

Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte 11 Empfehlungen



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.

Um Praxisinhaberinnen und Praxisinhaber zu unterstützen und weil auf Bundesebene bisher keine Empfehlungen vorliegen, hat die FMH Minimalanforderungen zum IT-Grundschutz für Arztpraxen erarbeitet. Die Minimalanforderungen haben Empfehlungscharakter und beinhalten Anforderungen, die ein Mindestniveau an Sicherheit für Daten, Informationen und die ICT-Infrastruktur sicherstellen.

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

Mitglied des Zentralvorstandes der FMH,
Departementsverantwortliche Digitalisierung/eHealth

Inhaltsverzeichnis

Übersicht	4
Empfehlung 1: Verantwortlichkeiten bestimmen und Vorgaben erlassen	5
Empfehlung 2: ICT-Mittel in ein Inventar aufnehmen	6
Empfehlung 3: Zugriffsschutz regulieren und Benutzerrechte verwalten	7
Empfehlung 4: Praxismitarbeitende für Datensicherheit sensibilisieren	8
Empfehlung 5: Endgeräte vor Schadsoftware schützen	9
Empfehlung 6: Netzwerk schützen	10
Empfehlung 7: ICT-Umgebung konfigurieren und warten	11
Empfehlung 8: Digitale Daten sicher ablegen	12
Empfehlung 9: Digitale Daten sicher austauschen	13
Empfehlung 10: Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen	14
Empfehlung 11: Externe Dienstleister beauftragen und überwachen	15

Übersicht

Zielgruppe




Die Empfehlungen der FMH richten sich an kleine und mittelgrosse Arztpraxen und die dazugehörige ICT-Umgebung. Die Anforderungen und Massnahmen wurden in Interviews mit Praxisinhaberinnen und Praxisinhabern validiert und sind für Arztpraxen mit bis zu zwölf Ärztinnen und Ärzte zweckmässig. Direkter Adressat dieser Empfehlungen sind Ärztinnen und Ärzte, Mitarbeitende der Praxis sowie beauftragte Dritte (z.B. ICT-Dienstleister).

Zielsetzung

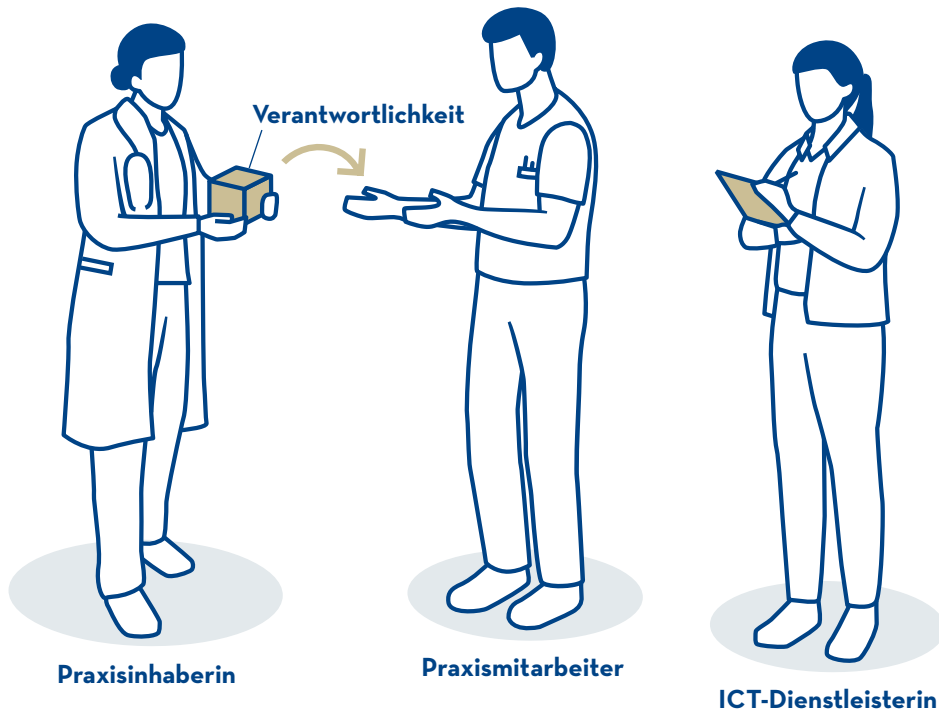
Die Empfehlungen der FMH sollen zu einem angemessenen Schutz sensibler Daten in Arztpraxen beitragen. Dabei wird den gesetzlichen Anforderungen an den Schutz besonders schützenswerter Personendaten Rechnung getragen.

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 Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte» weiter ausgeführt.

	 D1	 D2	 D3
	Grafische Übersicht	11-Punkte Programm	Detaillierte Massnahmen
Praxisinhaber/-in	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Praxismitarbeiter/-in	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
ICT-Dienstleister/-in	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

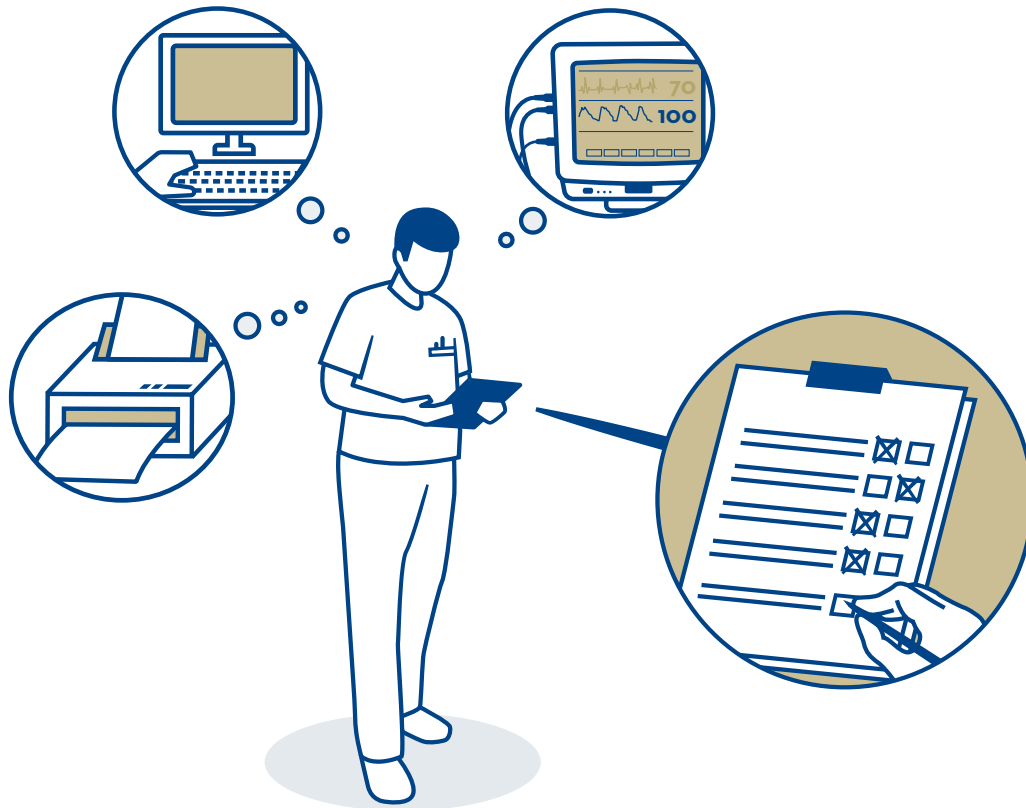
Verantwortlichkeiten bestimmen und Vorgaben erlassen



Das Thema Datenschutz und Datensicherheit erhält mit der Bestimmung der Verantwortlichkeiten, Aufgaben und Kompetenzen in der Arztpraxis die notwendige Bedeutung. Die Praxisinhaberin ist gleichzeitig die Inhaberin der Daten und somit verantwortlich für deren Sicherheit und deren Schutz. Der Datenschutz- und Datensicherheitsverantwortliche (DSDS-V) übernimmt typischerweise die Verantwortung für den Schutz und die Sicherheit der Daten. Die Rolle des Datenschutz- und Datensicherheitsverantwortlichen kann durch die Praxisinhaberin 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, die für den Aufbau, den Betrieb und den Unterhalt der ICT-Infrastruktur verantwortlich ist. Das Verhältnis der beiden Rollen ist so zu verstehen, dass die DSDS-V die Anforderungen an den Datenschutz und die Datensicherheit erlässt und die Implementierung auf technischer Ebene an den ICT-Betriebsverantwortlichen delegiert.



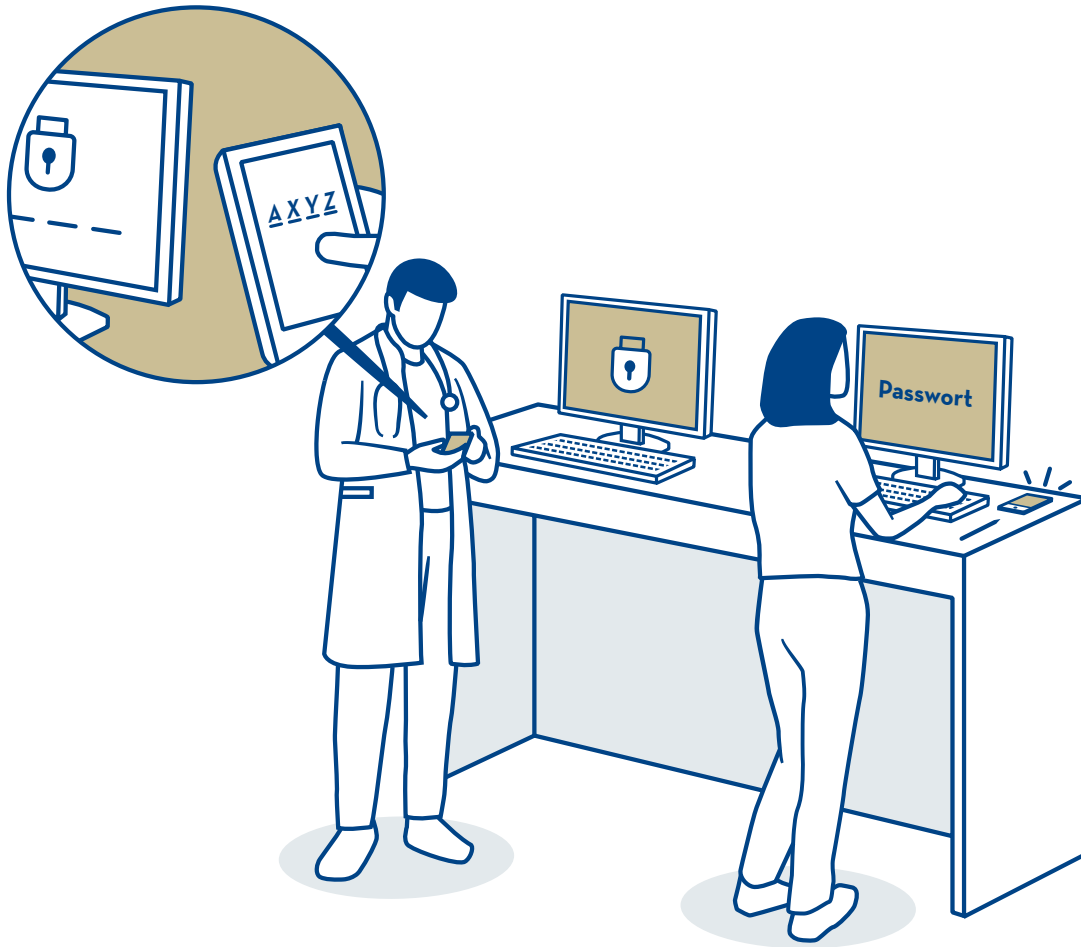
Der effektive Schutz von Daten und Informationen bedingt den Einsatz von sicheren ICT-Mitteln. Dabei gilt: Es kann nur geschützt werden, was bekannt ist. Deshalb sind alle schützenswerten ICT-Mittel zu identifizieren, entsprechend der Sensitivität der Daten und Informationen zu klassifizieren und mit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

Die Inventarliste dient als Hilfsmittel bei der Planung 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. Die Weitergabe oder der Verkauf von ICT-Mitteln ist zu unterlassen.

E3

Zugriffsschutz regulieren und Benutzerrechte verwalten



Eingeschränkte Zugriffsrechte helfen, das Risiko eines Missbrauchs zu reduzieren. Den Benutzenden und Administratoren 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 einmal im Jahr geändert 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 starke Authentifizierung erfolgen (mittels zweier unabhängiger Faktoren, zum Beispiel Passwort und Token).

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

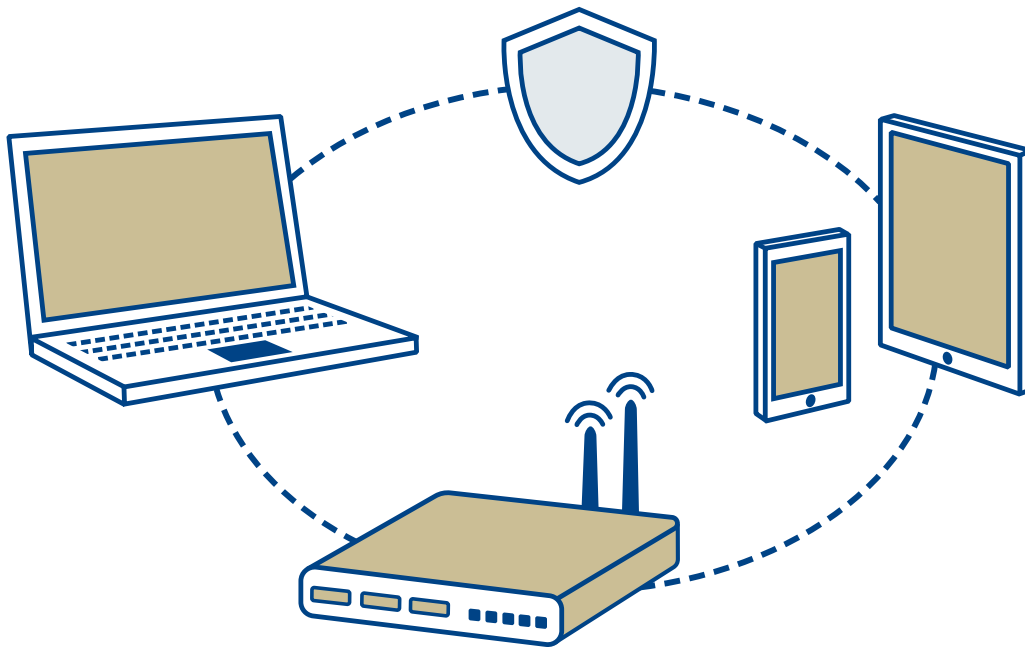


Die Mitarbeitenden eines Unternehmens sind ein beliebtes Angriffsziel für kriminelle Hacker, weshalb Angreifer oftmals versuchen, sich mittels Social-Engineering-Attacken Zugang zur ICT-Infrastruktur und zu Daten zu verschaffen. Um dies zu verhindern, ist die Sensibilisierung der Praxismitarbeitenden 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 regelmässig sensibilisiert werden, sodass die Aufmerksamkeit für das Thema Datensicherheit und Datenschutz sowie der bewusste Umgang mit Daten nachhaltig gefördert werden.

E5

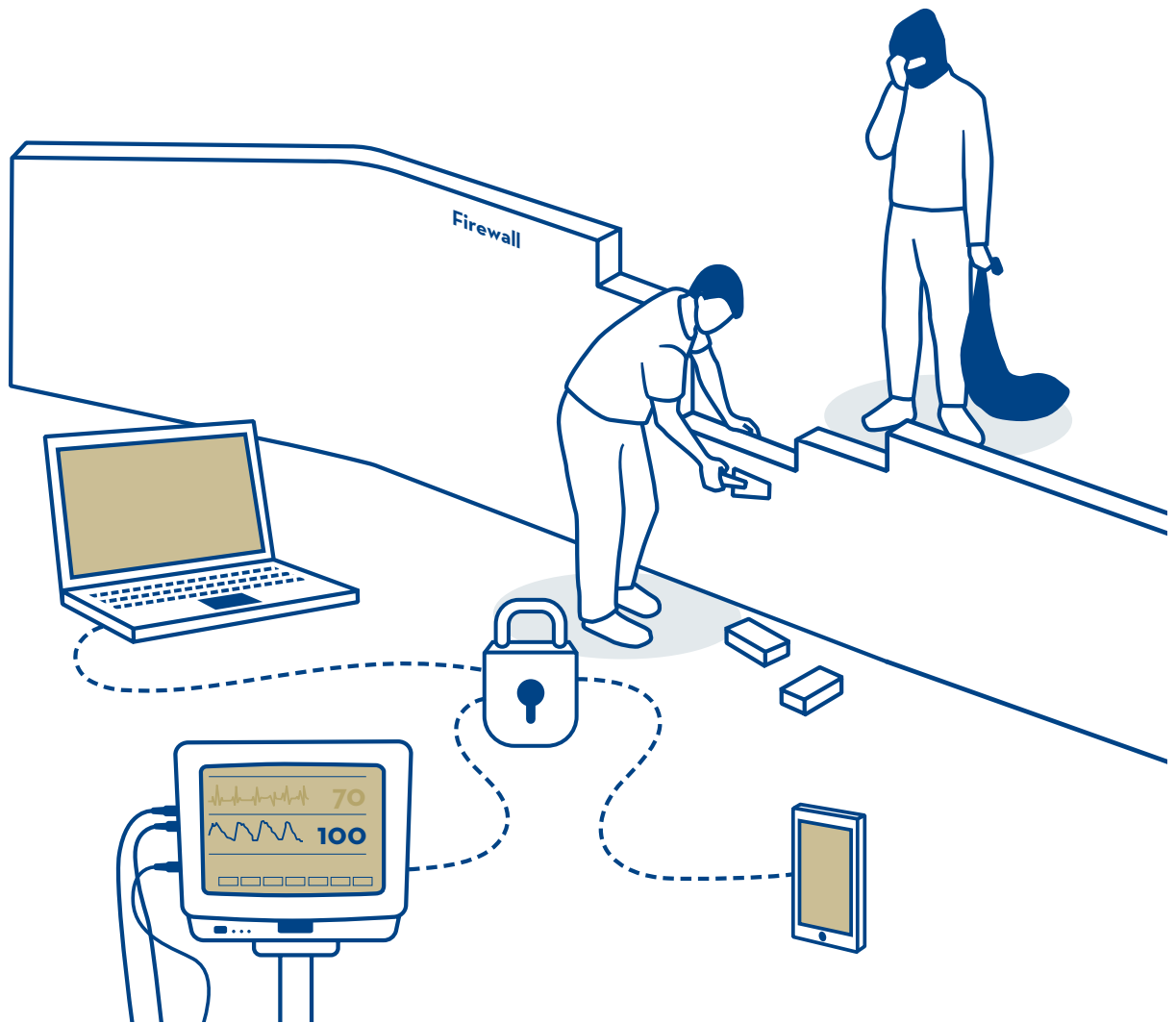
Endgeräte vor Schadsoftware schützen



Endgeräte wie Smartphones oder Laptops können leicht mit Schadsoftware infiziert werden. Sämtliche Endgeräte müssen daher über ein aktuelles Virenschutzprogramm verfügen. Dieses 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.

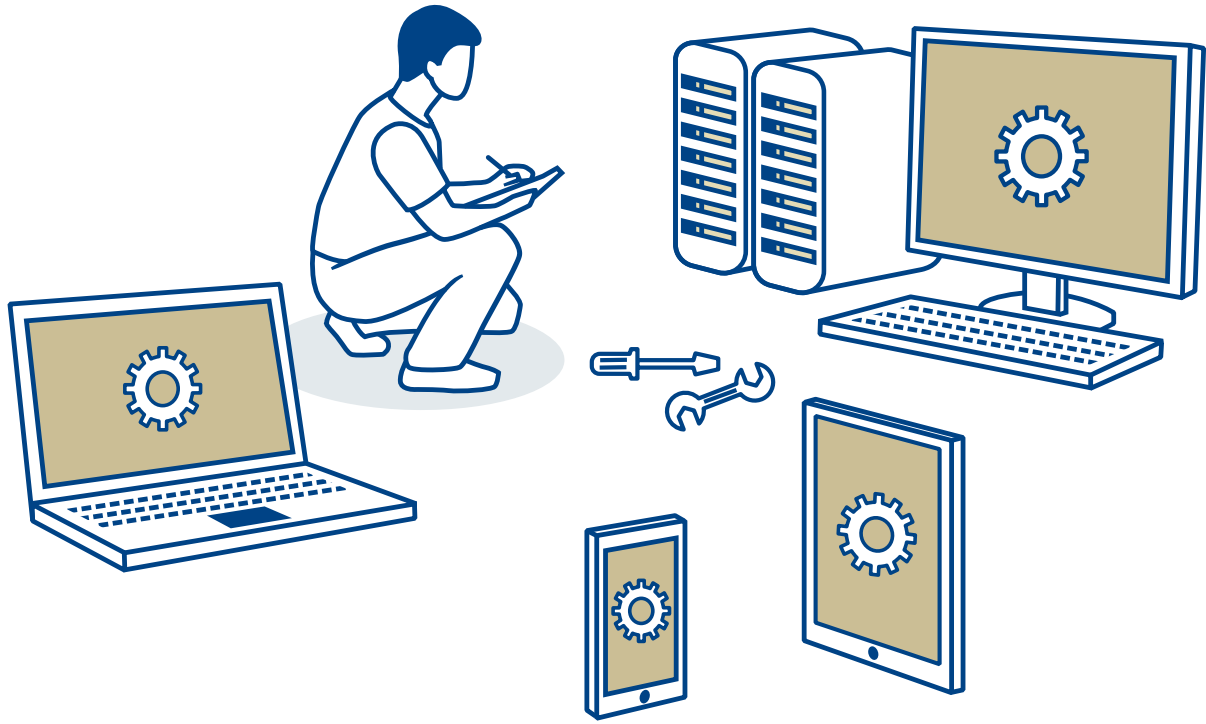


Bleibt der Zugriff auf das Computernetzwerk einer Arztpraxis ungeschützt, können sich unberechtigte Dritte (beispielsweise kriminelle Hacker) Zugang zum Netzwerk verschaffen, die Kommunikation abhören oder Daten entwenden.

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 Virens Scanner 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.

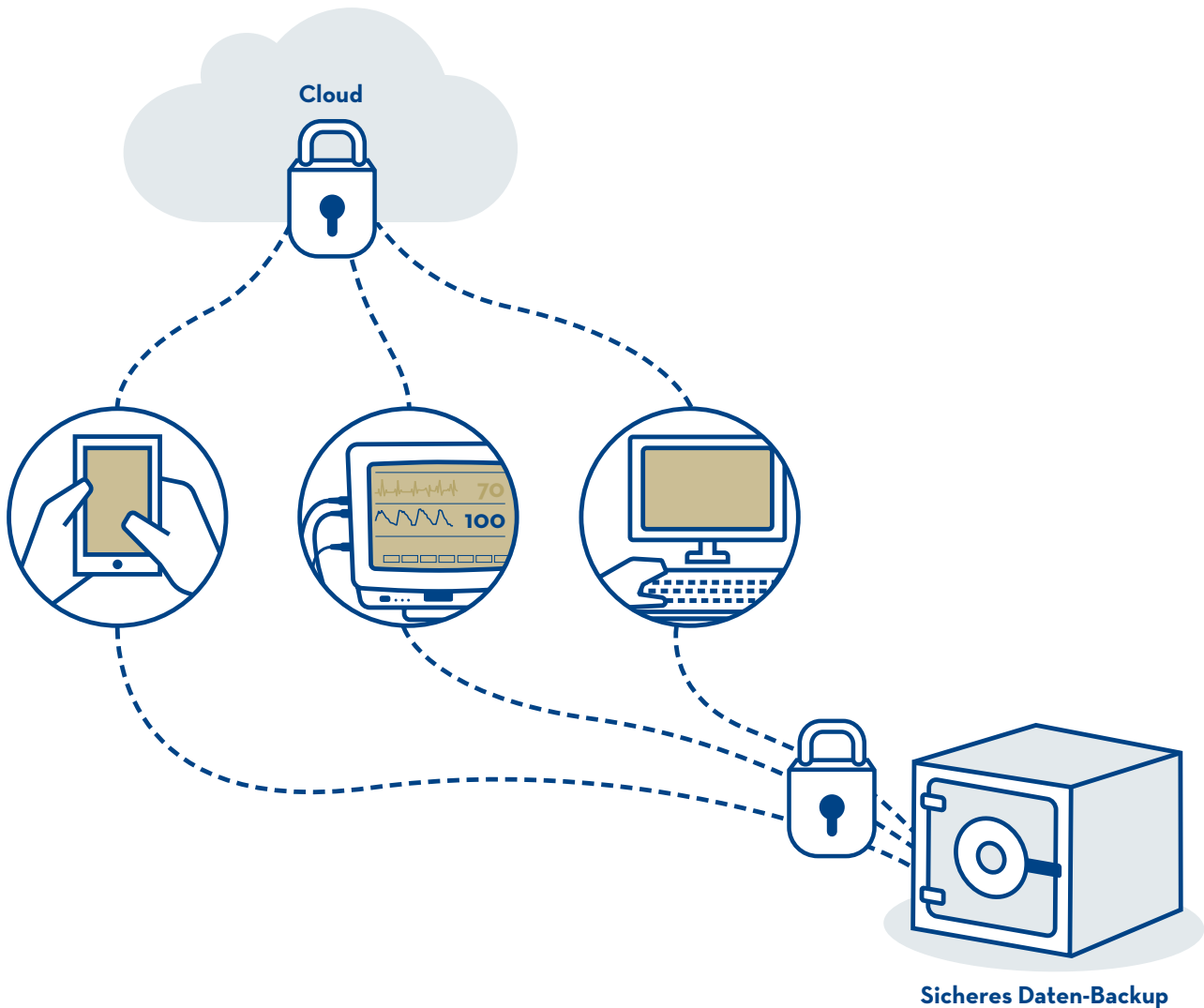
ICT-Umgebung konfigurieren und warten



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 sicherheitsrelevanten Konfigurationen vorgenommen (härten) werden können.

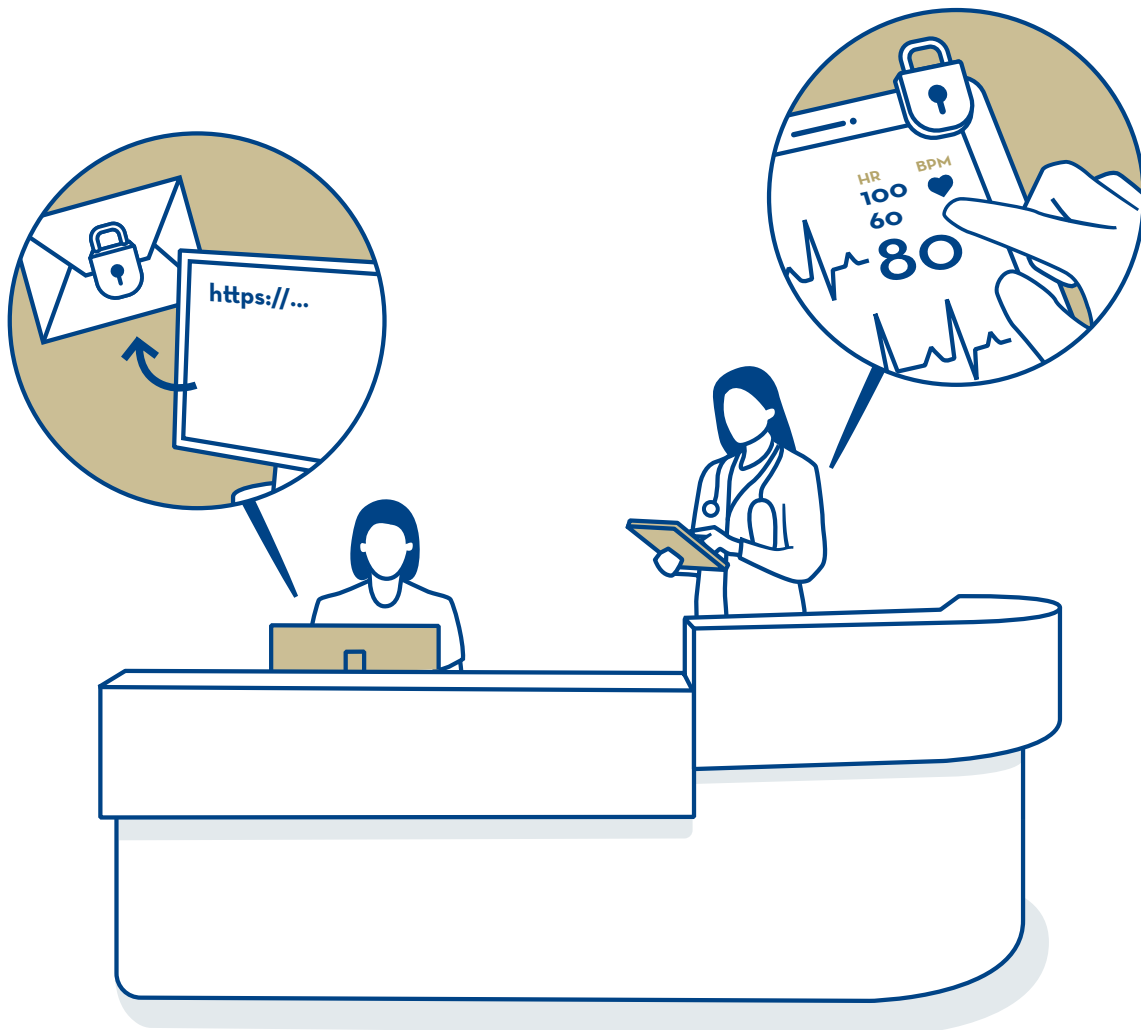
ICT-Systeme sollten mit verschiedenen Massnahmen «gehärtet» werden, zum Beispiel durch automatische Installationen von Sicherheitsupdates, Verschlüsselung der Festplatten oder durch die Verwendung sicherer Passwörter für Benutzerkonten. Zur betrieblichen Überwachung sollten ICT-Systeme und eingesetzte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



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 gesichert werden.

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

Die Datensicherung in der Cloud unterliegt strengen Vorschriften. Ausserdem müssen die gesetzlichen Anforderungen des Datenschutzgesetzes und der Geheimhaltungspflicht eingehalten werden.



Sensible Daten 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 diese 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.

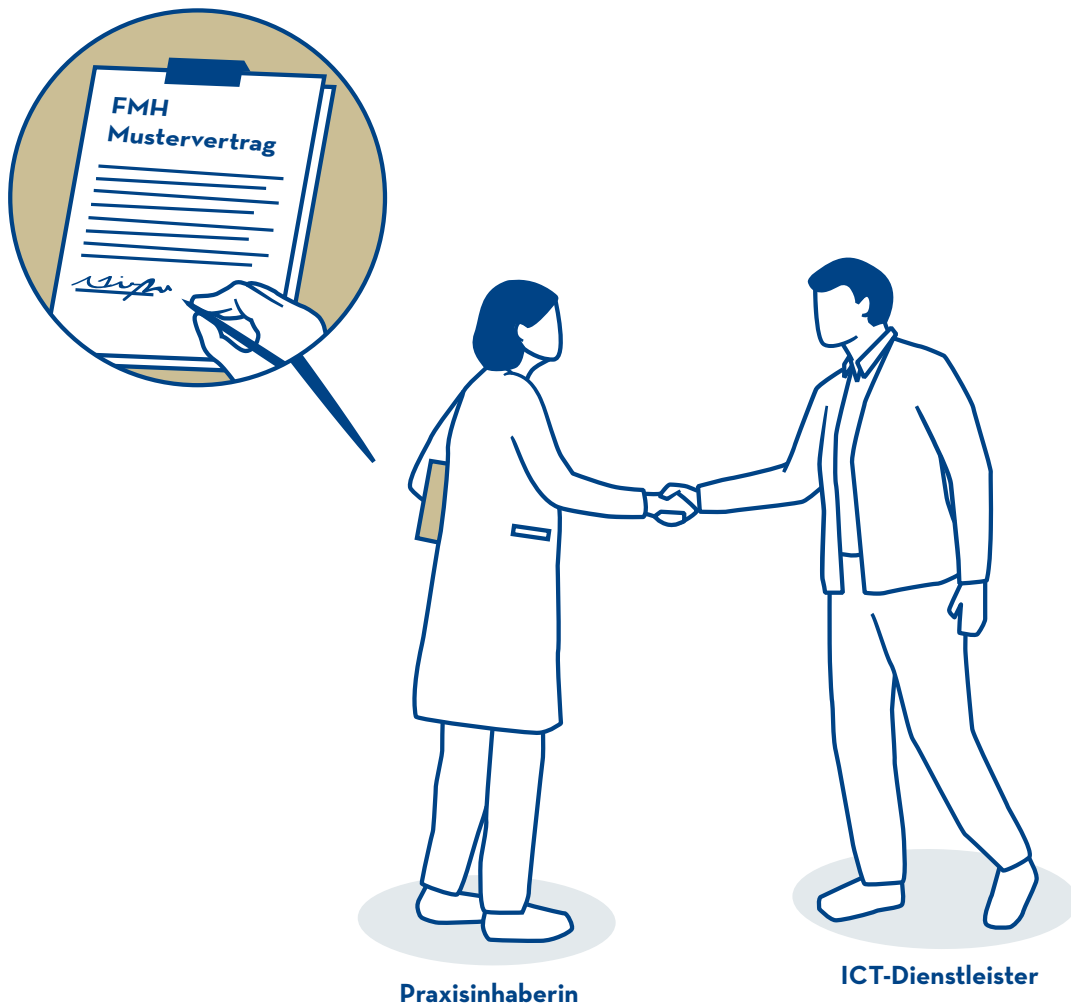
E10 Vorkehrungen für die Behandlung von Sicherheitsvorfällen treffen



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.

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 gelten die allgemeinen Geschäftsbedingungen der Schweizerischen Informatikkonferenz (SIK) für ICT-Dienstleistungen und für Leistungsvereinbarungen mit Cloud-Anbietern der Rahmenvertrag der FMH 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

www.fmh.ch

