernetzten Medizinprodukten bzw. gleichen Sie diese bei Neubeschaffungen an.

# Digitalisierung und Patientensicherheit – Relevante Risiken für die Patientensicherheit

Im Folgenden finden Sie eine Darstellung der sechs Risiken, die von den Autoren in einem mehrstufigen, teils anonymisierten Konsensus-Verfahren in Bezug auf die Auswirkung von Digitalisierung auf Patientensicherheit als wesentlich angesehen wurden.

## Risiko ▶ Unzureichender Schutz des IT-Netzes vor externen Angriffen

**THEMATISCHER EINSTIEG:**

Eine elektronische Vernetzung zwischen therapeutischen Teams untereinander wie auch mit Patienten, birgt das Risiko einer bewusst durchgeführten „Attacke" von Kriminellen. Personen versuchen aus verschiedenen Gründen, in IT-Netze einzudringen und sensible Daten abzufangen, zu löschen, zu manipulieren oder den Zugriff darauf bis zur Zahlung von Lösegeldern zu sperren.

**PRAKTISCHE BEISPIELE:**

In einem Krankenhaus erhalten Mitarbeiter E-Mails mit gefälschtem Absender der IT-Abteilung. Die E-Mail informiert über eine neue Anwendung und bittet den Empfänger und einem angegebenen Link zu testen, ob auf das System Zugriff hat. Als Einwahldaten sollen der Benutzername und das Passwort seines Benutzerprofils verwendet werden. Der Link führt auf eine externe Seite mit Logo des Krankenhauses, die eingegebenen Daten werden abgefangen und für einen Angriff auf das IT-System genutzt.

Im Behandlungszimmer einer Psychotherapiepraxis sitzt Herr M., welcher sich durch das Vortäuschen psychosomatischer Beschwerden Zutritt verschafft hat. Im Behandlungszimmer ist aufgrund von dringlicheren Behandlungen zeitweise kein Personal anwesend.

Herr M. schließt sein Smartphone über das USB-Kabel am frei zugänglichen Praxis-PC an und lädt sich die Patientendatenbank herunter. Herr M. erpresst mit den gewonnenen Daten sowohl den Praxisinhaber als auch die Patienten.

**AUSGANGSLAGE**:

Die Möglichkeiten der Attacke eines IT-Systems sind vielfältig und vielschichtig. So weist die verwendete Software immer wieder Sicherheitslücken auf, insbesondere, wenn regelmäßige Software-Updates und Firewalls fehlen. Hacker können diese bekannten Lücken nutzen, um in die IT-Systeme einzudringen und dort Computerviren zu installieren.

Daten gelangen zudem über externe Schnittstellen beispielsweise in Form von Untersuchungsergebnissen per Daten-CD in das System. Ebenso können Daten von Apps oder gespeicherte Informationen auf Datenträgern wie USB-Sticks die Gefahr bergen, dass sich auf ein geschlossenes Praxissoftwaresystem Schadsoftware aufspielt.

E-Mail-Anhänge mit Schadsoftware oder Fake E-Mails können dazu führen, dass Schadsoftware installiert wird. Durch das Verwenden von Datenübertragungen ohne Verschlüsselung sind sensible Daten durch Dritte abfangbar und auslesbar.

Eine ungeschützte, für jedermann zugängige Administration ermöglicht unkontrolliertes Herunterladen und Installieren von Software.

Netzwerke benötigen Schnittstellen, die die Verknüpfung von Programmen ermöglichen. Große Netzwerke bergen die Gefahr, dass sich bei Angriffen und Systemausfällen der Datenverlust im Netzwerk ausweitet (Dominoeffekt) und nicht nur auf ein Softwaremodul (z.B. des Labors oder der Röntgenabteilung) begrenzt.

Die Motive für die Verwendung von Schadsoftware können vielfältig sein (z.B. Unwissenheit, Erpressung, Schädigung, Informationsdiebstahl/Spionage). Cyberkriminalität im Gesundheitswesen führt bereits jetzt zu hohem wirtschaftlichen Schaden und ist für Kriminelle häufig sehr lukrativ.

Erpressungsversuche mit unterschwelligen Geldbeträgen werden durch den hohen Leidensdruck und der Angst vor Reputationsverlust begünstigt. Ebenso werden Angriffe offiziellen Stellen ggf. aus falscher Scham oder Angst vor Reputationsverlust nicht gemeldet und können sich so leichter verbreiten.

**RISIKEN**:

- Sensible Patientendaten sind nicht geschützt und können an externe Personen verbreitet werden. (Datenschutz)
- Es kann zu Systemzusammenbrüchen kommen z.B. durch Viren, die überlastende Datenmengen erzeugen (buffer overflow), welche die Prozesse einer Einrichtung stören und somit den Versorgungsauftrag gefährden.

- Es kann zu Verschlüsselungen von vorhandenen Daten kommen. Kriminelle können Einrichtungen hierdurch erpressen und die Arbeitsprozesse zum Erliegen bringen.
- Daten (z.B. Laborwerte, Medikationen, etc.) können manipuliert werden und somit eine direkte Gefährdung des Patienten bedeuten.

**AUSWIRKUNGEN:**

- Gelangen patientenrelevante Informationen unberechtigt an Dritte, können diese die Information nutzen, um am Arbeitsplatz, im privaten Umfeld oder auch bei Vertragsabschlüssen von Versicherungen die betroffenen Menschen zu benachteiligen, zu stigmatisieren und ihre Persönlichkeitsrechte zu verletzen.
- Durch Schadsoftware können relevante Behandlungsdaten nicht verfügbar sein (siehe Risiko Nichtverfügbarkeit von IT-Infrastruktur/Patientendaten).
- Durch Datenmanipulation kann es zu fehlerhaften Beurteilungen, Diagnosen und dadurch auch zu Fehlbehandlungen kommen. Außerdem können Funktionen von Medizinprodukten beeinflusst werden (z.B. Ausschalten von Alarmsystemen).

**MÖGLICHE URSACHEN:**

- Unzureichendes Risikobewusstsein durch fehlende digitale Kompetenz (siehe Risiko Unzureichende Digitale Kompetenz der therapeutischen Teams).
- Eine fehlende Absicherung des IT-Netzes mittels Firewall, Virenschutz und Quarantänebereich für E-Mails ermöglicht es externen Personen mit geringem Aufwand, das vorhandene Netzwerk zu infiltrieren.
- Unverschlüsselte E-Mails können durch Viren für externe Personen einsehbar gemacht werden. Informationen und Daten können so leicht gestohlen werden.
- Mögliche Eintrittspforten für schädliche Software sind z.B. ungesicherte USB-Anschlüsse an PCs oder unverschlüsselte WLAN-Netze. Es werden auch gezielt USB-Sticks mit Viren platziert.
- Medizinprodukte und IT-Netze sind oftmals miteinander verbunden. Ein Virus lässt sich über den USB-Stick bei einem Serviceeinsatz eines Mitarbeiters an einem Medizinprodukt auf das IT-Netzwerk übertragen (siehe Risiko Unsichere Einbindung aktiver Medizinprodukte in IT-Netze).

## EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG:

- Regelmäßige Personalschulungen zu Datenschutz, bei denen auf die Dringlichkeit von Passwortverschlüsselung hingewiesen wird (bereits das Ermöglichen eines unberechtigten Zugriffs auf Daten ist ein Datenschutzverstoß).
- Jedes Netzwerk benötigt autorisierte Personen, die die Netzwerkadministration durchführen. Der Zugang dafür muss limitiert und mit speziellen Passwörtern, sowie Sicherheitsstufen geschützt sein.
- Regelmäßige Updates von Softwares und Firewalls, um die Sicherheitsbarrieren Ihres IT-Netzes immer auf dem aktuellen Stand zu halten.
- Eintrittspforten wie z.B. USB-Anschlüsse an Computerarbeitsplätzen sperren. Speichermedien werden vorab an einem gesicherten PC auf Viren überprüft.
- Sicherung der Verbindung zwischen Medizinprodukten und IT-Netz mittels zusätzlicher Virensoftware und Sperren der externen Zugänge von Medizinprodukten bzw. Freigabe der Zugänge erst nach Überprüfung externer Speichermedien.
- Inanspruchnahme von (externer) Expertise für die Sicherung des IT-Netzes aufgrund der sehr dynamischen Entwicklung auf dem Gebiet der IT-Sicherheit.
- Angriffe bzw. Schäden nicht verbergen sondern kommunizieren (melden), damit andere daraus lernen und rechtzeitig reagieren können (Meldesystem).

## WEITERFÜHRENDE LITERATUR:


Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2014;111(21):A963-72, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=160315

Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Technische Anlage, Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2008;105(19):A1026-30, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=60114

Bundeszahnärztekammer, Kassenzahnärztliche Bundesvereinigung (Hrsg.): Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV, April 2018 Im Internet: https://www.bzaek.de/fileadmin/PDFs/za/datenschutzleitfaden.pdf

Deutscher Ärztetag 2017, Beschlussprotokoll, TOP II „Digitalisierung im Gesundheitswesen", S. 246-300, Im Internet: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/120.DAET/Beschlussprotokoll_120_DAET.pdf

Krüger-Brandt H: Cybersicherheit als Herausforderung, Deutsches Ärzteblatt 2016;113(9):A364-9, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=175147

# Risiko ▶ Unzureichender Schutz des IT-Netzes vor unberechtigten Zugriffen

**THEMATISCHER EINSTIEG:**

In Praxen oder Krankenhäusern kommt es immer wieder dazu, dass ungewollt fremde Personen Zugriff auf sensible Informationen erlangen. Dies geschieht z.B. durch Gespräche in Hörweite von Patienten (Aufzüge, Kantine etc.) aber zunehmend auch durch nicht richtig gesicherte IT-Strukturen.

**PRAKTISCHES BEISPIEL:**

In einer Hausarztpraxis dient ein zentraler PC, in den Patientendaten aufgenommen werden, als Informationsquelle. Der PC ist seitlich von Patienten einsehbar. Ein Bildschirmschoner ist nicht installiert und so von Besuchern einsehbar. Ein wartender Patient erkennt so zufällig den Namen seines Kollegen, der oft krank am Arbeitsplatz gemeldet war. Den begründeten Krankheitsgrund teilt er seinen Kollegen mit.

**AUSGANGSLAGE:**

Auf PCs fehlen oftmals Passwörter und Bildschirmschoner, welche es verhindern auf geöffnete Daten direkte Einsicht zu nehmen. PCs stehen in Behandlungsräumen oftmals unverschlüsselt zur Verfügung. Durch nicht räumlich getrennte Wartebereiche und Behandlungsräume sind Personen oftmals eine längere Zeit unbeaufsichtigt im Behandlungsraum. Lange Wartezeit, Neugier, Langeweile, Informationsbedürfnis von Patienten/Angehörigen/Dritten (z.B. Rettungsdienst) können zu unberechtigtem Zugriff führen. Aus platzsparenden Gründen sind PC-Monitore oftmals in unmittelbarer Blickrichtung der Patienten angebracht und ermöglichen somit eine direkte Einsicht. Durch eine unzureichende räumliche Trennung von PC-Arbeitsplätzen und Publikumsverkehr (z.B. Visitenwagen offen auf dem Flur), kann die Einsicht unbefugter Personen in sensible Daten gefördert werden.

**RISIKEN:**

- Sensible Patientendaten sind nicht geschützt und können an externe Personen verbreitet werden. (Datenschutz)
- Daten (z.B. Anordnungen etc.) können manipuliert werden und somit eine direkte Gefährdung des Patienten bedeuten.

**AUSWIRKUNGEN:**

Gelangen patientenrelevante Informationen unberechtigt an Dritte, können diese die Information nutzen, um am Arbeitsplatz, im privaten Umfeld oder auch bei Vertragsabschlüssen von Versicherungen die betroffenen Menschen zu benachteiligen, zu stigmatisieren und ihre Persönlichkeitsrechte zu verletzen.

**MÖGLICHE URSACHEN:**

- Der Faktor Zeit wird als häufige Ursache benannt. Das ständige Anmelden wird als zeitraubend und im Alltag als nicht umsetzbar empfunden.
- Häufig wechselndes Personal (z.B. Schichtwechsel, Teilzeitarbeit) führt dazu, dass nicht jeder ein eigenes Benutzerkonto hat. Um dem Personal trotzdem durchgängig den Zugriff zu ermöglichen, werden die PCs nicht passwortgeschützt.
- Mitarbeitern fehlt oftmals die nötige Sensibilisierung/Compliance. Ihnen ist teils nicht bewusst, welche Auswirkungen eine Vernachlässigung der IT-Sicherheit haben kann.

**EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG:**

- Regelmäßig Personalschulungen zu Datenschutz, bei der auf die Dringlichkeit von Passwortverschlüsselung hingewiesen wird (bereits das Ermöglichen eines unberechtigten Zugriffs auf Daten ist ein Datenschutzverstoß).
- Richtiges Einrichten der Computerarbeitsplätze in einsehbaren Bereichen, z.B. mittels Sichtschutzfolien.
- Bestimmte Funktionen des IT-Netzes mit speziellen Zugangsberechtigungen versehen, damit der Personenkreis mit Möglichkeit zum Datenzugriff möglichst klein gehalten wird.
- Einrichten von Kennwörtern zur Sicherung von IT-Netzen. Kennwörter sind jedoch nur dann hilfreich, wenn diese regelmäßig gepflegt/aktualisiert werden und Kennwörter nicht schriftlich am Arbeitsplatz hinterlegt werden.
- Verwenden von Transpondersystemen/biometrischen Datenprofilen zur Verschlüsselung von IT-Netzen, um Arbeitsplätze zu sichern aber gleichzeitig einen schnellen Zugriff auf das Netzwerk zu gewährleisten

## WEITERFÜHRENDE LITERATUR:

Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2014;111(21):A963-72, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=160315

Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Technische Anlage, Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2008;105(19):A1026-30, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=60114

Bundeszahnärztekammer, Kassenzahnärztliche Bundesvereinigung (Hrsg.): Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV, April 2018 Im Internet: https://www.bzaek.de/fileadmin/PDFs/za/datenschutzleitfaden.pdf

Deutscher Ärztetag 2017, Beschlussprotokoll, TOP II „Digitalisierung im Gesundheitswesen", S. 246-300, Im Internet: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/120.DAET/Beschlussprotokoll_120_DAET.pdf

Krüger-Brandt H: Cybersicherheit als Herausforderung, Deutsches Ärzteblatt 2016;113(9):A364-9, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=175147

# Risiko ▶ Risiko Nichtverfügbarkeit von IT-Infrastruktur/Patientendaten

**THEMATISCHER EINSTIEG:**

Die Anwendung von IT-Infrastruktur ermöglicht den schnellen und verlustarmen Austausch von Daten zur Patientenversorgung bei Reduzierung des räumlichen Bedarfs für Archivierung und somit eine effektivere und schnellere Behandlung. Elektronische Patientenakten und digital verfügbare Bildgebung ermöglichen die gleichzeitige Verfügbarkeit an verschiedenen Orten und durch Schaffung von Backups, die Datensicherung zu verbessern.

**PRAKTISCHES BEISPIEL:**

Aufgrund des Ausfalls eines Servers kann in einem Medizinischen Versorgungszentrum (MVZ) nicht mehr auf die Patientendaten zugegriffen werden. Gleichzeitig können eintreffende Befunde nicht mehr in der digitalen Patientenakte abgespeichert werden. Weiterführende medizinische Leistungen sind ohne Rückgriff auf Patientendaten ggf. nicht erbringbar. Die noch erbringbaren Leistungen werden auf Papier dokumentiert, um diese nachträglich in die digitalen Patientenakten einzupflegen. Die Leistungsfähigkeit des gesamten MVZ ist auf ein Minimum reduziert, die meisten Termine werden abgesagt, da auf die digitale Terminvergabe ebenfalls nicht zugegriffen werden kann. Anfragen einer Notaufnahme des nahegelegenen Krankenhauses zur Anamnese eines zuvor im MVZ behandelten Patienten können nur unzureichend beantwortet werden. Die zuständige IT-Firma ist zunächst über Stunden telefonisch nicht erreichbar und bietet nach Erreichen eine Reparatur Anfang übernächster Woche an, da ein entsprechend zu konfigurierender Ersatz-Server nicht früher zur Verfügung stünde. Auf die Frage nach einem Notfallplan für diese Situation blicken sowohl der Geschäftsführer des MVZ als auch die Mitarbeiter nur in fragende Gesichter.

**AUSGANGSLAGE:**

Die Patientenversorgung ist in allen Sektoren und Professionen zunehmend von IT-Infrastruktur abhängig. So wird vielerorts die Anamnese mit digitaler Aufzeichnung erhoben, Diagnostik wie beispielsweise Bildgebung erfolgt durch IT-Systeme bzw. wird über diese versandt, einzelnen Patientenakten zugeordnet und dort abrufbar abgelegt. Ebenso werden therapeutische Maßnahmen jedweder Art zunehmend elektronisch dokumentiert und IT-Systeme zur Informationsweitergabe an

weiterbehandelnde Akteure beispielsweise durch Arztbriefe oder Rezepte genutzt. Dies kann im Normalbetrieb ressourcenschonend gegenüber einer reinen papierbasierten Dokumentation sein und die Datenqualität erhöhen (z.B. bessere Lesbarkeit von Anordnungen). Bei Verlust der IT-Infrastruktur fallen jedoch einerseits diagnostische und therapeutische Optionen in der Patientenbehandlung ggf. kurzfristig aus, andererseits kann auf bisher erhobene Patientendaten ggf. nicht mehr zurückgegriffen werden. Die Überbrückung eines Ausfalls durch Vorhaltung papiergebundener Verfahren der Behandlungsdokumentation ist individuell sehr unterschiedlich geregelt und ermöglicht je nach Umfang und zeitlichem Verzug ggf. eine verlustarme Weiterbehandlung des Patienten, bringt jedoch neue Probleme mit sich. Während bestimmte elektive Maßnahmen ggf. bis zur Wiederherstellung der Verfügbarkeit des IT-Systems verschoben werden können, stellt der Informationsverlust insbesondere bei Behandlungsnotwendigkeit ein enormes Sicherheitsrisiko dar: Auf eigentlich verfügbares Vorwissen (z.B. Vorerkrankungen, Vormedikation oder bekannte Allergien oder Medikamentenunverträglichkeiten) kann nicht zurückgegriffen werden, insbesondere bei kritisch erkrankten, gebrechlichen und/oder polymorbiden Patienten kann häufig auch durch Rückfragen dieses Defizit nicht kompensiert werden. Somit kann die ggf. notwendig einzuleitende Behandlung im Widerspruch zur bisherigen Therapie stehen. Ebenso ist der Wegfall IT-basierter Diagnostik und Therapie für akut behandlungsbedürftige Patienten mit deutlichen Risiken verbunden, da ggf. eine Verlegung des Patienten in eine andere Einrichtung notwendig wird.

**RISIKEN:**

- Wegfall der diagnostischen und therapeutischen Möglichkeiten einer Einrichtung.
- fehlende Möglichkeit, vorhandene relevante Gesundheitsinformationen des Patienten abzurufen und ggf. weiterzugeben.
- Wegfall des Wissens über die organisatorischen Abläufe.
- Einschränkung bzw. erhebliche Verzögerung der internen und externen Kommunikation
- Offline-Bearbeitung der Daten mit Übertragungsverlusten bei Wiederherstellung der IT-Verfügbarkeit (Informationsverlust).

**AUSWIRKUNGEN**:

Durch den Wegfall bestimmter diagnostischer und therapeutischer Möglichkeiten und/oder des Zugriffs auf relevante Gesundheitsinformationen kann es zu einer relevanten Behandlungsverzögerung kommen, die vor allem bei akut behandlungsbedürftigen Zuständen zu relevanter Schädigung des Patienten führen kann, beispielsweise durch

- Wechselwirkung neuer Medikamente mit bisheriger (jetzt unbekannter) Medikation
- Abbruch der Versorgungskontinuität durch unfreiwilliges Beenden der bisherigen Therapie oder unzureichende Therapieüberwachung
- Ausfall therapeutischer Systeme während einer Intervention
- unnötige Belastungen durch Doppeluntersuchungen
- notwendige Verlegung/Überweisung nach extern
- Fehler bei der manuellen Nachdokumentation nach Wiederherstellung der Funktionalität des IT-Systems

Es entsteht ein hoher Aufwand für kompensatorische Maßnahmen, bis hin zur persönlichen Einzelüberwachung von Patienten bei Ausfall einer Überwachungsanlage. Aus dieser akuten Überlastung können weitere Schäden durch eine erhöhte allgemeine Fehlerrate resultieren. Ausfälle zu Beginn der Versorgungskette können als Domino-Effekt nachbehandelnde Stellen mit betreffen. Die Leistungsfähigkeit der Organisation wird erheblich eingeschränkt und kann in Teilbereichen zum Erliegen kommen, die Reputationsschäden können beträchtlich sein.

**MÖGLICHE URSACHEN:**

- Unzureichende Sensibilität bezüglich Ausfallkonzepten und notwendigen Redundanzen, insbesondere in mutmaßlich „unkritischen" Bereichen außerhalb der Notfallversorgung.
- Hoher Innovationsdruck ohne ausreichende Validierung und Testung vor Inbetriebnahme im jeweiligen zunehmend komplexer werdenden IT-Gesamtsystem.
- Fehlende Ausfallkonzepte zur schnellen Behebung einer Betriebsunterbrechung des IT-Systems.
- Fehlende Sensibilisierung und Schulung des betroffenen Personals zum Verhalten bei IT-Ausfall zur Verhinderung von Dokumentationsfehlern während des Ausfalls.

- Unzureichende personelle und materielle Ressourcen zum Schutz des IT-Systems vor Störung bzw. Ausfall.
- Fehlende Vorhaltung redundanter Systeme (vorkonfiguriertes Ersatzsystem).

**EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG:**

- Sensibilisierung der Führungskräfte bezüglich der Notwendigkeit individueller Ausfallkonzepte (Service Level Agreements) und Redundanzen auf Basis einer individuellen Risikoanalyse der vorhandenen IT-Infrastruktur in Abhängigkeit der Tätigkeit der Organisation
- Erstellung einer individuellen Risikoanalyse zur Einschätzung der jeweiligen Auswirkung von Ausfallszenarien und Ableitung individueller Präventionsmaßnahmen bereits vor Beschaffung des Produktes
- Erstellung von Notfallplänen zur Absicherung im „worst case" ggf. durch erhöhten Personaleinsatz, analoge Verfahren (z.B. mit Papier und Bleistift) und Krisenkommunikation, damit unter strikter Priorisierung die wichtigsten Funktionen aufrechterhalten und Patientensicherheitsrisiken minimiert werden
- Vorhaltung redundanter und kompatibler Systeme, die als notwendig erachtet werden, unter Einbeziehung von Versorgungsstrukturen wie Kommunikationstechnik, Energieversorgung, Medikamentenversorgung und Entsorgung
- Trennung von Netzwerken mit kritischen Funktionen (lebenserhaltende Funktionen) von anderen IT-Komponenten zur Minimierung des Ausfallrisikos bei einer Störung anderer Subsysteme
- Einbindung des Szenarios IT-Ausfall in bestehende Notfall- und Krisenkonzepte, sofern vorhanden (z.B. Krankenhauseinsatzplan, QM-System etc.)
- Angemessene und ggf. wiederholte Schulung der Notfallszenarien damit das Ausfallkonzept im Notfall bekannt ist und greifen kann, dabei aber Konzentration auf das Allerwichtigste (siehe Risiko Unzureichende Digitale Kompetenz der therapeutischen Teams)

**WEITERFÜHRENDE LITERATUR:**

Austrian Standards (Hrsg.): ONR 49002-3:2014. Risikomanagement für Organisationen und Systeme - Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement - Umsetzung von ISO 31000 in die Praxis

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-1: Managementsysteme für Informationssicherheit

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-4: Notfallmanagement

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden, 2013

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Management-Kurzfassung, 2013,

Deutsches Institut für Normung (Hrsg.): DIN ISO/IEC 27001:2017. IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen

# Risiko ▶ Überlassung von Daten an externe Dienstleister (z.B. Cloud)

**THEMATISCHER EINSTIEG:**

Cloud-Computing ist ein verbreitetes Anwendungsgebiet der Digitalisierung im Gesundheitswesen. Bei der Nutzung dieser IT-Services überlassen die Leistungserbringer ihre Daten Dritten (Cloud-Computing-Anbietern) zur Verarbeitung und Speicherung außerhalb ihres direkten Einflussbereichs. Leistungserbringer können so ihre Prozesse rationalisieren, optimieren und neue Services für Ihre Patienten anbieten (z.B. Terminvereinbarungen, elektronische Gesundheitsakte).

**PRAKTISCHES BEISPIEL:**

Ein Krankenhausträger überträgt Patientendaten aus dem OP an einen externen Anbieter. Grund dafür ist, dass der IT-Provider eine Sprache-zu-Text Kommunikationslösung mithilfe eines kommerziellen digitalen Assistenten zur Nutzung im OP anbietet. Das Grundkonzept ist, dass Sprache mittels Mikrofon aufgezeichnet wird, eine Umwandlung in Text mittels digitalem Assistenten durchgeführt wird – die Daten werden auf externen Rechnern analysiert und gespeichert – und der resultierende Text entweder zur Sprachsteuerung von OP-Geräten (im Sinne einer gesteigerten Hygiene, da keine Berührung notwendig ist) oder zur direkten und zeitnahen Dokumentation der Operation genutzt wird.

Ein Krankenhausträger entscheidet sich, das angebotene System zu nutzen. Nach einigen Monaten Testlauf finden sich plötzlich OP-Diktate des Trägers in diversen Hacker-Foren des Darknets wieder; es wäre auch ein Erpressungsversuch ähnlich wie dem Fall von Ransomware-Attacken denkbar – somit wäre der Leistungserbringer doppelt bedroht/geschädigt. Oben genanntes System wird sofort außer Betrieb gestellt. Die nachfolgende Recherche zeigt einen Bug in der Verschlüsselung der Datenübertragungskette zwischen der OP-Software und dem digitalen Assistenten. Ein Sammelprozess geschädigter Patienten gegen den Krankenhausträger ist absehbar, ebenso ist ein nachhaltiger Imageschaden denkbar.

**AUSGANGSLAGE:**

Beim Cloud-Computing werden sensible Daten außerhalb des Betriebes (Krankenhaus, Praxis) versandt und aufbewahrt. Vorteile von Cloud-Lösungen bzw. Auslagerung von IT-Infrastruktur sind sicherlich einerseits die Möglichkeit, sich auf

das Kerngeschäft zu konzentrieren, bei Cloud-Lösungen insbesondere auch die räumlich nahezu uneingeschränkte Verfügbarkeit der entsprechenden Services.

Bei der Nutzung von IT-Unterstützung betrieblicher Prozesse werden üblicherweise drei Ebenen unterschieden. Die Nutzung der Cloud bietet grundsätzlich Vorteile auf allen drei Ebenen, im Folgenden mit zunehmendem Ausmaß des Servicegrades durch den Cloud-Provider gelistet:

- **Infrastruktur** (infrastructure as a service): Lediglich die Hardware (Server, Netz) wird gewartet, der Benutzer ist für die Wartung des Betriebssystems und der Software zuständig.
- **Plattform** (platform as a service): Zusätzlich zur Hardware wird auch das Betriebssystem gewartet.
- **Software** (software as a service): Zusätzlich zur Hardware und zum Betriebssystem, auf dem die Software läuft, wird auch diese selbst vom Cloud-Provider gewartet.

Insbesondere für kleinere Organisationen oder einzelne Professionals, wie beispielsweise niedergelassene Ärzte oder Psychotherapeuten in Einzelpraxen, erscheint der Betrieb eines eigenen IT-Departments nicht kosteneffizient und daher die Auslagerung bestimmter IT-Leistungen an eDienstleister interessant. Dadurch ist Konzentration auf das Kerngeschäft möglich. Den möglichen Vorteilen stehen allerdings Nachteile gegenüber.

**RISIKEN:**

- Datenverlust: Untersuchungsergebnisse stehen z.B. nicht mehr zur Verfügung. Dokumentationspflichten werden verletzt, Patienten erfahren redundante Diagnostik. Behandlungen können aufgrund mangelhafter Informationsbasis für die Behandler u.U. nicht mehr zeitgerecht erfolgen.
- Datenmissbrauch: Sensible und wertvolle Daten geraten in die "falschen Hände". Erpressungsversuche der Datenhalter oder Kommerzialisierung der Daten. Es erfolgt Publikation der Daten.
- Datenmanipulation: Social Engineering (z.B. Vorspiegelung von Identität, der Chef benötige Daten, Schaden für den Patienten, Kosten).
- Kann in der Cloud nicht mehr gespeichert werden, wird eine weitere Tätigkeit, z.B. Archivierung nicht mehr möglich und führt u.U. innerhalb von Stunden zum „System-Kollaps".

**AUSWIRKUNGEN:**

- **Gesundheitliche Schädigung**: Aufgrund Nichtverfügbarkeit von Daten wird beispielsweise eine bekannte Medikamentenunverträglichkeit nicht beachtet, der Pat. erleidet einen anaphylaktischen Schock und wird intensivpflichtig.
- **Soziale Stigmatisierung und Diskriminierung**: Wenn sensible Patientendaten einer breiten Öffentlichkeit zugänglich werden, besteht die reale Möglichkeit der sozialen Stigmatisierung einzelner Menschen oder Gruppen. Beispielsweise könnte Menschen mit chronischen oder infektiösen Erkrankungen der Zugang zum Arbeitsmarkt real erschwert werden.
- **Kosten**: Aufgrund primär nicht verfügbarer oder verloren gegangener Daten könnte die erneute Durchführung (evtl. invasiver) diagnostischer Verfahren nötig werden. Dies verursacht gegebenenfalls für Träger und Patienten Zusatzkosten. Im Falle einer Schädigung des Patienten können Schadensersatzforderungen drohen.
- Verletzung der **Patienten-Autonomie**: Eine immaterielle Schädigung von Patienten liegt vor, falls Daten ohne Wissen und Zustimmung von Patienten bei Externen verarbeitet werden.

**MÖGLICHE URSACHEN:**

- **Kostendruck**: Garantien der sicheren Anwendung erfordern Aufwände. Rendite-orientierte Anwender im Wettbewerb stehen unter Kostendruck der zur Aufweichung von notwendigen Standards führen kann.
- **Verantwortungsdiffusion**: Die Cloud-Service-Architektur kann die Gefahr erhöhen, dass die Verantwortung bei einem schwächeren Glied in der Kommunikationskette erhöht wird und den Eintritt eines Schadensfalls strukturell mit der Zeit wahrscheinlicher macht.
- **Unzureichende Performance**: Die Leistungsfähigkeit und rechtliche Absicherung von Angeboten kann ungenügend sein. Anbieter versprechen möglicherweise mehr als sie halten können.
- **Sabotage bzw. kriminelle Aktivitä**t: Daten des Gesundheitswesens sind ihrer Natur nach sensibel und damit ein potentiell relevantes Ziel für Angriffe Cyberkrimineller.
- **Umwelteinflüsse**: unter Umständen könne extreme Wetterbedingungen z.B. Blitzschlag oder Überschwemmung zum Ausfall bzw. zur Fehlfunktion von Systemen führen.

- **Wirtschaftliche Interessen im Graubereich bzw. im Nachhinein legalisiert**: Nutzung von im Routinebetrieb erhobenen Daten im Sinne unternehmerischer Aktivität ohne entsprechendes Ethikvotum.
- **Ausmaß der digitalen Kompetenz bei Gesundheitsfachpersonen**: Externe Verarbeitung von Patientendaten bergen erhebliche technische und rechtliche Implikationen, die nicht immer korrekt eingeschätzt werden können (siehe Risiko Unzureichende Digitale Kompetenz der therapeutischen Teams).

**EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG:**

- Garantien: Anbieter von Cloud-Lösungen gehen vertraglich abgesicherte, klar garantierte Verpflichtungen ein. Anzumerken ist hier, dass die Letztverantwortung dem Patienten gegenüber nach wie vor beim medizinischen Leistungserbringer liegt.
- Standards: Einschlägige Standards und gesetzliche Vorgaben sind zu beachten. Umsetzung von Datenschutz-Standards und Standards der Daten-Ethik (Gute Praxis).
- Reporting: öffentliche Dokumentation der Verfahren, Nachweis z.B. in Qualitätsberichten.
- Reversibilität der Speicherung in der Cloud: Das Konzept der ePrivacy steht dafür, dass ein „Konsens" hinsichtlich der Speicherung, Nutzung und Weiterverarbeitung der Daten der Betroffenen vorliegen muss, dem die verschiedenen Parteien zustimmen müssen, und der auch wieder rückgängig gemacht werden kann. Empfehlenswert ist, einen Anbieter auszuwählen, der es ermöglicht, Daten wieder lokal verfügbar zu machen und sämtliche in der Cloud durchgeführten Speicherungen, Verarbeitungen und Weitergaben zu dokumentieren und rückgängig zu machen.
- Digitale Kompetenzen stärken: Ausbau der digital health literacy von therapeutischen Teams, Organisationen aber auch PatientInnen (siehe APS-Checkliste für die Nutzung von Gesundheits-Apps).
- Anwendung und Umsetzung der europäischen Datenschutzgrundverordnung

**WEITERFÜHRENDE LITERATUR:**

eHealth Swiss (Hrsg.): Strategie eHealth Schweiz 2.0 (Entwurf vom 5.September 2017). OID: 2.16.756.5.30.1.127.1.1.5.1.1, Im Internet: https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/170911_Entwurf_Strategie_eHealth_2.0_d.pdf

Europäische Kommission: Shaping the Digital Single Market, im Internet: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

KMA Online: Amazon will mit Expertenteam in digitale Gesundheitswirtschaft, Im Internet: https://www.kma-online.de/aktuelles/it-digital-health/detail/amazon-will-mit-expertenteam-in-digitale-gesundheitswirtschaft-a-35414

Mertz M*, Jannes M*, Schlomann A*, Manderscheid E, Rietz C[t] , Woopen C[t] (2016) Digitale Selbstbestimmung. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Köln.

Vollmar HC, Kramer U, Müller H, Griemmert M, Noelle G, Schrappe M.: Digitale Gesundheitsanwendungen – Rahmenbedingungen zur Nutzung in Versorgung, Strukturentwicklung und Wissenschaft. Positionspapier der AG Digital Health des Deutschen Netzwerks Versorgungsforschung e.V. (DNVF), Das Gesundheitswesen, 2017;79(12):1080-92

# Risiko ▶ Unsichere Einbindung aktiver Medizinprodukte in IT-Netze

**THEMATISCHER EINSTIEG:**

Medizinprodukte sind Produkte mit medizinischer Zweckbestimmung, die vom Hersteller für die Anwendung beim Menschen bestimmt sind. Zu den Medizinprodukten gehören z.B. Röntgengeräte, ärztliche Instrumente oder auch medizinische Software. Die Einbindung von Medizinprodukten in IT-Netze ist abhängig von inneren und äußeren Einflüssen, die von IT-Netzwerken und eigener Software beeinflusst werden.

Zunehmend werden auch Apps als Medizinprodukte zugelassen und interagieren mit IT-Netzen (Medical Apps). > siehe auch APS-Checkliste für die Nutzung von Gesundheits-Apps.

**PRAKTISCHE BEISPIELE:**

1. Beispiel:
In einer Gesundheitseinrichtung wurden zur besseren Praxisorganisation die bildgebenden Systeme (Röntgen, Ultraschall, Endoskopie, OP-Kameras etc.) in ein Netzwerk eingebunden, sodass die damit erzeugten Daten in jedem Behandlungszimmer und auch anderen „Behandlern" (oder Praxen etc.) zur Verfügung stehen. Während einer radiologischen Untersuchung friert die Bildschirmdarstellung ein. Durch einen Neustart gehen die bisherigen Untersuchungsverläufe verloren. Das neuwertige Röntgengerät lässt sich aufgrund eines Virusbefalls bei veraltetem Betriebssystem trotz Vollwartungsvertrag nicht mehr starten. Der Patient muss in eine andere Einrichtung verlegt werden, da auch die Ausweichanlage nicht funktioniert. Die gesamte digitale Infrastruktur ist betroffen.

2.Beispiel:
Ein Patient verstirbt unbemerkt in einem Überwachungsbereich, da eine Alarmierung über die zentrale Überwachungsanlage der Station nicht erfolgte und dementsprechend nicht rechtzeitig eingegriffen werden konnte. Die Alarmweiterleitung auf ein Mobiltelefon wurde ebenfalls nicht ausgelöst.

**AUSGANGSLAGE:**

**Medizinprodukterecht**: Hersteller medizintechnischer Systeme sind stark an regulatorische Auflagen gebunden und müssen in aufwendigen Verfahren die Sicherheit Ihrer Systeme nachweisen. Bei jeder Systemveränderung muss diese

Prüfung wiederholt werden. Daher kann nicht zeitnah auf Bedrohungen reagiert werden. Selbst eine vertragliche Vereinbarung stellt keinen Schutz dar.

**Miteinander verbundene Medizinprodukte**: Bilden Medizinprodukte und Computer/Netzwerk eine Einheit, so unterliegen sie gemeinsam dem Medizinproduktegesetz. Veränderungen an dieser Einheit dürfen nicht ohne weiteres vorgenommen werden. Dies steht üblichen Wartungsprozeduren (Einspielen Sicherheitsupdates, Firewalls, Virenscanner etc.) entgegen.

Eine steigende Komplexität von IT-Netzwerken durch Einbindung von Medizinprodukten in klinische IT- Netzwerke stellt aufgrund der Besonderheiten in der Administration von medizintechnischen Geräten und Medizinprodukte-Software höhere Anforderungen.

Gleichzeitig kann die Einbindung von Medizinprodukten (z.B. zu Überwachungszwecken) ein verändertes Gefühl von Sicherheit vermitteln und so zu fehlgeleiteter Aufmerksamkeit führen.

**RISIKEN:**

- Wechselwirkungen und Inkompatibilitäten zwischen Software, Hardware und Netzwerk bis hin zum Teil- oder Komplettausfall des Systems.
- Beeinträchtigungen durch äußere Störeinflüsse.

**AUSWIRKUNGEN:**

- Die Risiken für Patienten reichen von Fehldiagnosen bis hin zu körperlichen Schädigungen, wenn steuernde Funktionen von Medizingeräten betroffen werden.
- Wenn Daten fehlerhaft gespeichert, weitergeleitet, ausgewertet oder angezeigt werden, kann es zu Fehlentscheidungen bei der Behandlung und/oder zum Schaden der Patienten führen.

**MÖGLICHE URSACHEN:**

- Entwicklungszyklen und Zertifizierungsverfahren für Medizinprodukte dauern wesentlich länger als bei IT-Software und erlauben daher keine zeitnahe Reaktion auf Bedrohungen.
- Validierung von Firewalls durch den Medizintechnikhersteller erfolgen zeitversetzt und können daher nicht tagesaktuell auf Bedrohungen reagieren.

- Ein Vollservicevertrag wiegt den Betreiber von Medizintechnik in einer vermeintlichen Sicherheit.
- Servicetechniker können mit befallenen USB Sticks oder Servicerechnern zur Verbreitung von Schadsoftware beitragen (siehe Risiko Unzureichender Schutz des IT-Netzes vor unberechtigten Zugriffen).
- Software ist aufgrund der kurzen Entwicklungszyklen nicht fehlerfrei (Bugs). Geräte haben im laufenden Betrieb Fehlfunktionen und es gehen bei Neustart Daten verloren.
- Steuernde Software kann durch ständige Fehlererzeugung und Flags ausfallen. Diese Flags können von außen durch das Netzwerk/WLAN oder durch interne Software- oder Bauteilfehler Ausfälle hervorrufen.
- Zu großes Verlassen auf Technik (Technikgläubigkeit) und Unterschätzen der Wechselwirkungen zwischen Medizintechnik, Software und Hardware führt zu Sorglosigkeit (siehe Risiko Unzureichende Digitale Kompetenz der therapeutischen Teams).
- Einbeziehen kurzlebiger „Konsumerware" in Medizinprodukte-Kombinationen oder Verwendung unterschiedlicher Software-Versionen in einem System.
- Externe technische Einflüsse (Gewitter, elektromagnetische Störeinflüsse durch andere Geräte, Notstromschaltungen, Netzschwankungen, Handys, private Nutzung des IT-Systems).

**EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG:**

- Kontrolle aller USB Sticks mit aktueller Virensoftware vor Einsatz am Medizinprodukt.
- Wartung von medizintechnischen Geräten verantwortungsvoll planen. Für eine Wartung durch Externe sind immer auch gewisse Vorbereitungen in Absprache mit Techniker/Firma zu treffen.
- Bei der Beschaffung neuer Medizinprodukte Aspekte der Patientensicherheit mitbedenken (siehe APS-Handlungsempfehlung „Patientensicherheit durch Prävention medizinproduktassoziierter Risiken"). Medizinprodukte mit eigens entwickelten Betriebssystemen sind möglicherweise weniger angreifbar als solche, die auf weit verbreiteten Betriebssystemen laufen. Bei der Beschaffung von Medizinprodukten sollten sicherheitstechnische Aspekte der eigenen Infrastruktur Bestandteil der Anforderungsanalyse sein.

- Strikte Trennung von Medizingeräten und anderen Anwendungen auch in Netzwerken (z.B. durch andere, standardisierte WLAN Frequenzbänder, physisch getrenntes Alarmierungsnetzwerk etc.) als Schutz vor An- und Übergriffen.
- Kein Einsatz von kurzlebiger „Konsumerware" in Kombinationen mit sicherheitsrelevanter Medizintechnik. Die Zweckbestimmung des Herstellers muss unbedingt beachtet werden.
- Medizintechnische Netzwerke vom übrigen Netzwerk trennen, um Verwechselungen auszuschließen und die steigende Komplexität zu entzerren.
- Zonierung/Segmentierung von Netzwerken: Innerhalb einer Zone einen kompletten Satz vernetzter Notfallmedizingeräte vorhalten, in einer davon getrennten weiteren Zone einen zweiten Satz dieser Geräte. Bei Ausfall/Störung einer Zone bleibt eine Notfallversorgung mit geringerer Kapazität erhalten.
- Technik als unterstützendes Werkzeug für den Anwender sehen, die nicht von der Fürsorge- und Aufsichtspflicht gegenüber dem Patienten und Dritten entbindet (Technik ersetzt kein Personal).
- Sensibilisierung und Schulung von Anwendern (siehe Risiko Unzureichende Digitale Kompetenz der therapeutischen Teams).
- Medizinische Netzwerke auch bei Reparaturen oder bei Austausch nicht als Einzelkomponenten betrachten, sondern in ihrer Gesamtheit (einschließlich der vernetzungsbedingten Risiken) einer eigenen Risikobetrachtung unterziehen.
- Überprüfung der Softwareversion und der Grundkonfiguration von Geräten, insbesondere nach Reparaturen/Austausch (oft sind diese auf Werkseinstellungen zurückgesetzt).
- Anfordern einer Risikoanalyse durch den Hersteller oder IT-Partner, um auf mögliche Sicherheitslücken aufmerksam zu werden.
- Risikoanalysen, wie das Gerät vor Schaden aus dem eigenen Netz geschützt werden kann.
- Ändern von Standardpasswörtern für Administratorzugänge (siehe Risiko Unzureichender Schutz des IT-Netzes vor unberechtigten Zugriffen).
- Durchführen von Sicherheitsaudits oder Sicherheitstests durch Experten, um auf Sicherheitslücken aufmerksam zu werden.
- Notfallpläne auf die Besonderheiten von med. Netzwerken anpassen und bedarfsgerecht aktualisieren. (siehe Risiko Nichtverfügbarkeit von IT-Infrastruktur/Patientendaten).

## WEITERFÜHRENDE LITERATUR:

Bundesinstitut für Arzneimittel und Medizinprodukte: Empfehlung des BfArM, Risiken durch ungenügend abgesicherte WLAN-/Netzwerkschnittstellen bei Medizinprodukten, Referenz-Nr.: 3137/15, im Internet: https://www.bfarm.de/SharedDocs/Risikoinformationen/Medizinprodukte/DE/netzwerk_risiko.html

Deutsches Institut für Normung (Hrsg.): DIN EN 80001-2-1: Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten. Schritt-für-Schritt-Risikomanagement von medizinischen IT-Netzwerken. Praktische Anwendung und Beispiele,

RP Online: Riesiger internationaler Cyber-Angriff trifft britische Kliniken, 12. Mai 2017, im Internet: http://www.rp-online.de/panorama/ausland/wanna-cry-riesiger-internationaler-cyberangriff-trifft-britische-kliniken-aid-1.6816373

Scherschel FA: Gehackte Medizintechnik: FDA will mehr Sicherheit durchsetzen, 19.01.2016, https://heise.de/-3075367

Schwan B: Mehr Sicherheit für Implantate mit Funkschnittstelle, 6.11.2013, im Internet: https://heise.de/-1972146

Windeck C: WannaCry: Gewaltiger Schaden, geringer Erlös, 14.05.2017, im Internet: https://heise.de/-3713689

# Risiko ▶ Risiko Unzureichende Digitale Kompetenz der therapeutischen Teams

**THEMATISCHER EINSTIEG:**

Die Einführung digitaler Anwendungen und der Aufbau sowie die Benutzung von IT-Infrastrukturen führen dazu, dass therapeutische Teams sich oft unter hohem Zeitdruck mit neuen Anwendungen vertraut machen müssen. Dabei ist es im Alltag oft schwer – auch aufgrund der Vielzahl der neuen Anwendungen und dem unterschiedlich verteilten Wissen zum Umgang mit digitalen Produkten – alle Mitarbeiter eines therapeutischen Teams ausreichend zu schulen, um so die Sicherheit und den optimalen Einsatz der digitalen Anwendungen zu garantieren. Das kann dazu führen, dass Grundrechte von Patienten (z.B. Datenschutz) gefährdet werden oder wichtige digitale Anwendungen nicht ausreichend gegenüber Angriffen von außen geschützt sind. Unzureichende eigene digitale Kompetenz oder deren Überschätzung kann zu Patientengefährdungen führen. Kommt es tatsächlich zum Ausfall oder Fehleinsatz digitaler Produkte, fehlt zudem oft eine Strategie für das Krisenmanagement.

**PRAKTISCHE BEISPIELE:**

1. Beispiel:
Das Quartalsende und die Urlaubszeit stehen unmittelbar bevor. Die Patienten stehen ungeduldig vor der noch verschlossenen Praxis. Die Rechner werden hochgefahren. Der Systemstart dauert ungewöhnlich lange. Auf einige Komponenten kann nicht zugegriffen werden. Im Laufe des Morgens kommt der Kollege zum Dienst und stellt fest, dass der Virenscanner ausgeschaltet ist. Auf die Nachfrage eines Patienten, was das für den Schutz seiner persönlichen Daten bedeutet, kann ihm zunächst niemand Auskunft geben.

2. Beispiel:
Die geplante roboter-assistierte Operation droht abgesagt zu werden, da der eigentlich geplante und erfahrene Chirurg krankheitsbedingt ausfällt. Ein Kollege, welcher sich als digital kompetent einschätzt und diese Operation schon durchgeführt hat, bietet sich als Vertretung an. Während der Operation kommt es zu technischen Schwierigkeiten.

Aufgrund der mangelnden Erfahrung mit der Steuerungssoftware des Roboters und der Überschätzung der eigenen digitalen Kompetenz des Ersatzarztes kann die technische Störung nicht schnell genug behoben werden und dadurch tritt eine Patientenschädigung ein.

**AUSGANGSLAGE:**

Eine mangelnde Sensibilisierung bzw. fehlendes Wissen führt oft zu unzureichendem Schutz vor unberechtigtem Zugriff und zu unsachgemäßem Gebrauch von Informationstechnologie. Manche Bedrohungen der informationellen Selbstbestimmung der Patienten entstehen erst durch die zunehmende Digitalisierung und sind insofern nicht von vorneherein bekannt. Maßnahmen zum Datenschutz und zur Weiterbildung in Bezug auf digitale Kompetenzen werden als zusätzliche Belastungen wahrgenommen und vertraute Routine wird beibehalten. Gerade bei Arbeiten unter hohem Zeitdruck wird das Hauptaugenmerk auf den Patienten gerichtet und relevante Sicherheitsaspekte unter Umständen ignoriert.

Aber gerade liebgewonnene Routinen, mangelnde Selbsteinschätzung der Mitarbeitenden und veraltete Soft- und Hardware bergen erhebliche Risiken, und weil das Risikobewusstsein unzureichend ist, wird möglicherweise die IT-Verantwortung an das Umfeld abgegeben.

Insbesondere kleinere Organisationen sind häufig unzureichend vor Angriffen von außen geschützt, da der kleinere Personalschlüssel Aufgaben- und Kompetenzverteilung bzw. Spezialisierung erschwert.

**RISIKEN:**

- Therapeutische Teams sind nicht ausreichend in der Lage, Patienten angemessen über die Risiken von digitalen Anwendungen aufzuklären.
- Es fehlt Wissen über die Risiken von unzureichend abgesicherten IT-Infrastrukturen (z.B. Versenden von sensiblen Informationen über unverschlüsselte E-Mails).
- „Komplizierte“ Lösungen zum Absichern von IT-Infrastrukturen werden „einfachen“ digitalen Produkten vorgezogen, da das notwendige Wissen/Überblick über die erforderlichen Maßnahmen nicht vorhanden ist (Überreaktion).
- Fehleinschätzung vorhandener Systeme zur Entscheidungsunterstützung (Befundung/Diagnostik/Indikationsstellung) hinsichtlich ihrer Aussagekraft.

**AUSWIRKUNGEN:**

- Durch unzureichende digitale Kompetenz, auch mangelnde Einarbeitung in neue IT, finden Verzögerungen in der Behandlung statt, sodass durch den Zeitverzug Patientengefährdungen bis hin zum Tod des Patienten entstehen können.

- Fehldiagnosen durch Fehlinterpretation der Ergebnisses eines Entscheidungsunterstützungssystems.
- Verletzung der digitalen Selbstbestimmung bzw. von Grundrechten der Patienten.
- Sinnvolle digitale Anwendungen können im Gegenzug trotz Patientennutzen ggf. nicht eingesetzt werden.

**MÖGLICHE URSACHEN:**

- Fehlende Erfahrungswerte durch enorme Innovationsdynamik.
- Fehlendes allgemeines Risikobewusstsein bei digitalen Anwendungen, z.B. Unkritischer Umgang mit E-Mails, Anhängen.
- Fehlendes spezifisches Bewusstsein für die Veränderung von Risiken bei Umstellung auf innovative Technologien.
- Überschätzung der eigenen digitalen Kompetenz.
- Unbekümmertes Routineverhalten: „Das haben wir doch immer so gemacht.“.
- Individuelle, ungeregelte Verwendung von Software, Apps.
- Unangebrachter Einsatz von Social Media, z.B. Versand von Patientendaten per Messenger-Dienst.
- Vermischung von dienstlichen Anforderungen und geschätzten, privaten Tools/Geräten.
- Fehlende Passwörter, Bildschirmschoner, ungesicherte Schnittstellen, mangelnde Aufmerksamkeit und Sensibilität während des Einsatzes digitaler Anwendungen.
- Hoher Zeitdruck im Alltag mit der Konsequenz, dass „direkte Patientenversorgung“ höhere Priorität hat als Maßnahmen der IT-Sicherung.
- Unkenntnis hinsichtlich der Kompatibilität von verschiedenen digitalen Produkten und Systemen, die dann der IT-Sicherheit im Weg stehen.

**EMPFEHLUNGEN ZUR RISIKOMINIMIERUNG:**

**Teamkompetenz - Wissen gibt Sicherheit auf Leitungsebene:**

Verantwortung für Teamkompetenz und gesamte Organisation aktiv übernehmen.

- safety first – „Nicht alles was möglich ist, ist in Ordnung. Nicht alles, was in Ordnung ist, ist auch sinnvoll."
- Regelmäßige Schulungen, Einweisung von neuen Mitarbeitern, Benennen von Ansprechpartnern.
- Interne Regelungsrahmen schaffen; eindeutig, verbindlich kommunizieren; Aktualisierung sicherstellen.
- Kommunikation und Maßnahmen kontinuierlich prüfen.
- Kompetenzermittlung im Rahmen des Einstellungsverfahrens, im Rahmen von Mitarbeitergesprächen und ggfs. abgeleitetem Aufbau von notwendiger Kompetenz.

Für professionellen IT-Support sorgen.

- Verträge regelmäßig prüfen.
- Sichere Datenhaltung, effizienter Datenschutz – Verschlüsselung, Umgang mit privaten Mail-Accounts regeln, zentrale Löschbarkeit von Daten auf mobilen Geräten einrichten.
- Schadensbehebung - Wo erforderlich SLAs - Service Level Agreements abschließen.

**Teamkompetenz - Wissen gibt Sicherheit in der gesamten Organisation**

Griffige Indikatoren zur Beurteilung von Störungen und akutem Handlungsbedarf im Team verankern.

- Einfaches, zuverlässiges Alarmierungssystem nutzen.
- Whistleblower sind keine Störer, Blockierer oder Spaßbremsen.
- Richtige Beurteilung und Kommunikation von akuten Veränderungen im System.
- Aktuelle Rufnummern, auf die jeder im Team immer Zugriff hat.
- Nach Verhaltensmaßregeln arbeiten, die für jeden verbindlich sind.

- Regelmäßige Schulung zum Thema digitale Kompetenzen
- Sensibilisierung für den Umgang mit digitalen Anwendungen

**Einfache, konkrete Handlungsanweisungen und Maßnahmenpläne für den Schadensfall einführen.**

- Wie wird auf kritische Zustände des IT-Systems korrekt reagiert?
- Wer priorisiert im Ernstfall?

## WEITERFÜHRENDE LITERATUR:


Die Welt: System-Neustart am OP-Tisch, 11.04.2013, im Internet: https://www.welt.de/gesundheit/article160307851/System-Neustart-am-OP-Tisch.html?

Mertz M*, Jannes M*, Schlomann A*, Manderscheid E, Rietz C[1], Woopen C[1] (2016) Digitale Selbstbestimmung. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Köln.

Bundespsychotherapeutenkammer (2017) BPtK-Leitfaden für Internetprogramme im Praxisalltag. http://www.bptk.de/uploads/media/BPtK-Leitfaden_f%C3%BCr_Internetprogramme_im_Praxisalltag_01.pdf

# Selbstüberprüfung der IT-Sicherheit einer Gesundheitsorganisation

Ein Gerät oder eine Software heutiger Zeit besteht zu einem erheblichen Teil aus Standard-Komponenten bzw. Standard-Softwaremodulen, die ursprünglich nicht dazu entwickelt wurden, in hochverfügbaren und jederzeit fehlerfrei funktionierenden Systemen eingesetzt zu werden. Daher führen diese Standard-Komponenten eine Vielzahl an Schwachstellen, unerwünschten Seiteneffekten und Defekten mit sich.

Spezialisten in der Patientenversorgung müssen an dieser Stelle weniger Kenntnisse über Bedrohungsszenarien und -lagen in der IT besitzen, als sich den übergeordneten Blick auf die Schadensszenarien solcher Systeme aneignen, um einschätzen zu können, welches Risiko ein neues System für ihre Arbeit darstellt. Für die IT-sicherheitsrelevanten Betrachtungen sollten Sie sich allerdings der Unterstützung eines entsprechend qualifizierten internen oder externen IT-Spezialisten bedienen.

Wenn Sie als Mitglied eines therapeutischen Teams ein System, sei es ein Gerät oder eine Anwendung, an Ihrem Arbeitsplatz einführen oder verwenden (wollen), sollten Sie sich zunächst einen Überblick über die Bedeutung dieses Systems für Sie und Ihre Patienten verschaffen. Wesentliche Aspekte für die Entscheidung zur Nutzung eines neuen Systems sind die Abhängigkeit Ihrer Tätigkeit von diesem System, Herkunft und technische Unterstützung des einzusetzenden Systems und die Auswirkung von Fehlfunktionen bzw. Ausfällen des Systems auf Sie, Ihre Patienten und/oder Dritte.

Zur Einschätzung der Risikoausprägung werden Risiken wie im neben stehenden Bild üblicherweise in einer Risikomatrix grafisch dargestellt (Abb. 1). Im klinischen Risikomanagement sollte dabei immer auf den glaubhaft schlimmst möglichen Fall („credible worst case"), der sowohl Behandelnde als auch Patienten besonders schwer treffen kann, abgestellt werden. Dieser tritt zwar seltener ein als kleinere Routineprobleme, ist aber letztlich der eigentliche Grund für eine Risikoanalyse.

Die Bewertung der Risiken in einer Risikomatrix erfolgt in den Dimensionen Eintrittshäufigkeit bzw. Eintrittswahrscheinlichkeit und Auswirkung des Risikos anhand zuvor festgelegter Risikokriterien. Folgende Musterbeispiele in Anlehnung an das Risikomanagement-Regelwerk ONR 49002-2:2014 können für die eigene Risikobewertung als Anhaltspunkt dienen:

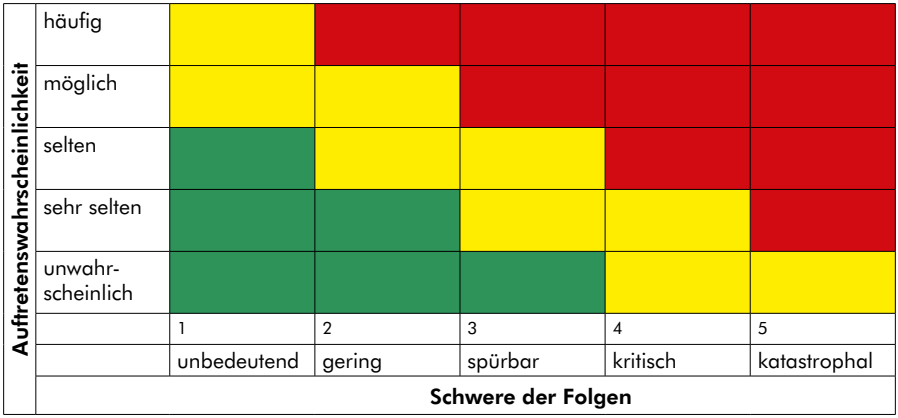


*Abb. 1: Risikomatrix*

| STUFE | HÄUFIGKEIT |
|---|---|
| häufig | einmal pro Monat oder häufiger |
| möglich | einmal pro Quartal |
| selten | einmal pro Jahr |
| sehr selten | einmal in 3 Jahren |
| unwahrscheinlich | weniger als einmal in 3 Jahren |

*Eintrittshäufigkeit, Tabelle A3 ONR 49002-2:2014*

| STUFE | PATIENT/ MITARBEITER | LEISTUNGS-FÄHIGKEIT |
|---|---|---|
| unbedeutend | Vorkommnis, jedoch ohne Folgen (critical incident, near miss) | Die Leistungsfähigkeit des Behandelnden bleibt unberührt. |
| gering | leichter Gesundheitsschaden mit vorübergehenden Beschwerden/Schmerzen, verlängerte Behandlungsdauer | Die Leistungsfähigkeit des Behandelnden bleibt unberührt, es entstehen kurzzeitige Störungen im Betriebsablauf und Mehrkosten. |
| spürbar | schwerer Gesundheitsschaden ohne Dauerfolgen, deutlich verlängerte Behandlungsdauer | Vorübergehende Minderung der Leistungsfähigkeit des Behandelnden, es entstehen Mehrkosten aus der Behandlung sowie aus den zusätzlichen Störungen der Prozesse. |
| kritisch | schwerer Gesundheitsschaden mit Dauerfolgen ohne dauerhafte Pflegebedürftigkeit jedoch mit Berufseinschränkung | Die Leistungsfähigkeit des Behandelnden wird dauerhaft beeinträchtigt. Das Leistungsangebot wird eingeschränkt. |
| katastrophal | schwerer Gesundheitsschaden mit Dauerfolgen und dauerhafter Pflegebedürftigkeit, Tod des Patienten/ Mitarbeiters | Die Fortführung der Betriebstätigkeit mit dem bisherigen Leistungsspektrum ist bedroht. |

*Auswirkung des Risikos, Modifizierte Tabelle A9, ONR 49002-2:2014*

Die Ergebnisse der Risikobewertung in der Risikomatrix müssen auf ihre Tragbarkeit hin bewertet und priorisiert werden, um entsprechende Maßnahmen in entsprechender zeitlicher Reihenfolge ableiten zu können.

# Fragenkatalog zur Selbstüberprüfung der IT-Sicherheit einer Gesundheitsorganisation

**1. Wie notwendig ist das einzusetzende System für Ihre Arbeit?**

- ☐ Das System stellt eine Ergänzung meines Wissens und meiner Fähigkeiten dar, d. h., die Qualität meiner Arbeit bleibt davon unberührt.
- ☐ Das System stellt eine Unterstützung meines Wissens und meiner Fähigkeiten dar, d. h., die Qualität meiner Arbeit wird durch den Einsatz dieses Systems gesteigert.
- ☐ Das System stellt eine notwendige Voraussetzung für den Einsatz meines Wissens und meiner Fähigkeiten dar, d. h., ohne das System kann ich meine Arbeit nicht (in der fachlich notwendigen/geforderten Qualität) erbringen.

Die Notwendigkeit des Systems sollte bei der Höhe des zu akzeptierenden Restrisikos einer Maßnahme berücksichtigt werden.

**2. CE-Zertifizierung, Herkunft, technische Unterstützung**

- ☐ Ist das System ein CE-zertifiziertes Medizinprodukt?
- ☐ Wenn nein: Stammt das IT-System von einer vertrauenswürdigen Quelle?
- ☐ Gibt es einen qualifizierten (technischen) Dienstleister, der Sie bei der Einrichtung und dem Betrieb des Systems unterstützen kann?
- ☐ Ist der Dienstleister während Ihrer Arbeits-/Servicezeiten erreichbar und kann auch außerhalb dieser Zeiten (z.B. am Wochenende) bei Ausfall oder Störung rechtzeitig für Sie tätig werden?

**3. Wie würde sich ein Totalausfall oder eine (IT-bedingte) Fehlfunktion des Systems auswirken auf...**

- ☐ die Qualität Ihrer Leistung und die Ihrer Mitarbeiter?
- ☐ die Verfügbarkeit Ihrer Leistung und die Ihrer Mitarbeiter?
- ☐ das Wohlergehen Ihrer Patienten, von Ihnen und Ihren Mitarbeitern?
- ☐ die Vertraulichkeit, Verfügbarkeit und Integrität Ihrer Patientendaten?
- ☐ die Vertraulichkeit, Verfügbarkeit und Integrität Ihrer Betriebsdaten?

# GLOSSAR

## Administrator

Betreuer eines Rechnersystems bzw. eines Netzwerks (z.B. eines Intranets) mit besonderen Zugriffsrechten. (Duden)

## App/Applikation

Der Begriff "App" ist eine Abkürzung und steht für "Applikation", übersetzt Anwendung. Dies sind verschiedene Programme z.B. zur Bildbearbeitung oder Nachrichtenversendung für mobile Geräte wie Smartphones und Tablets, die heruntergeladen und installiert werden können. (eigene Definition)

## Buffer Overflow

Werden einem Modul über eine Schnittstelle mehr Daten als erwartet übergeben, so kann es zu einem sogenannten "Buffer Overflow" kommen. Wenn das Modul nicht die Länge der übermittelten Daten prüft, werden die Daten über den vorgesehenen Bereich hinaus geschrieben und somit die Speicherstruktur (Heap oder Stack) zerstört. Durch geeignete Codierung der Daten kann zudem der Stack gezielt manipuliert werden, sodass die Ausführung schadhaften Codes möglich ist. (BSI)

## Bug

Umgangssprachliche Bezeichnung eines Programm- bzw. Softwarefehlers, der zu einem Fehlverhalten des IT-Systems führt. (eigene Definition)

## CE-Zertifizierung

Die CE-Zertifizierung von Medizinprodukten durch externe „Benannte Stellen“ ist eine Konformitätsbewertung mit den von Medizinprodukten zu erfüllenden rechtlichen Anforderungen der Europäischen Union. (eigene Definition)

## Cloud

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die im Rahmen von Cloud Computing angebotenen Dienstleistungen umfassen das komplette Spektrum der Informationstechnik und beinhalten Infrastrukturen (Rechenleistung, Speicherplatz), Plattformen und Software. (BSI)

## Computer-Virus

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.) (BSI)

## Darknet

Das Darknet ist ein loser Verbund von vielen privaten Computern, die als Netz untereinander verbunden sind und zwischen denen die Daten häufig verschlüsselt übertragen werden. Der Zugang zum Darknet erfolgt über spezielle Programme. Neben legalen Anwendungen, die Anonymität erfordern, nutzen viele Kriminelle die Anonymität des Darknet für illegale Aktivitäten, u.a. Erpressung von Lösegeldern mittels Ransomware. (eigene Definition)

## Datenschutzgrundverordnung

Verordnung der Europäischen Union zur Vereinheitlichung des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und zur Sicherstellung des freien Datenverkehrs im Europäischen Binnenmarkt, die ab 25. Mai 2018 anzuwenden ist. (eigene Definition)

## Fake E-Mail

Täuschend echt aussehende E-Mails unbekannter Dritter mit einem vertrauten Absender, die im Rahmen von Social Engineering Nutzerdaten für illegale Aktivitäten abschöpfen sollen. (eigene Definition)

## Firewall

Eine Firewall (besser als Sicherheitsgateway bezeichnet) ist ein System aus soft- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. (BSI)

## Flag/Fehlerflag

Bezeichnung für eine Markierung im IT-System, die auf einen bestimmten Status hinweist, beispielsweise einen Systemfehler. (eigene Definition).

## Internet of Things (IoT)

IoT steht für Internet of Thing. Dies sind im Gegensatz zu "klassischen" IT-Systemen "intelligente" Gegenstände, die zusätzliche "smarte" Funktionen enthalten. IoT-Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden. (BSI)

## IT-Sicherheitsaudit

Systematischer Prozess zur Überprüfung eines IT-Systems auf Schwachstellen und Risiken mit dem Ziel, Sicherheitslücken zu schließen und dadurch IT-Sicherheitsrisiken zu minimieren. (eigene Definition)

## IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways. (BSI)

## Konsumerware

Konsumerware bezeichnet Produkte, die für den Endverbraucher zur privaten Nutzung entwickelt wurden und keine erhöhten Sicherheitsanforderungen für den professionellen Gebrauch beinhalten. (eigene Definition)

## Messenger-Dienst

Software, die den Austausch von Nachrichten und ggf. auch Dateien verschiedender Formate zwischen einzelnen Nutzern oder Nutzergruppen ermöglicht (eigene Definition)

## ON-Regel (ONR)

ON-Regeln sind normative Dokumente des Austrian Standards Institute, die in ihrem Entwicklungsprozess nicht alle Anforderungen an eine klassische Norm erfüllen müssen. (Austrian Standards)

## Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern, und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch "ransom") wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung. (BSI)

## Risiko

Risiko im Kontext des Klinischen Risikomanagements ist eine Unsicherheit in der Versorgung von Patienten, die mit einer geschätzten Eintrittswahrscheinlichkeit und Auswirkung Patienten, die an der Versorgung Beteiligten und/oder die Organisation schädigt. (APS 2016)

## Risikokriterien

Die Risikokriterien sind Bezugspunkte, zu welchen die Bedeutung eines Risikos für die Organisation oder für das System bewertet wird. (ONR 49000:2014)

## Risikomatrix

Die Risikomatrix ist eine graphische Darstellung, in der Risiken anhand einer Skala nach Auswirkungen und nach Wahrscheinlichkeiten bzw. nach Häufigkeit eingeordnet werden. (ONR 49000:2014)

## Service Level Agreement (SLA)

Engl. für Dienstgütevereinbarung, kurz SLA; Vereinbarung zwischen Dienstleistungserbringer und -nachfrager, in welcher Qualität eine bestellte Dienstleistung erbracht werden muss. Ein SLA umfasst i.d.R. Angaben zum Leistungsspektrum (z.B. Zeit, Umfang), zur Verfügbarkeit, zur Reaktionszeit des Anbieters etc. (Gablers Wirtschaftslexikon)

## Social Engineering

Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten. (BSI)

## Whistleblower

Person, die Hinweise auf Missstände in Unternehmen, Hochschulen, Verwaltungen etc. gibt. Der Whistleblower ist meist Mitarbeiter oder Kunde und berichtet aus eigener Erfahrung. Er informiert Mittler und Medien oder direkt die Öffentlichkeit. (Gablers Wirtschaftslexikon)

## WLAN-Frequenzband

Bereich elektromagnetischer Frequenzen, in dem ein drahtloses lokales Netzwerk (Wireless Local Area Network) über Funk nach dem IEEE 802.11 Standard betrieben wird. Es existieren verschiedene Frequenzbänder (2,4/3,7/5 GHz) zum Betrieb eines solchen Netzwerkes, so dass eine Trennung des Datenverkehrs zweier Netzwerke durch Einsatz verschiedener Frequenzbänder vorgenommen werden kann. (eigene Definition)

# Literaturverzeichnis

Hinweis: Alle Links wurden am 15.02.2018 überprüft.


1. Aktionsbündnis Patientensicherheit (Hrsg.): Handlungsempfehlung Anforderungen an klinische Risikomanagementsysteme im Krankenhaus, 2016, Im Internet: http://www.aps-ev.de/wp-content/uploads/2016/08/HE_Risikomanagement-1.pdf
2. Austrian Standards (Hrsg.): ONR 49000:2014. Risikomanagement für Organisationen und Systeme - Begriffe und Grundlagen - Umsetzung von ISO 31000 in die Praxis
3. Austrian Standards (Hrsg.): ONR 49002-3:2014. Risikomanagement für Organisationen und Systeme - Teil 3: Leitfaden für das Notfall-, Krisen- und Kontinuitätsmanagement - Umsetzung von ISO 31000 in die Praxis
4. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-1: Managementsysteme für Informationssicherheit
5. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
6. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
7. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-4: Notfallmanagement
8. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Glossar der Cyber-Sicherheit, Im Internet: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/cyberglossar_node.html
9. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden, 2013
10. Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Management-Kurzfassung, 2013,
11. Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2014;111(21):A963-72, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=160315
12. Bundesärztekammer, Kassenärztliche Bundesvereinigung (Hrsg.): Bekanntmachung Technische Anlage, Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Deutsches Ärzteblatt 2008;105(19):A1026-30, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=60114
13. Bundesinstitut für Arzneimittel und Medizinprodukte: Empfehlung des BfArM, Risiken durch ungenügend abgesicherte WLAN-/Netzwerkschnittstellen bei Medizinprodukten, Referenz-Nr.: 3137/15, im Internet: https://www.bfarm.de/SharedDocs/Risikoinformationen/Medizinprodukte/DE/netzwerk_risiko.html
14. Bundespsychotherapeutenkammer (Hrsg.) BPtK-Leitfaden für Internetprogramme im Praxisalltag. Im Internet: http://www.bptk.de/uploads/media/BPtK-Leitfaden_f%C3%BCr_Internetprogramme_im_Praxisalltag_01.pdf

15. Deutscher Ärztetag 2017, Beschlussprotokoll, TOP II „Digitalisierung im Gesundheitswesen“, S. 246-300, Im Internet: http://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/120.DAET/Beschlussprotokoll_120_DAET.pdf
16. Deutsches Institut für Normung (Hrsg.): DIN ISO/IEC 27001:2017. IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen
17. Die Welt: System-Neustart am OP-Tisch, 11.04.2013, im Internet: https://www.welt.de/gesundheit/article160307851/System-Neustart-am-OP-Tisch.html?
18. eHealth Swiss (Hrsg.): Strategie eHealth Schweiz 2.0 (Entwurf vom 5.September 2017). OID: 2.16.756.5.30.1.127.1.1.5.1.1, Im Internet: https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2017/D/170911_Entwurf_Strategie_eHealth_2.0_d.pdf
19. Europäische Kommission: Shaping the Digital Single Market, im Internet: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market
20. KMA Online: Amazon will mit Expertenteam in digitale Gesundheitswirtschaft, Im Internet: https://www.kma-online.de/aktuelles/it-digital-health/detail/amazon-will-mit-expertenteam-in-digitale-gesundheitswirtschaft-a-35414
21. Krüger-Brandt H: Cybersicherheit als Herausforderung, Deutsches Ärzteblatt 2016;113(9):A364-9, Im Internet: https://www.aerzteblatt.de/pdf.asp?id=175147
22. Mertz M*, Jannes M*, Schlomann A*, Manderscheid E, Rietz C[t] , Woopen C[t] (2016) Digitale Selbstbestimmung. Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres), Köln.
23. RP Online: Riesiger internationaler Cyber-Angriff trifft britische Kliniken, 12. Mai 2017, im Internet: http://www.rp-online.de/panorama/ausland/wanna-cry-riesiger-internationaler-cyberangriff-trifft-britische-kliniken-aid-1.6816373
24. Scherschel FA: Gehackte Medizintechnik: FDA will mehr Sicherheit durchsetzen, 19.01.2016, https://heise.de/-3075367
25. Schwan B: Mehr Sicherheit für Implantate mit Funkschnittstelle, 6.11.2013, im Internet: https://heise.de/-1972146
26. Springer Gabler Verlag (Hrsg.): Gabler Wirtschaftslexikon, Stichwort: Service Level Agreement, Im Internet: http://wirtschaftslexikon.gabler.de/Archiv/596505791/service-level-agreement-v5.html
27. Vollmar HC, Kramer U, Müller H, Griemmert M, Noelle G, Schrappe M.: Digitale Gesundheitsanwendungen – Rahmenbedingungen zur Nutzung in Versorgung, Strukturentwicklung und Wissenschaft. Positionspapier der AG Digital Health des Deutschen Netzwerks Versorgungsforschung e.V. (DNVF), Das Gesundheitswesen, 2017;79(12):1080-92
28. Windeck C: WannaCry: Gewaltiger Schaden, geringer Erlös, 14.05.2017, im Internet: https://heise.de/-3713689

# Feedback

Die APS-Handlungsempfehlungen sind Instrumente zur Verbesserung der Patientensicherheit. Diese Instrumente bedürfen kontinuierlicher Weiterentwicklung und Anpassung. Rückmeldungen jedweder Art an das APS sind deshalb ausdrücklich erwünscht. Sollten Sie bei der Durchsicht und/oder dem Gebrauch dieser Handlungsempfehlungen auf Ungereimtheiten, Missverständliches oder Fehler stoßen, bitten wir Sie ebenso um einen Hinweis, wie wir auch gerne Verbesserungsvorschläge aufnehmen.

Zudem besteht für Sie die Möglichkeit, Fragen, die in der vorliegenden Handlungsempfehlung nicht behandelt werden, an das APS zu richten.

Hinweis:
Die Handlungsempfehlung bedarf regelhaft nach 3 Jahren der Überarbeitung durch den Herausgeber.

Ihre Fragen, Anregungen und Rückmeldungen richten Sie bitte an:

Aktionsbündnis Patientensicherheit e.V.
Am Zirkus 2
10117 Berlin
info@aps-ev.de

# Impressum

**Herausgeber**

Aktionsbündnis Patientensicherheit e.V.
Plattform Patientensicherheit Österreich
Stiftung Patientensicherheit Schweiz

**AG Digitalisierung und Risikomanagement**

**Leitung**: Strametz, Prof. Dr. Reinhard, Wiesbaden Business School, Hochschule RheinMain
**Stellvertreter**: Jahn, Dirk, Dipl. Ing. biomed. Technik
**APS-Vorstandsvertreter**: Hardy Müller, Wissenschaftliches Institut der TK für Nutzen und Effizienz im Gesundheitswesen.

**Mitglieder der Arbeitsgruppe und Autoren der Handlungsempfehlung:**

Nico Brinkkötter (Krankenhausgesellschaft Nordrhein-Westfalen e. V.); Dr. Eike Eymers (AOK Bundesverband e.V.); Dr. Wolfgang Huf (Wiener Krankenanstaltenverbund, Krankenhaus Hietzing mit Neurologischem Zentrum Rosenhügel) Altfried Inger (Verbund Katholischer Kliniken Düsseldorf); Dr. Alessa Jansen (Bundespsychotherapeutenkammer); Dr. Wolfgang Lauer (Bundesinstitut für Arzneimittel und Medizinprodukte); Moritz Matschke (WELL IT); Frederik Meilwes (GRB Gesellschaft für Risiko-Beratung mbH); Oliver Steidle (Universitätsklinikum Essen (AöR)); Dr. Stefan Wind (Apothekerkammer Berlin)

**Mit freundlicher Unterstützung des**

Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM).

**Mit freundlicher Unterstützung des**

Bundesamtes für Sicherheit in der Informationstechnik (BSI).
Wir danken Herrn René Salamon.

**Redaktionsteam**

Prof. Dr. Reinhard Strametz (Wiesbaden Business School, Hochschule RheinMain), Dipl. Ing. Dirk Jahn, Hardy Müller, (Wissenschaftliches Institut der TK für Nutzen und Effizienz im Gesundheitswesen), Dr. Wolfgang Huf (Wiener Krankenanstaltenverbund, Krankenhaus Hietzing mit Neurologischem Zentrum Rosenhügel)

**Layout und Grafik:** Alice Golbach (APS)
**Fotonachweis**: Fotolia.com/Paulista
**DOI**: 10.21960/201803
**1. Auflage:** Mai 2018

**Hinweis:** Zur erleichterten Lesbarkeit wird in dieser Handlungsempfehlung auf eine Geschlechterdifferenzierung verzichtet und stattdessen das maskuline Neutrum verwendet.



**Zitation**: APS e.V. (Hrsg, 2018): Digitalisierung und Patientensicherheit – HE 1) Handlungsempfehlung für das Risikomanagement in der der Patientenversorgung, Berlin

AKTIONSBÜNDNIS
PATIENTENSICHERHEIT

patientensicherheit schweiz

Plattform
Patientensicherheit