FMH

D2

IT-Grundschutz für Praxisärztinnen und Praxisärzte

11 Empfehlungen

Aktualisierung der Empfehlungen im Rahmen des neuen Datenschutzgesetzes 2023

Sehr geehrte Praxisinhaberin
Sehr geehrter Praxisinhaber

Die zunehmende Digitalisierung und Vernetzung im Gesundheitswesen eröffnet neue Möglichkeiten und trägt damit zur Verbesserung der Behandlungsabläufe und zur Entwicklung der Qualität in der Medizin bei.

Neben den Vorteilen birgt sie jedoch auch Risiken im Bereich des Datenschutzes und der Datensicherheit: Cyberangriffe auf Gesundheitsdaten und auf die ICT-Infrastruktur können die Privatsphäre von Patientinnen und Patienten beeinträchtigen, das Tagesgeschäft einer Arztpraxis stark einschränken, finanziellen Schaden sowie Reputationsschaden nach sich ziehen und nicht zuletzt die Behandlung der Patientinnen und Patienten beeinflussen.

Die Arztpraxis ist für die Gewährleistung des Datenschutzes und der Datensicherheit verantwortlich. Der Gesetzgeber hat medizinische Daten im Bundesgesetz zum Datenschutz (DSG) als besonders schützenswerte Personendaten eingestuft, sodass umfangreiche Massnahmen für einen angemessenen Schutz dieser Daten erforderlich sind.

Aufbau, Unterhalt und Wartung einer sicheren ICT-Infrastruktur, die Erarbeitung von Sicherheitsanforderungen und die Sensibilisierung der Mitarbeitenden zugunsten einer neuen Sicherheitskultur sind umfassende Aufgaben, die personelle und finanzielle Ressourcen erfordern.

Die nachfolgenden Empfehlungen sollen Ihnen helfen, den Aufbau und den Erhalt des Datenschutzes und der Datensicherheit in Ihrer Arztpraxis zu gewährleisten.

Dr. med. Yvonne Gilli

Präsidentin FMH

Die vorliegenden Empfehlungen wurden hinsichtlich des am 1. September 2023 in Kraft getretenen revidierten Datenschutzgesetzes auf ihre inhaltliche Kompatibilität überarbeitet.

Inhaltsverzeichnis

Übersicht

Zielgruppe

Die Empfehlungen der FMH betreffen die Organisation und IT-Infrastruktur von kleinen und mittelgrossen Arztpraxen. Die Anforderungen und Massnahmen wurden in Interviews mit Praxisinhabern validiert und sind für Arztpraxen mit bis zu zwölf Ärztinnen oder Ärzten zweckmässig. Direkte Adressaten dieser Empfehlungen sind die Ärzteschaft, Mitarbeitende der Praxis sowie beauftragte Dritte (z. B. ICT-Dienstleister).

Zielsetzung

Die Empfehlungen der FMH sollen zu einem angemessenen Schutz sensibler Personendaten in Arztpraxen beitragen. Dabei wird den gesetzlichen Anforderungen an den Schutz besonders schützenswerter Personendaten Rechnung getragen.

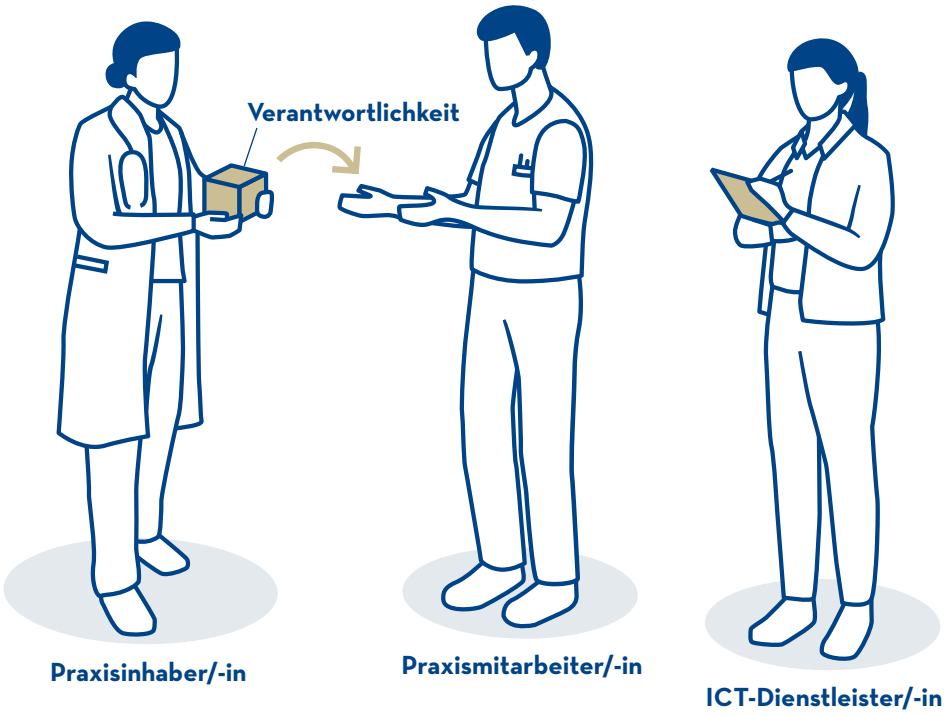
Aufbau

Das vorliegende Dokument gibt eine Übersicht über die Empfehlungen der FMH zum IT-Grundschutz in Arztpraxen und über die dazugehörigen Massnahmen. Die hier aufgeführten Empfehlungen und Massnahmen werden im Dokument «D3 IT-Grundschutz für Praxisärztinnen und Praxisärzte» weiter ausgeführt.

	 Grafische Übersicht	 11-Punkte Programm	 Detailierte Massnahmen
Praxisinhaber/-in	○	◉	○
Praxismitarbeiter/-in	○	◉	○
ICT-Dienstleister/-in	✕	✕	○

E1

Verantwortlichkeiten bestimmen und Vorgaben erlassen

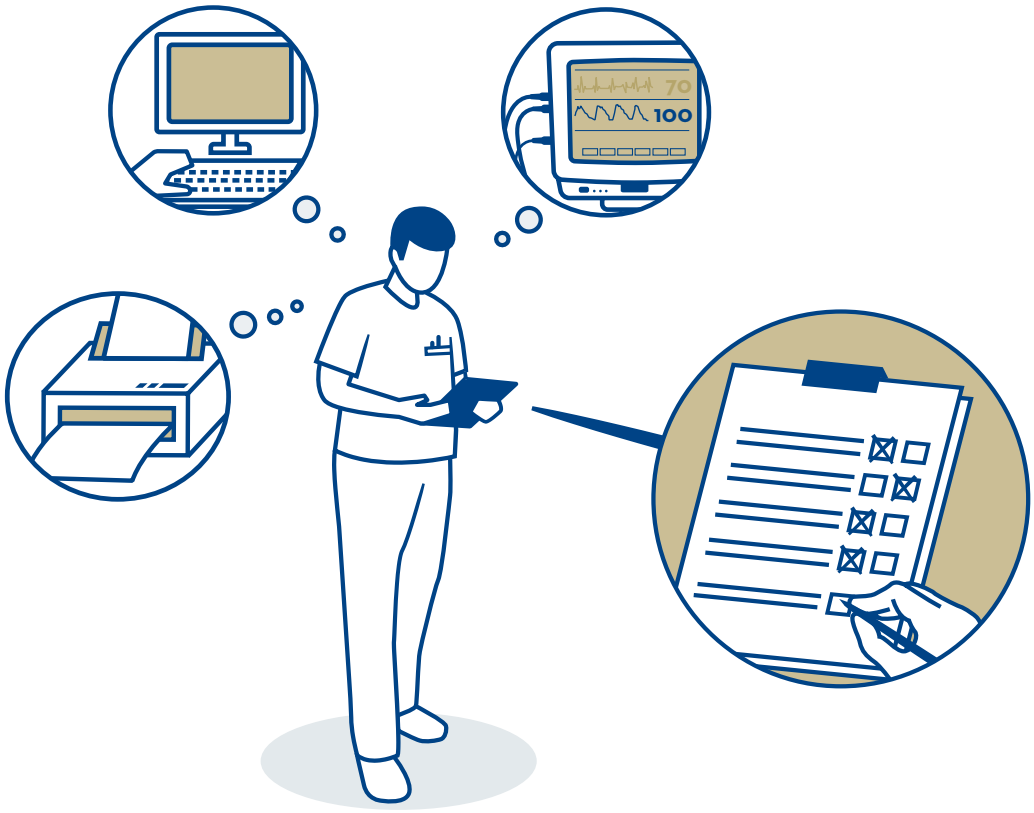


Das Thema Datenschutz und Datensicherheit erhält mit der Bestimmung der Verantwortlichkeiten, Aufgaben und Kompetenzen in der Arztpraxis die notwendige Bedeutung. Die Praxisinhaberin oder der Praxisinhaber ist verantwortlich für die Sicherheit und den Schutz der Daten. Der oder die Datenschutz- und Datensicherheitsverantwortliche (DSDS-V) übernimmt typischerweise die operationelle Verantwortung für den Schutz und die Sicherheit der Daten und die Umsetzung der notwendigen Massnahmen. Die Rolle der oder des Datenschutz- und Datensicherheitsverantwortlichen kann durch die Praxisinhaberin oder den Praxisinhaber selbst, den externen ICT-Dienstleister oder einen Praxismitarbeitenden übernommen werden.

Das Aufgabenspektrum des DSDS-V umfasst sowohl den Erlass als auch die Umsetzung und die Sicherstellung der Sicherheitsvorgaben. Diese Vorgaben umfassen den Umgang mit Daten, den Austausch von Daten, die Handhabung von ICT-Mitteln sowie den Schutz von Endgeräten und des Netzwerks. Die Umsetzung der Vorgaben kann sowohl auf technischer als auch auf organisatorischer oder personeller Ebene erfolgen.

Die Rolle des DSDS-V ist abzugrenzen von der Rolle der ICT-Betriebsverantwortlichen, der für den Aufbau, den Betrieb und den Unterhalt der ICT-Infrastruktur verantwortlich sind. Das Verhältnis der beiden Rollen ist so zu verstehen, dass die DSDS-V die Anforderungen an den Datenschutz und die Datensicherheit erlassen und die Implementierung auf technischer Ebene an die ICT-Betriebsverantwortlichen delegieren sowie die Umsetzung überwachen.

E2 ICT-Mittel in ein Inventar aufnehmen



Der effektive Schutz von Daten und Informationen bedingt den Einsatz von sicheren ICT-Mitteln. Dabei gilt: Es kann nur geschützt werden, was bekannt ist. Deshalb sind alle schützenswerten ICT-Mittel zu identifizieren, entsprechend der Sensitivität der Daten und Informationen zu klassifizieren und mit zuvor festgelegten Attributen in einer Inventarliste zu dokumentieren. Die Inventarliste kann im Rahmen eines Verzeichnisses der Bearbeitungstätigkeiten geführt werden.

Die Inventarliste dient als Hilfsmittel bei der Planung und Umsetzung von Sicherheitsmassnahmen und verbessert die Reaktionsfähigkeit bei einem Sicherheitsvorfall. Die Inventarliste sollte regelmässig aktualisiert werden.

Bei der Ausserbetriebnahme von ICT-Mitteln, insbesondere von Endgeräten, müssen alle Daten vollständig und unwiderruflich gelöscht werden.

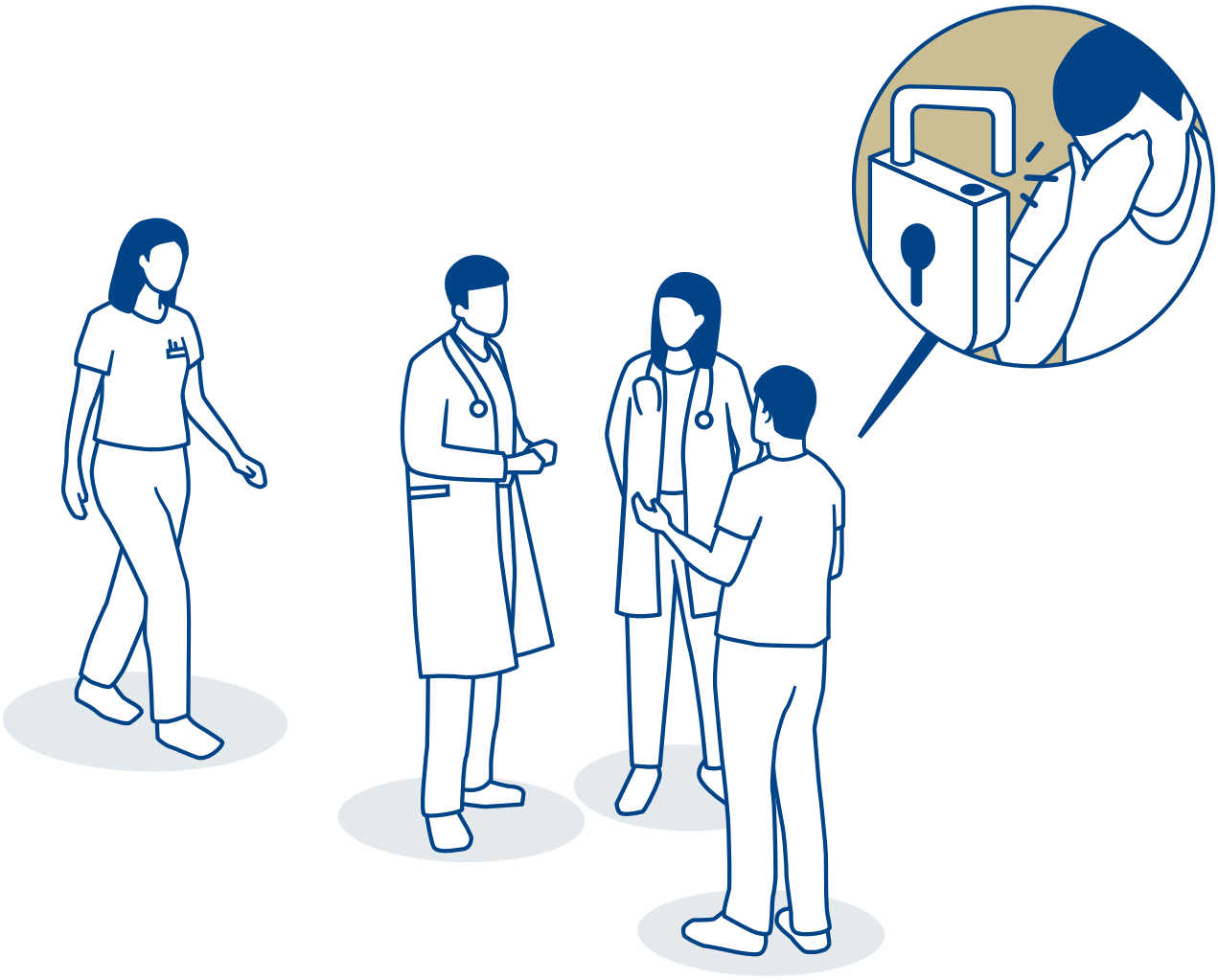
E3 Zugriffsschutz regulieren und Benutzerrechte verwalten

Eingeschränkte Zugriffsrechte helfen, das Risiko eines Missbrauchs zu reduzieren. Den Benutzenden und Administrierenden sollten nur diejenigen Berechtigungen erteilt werden, die für die tägliche Arbeit notwendig sind (Need-to-know-Prinzip). Verwendete Passwörter müssen mindestens zehn Zeichen lang sein und sollten zusätzliche Sicherheitskriterien erfüllen. Alle Passwörter müssen in regelmässigen Abständen geändert werden. Der Passwortwechsel sollte nach Möglichkeit (z. B. für Benutzerkonten) regelmässig technisch erzwungen werden (begrenzte Gültigkeit). Falls dies nicht möglich ist, muss die organisatorische Umsetzung des Passwortwechsels sichergestellt werden.

Für den Zugriff auf die medizinischen Daten der Patienten müssen alle Praxismitarbeitenden über ein persönliches Benutzerkonto verfügen. Für Zugriffe über das Internet sind separate persönliche Benutzerkonten zu verwenden. Vor jedem Zugriff sollte eine Zwei-Faktor-Authentisierung erfolgen.

Die Aktivitäten auf den Benutzerkonten, wie zum Beispiel Log-in- und Log-out-Versuche, sind zur Erkennung von atypischem Verhalten und zur Sicherstellung der Nachvollziehbarkeit aufzuzeichnen und zu überwachen.

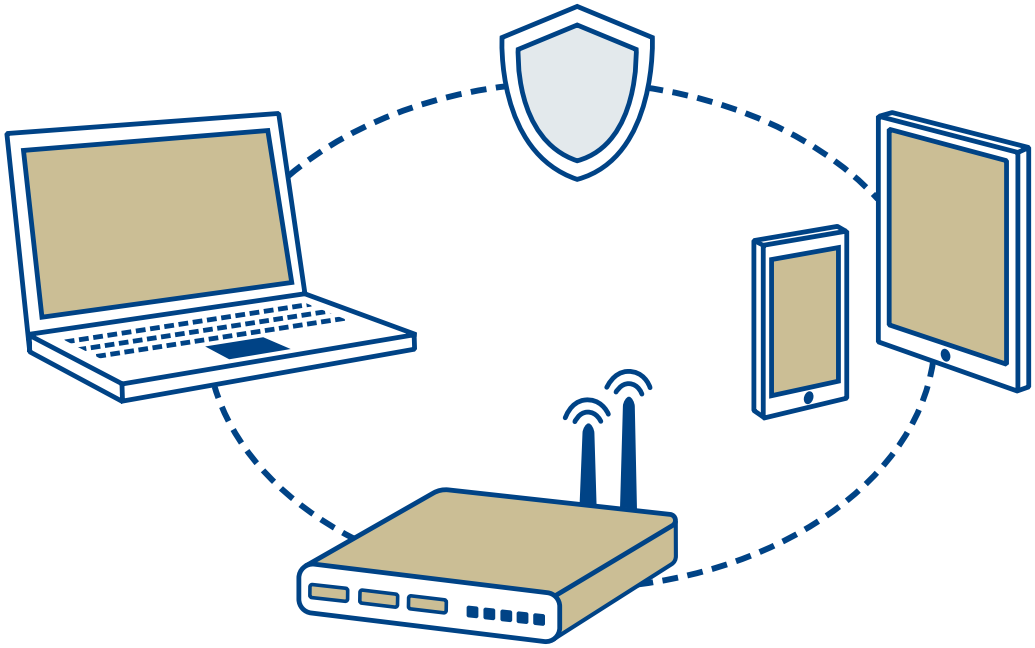
E4 Praxismitarbeitende für Datensicherheit sensibilisieren



Die Mitarbeitenden eines Unternehmens sind ein beliebtes Angriffsziel für Cyberkriminelle, weshalb Angreifer oftmals versuchen, sich mittels Social-Engineering-Attacken Zugang zur dieser ICT-Infrastruktur und zu Daten zu verschaffen. Um dies zu verhindern, ist die Sensibilisierung der Praxismitarbeitenden von zentraler Bedeutung.

Die Sensibilisierung für mögliche Angriffe und der bewusste Umgang mit sensiblen Daten können über verschiedene Kanäle erreicht werden. Beispiele hierfür sind Schulungen, Merkblätter oder die zeitnahe Kommunikation von sicherheitsrelevanten Ereignissen an die Mitarbeitenden. Die Vermittlung von Sicherheitsvorgaben zu Passwörtern und PINs, zum richtigen Umgang mit ICT-Mitteln und Daten sowie Handlungsanweisungen für Sicherheitsvorfälle unterstützen die erwähnten Ziele. Die Praxismitarbeitenden müssen sowohl bei Eintritt in die Praxis als auch während der Anstellung wie auch beim Austritt regelmässig über Datensicherheit und Datenschutz aufgeklärt werden, sodass die Aufmerksamkeit für diese Thematik sowie der bewusste Umgang mit Daten nachhaltig gefördert werden.

E5 Endgeräte vor Schadsoftware schützen

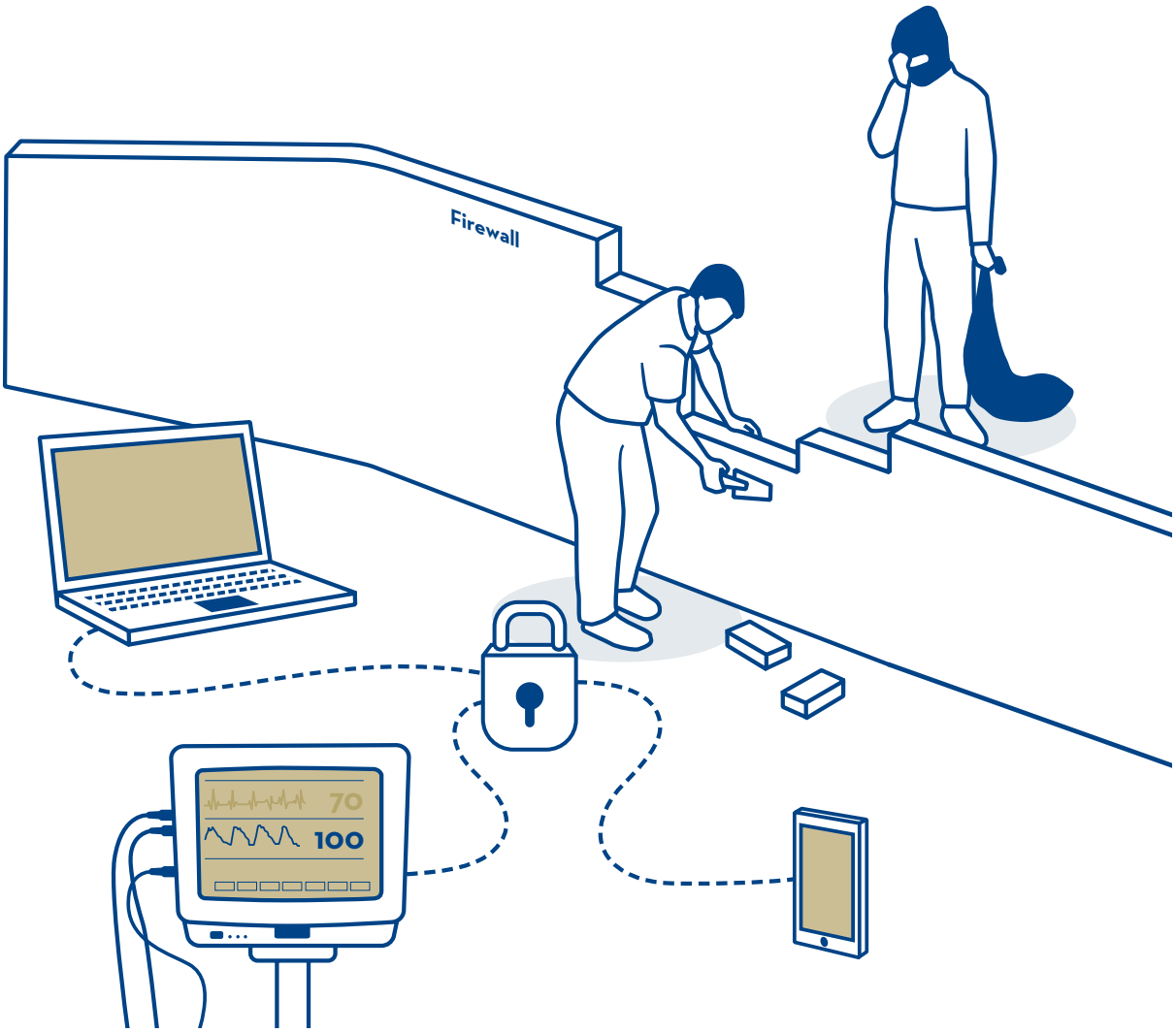


Endgeräte wie Smartphones oder Laptops können leicht mit Schadsoftware infiziert werden. Sämtliche Endgeräte müssen daher über einen aktuellen Virenschutz verfügen. Dieser sollte so konfiguriert werden, dass alle Dateien beim Zugriff auf schädliche Inhalte geprüft werden. Zudem müssen die Virensignaturen mindestens täglich aktualisiert und das eingesetzte Betriebssystem regelmässig mit Updates versorgt werden.

Die praxisinternen Endgeräte sollten nicht für private Zwecke verwendet werden.

Mit diesen Massnahmen lässt sich das Risiko von Schadsoftware stark reduzieren. Es gilt jedoch zu beachten, dass Virenschutzprogramme nur bekannte Schadsoftware erkennen. Ein vollständiger Schutz ist damit nicht gewährleistet und ein sensibilisierter Umgang mit potenziellen Gefahren, insbesondere bei der Bearbeitung von E-Mails und Anhängen, bleibt von zentraler Bedeutung.

E6 Netzwerk schützen

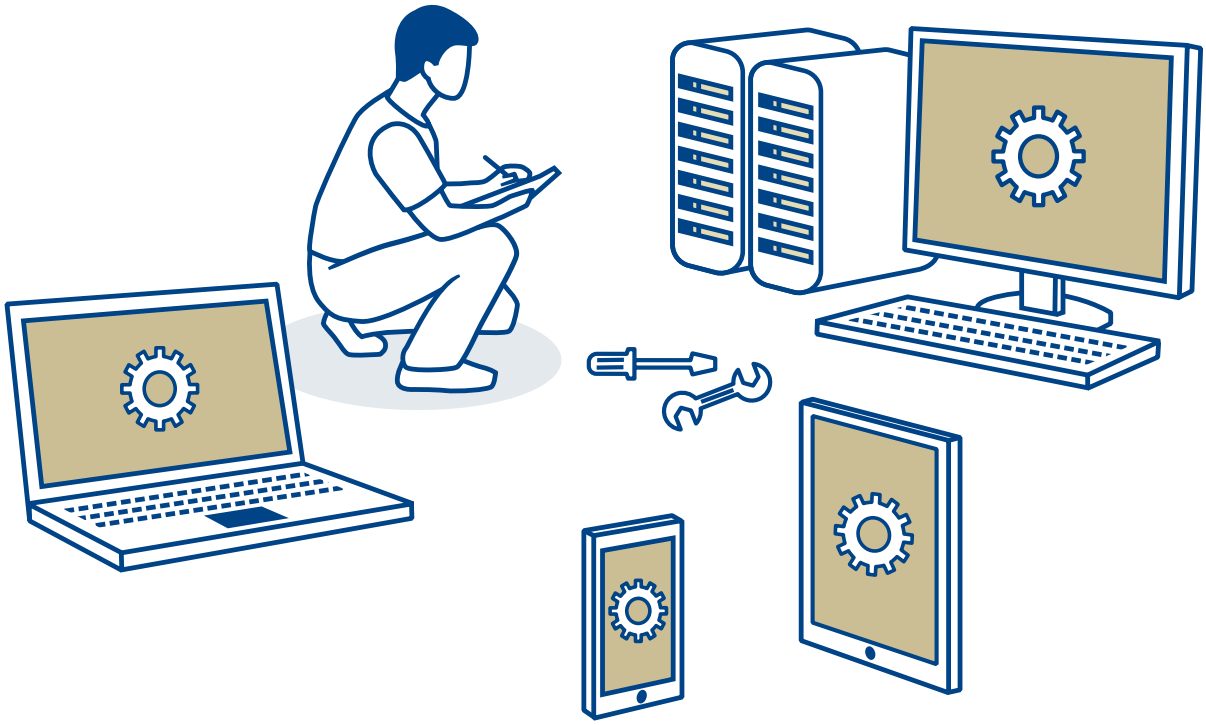


Bleibt der Zugriff auf das Computernetzwerk einer Arztpraxis ungeschützt, können sich unberechtigte Dritte (z. B. kriminelle Hacker) Zugang zum Netzwerk verschaffen, die Kommunikation abhören oder Daten entwenden.

Um den unberechtigten Zugriff auf das praxisinterne Netzwerk zu verhindern, müssen Sicherheitsvorkehrungen bei den Schnittstellen zum Internet sowie bei den kabelgebundenen und kabellosen Anschlüssen im lokalen Netzwerk getroffen werden.

Zum Schutz von Netzübergängen vom Computernetzwerk der Arztpraxis zum Internet sind Firewalls zu konfigurieren und einzusetzen. Sie dienen dazu, den Netzwerkverkehr zu regulieren, und können weitere Sicherheitsfunktionen wie zum Beispiel Virenscanner auf Netzwerkebene wahrnehmen. Ungenutzte Netzwerkdosen sollten verschlossen werden, da sich andernfalls unberechtigte Personen ans Netzwerk anschliessen können. Kabellose Verbindungen, beispielsweise Wi-Fi, sollten mittels eines Passwortes geschützt werden.

E7 ICT-Umgebung konfigurieren und warten

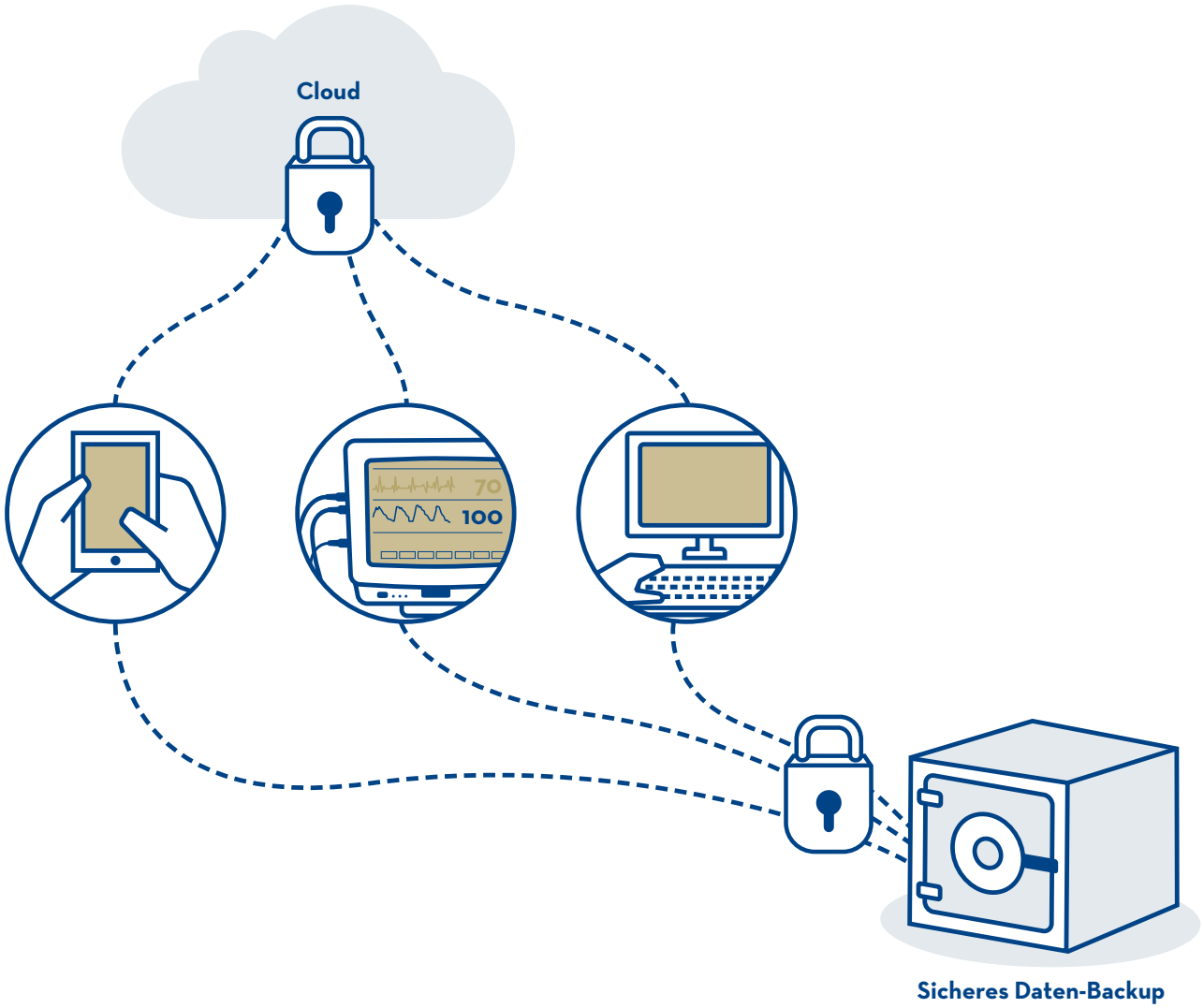


Durch eine sichere Konfiguration der Systeme und Netzwerkkomponenten können die Angriffsfläche und damit die Wahrscheinlichkeit und die Auswirkungen eines Cyberangriffs verringert werden.

Auf ICT-Systeme, beispielsweise Laborgeräte, die vollständig von Drittanbietern geliefert werden, kann infolge vertraglicher und technischer Hürden kein oder kaum Einfluss genommen werden. Solche ICT-Systeme sollten gesondert behandelt und beispielsweise in eine eigene Netzwerkzone verschoben werden, da auf ihnen meistens keine Updates installiert oder sicherheitsrelevante Konfigurationen vorgenommen (härten) werden können.

ICT-Systeme sollten mit verschiedenen Massnahmen «gehärtet» werden, zum Beispiel durch automatische Installationen von Sicherheitsupdates, Verschlüsselung der Festplatten oder durch die Verwendung sicherer Passwörter für Benutzerkonten. Zur betrieblichen Überwachung sollten ICT-Systeme und eingesetzte Applikationen die Aktivität der Benutzenden aufzeichnen und auswerten sowie beim Ausfall eines ICT-Systems eine Alarmierung auslösen.

E8 Digitale Daten sicher ablegen

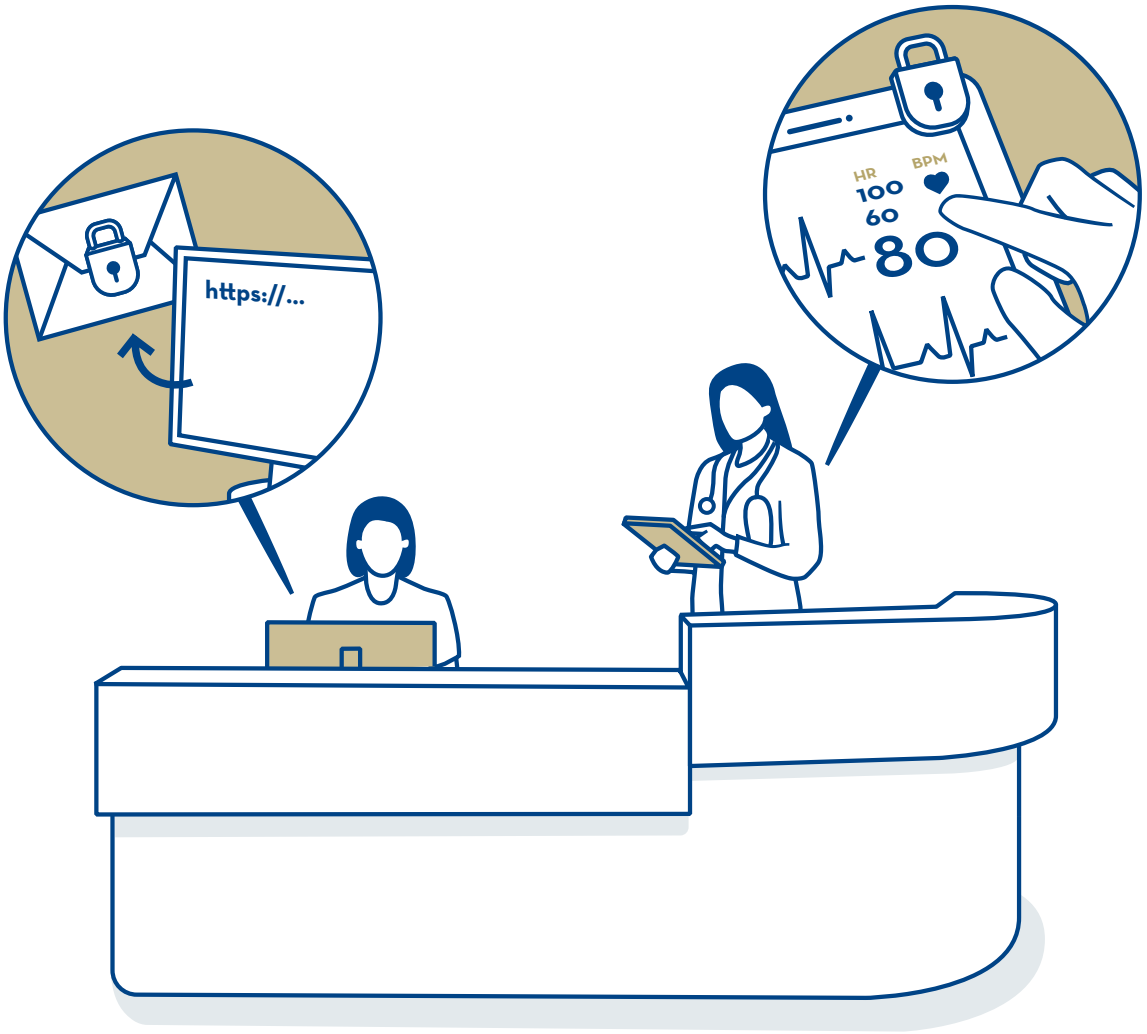


Um dem Risiko eines Datenverlustes entgegenzuwirken, ist es wichtig, eine regelmässige Datensicherung aller Daten zu erstellen (Backup), da gespeicherte Daten versehentlich von Mitarbeitenden, von fehlerhafter Hardware oder von Schadsoftware gelöscht werden können. Damit die Vertraulichkeit und die Integrität dieser Daten nicht verloren gehen, müssen die Zugriffs- und Benutzerrechte der ursprünglichen Daten ebenfalls in der Arztpraxis definiert und gesichert werden.

Das Backup muss regelmässig durchgeführt und ausserhalb der Praxisräumlichkeiten aufbewahrt werden. Zusätzlich sollte das Wiederherstellen der Daten aus den Backups mindestens einmal jährlich getestet werden.

Auch bei einer Datensicherung in der Cloud sind die gesetzlichen Anforderungen des Datenschutzgesetzes und der Geheimhaltungspflicht einzuhalten, was zusätzliche technische Massnahmen erfordert.

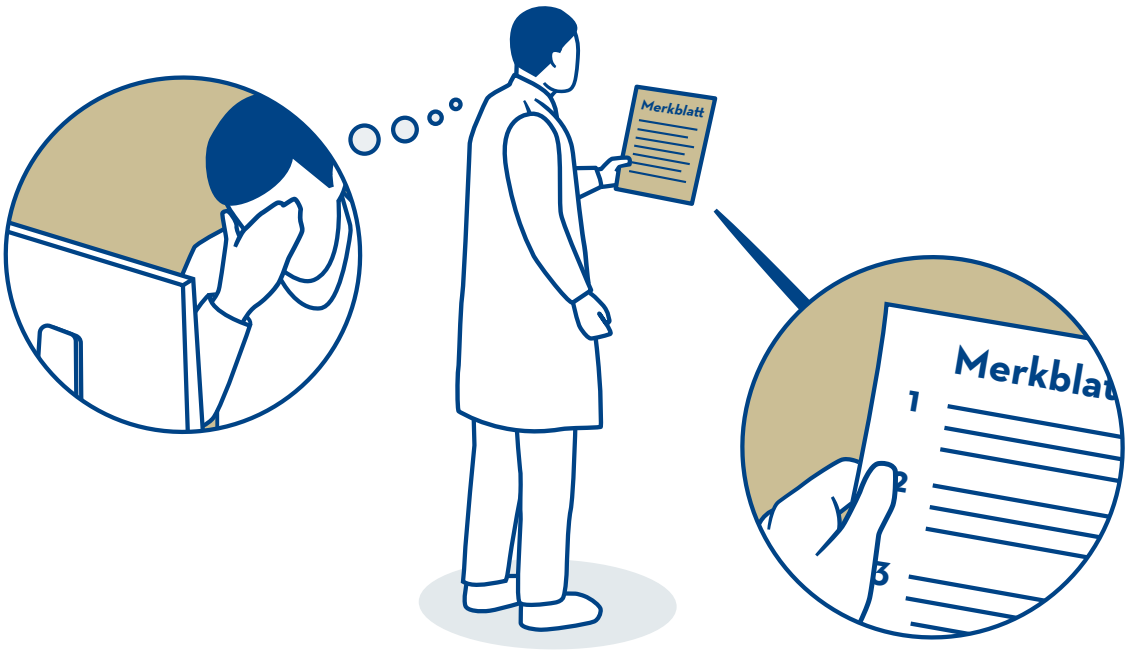
E9 Digitale Daten sicher austauschen



Sensible Personendaten sollten zum Schutz vor Zugriff durch Unbefugte verschlüsselt werden. Dadurch wird sichergestellt, dass die Daten nur von Personen eingesehen, gelöscht oder verändert werden, die dazu auch befugt sind. Ausserdem wird so verhindert, dass Daten unbemerkt verändert werden.

Werden Patientendaten via E-Mail ausgetauscht, so müssen die E-Mails verschlüsselt sein. Der Austausch via Fax erfolgt unverschlüsselt und sollte auf ein Minimum beschränkt werden. Zugriffe auf Anwendungen über das Internet dürfen nur über einen verschlüsselten Kanal, beispielsweise mittels HTTPS, erfolgen. Medizinische Daten sowie Authentifikationsmerkmale wie beispielsweise Passwörter dürfen nie unverschlüsselt übermittelt werden.

E10 Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen

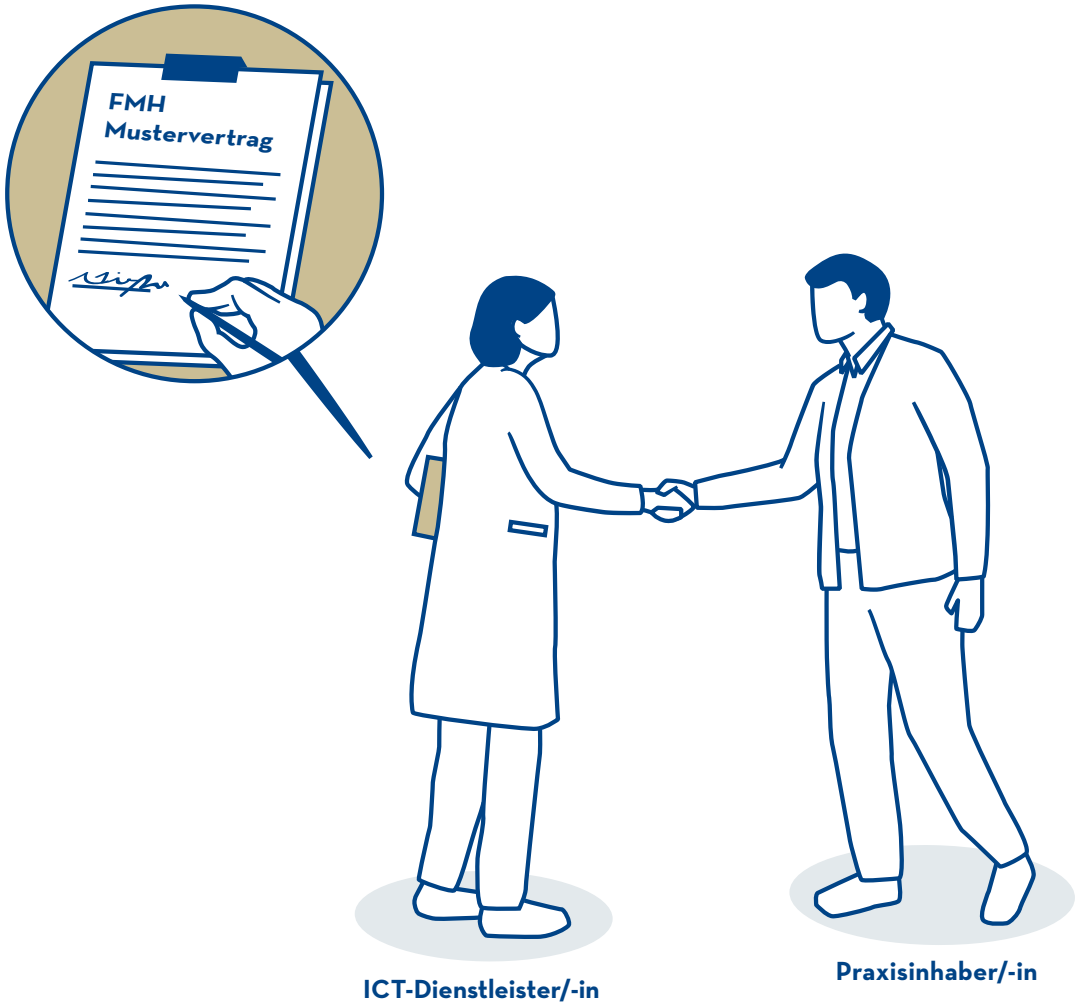


Sicherheitsvorfälle sind Ereignisse, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten beeinträchtigen. Phishingangriffe, die Ausnutzung einer Schwachstelle oder der Befall eines Endgeräts mit Schadsoftware (Viren, Würmer oder Trojaner) sind Beispiele für Sicherheitsvorfälle, die eine erhebliche Auswirkung auf den Betrieb einer Arztpraxis haben können. Zur zeitnahen und effizienten Erkennung und Behandlung von Sicherheitsvorfällen müssen geeignete technische und organisatorische Vorkehrungen getroffen werden.

Es muss definiert werden, an wen sich Praxismitarbeitende bei einem Sicherheitsvorfall wenden können. Die Praxismitarbeitenden müssen die Meldestelle und die entsprechenden Kontaktdaten kennen. Zudem sollten Merkblätter zur Vorgehensweise sowie zur Analyse eines Sicherheitsvorfalls erarbeitet und die Praxismitarbeitenden davon in Kenntnis gesetzt werden.

Eine Verletzung der Datensicherheit ist so rasch als möglich dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu melden, sofern ein hohes Risiko für die Persönlichkeits- oder Grundrechte der betroffenen Person besteht.

E11 Externe Dienstleister beauftragen und überwachen



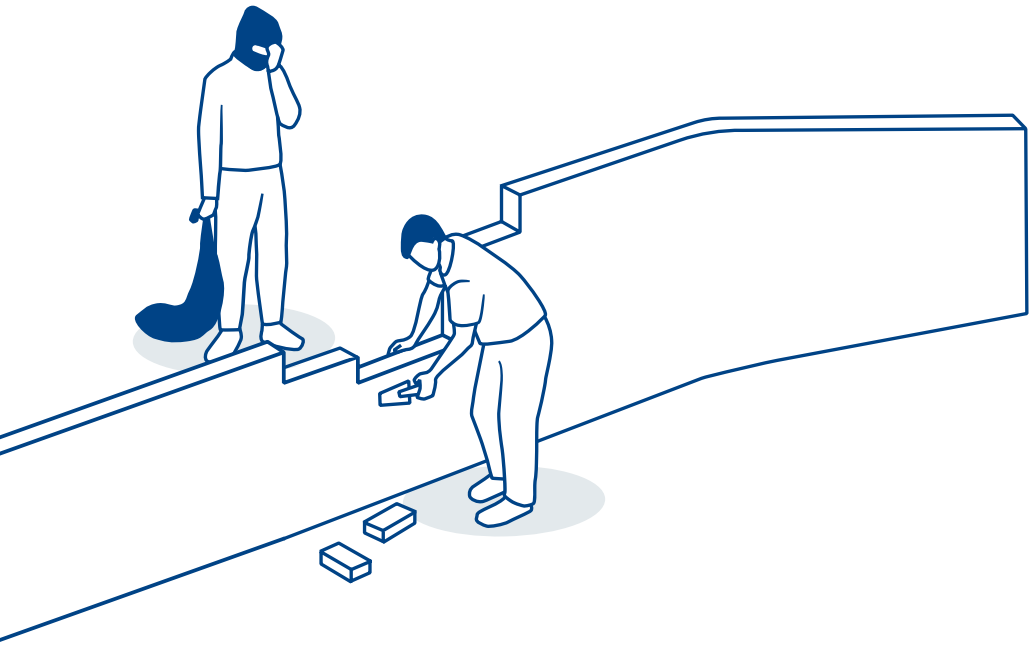
Da externe Dienstleister je nach Vertragsvereinbarung für den Aufbau, den Betrieb, den Unterhalt und die Wartung der ICT-Infrastruktur verantwortlich sind, ist die Auswahl auf eine solide Evaluation des Dienstleistungsangebots zu stützen und durch monatliche oder nach Bedarf erstellte Rapporte zu überwachen.

Die Koordination der Zusammenarbeit mit den Sicherheitsverantwortlichen von externen ICT-Dienstleistern umfasst die Bereitstellung der vorliegenden Empfehlungen und der praxisinternen Sicherheitsvorgaben sowie die vertragliche Festlegung der Nachweise zur Überwachung der Sicherheitsvorgaben. Die externen ICT-Dienstleister sollten vertraglich festhalten, wie sie die Sicherheitsvorgaben einhalten und umsetzen werden.

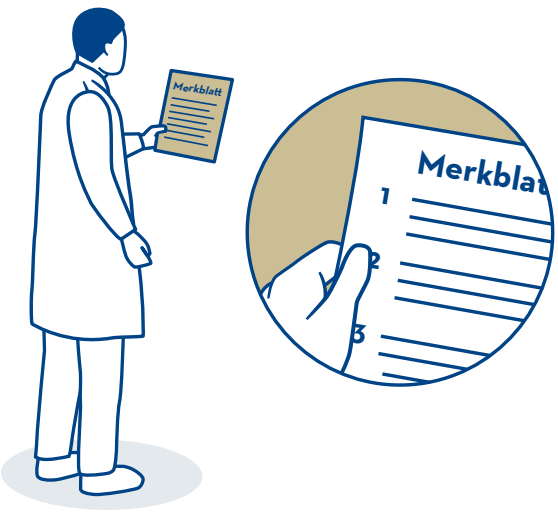
Für die Leistungsvereinbarung mit externen ICT-Dienstleistern können die Allgemeinen Geschäftsbedingungen für IKT-Leistungen, Ausgabe Januar 2020, auf der Webseite der digitalen Verwaltung Schweiz (DVS) als Grundlage dienen. Für Leistungsvereinbarungen mit Cloud-Anbietern empfiehlt die FMH den Rahmenvertrag für Cloud-Services.

Glossar
Das Glossar ist online unter
https://www.fmh.ch/themen/ehealth/praxisinformatik.cfm abrufbar.

Impressum
Herausgeberin: FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern
Text: Redguard AG, Bern
Grafikdesign/Illustration: Hahn+Zimmermann, Bern
Publikation: Dezember 2019 (Version September 2023)
www.fmh.ch




FMH
Mustervertrag


Merkblatt
Merkblat
1
2
3