PIS in der Cloud - was gilt es zu beachten?

Dr. Reinhold Sojer

Leiter Digitalisierung / eHealth FMH

Courant normal?

RTS Info

Plus de 40'000 dossiers de patients ont été diffusés mercredi sur le darkweb. Une enquête de la RTS révèle que le piratage pourrait être plus important que prévu: il concernerait d'autres cabinets en Suisse romande.

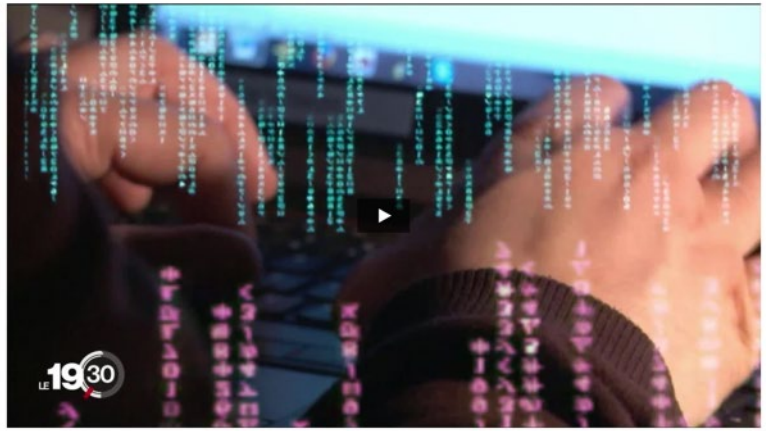
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Hackerangriffe auf Arztpraxen in der Romandie

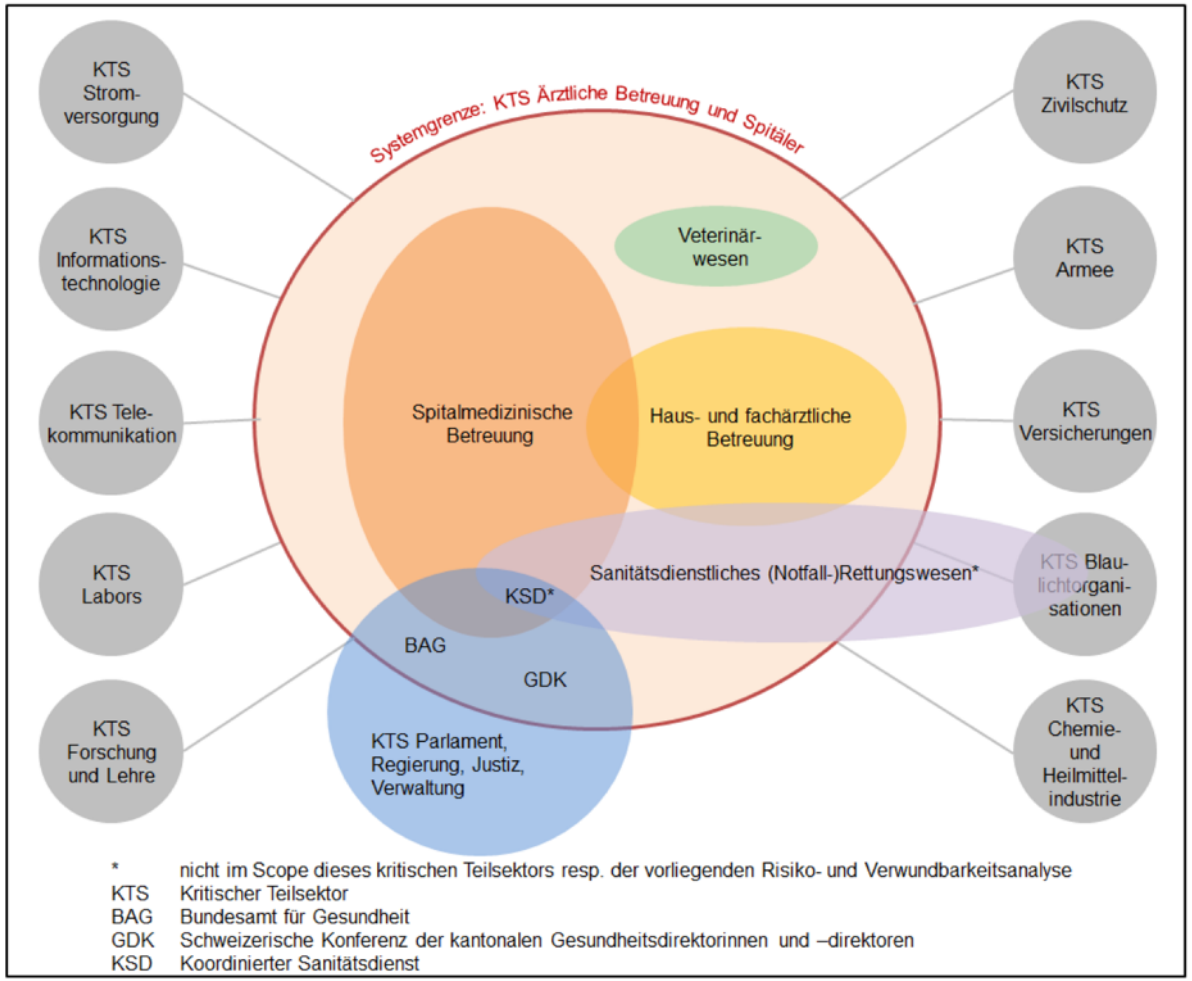
31.03.2022 - Gestern wurde bekannt, dass Hacker mehreren Arztpraxen in der Romandie Patientendossiers entwendet und eine grosse Menge medizinischer Daten im Darknet publiziert haben. Der EDÖB steht mit den fraglichen Praxen in Kontakt und erwartet, dass die betroffenen Patientinnen und Patienten umfassend informiert werden. Der Vorfall ist ein erneuter Hinweis darauf, dass die besonders schützenswerten Gesundheitsdaten in der Schweiz ungenügend geschützt sind.

Après Neuchâtel, d'autres médecins romands pourraient être concernés par des fuites de données



Une cyberattaque contre trois cabinets médicaux neuchâtelois pourrait concerner d'autres médecins en Suisse romande / 19h30 / 2 min. / le 31 mars 2022

Courant normal?

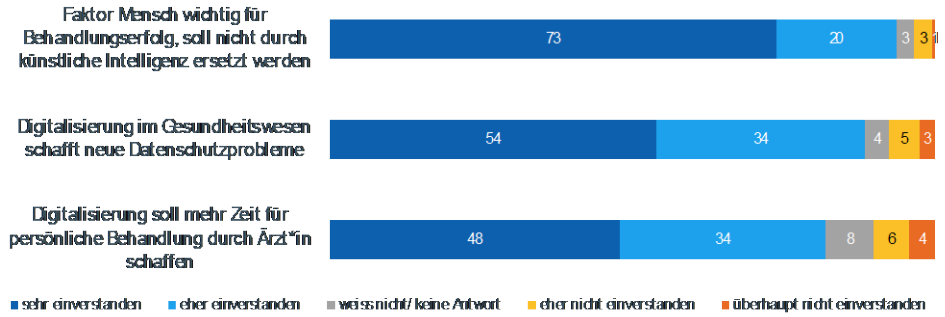


Courant normal?

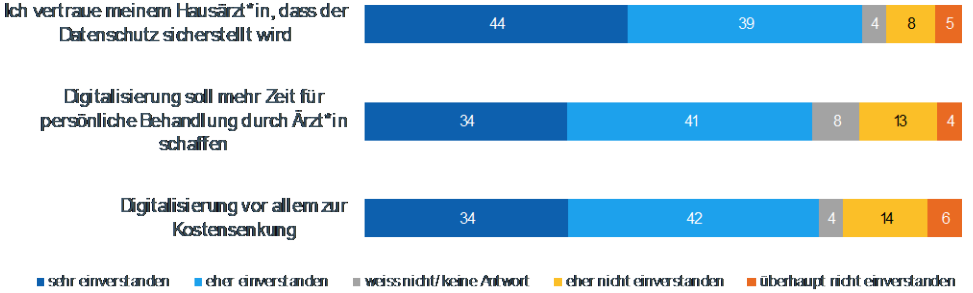
Jede Haftung des Providers oder seiner Erfüllungsgehilfen für andere oder weitergehende Ansprüche und Schäden, insbesondere Ansprüche auf Ersatz von mittelbaren, indirekten oder Folgeschäden, entgangenen Gewinn, entgangener Nutzung, nicht realisierten Einsparungen, Verdienst-, Betriebs- oder Produktionsausfall unabhängig von ihrem Rechtsgrund ist ausdrücklich ausgeschlossen.

Wer ist in der Pflicht?

© gfs.bern, FMH Digital Trends Survey, Oktober/November 2020 (N = 507)



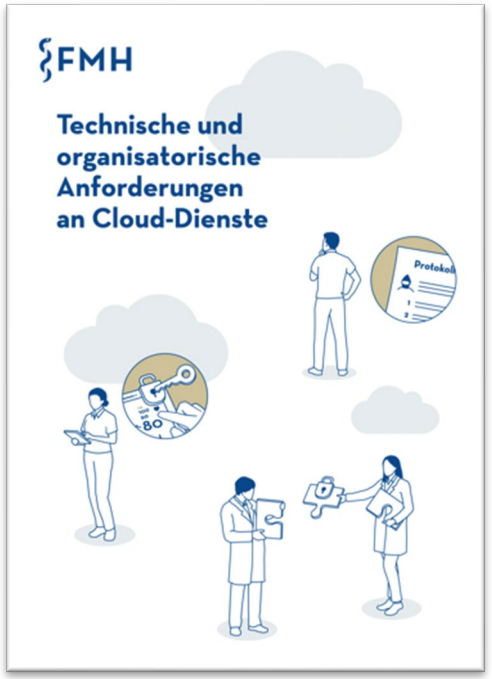
© gfs.bern, FMH Digital Trends Survey, Oktober/November 2020 (N = 2096)



Datenbearbeitung durch Dritte

- Die Sorgfaltspflicht des Arztes oder der Ärztin beginnt bereits bei der Auswahl eines Dienstleisters. Dieser muss grundsätzlich in der Lage sein, die datenschutzrechtlichen Anforderungen zu erfüllen.
- Probleme ergeben sich insbesondere bei Standardprodukten, wo kein Einfluss auf den Anbieter genommen werden kann und sich die Vertragsbedingungen durch die Akzeptanz Allgemeiner Geschäftsbedingungen (AGB) umfassend festgelegt werden.
- Es ist sicherzustellen, dass der Dritte die Daten nicht zu eigenen Zwecken verwendet, sondern nur so wie der Auftraggeber es ihm auferlegt hat.
- Auch das Berufsgeheimnis ist gegenüber dem Dritten zu wahren. In vielen Fällen kann der Dritte nicht als Hilfsperson des Arztes oder der Ärztin betrachtet werden, weshalb der Geheimnisschutz mit technischen Massnahmen (Verschlüsselung) zu gewährleisten ist.

Hilfestellungen der FMH



Technische und organisatorische Anforderungen an Cloud-Dienste

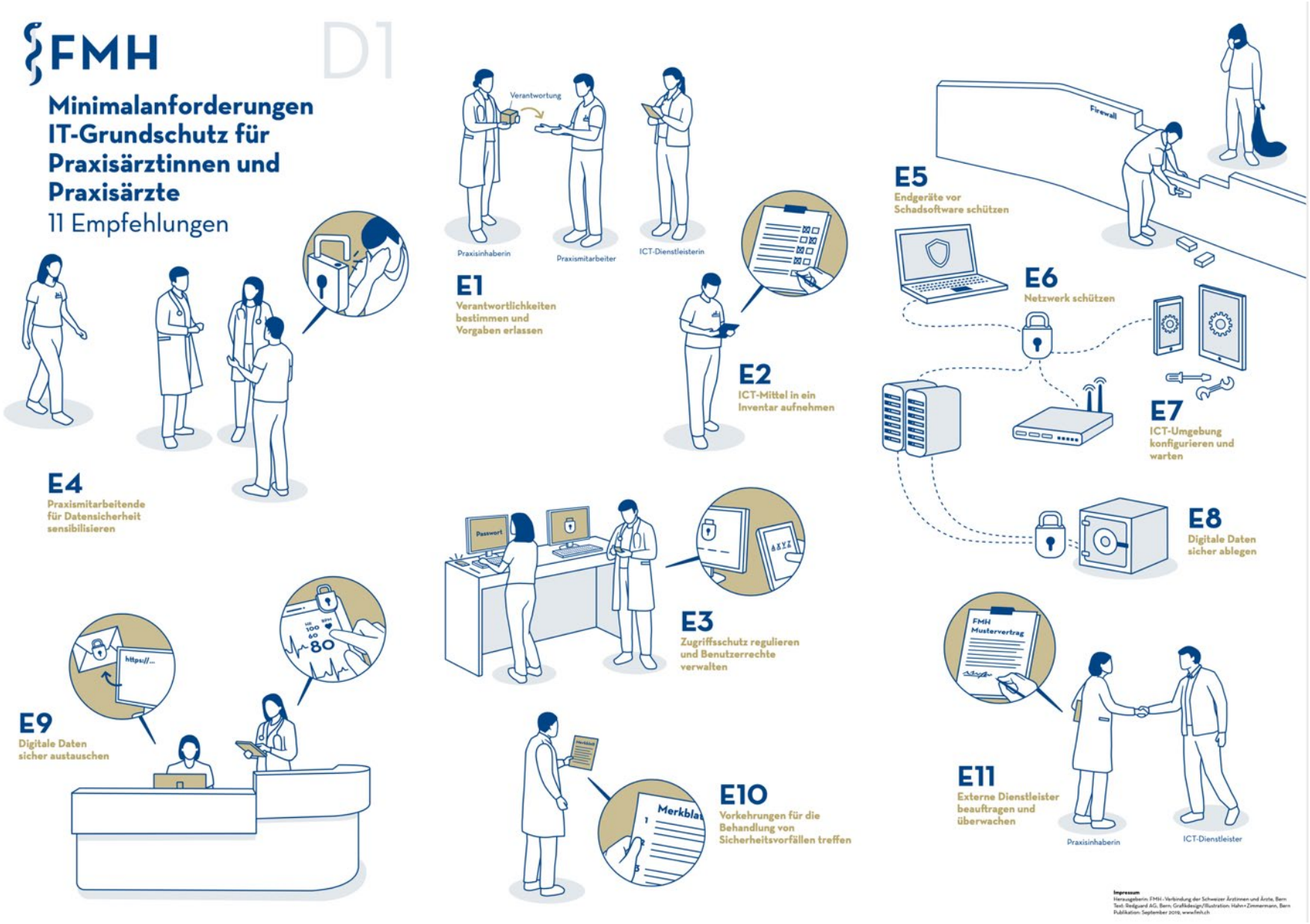
Minimalanforderungen IT-Grundschutz

FMH Rahmenvertrag für Cloud-Dienste

Leitfaden Microsoft 365 in Artpraxen
Publikation Q4/2022

FMH Newsletter Cybersicherheit

IT-Grundschutz Empfehlungen der FMH



Datenschutz- und Sicherheit in der Arztpraxis

Datenschutz- und Sicherheit in der Arztpraxis

Cloud-Dienste

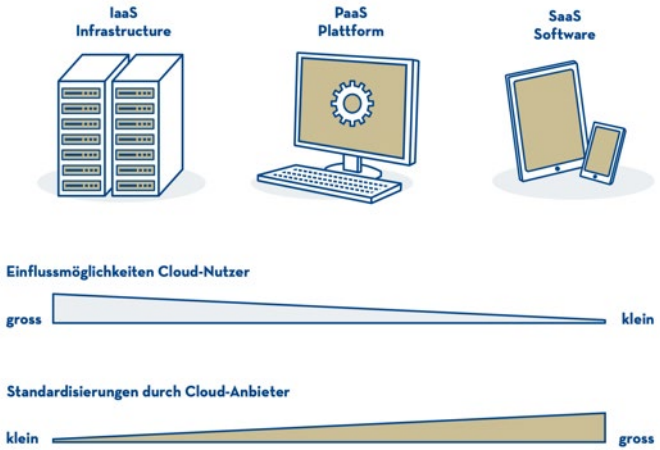
Cloud-Servicemodell

- Legt fest, welchen Umfang die Dienstleistungen eines Cloud-Anbieters haben. Mit zunehmendem Umfang der bereitgestellten Cloud-Dienste steigen der Verantwortungsbereich und die Einflussmöglichkeiten des Cloud-Nutzers auf die Infrastruktur für die Informations- und Kommunikationstechnologie.
- Software-as-a-Service (SaaS)
  - Bereitstellung einer vollwertigen Applikation, welche durch den Cloud-Anbieter bewirtschaftet und verwaltet wird.
  - Nutzer einer SaaS-Lösung können mithilfe eines Webbrowsers oder einer Applikation auf dem Endgerät auf Anwendungen von Dritten zugreifen.
- Platform-as-a-Service (PaaS)
  - Umfassen eine komplette Plattform zur Entwicklung, zum Betrieb oder zur Verwaltung von Applikationen, die durch den Cloud-Anbieter verwaltet wird.
- Infrastructure-as-a-Service (IaaS)
  - Umfassen Ressourcen für eine komplette Informatikinfrastruktur, wie zum Beispiel Rechenleistung, Netzwerke oder Speicher.

Verantwortlichkeiten

- Unterschiedliche Verantwortlichkeiten der Betriebsumgebung, einschliesslich ihrer Anwendungen, physischer Server, Benutzerkontrollen oder die physikalische Umgebung.

- Ungeachtet des Servicemodells sind Nutzerinnen und Nutzer bzw. die datenschutzrechtlich Verantwortlichen bei Cloud-Diensten stets für diejenigen Schutzobjekte verantwortlich, die unter ihrer direkten Kontrolle sind. Die Verwendung der Informationen und Daten verbleibt stets beim Verantwortlichen.



Verantwortlichkeiten

Der Verantwortliche ist derjenige, der über den Zweck und die Mittel der Datenbearbeitung entscheidet (Art. 5 Abs. 1 lit. j revDSG).

Verantwortlichkeiten	SaaS	PaaS	IaaS
Daten	○	○	○
Anwendung	●	○	○
Laufzeitumgebung/Container	●	●	○
Betriebssystem	●	●	○
Virtualisierungsschicht	●	●	●
Bereitstellung und Betrieb Hardware	●	●	●
Physische Sicherheit	●	●	●

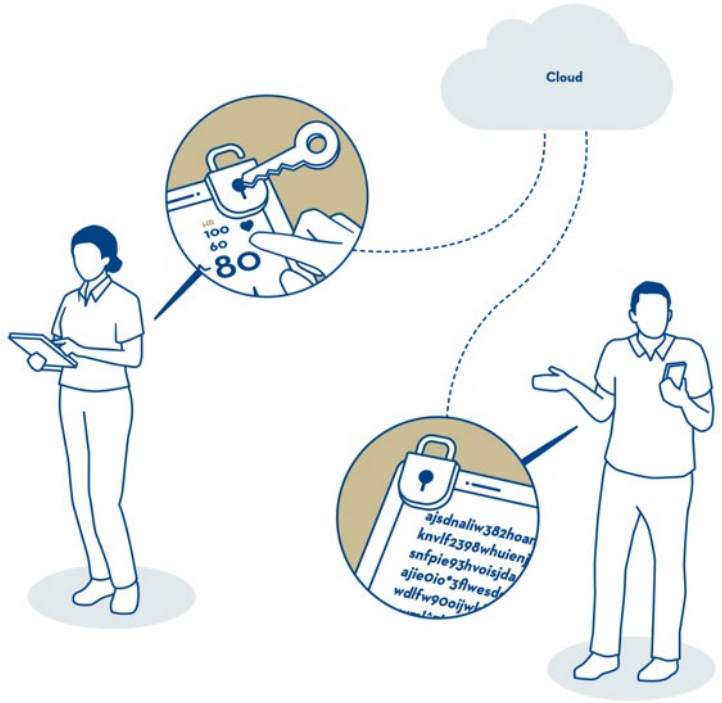
○ Cloud-Nutzer ● Cloud-Anbieter

Datensicherheit und Datenschutz durch Technik

- Art. 8 des neuen DSG verlangt eine dem Risiko angemessene Datensicherheit, die durch geeignete technische und organisatorische Massnahmen zu gewährleisten ist.
- Mit den technischen und organisatorischen Massnahmen der Datensicherheit sind insbesondere die Schutzziele der Vertraulichkeit, der Integrität und Verfügbarkeit der Personendaten sowie die Authentizität und der Nachvollzug der Datenbearbeitungen zu erreichen.
- Die Beurteilung der Angemessenheit der Datensicherheit ergibt sich aus einer Risikobetrachtung. Die Datensicherheit bezweckt den Schutz der Personendaten und damit mittelbar den Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen.

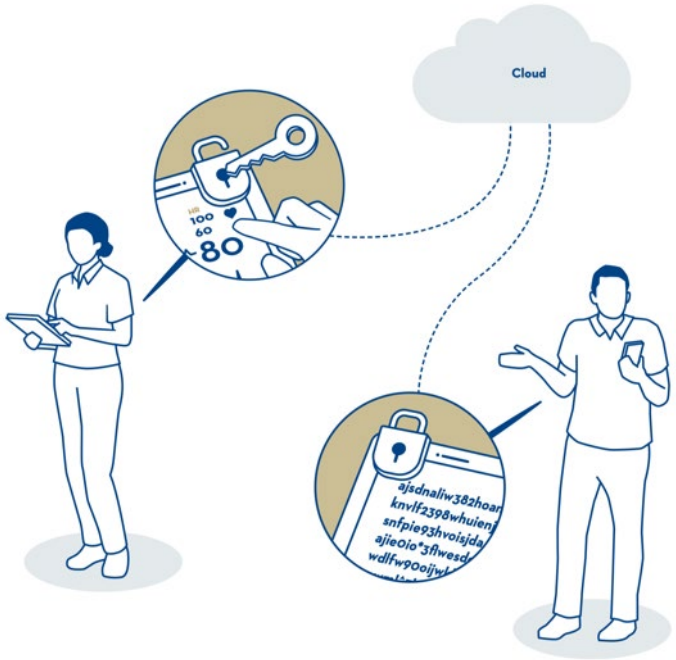
Verschlüsselung und Schlüsselmanagement

Gespeicherte Daten (Data at Rest) wie auch die übertragenen Daten (Data in Transit) müssen mit kryptografischen Verfahren entsprechend geschützt werden. Ebenso muss die Kommunikation über alle ein- und ausgehenden Verbindungen zur und von der Cloud-Infrastruktur einschliesslich der Schnittstellen innerhalb der Cloud-Infrastruktur authentisiert und verschlüsselt erfolgen.



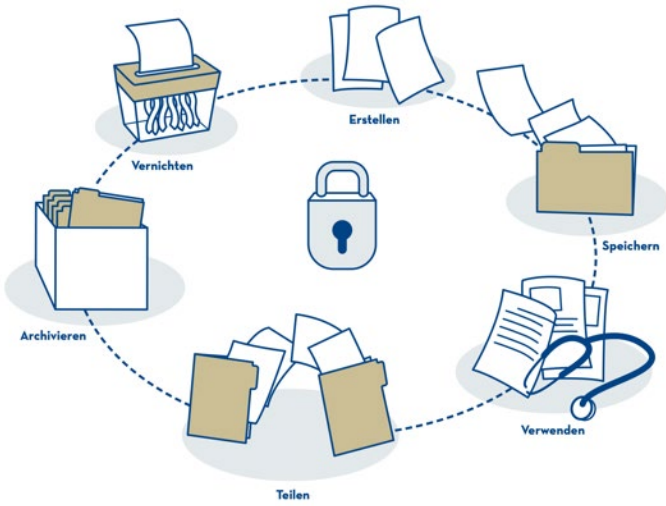
Verschlüsselung und Schlüsselmanagement

Anforderungen		
A-6.01	M	**Speicherverschlüsselung der Inhaltsdaten (Data at Rest)** Die Daten beim Cloud-Anbieter müssen in jeder Phase des Lebenszyklus der Daten verschlüsselt gespeichert werden. Die für die Verschlüsselung verwendeten privaten Schlüssel dürfen ausschliesslich dem Cloud-Nutzer bekannt gemacht werden. Der Cloud-Anbieter darf keine Möglichkeiten haben, die Daten einzusehen.
A-6.02	M	**Schlüsselmanagement** Es muss ein effektives Recovery-Verfahren existieren, um im Notfall die verschlüsselten Daten wiederherzustellen. Falls es notwendig ist, den Schlüssel wiederzubeschaffen, existiert ein effektives Recovery-Verfahren. Eine Möglichkeit ist es, dafür Teilschlüssel an verschiedene Akteure zu verteilen, welche im Tresor verwahrt werden und im Notfall nach einem Konsensverfahren verwendet werden.
A-6.03	M	**Transportverschlüsselung (Data in Transit)** Die Kommunikation muss über ein aktuelles Internet-Standardprotokoll erfolgen. Die Kommunikation über alle ein- und ausgehenden Verbindungen zur und von der Cloud-Infrastruktur einschliesslich der Schnittstellen innerhalb der Cloud-Infrastruktur muss authentisiert und verschlüsselt erfolgen. Die Kommunikation muss mindestens mit TLS 1.2 verschlüsselt werden.
A-6.04	M	**Verschlüsselungsverfahren** Es müssen Verschlüsselungsverfahren gemäss den aktuellen Best-Practice-Ansätzen eingesetzt werden. Die nachfolgenden Verfahren oder gleichwertige Verfahren sind zugelassen. – Hashing-Verfahren: SHA2-256, SHA2-384, SHA2-512 oder SHA3-256, SHA3-384, SHA3-512 – Symmetrische Verfahren: AES-256 – Asymmetrische Verfahren: RSA-2048, ECDSA-224 oder Ed25519 Adaptierte Verfahren oder Eigenentwicklungen sind nicht zugelassen. Es sind aktuelle Protokolle zu verwenden. Protokolle mit bekannten kritischen Sicherheitslücken dürfen nicht eingesetzt werden.



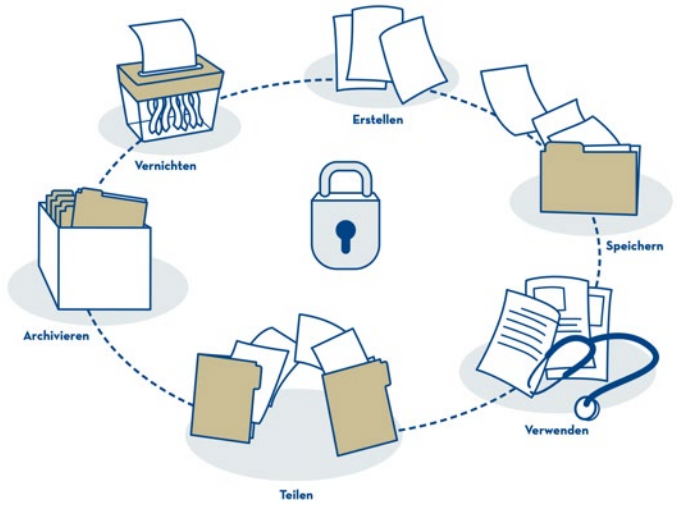
Verschlüsselung und Schlüsselmanagement

- Die Daten beim Cloud-Anbieter müssen in jeder Phase des Lebenszyklus der Daten verschlüsselt gespeichert werden
  (→ effektives Recovery-Verfahren).
- Erstellung und Verwaltung von krypto-graphischen Schlüsseln in spezialisierten Hardware-Geräten mit kryptographischen Funktionen (HSM)
- «*Bring your own key*» (BYOK) ermöglicht es Unternehmen, das Schlüsselmanagement vollständig zu kontrollieren. Da die Datenverschlüsselung immer noch in der Cloud stattfindet, sind die Daten im Speicher bis zur Verschlüsselung unverschlüsselt.



Verschlüsselung und Schlüsselmanagement

Um das Risiko eines durch den Cloud-Dienstanbieter beabsichtigten Datenzugriffes zu minimieren, können Verfahren wie «*Hold your own key*» (HYOK) eingesetzt werden, bei dem die Daten vor der Übermittlung zum Dienstanbieter verschlüsselt werden.



Information Governance und Risikomanagement

- DSG Art. 10a Datenbearbeitung durch Dritte

> [1] Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn:
>
> a. die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte; und
> b. keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.

- Arztpraxis erlässt Vorgaben, Prozesse und interne Kontrolle zur Validierung u. a. von:
  - Zugriffskontrollen,
  - Erfassen, Speichern und Löschen von Daten,
  - Einhaltung regulatorischer Anforderungen,
  - Risikomanagement
  - weitere
- Bei der Auslagerung der Datenbearbeitung in die Cloud verbleibt die Governance stets beim Unternehmen (Arztpraxis). Die Governance kann nicht ausgelagert werden, selbst wenn externe Anbieter einbezogen werden.

Information Governance und Risikomanagement

Bei der Auswahl des Anbieters ist insbesondere zu beurteilen:

- Die Einhaltung der datenschutzrechtlichen Grundsätze durch den Verantwortlichen,
- beim Einbezug von Dritten (z.B. Cloud-Lösungen) die klare Festlegung der gegenseitigen Rechte und Pflichten,
- bei Auslandsbezug die Gewährleistung eines gleichwertigen Datenschutzes,
- das Vorliegen von dem Risiko angemessenen technischen und organisatorischen Massnahmen für die Sicherheit der Daten (Art. 6 revDSG),
- Vertragliche Vereinbarung mit dem Dritten (Art. 9 revDSG),
- Einhaltung der Grundsätze bei Bekanntgabe von Personendaten ins Ausland (Art. 16f revDSG).

Information Governance und Risikomanagement

Einhaltung der datenschutzrechtlichen Grundsätze

- Konformität gegenüber den Vorgaben aus dem Schweizer DSG und der EU DSGVO, soweit anwendbar.
- Nachweis eines Informationssicherheitsmanagementsystems (mit einer Zertifizierung nach ISO/IEC 27001 wird lediglich das ISMS zertifiziert und nicht der Grad der Informationssicherheit).

Gegenseitige Rechte und Pflichten

- Sind abhängig vom gewählten Servicemodell festzulegen.

Wirksamkeit des Kontrollsystems

- Prüfberichte nach dem Standard ISAE3402, SSAE und SOC 2 im Bereich des Risikomanagements für Cybersicherheit.

Information Governance und Risikomanagement

Anforderungen		
A-7.01	S	**Transparenz Zertifizierungen** Der Cloud-Anbieter soll vorhandene Zertifikate und vorhandene Auditberichte zur Verfügung stellen: – Zertifizierung nach ISO/IEC 27001 – Prüfberichte nach ISAE340, SSAE16 oder SOC2-Berichte – von den zuständigen Datenschutzbehörden akzeptierter Nachweis über die Einhaltung des Datenschutzes
A-7.02	M	**Auditrecht** Sofern keine Auditberichte von Drittparteien vorgelegt werden können, muss dem Cloud-Nutzer durch den Cloud-Anbieter vertraglich zugesichert werden, dass der Cloud-Nutzer selbst oder durch einen beauftragten Dritten die Durchführung von Audits oder von technischen Überprüfungen (z. B. Penetrationtests) vornehmen kann.
A-7.03	M	**Service Level Agreement (SLA)** Das SLA zwischen Cloud-Anbieter und Cloud-Nutzer muss das Service Level für den Endkunden (die Arztpraxis) abdecken.
A-7.04	S	**SLA-Reporting** Der Cloud-Anbieter soll auf Anfrage einen Bericht zur Verfügung stellen, in welchem mindestens folgende Angaben enthalten sind: – Kennzahlen über die definierte Verfügbarkeit, Performance oder Datenkapazität des Dienstes – Ansprechzeiten und Reaktionszeiten der Serviceorganisation des Anbieters – Definition von Wartungsfenstern und weiteren geplanten Ausfallzeiten – Definition von Frequenz und Qualität der Wartungsprozesse – Definition der gelieferten Artefakte wie Testberichte oder Backupmedien – Massnahmen und Konsequenzen bei Nichteinhaltung der Vereinbarungen – Ereignisse und Vorfälle in der Berichtsperiode
A-7.05	M	**Subdienstleister** Der Cloud-Anbieter muss alle Subdienstleister gegenüber dem Cloud-Nutzer sowie ein Nachweis der Geheimhaltungsverpflichtung offenlegen.[3]
A-7.06	M	**Notifikation bei geplanten Ausfällen** Der Cloud-Anbieter muss den Cloud-Nutzer über geplante Ausfälle mindestens zehn Arbeitstage im Voraus per E-Mail informieren.

Fazit

- Aus Sicht der Informationssicherheit sind mit der Bearbeitung der Daten von Arztpraxen in der Cloud Themen wie Verschlüsselung, Zugriffskontrollen, Governance sowie Verfügbarkeit, Backup oder Disaster Recovery zu klären.
- Im Bereich der Rollen und Zuständigkeiten ist zu definieren, welche Aufgaben durch die Nutzer / Kunden (Ärztinnen und Ärzte) und welche durch den Cloud-Anbieter wahrgenommen werden (die Verantwortung für den Schutz der Daten bleibt stets bei den Ärztinnen und Ärzten)
- Im Servicemodell «Software-as-a-Service» werden oftmals Vereinbarungen durch den Cloud-Anbieter getroffen, die nur im Ganzen akzeptiert oder abgelehnt werden können.

Herzlichen Dank!