Merkblatt
Technisch-organisatorische Maßnahmen zum Datenschutz

Hinweis: Die nachfolgenden Fragen und Antworten sind sorgfältig erstellt, jedoch nicht durch die Aufsichtsbehörden geprüft worden. Die Landesärztekammer Baden-Württemberg kann daher keine Haftung für die Fragen und Antworten übernehmen. Der Fragenkatalog ersetzt keinesfalls eine Beratung durch einen Rechtsanwalt.

Grundsätzlich geht es darum, sich in einer Praxis mit den nachfolgend aufgeführten Punkten auseinander zu setzen und so gut wie möglich auf die eigenen Praxisgegebenheiten anzupassen. Die DSGVO schreibt diese Maßnahmen nicht im Detail vor, sondern spricht in Art. 32 davon, "Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken … trifft der Verantwortliche geeignete technische und organisatorische Maßnahmen…".

Organisatorische Maßnahmen

1. Wie sollte der Empfangsbereich der Praxis gestaltet sein?

Der Empfangsbereich sollte so gestaltet sein, dass eine Einsichtnahme auf Bildschirme durch wartende Patienten verhindert wird. Für die Zeiträume, in denen der Empfang nicht besetzt ist, kann mit Bildschirmschonern und Passwortsperre gearbeitet werden. Wenn die Räumlichkeiten es ermöglichen, sollte eine Diskretionszone vor dem Empfang eingerichtet werden. Der vor der Rezeption stehende Patient sollte keinen Einblick auf herumliegende Dokumente im Rezeptionsbereich haben. Es sollten im Rezeptionsbereich keine Telefongespräche geführt werden, wenn Patienten mithören können. Vertrauliche Gespräche sollten in einem separaten Raum stattfinden.

2. Was ist für den Wartezimmerbereich zu beachten?

Das Wartezimmer sollte ein möglichst abgeschlossener Raum sein, um den Wartenden keine Möglichkeit zu geben, Patientengespräche oder Telefonate an der Rezeption mitzuhören. Im täglichen Betrieb sollte darauf geachtet werden, dass die Türe zum Wartezimmer geschlossen ist. Offene Wartebereiche neben der Rezeption sollten vermieden werden.

3. Was ist im Behandlungszimmer oder einem eventuell vorhandenen Besprechungsraum zu beachten?

Bevor ein Patient das Zimmer betritt, sollten Karteikarten der vorher behandelten Patienten nicht mehr sichtbar herumliegen. Auch die Monitore sollten keine Röntgenbilder oder Akteninhalte des vorher behandelten Patienten mehr anzeigen. Ein Patient sollte nach Möglichkeit nicht allein im Zimmer sitzen, um unbefugtes Agieren an PCs (USB Slots, CD Laufwerke) oder unbefugtes Aufrufen von Daten zu verhindern.

4. Was ist bei der Kommunikation innerhalb der Praxis zu beachten?

Es sollten keine Patientennamen in Gesprächen (sowohl persönlich als auch fernmündlich) erwähnt werden, wenn die Möglichkeit besteht, dass diese Gespräche von Dritten mitgehört werden können.

Technische Maßnahmen

Grundsätzlich kann die Landesärztekammer, was die Hard- und Softwareausstattung in den Praxen zur Erfüllung der Vorschriften der EU-DSGVO betrifft, nur allgemeine Empfehlungen geben. Die Umsetzung sollte bei fehlender Kenntnis zusammen mit dem IT Dienstleister durchgeführt werden.

Technische Maßnahmen -Software-

5. Wie sollen Daten in der Praxis gesichert werden?

Daten sollten je nach technischen Möglichkeiten zentral über einen Server verwaltet werden. Über diesen Server können Datenzugriffe und Backups einfacher und zuverlässiger verwaltet werden. Es sollte für die Daten in der Arztpraxis ein Sicherungssystem (Backup) installiert sein, um bei einem Datenverlust diese wieder herstellen zu können. Empfehlenswert sind eine tägliche Sicherung, eine wöchentliche und eine monatliche Sicherung auf mehrere transportable Speichermedien. Die Sicherungen sollten verschlüsselt (das bei Verlust des Datenträgers ein Unbefugter keine Zugriff darauf hat) sein und außerhalb der Praxis aufbewahrt werden. Auch eine Sicherung der Daten in eine Cloud ist möglich. Mit der Nutzung derartiger Cloud-basierter IT-Dienste bezüglich personenbezogener Patientendaten sind derzeit allerdings eine Vielzahl rechtlicher Unsicherheiten verbunden, und zwar sowohl im Hinblick auf das Datenschutzrecht als auch die ärztliche Schweigepflicht. Diesbezüglich sei die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene Broschüre “Sichere Nutzung von Cloud-Diensten – Schritt für Schritt von der Strategie bis zum Vertragsende” (abrufbar unter https://www.bsi.bund.de) empfohlen.

In regelmäßigen Abständen sollte überprüft werden, ob die Sicherungen den Datenbestand auch wieder herstellen können. In der Praxis sollte ein Konzept für die Durchführung und Organisation der Datensicherung erarbeitet werden.

6. Was ist beim Einlesen von fremden Wechseldatenträgern (z.B. Fremdröntgenfotos) zu beachten?

Beim Einlesen von externen Wechselmedien (USB-Stick, CD-ROM) sollte vor dessen Benutzung das Virenprogramm den Datenträger auf Schadsoftware prüfen. Entsprechende Weisungen sollten an die Mitarbeiter der Praxis gegeben werden. Die Benutzung privat mitgebrachter Wechselmedien auf Praxishardware sollte den Mitarbeitern untersagt sein.

7. Durch welche Maßnahmen sollten die Patientendaten gegen unbefugten Zugriff geschützt werden?

Es sollte sichergestellt werden, dass die Computer, über die ein Zugriff auf Patientendaten erfolgen kann, durch Passwörter gesichert sind. Passwörter dürfen nur den zugriffberechtigten Mitarbeitern der Praxis bekannt sein. Zu bevorzugen ist, dass jeder zugriffsberechtigte Mitarbeiter über ein eigenes Passwort verfügt. So kann auch nachvollzogen werden, wer, wann auf den Datenbestand zugegriffen hat. Passwörter sollten in regelmäßigen Abständen geändert werden. Sobald ein Mitarbeiter aus der Praxis ausscheidet, sollte dessen Passwort für den Zugriff gesperrt werden. Diese Maßnahmen können in das interne QM der Praxis aufgenommen werden.

8. Was ist bei der Nutzung von Software zu beachten?

Sowohl das Betriebssystem als auch die verwendeten Softwareprogramme sollten regelmäßig mit den vom Hersteller bereitgestellten Updates auf dem aktuellsten Stand gehalten werden. Automatisierte Updateroutinen sind zu präferieren, um keine Updates zu vergessen.

9. Was ist bei der Nutzung von E-Mail-Programmen zu beachten?

Um eine Gefährdung der Praxis-EDV durch E-Mails auszuschließen, empfiehlt das Bundesamt für Sicherheit in der Informationstechnik folgende Maßnahmen:

- ein **Virenschutzprogramm**, das eingehende und ausgehende E-Mails auf Schadprogramme prüft,
- eine **Anti-Spam-Software**, die unerwünschte E-Mails erkennt und aussortiert,
- eine **Anti-Phishing-Software**, die Angriffe abwehrt, bei denen der Benutzer mittels gefälschter E-Mails dazu verführt wird, vertrauliche oder persönliche Daten preiszugeben, und
- eine **Personal Firewall**, die alle eingehenden und ausgehenden Verbindungen filtert.

Darüber hinaus wird empfohlen, eine **E-Mail-Richtlinie** zu erstellen, die beschreibt, wie sich Anwender bei der Nutzung von E-Mail zu verhalten haben. Beispielsweise sollten Dateianhänge nicht unbedacht geöffnet werden, um einer Infizierung mit Schadprogrammen vorzubeugen. Oder es kann ein separater, vom Praxisnetz getrennter PC, für E-Mails genutzt werden oder alle E-Mails nur von einer speziell geschulten Person geöffnet und bearbeitet werden.

10. Was ist bei der Fernwartung durch den Softwareanbieter zu beachten?

Die Fernwartung durch den Anbieter der Praxisverwaltungssoftware ist vorher mit der Praxis abzustimmen. Die Praxis erteilt dann die Freigabe für den Zugriff und muss die Möglichkeit haben, denn Zugriff jederzeit unterbrechen zu können. Während die Fernwartung durchgeführt wird, sollte möglichst die Tätigkeit der Firma auf dem Computer mitverfolgt werden.

11. Was ist bei der Einrichtung eines Fernzugriffs auf die Praxis EDV zu beachten?

Bei einem Fernzugriff auf die Praxis-EDV von z.B. zu Hause aus ist auf eine Zwei-Faktor- Authentifizierung zu achten, um unberechtigte Zugriffe zu vermeiden. Der Zugriff sollte über eine gesicherte Verbindung (VPN-Tunnel) hergestellt werden.

Technische Maßnahmen -Hardware-

12. Was ist bei einem praxisinternen Netzwerk zu beachten?

Der Zugang zum Internet sollte möglichst nur über einen Router mit Firewall erfolgen. Weiter gehende Möglichkeiten sind die Nutzung eines (Proxy) Servers, eines Authentifizierungsverfahrens über den Router oder eines gesonderten PC`s, der die Anbindung des praxisinternen Netzwerkes an das Internet managt und somit für zusätzliche Sicherheit sorgt. Sicher für Internetrecherchen ist natürlich auch ein Stand Alone PC, der keine Verbindung zum Praxisnetzwerk hat. Computer, auf denen Patientendaten gespeichert sind, sollten nicht direkt mit dem Internet verbunden sein, damit ein Zugriff von außen nicht ermöglicht wird.

Bei der Betreibung eines WLANs in der Praxis sollte darauf geachtet werden, dass das Netzwerk vom eigentlichen Praxisnetzwerk getrennt wird (VLANs) und weiterhin über eine ausreichende Verschlüsselung verfügen (WPA2-Verfahren).

13. Was ist bei der Entsorgung von Patientenunterlagen zu beachten?

Die Vernichtung von Akten ist in der DIN 66399 geregelt. Sie gilt unabhängig davon, auf welchem Medium die Daten gespeichert sind (Papier, CD, DVD, USB-Stick, Röntgenfilm etc.) Die Norm differenziert sich in drei Schutzklassen (1-3) und daraus ergeben sich die Sicherheitsstufen (1-7). Es ist zu empfehlen, Gesundheitsdaten von Patienten der Schutzklasse 3 (Sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten) und daraus ergebend mindestens der Sicherheitsstufe 4 (Besonders sensible und vertrauliche Daten sowie personenbezogenen Daten, die einem erhöhten Schutzbedarf unterliegen) zuzuordnen.

Bei der Wahl eines Entsorgungsunternehmens sind diese Vorgaben zu berücksichtigen.

Bei der Entsorgung von PCs (HDD, SSD) ist die Effektivität einer softwaremäßig durchgeführten Löschung umstritten. Auch bei der physische Zerstörung der Festplatte ist darauf zu achten, dass die Daten wirklich nicht mehr lesbar sind. Es gibt auch zertifizierte Entsorgungsfirmen, die gegen Entgelt Datenträger unlesbar machen und dafür auch haften.

Auch bei der Entsorgung oder Rückgabe von geleasten Druckern ist darauf zu achten, dass im Speicher abgelegte Daten gelöscht werden.

14. Was ist bei der Aufstellung der Hardware zu beachten?

Der Server sollte - wenn möglich - vor Fremdzugriffen durch einen abschließbaren Serverraum oder einen abschließbaren Serverschrank gesichert sein. Ansonsten sollte er sich zumindest nicht in einem sichtbaren und für den Patienten zugänglichen Bereich befinden.

Auch die Arbeitsstationen sind besser in einem Schrank (aber Achtung: Kühlung ermöglichen) als frei zugänglich aufzustellen. Vorhandene USB Eingänge und CD/DVD Laufwerke sollten hard- oder softwareseitig verriegelt sein.

Bei Fragen steht die zuständige Bezirksärztekammer zur Verfügung:

Nordbaden
Tel. 0721 16024-0
Fax 0721 16024-222
E-Mail:
baek-nordbaden@baek-nb.de

Südbaden
Tel. 0761 600-470
Fax 0761 892-868
E-Mail:
kontakt@baek-sb.de

Nordwürttemberg
Tel. 0711 76981-0
Fax 0711 76981-500
E-Mail:
info@baek-nw.de

Südwürttemberg
Tel. 07121 917-0
Fax 07121 917-2400
E-Mail:
zentrale@baek-sw.de