6 Informationssicherheit und Datenschutz in der Arztpraxis

In Ihrer Arztpraxis müssen Sie besondere Vorkehrungen treffen, um Informationen, welche sich auf Ihre Patienten beziehen, ausreichend zu schützen. Dies ist zur Einhaltung der ärztlichen Schweigepflicht aus straf- und haftungsrechtlichen Gründen unerlässlich. Gleichzeitig ist sicherzustellen, dass behandlungsrelevante Informationen des Patienten für die berechtigten Praxismitarbeiter verfügbar sind, wenn sie benötigt werden.

Informationen können in vielen Formen vorliegen. Sie können auf Papier ausgedruckt, geschrieben, elektronisch gespeichert, auf dem Postweg oder elektronisch übertragen und in Gesprächen oder Telefonaten weitergegeben werden. Unabhängig von der Form und dem Speicher- sowie Transportmedium müssen Informationen in der Arztpraxis jederzeit angemessen geschützt werden und trotzdem im Behandlungsfall den befugten Mitarbeitern zur Verfügung stehen. Die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen zu wahren, ist das Ziel der Informationssicherheit und wird durch Umsetzung geeigneter Maßnahmen erreicht.

Während die im Abschnitt 6.1 beschriebenen Maßnahmen zur Umsetzung von Informationssicherheit unabhängig von der elektronischen Datenverarbeitung zu betrachten sind, beziehen sich die Empfehlungen zu Datenschutz und Datensicherheit im Abschnitt 6.2 auf die EDV und die technische Infrastruktur.

6.1 Maßnahmen zur Gewährleistung von Informationssicherheit

Die Leitung einer Praxis bzw. eines MVZ trägt die Verantwortung für eine sichere, gesetzeskonforme und qualitativ hochwertige Patientenversorgung. Ein verlässliches und sicheres Informationsmanagement ist eines der zentralen Elemente zur erfolgreichen Führung der Praxis oder des MVZ. Durch Überprüfung und Umsetzung der in den folgenden Abschnitten beschriebenen Maßnahmen können Sie die Informationssicherheit in Ihrer Praxis verbessern.

Wie es um die Informationssicherheit Ihrer Praxis steht, können Sie übrigens schnell und unkompliziert mit der elektronischen Checkliste „Mein PraxisCheck“ der KBV testen. Der PraxisCheck im Internet nimmt nur etwa fünfzehn Minuten Zeit in Anspruch und zeigt interaktiv auf, was Praxen in punkto Datenschutz und Datensicherheit noch optimieren können. Wenn Sie sich durch die rund zwanzig Fragen klicken, erhalten Sie sofort einen Ergebnisbericht mit konkreten Hinweisen, Anregungen und Linktipps zu weiterführenden Informationen. Der Online-Selbsttest steht auf der Website der KBV unter http://www.kbv.de/html/mein_praxischeck.php für Sie bereit.

6.1.1 Erhebung und Weitergabe von Patientendaten

Jeder Patient hat ein Recht auf Schutz der Intimsphäre. Hilfreich für eine diskrete Datenerhebung und Kommunikation sind zum Beispiel eine separate Anmeldung, Trennwände oder Hintergrundmusik. Sensibilisieren und schulen Sie das Team entsprechend. Versuchen Sie sich gegenseitig auf Diskretion aufmerksam zu machen, um einer gewissen Betriebsblindheit entgegenzuwirken.

Um die Einsicht auf Computerbildschirme durch Unbefugte zu verhindern, sollten Sie die Bildschirme gegebenenfalls mit Blickschutzfiltern ausstatten und so aufstellen, dass nur befugte Mitarbeiter Sichtkontakt und Zugriff darauf haben. Weisen Sie Ihre Mitarbeiter an, beim Verlassen des Arbeitsplatzes immer den Bildschirmschoner so zu aktivieren, dass er nur durch ein Passwort deaktiviert werden kann.

Patientenbezogene Auskünfte sind beispielsweise Fragen zu Befunden und zu Behandlungen. Sie dürfen nur an berechtigte Personen erteilt werden, deren Identität zweifelsfrei geklärt ist. Dies können - abgesehen vom Patienten selbst - mitbehandelnde Ärzte

oder Angehörige sein. Dazu sollte in der Arztpraxis eine schriftlich formulierte Verfahrensanweisung zum Umgang mit patientenbezogenen Auskünften vorliegen, die allen Mitarbeitern bekannt ist und die von allen angewendet wird.

Am Telefon ist es besonders wichtig, den Anrufer zweifelsfrei identifizieren zu können. Eine einfache Möglichkeit dazu ist die regelhafte Nachfrage nach dem Geburtsdatum, der kompletten Anschrift, dem Versicherungsstatus oder den letzten Ziffern der Versichertennummer. Die Mitarbeiter am Telefon sollten wissen, welche Patientenanfragen sie selbst beantworten dürfen und welche den ärztlichen bzw. psychotherapeutischen Mitarbeitern zur Klärung durchgestellt werden müssen. Letzteres sollte, außer in Notfällen, nicht während der Konsultation anderer Patienten erfolgen. Analoge Regelungen sollten für schriftliche Anfragen (Brief, Fax, E-Mail) getroffen werden.

Innerhalb Ihrer Praxis sollte eine Regelung zur internen Weitergabe von patientenbezogenen Informationen in schriftlicher Form, zum Beispiel mit sogenannten Laufzetteln, allen Mitarbeitern vorliegen, damit diese ihre Verantwortung und Befugnisse kennen.

Die sichere Behandlung von Patienten erfordert eine eindeutige Kommunikation zwischen allen Teammitgliedern der Praxis, um Missverständnisse und sicherheitsrelevante Ereignisse bei Diagnostik und Therapie zu vermeiden. Alle Führungskräfte sollten hinsichtlich der interprofessionellen Kooperation und Abstimmung eine Vorbildfunktion wahrnehmen. Selbstverständlich sind auch hier die datenschutzrechtlichen Belange zu berücksichtigen.

6.1.2 Gesetzliche Fristen bei der Aufbewahrung von Patientenakten und –unterlagen

Die Patientenakten mit allen ärztlichen Aufzeichnungen einschließlich eigener und externer Untersuchungsbefunde sind nach Abschluss der Behandlung mindestens zehn Jahre lang aufzubewahren, soweit nicht nach anderen gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Jede Patientenakte sollte strukturiert geführt und der Inhalt auch bei stichwortartiger Dokumentation nachvollziehbar sein.

Akten können sich aus zwei Teilen zusammensetzen: einem Teil in Papier- und einem anderen Teil in elektronischer Form. Dabei muss die Zusammenführung der schriftlichen und der elektronischen Daten und Informationen verlässlich geregelt sein. Wenn Akten elektronisch geführt werden, müssen bestimmte Anforderungen eingehalten werden (siehe § 10 Abs. 5 MBO-Ä, § 10 Abs. 2 MBO-Pt). Durch die Historie muss nachvollziehbar bleiben, wer was wann eingetragen hat. Dazu sollten Schreibrechte vergeben werden und die Überschreibung der Einträge ausgeschlossen sein. Die ausschließlich elektronische Dokumentation erfordert besondere Sicherheits- und Schutzmaßnahmen.

Der vertrauliche sichere Umgang mit diesen Unterlagen und Daten umfasst auch deren Schutz vor Verlust, Zerstörung, Manipulation und unbefugtem Zugang und Gebrauch. Hierfür sollen die Daten und Aufzeichnungen in abschließbaren Aktenschränken in Räumen aufbewahrt werden, die ausreichend gegen Brand und Diebstahl geschützt sind.

6.1.3 Vernichtung vertraulicher Unterlagen und Daten

Als „Vertrauliche Patientendaten" gelten sämtliche patientenbezogenen Daten und Informationen: von der Tatsache eines Kontaktes über den Gesundheitszustand der Patienten, zur Krankengeschichte oder zu vergangenen bzw. zukünftigen Behandlungen.

Nach Ablauf der gesetzlichen Aufbewahrungsfristen können Aufzeichnungen und Unterlagen, die nicht mehr gebraucht werden, vernichtet und entsorgt werden. Aus Datenschutzgründen müssen diese vor der Entsorgung ordnungsgemäß vernichtet werden. Das heißt, die Daten dürfen nicht mehr lesbar oder wiederherstellbar sein.

Die Entsorgung über den Hausmüll ist möglich, wenn papiergebundene Aufzeichnungen vorher mittels eines Aktenvernichters mindestens der Sicherheitsstufe 3 nach DIN 66399 zerkleinert wurden. Magnetische und elektronische Datenträger sowie Filme sind vor der Entsorgung zu löschen und möglichst physikalisch zu zerstören. Erfolgt die Vernichtung durch einen externen Dienstleister, prüfen Sie regelmäßig dessen Eignung und Vertraulichkeit.

6.1.4 Regelung von Zutrittsrechten

Zur Informationssicherheit gehören neben der Definition von rollen- bzw. personenbezogenen Zugriffsrechten auf Daten auch Regeln für den Zugang zum Netzwerk und Festlegungen zum Zutritt zu den Praxisräumen. Protokollieren Sie die Schlüsselausgabe an die Mitarbeiter, schließen Sie den Serverraum ab und sichern Sie Räume, die nicht für den Zutritt von Besuchern und Patienten vorgesehen sind. Schützen Sie Ihre Praxis gegen Einbruch und Diebstahl durch eine Alarmanlage, insbesondere die Räume, in denen sich Patienten- und Abrechnungsdaten sowie die Praxis-EDV befinden.

Um die Sicherheit für Patienten und Mitarbeiter zu erhöhen, ist eine nachvollziehbare Dokumentation nötig. Daher sollten Befugnisse und Verantwortlichkeiten für Einträge in Patientenakten durch die Vergabe von Lese- und Schreibrechten für alle Mitarbeiter geregelt werden. Dies gilt unabhängig davon, ob die Patientenakte elektronisch oder papiergebunden geführt wird, damit Zugriffe und Einträge nur von berechtigten Personen erfolgen. Bei handschriftlichen Eintragungen sollte ein dokumentenechter Stift verwendet werden.

Bei der Beendigung des Arbeitsverhältnisses sind Zugriffsrechte auf das PVS zu sperren.

6.2 Empfehlungen zu Datenschutz und Datensicherheit

Die zunehmende elektronische Kommunikation und Vernetzung der Ärzte bietet Chancen, birgt aber auch Gefahren hinsichtlich der Datensicherheit. Als Arzt bzw. Psychotherapeut sind Sie deshalb beim beruflichen Einsatz von EDV verpflichtet, die Sicherheit der Patientendaten zu gewährleisten. Zusätzlich zu den Regelungen der ärztlichen Schweigepflicht gelten für Sie auch die Datenschutzgesetze, allen voran die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Dieses regelt die verschiedenen Phasen der Datenverarbeitung und die Anforderungen an die Datensicherheit.

Vor diesem Hintergrund haben die Bundesärztekammer und die Kassenärztliche Bundesvereinigung im Jahre 2008 „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ und eine zugehörige technische Anlage [7] veröffentlicht. Darin enthalten sind rechtliche, technische und organisatorische Orientierungshilfen bei der Umsetzung von Datenschutz und Datensicherheit in der Praxis.

Ein Schwerpunkt betrifft die ärztliche Dokumentation, die Datenkommunikation in der Praxis und die Online-Anbindung. Sehr viel detaillierter als die Empfehlungen geht die Technische Anlage auf erforderliche IT-Schutzmaßnahmen ein. Das inhaltliche Spektrum reicht vom Umgang mit Passwörtern über die Nutzung des Internets und Intranets, das Einrichtungen von lokalen und drahtlosen Netzwerken bis hin zur Entsorgung von Datenträgern und Archivierung. Teilweise existieren Überschneidungen mit dem Thema der Informationssicherheit. Einige wichtige Punkte haben wir nachfolgend zusammengestellt:

- Erstellen Sie Regeln für die Verwendung von effektiven und individuellen Passwörtern durch ihre Mitarbeiter. Dazu zählen auch Schreibweisen (zum Beispiel mindestens 6 Buchstaben und 1 Zeichen) und eine begrenzte Gültigkeit (zum Beispiel 40 Tage). Die Option „Speicherung von Passwörtern“ sollte im Betriebssystem deaktiviert werden.
- Viren-Schutz
  Die meisten IT-Sicherheitsvorfälle ereignen sich im Zusammenhang mit Computerviren.

Daher sind aktuelle Viren-Schutzprogramme unverzichtbar. Schadprogramme können über Datenträger oder über Netze (Internet, Intranet) verbreitet werden. Auch für Rechner ohne Internetanschluss sind Schutzprogramme erforderlich. Es empfiehlt sich, E-Mails und jegliche Kommunikation über das Internet zentral auf Viren zu untersuchen. Zusätzlich sollte jeder Computer mit einem lokalen Viren-Schutzprogramm ausgestattet sein, das ständig im Hintergrund läuft. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen, zum Beispiel vor einer Tages- oder Monatssicherung, und ist bei einem festgestellten Befall durch Schadprogramme immer notwendig. Aktuelle Empfehlungen und ausführliche Hintergrundinformationen finden Sie auf www.bsi.de unter dem Stichwort Schadprogramme.

Sie sollten Strategien zur Datensicherung und Datenwiederherstellung erarbeiten, damit Sie im Notfall kurzfristig zumindest eine eingeschränkte Funktionsfähigkeit herstellen können.

- Vergeben Sie rollen- bzw. personenbezogenen Zugriffsrechte auf das EDV-System und prüfen Sie deren Vergabe. Die Konfiguration der Datenzugriffsrechte sollte für jeden Benutzer auf das Notwendige beschränkt werden. Es sollten keine Administratorrechte für normale Benutzer vergeben werden. Informieren Sie die Mitarbeiter über die sichere Verwendung von Passwörtern (siehe oben) und machen Sie deutlich, dass diese konsequent einzuhalten ist.
- Nutzen Sie Chip-Karten, wenn Sie elektronische Patientendaten für den Transport verschlüsseln oder sich zum Beispiel gegenüber einem Web-Portal als Arzt authentisieren wollen.

6.2.1 Einhaltung von Schweigepflicht- und Datenschutzvorgaben

Informieren Sie Ihre Mitarbeiter über die nach der Berufsordnung geltende gesetzliche Schweigepflicht. Alle Praxismitarbeiter, aber auch externe Personen wie EDV-Berater, Support-Mitarbeiter und Reinigungspersonal, die Zugang zu personenbezogenen Daten haben, müssen die Regelungen zum Datenschutz kennen und Datenschutzerklärungen unterschreiben. Wenn Sie eine elektronische Patientenverwaltung per PVS führen, sind alle Mitarbeiter im Arbeitsvertrag oder durch eine separate Verpflichtungserklärung auch auf das Datengeheimnis nach § 5 BDSG zu verpflichten.

Externe Dienstleister dürfen nur bei Bedarf Zugang zu diesen Daten erhalten. Weisen Sie nicht nur bei der Einstellung neuer Mitarbeiter auf die gesetzlichen Vorgaben hin, nutzen Sie dazu auch die regelmäßigen Teamsitzungen und Mitarbeitergespräche.

Wenn in Ihrer Praxis oder dem MVZ mehr als neun festangestellte Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, muss die Leitung einen Datenschutzbeauftragten schriftlich festlegen (§ 4f Beauftragter für den Datenschutz, BDSG). Zu den neun Mitarbeitern zählen alle in der Praxis oder dem MVZ tätigen Mitarbeiter einschließlich der Ärzte, Psychotherapeuten, Auszubildenden, Mitarbeitern mit Mini-Job und Teilzeitkräfte.

6.2.2 Maßnahmen beim Einsatz von Fernwartung

Zusätzlich zur unterschriebenen Datenschutzerklärung von EDV-Beratern und Support-Mitarbeitern sollten Sie beim Einsatz von Fernwartung folgende Punkte beachten:

- Beim Einsatz von Fernwartung des EDV-Systems müssen grundlegende Sicherheitsvorkehrungen wie die Autorisierung des Technikers über ein Passwort erfolgen.
- Nach jeder Beendigung der Fernwartungssitzung sollten Sie das Passwort ändern.

- Die Zugriffsrechte des Technikers sollten auf ein Minimum beschränkt werden.
- Die Fernwartungsdaten dürfen nur verschlüsselt über eine geschützte Verbindung übermittelt werden.
- Grundsätzlich sollten Sie dem Techniker nur Testdaten zur Verfügung stellen, keine Echtdaten.
- Stellen Sie sicher, dass alle Maßnahmen der Fernwartung durch den Dienstleister protokolliert werden.

6.2.3 Sicherheit bei der Übermittlung von Patientendaten

Patientendaten können auf dem Postweg, per Fax oder E-Mail übermittelt werden. Eine weitere sichere Möglichkeit ist auch die persönliche Aushändigung der Unterlagen an den Patienten als Übermittler. Die Übermittlung von Patientendaten per Fax kann nur dann als sicher bezeichnet werden, wenn die Faxgeräte an zutrittsgeschützten Orten stehen und die Faxnummern der häufigsten Empfänger im Gerät einprogrammiert sind. Achten Sie genau auf die Wahl der korrekten Empfänger und vereinbaren Sie vor dem Versand des Fax telefonisch die Entgegenahme durch eine berechtigte Person.

Bedenken Sie bei der Nutzung von E-Mail, dass die Inhalte unbedingt vor unbefugtem Zugriff geschützt werden müssen. Zur elektronischen Übermittlung von Patientendaten sollten Sie deshalb immer digital signierte und verschlüsselte E-Mails verwenden. Über das Datennetz der KVen, das KV-SafeNet (siehe Abschnitt 4.2.1) können Sie schnell und sicher kommunizieren und auf weitere Anwendungen zugreifen.

Denken Sie daran: Die Internet-Telefonie (Voice-over-IP) ist nicht abhörsicher und kann in der Arztpraxis nur mit besonderen Schutzvorkehrungen zur Übermittlung von Patientendaten verwendet werden.

6.2.4 Schutzmaßnahmen bei der Nutzung von Internet und Intranet

Im Hinblick auf die Online-Anbindung galt früher die Empfehlung, nach Möglichkeit den Praxisrechner und den Internetanschluss getrennt vorzuhalten. Dies ist heute kaum noch sinnvoll realisierbar. Um dennoch optimalen Datenschutz zu erreichen, sollten Sie die folgenden Punkte beachten:

- Für die Internetnutzung in der Praxis empfiehlt sich die Nutzung eines einzelnen Internet-Rechners, der keine Patientendaten enthält.
- Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze überwachen und sich auf dem aktuellen Stand halten.
- Setzen Sie eine Firewall ein, die den Datenverkehr zwischen verschiedenen Netzsegmenten wie zum Beispiel LAN und Internet reguliert und absichert.
- Die Konfiguration des Internetbrowsers und der Firewall sollte durch Experten überprüft werden.
- Generell wird der Einsatz einer hochwertigen symmetrischen Verschlüsselung für Patientendaten empfohlen, mit der alle auf Datenträgern, Notebooks und PC befindlichen Patientendaten verschlüsselt abgelegt werden sollten.

6.2.5 Elektronische Datensicherung und Archivierung

Der Verlust von Daten kann erhebliche Auswirkungen haben. Sind Anwendungsdaten oder Patientendaten verloren oder verfälscht, kann dies die Existenz der Praxis bedrohen. Für die Datensicherung, auch als „Backup“ bezeichnet, stehen zahlreiche Software- und Hardwarelösungen zur Verfügung.

Die Datensicherungen erfolgen nach dem Drei-Generationen-Prinzip am Abend eines Praxistages, am Ende einer Woche und am Ende eines Monates. Dabei sind alle Rechner, auch die Laptops, zu berücksichtigen. Alle personenbezogenen Gesundheitsdaten werden dabei in verschlüsselter Form gesichert.

Für die einzelnen IT-Systeme sind Datensicherungspläne zu erstellen. Folgende Punkte sollten in einem Datensicherungsplan aufgeführt werden:

- Art der Daten (Anwendungsdaten, Systemdaten, Software)
- Art der Datensicherung (zum Beispiel inkrementell, voll, komprimiert, verschlüsselt)
- Wer für Sicherung bzw. Rekonstruktion zuständig ist
- Hinweise zur Rekonstruktion
- Häufigkeit und Zeitpunkt der Datensicherung
- Datensicherungsmedium
- Aufbewahrungsdauer und Anzahl der Generationen

Die Datensicherung erfolgt auf Basis der Datensicherungspläne. Datensicherungen sollten möglichst automatisiert ablaufen, um Fehler zu vermeiden. Mit einer regelmäßigen Verifizierung in Form eines Vergleichs sollten Sie sichergehen, dass das Backup funktioniert und die Daten auch wieder erfolgreich zurückgespielt werden können. Wenn EDV-Benutzer mit der Datensicherung betraut wurden, sind ihnen entsprechende Anwendungen zur Verfügung zu stellen und ein sicherer Aufbewahrungsort, wie ein Tresor, für die Verwahrung der Datensicherungen bereitzustellen. Der Aufbewahrungsort sollte den Schutz vor Diebstahl sowie Feuer- und Wasserschäden garantieren.

Nicht alles muss gleich häufig gesichert werden. Bei Software reicht eine einmalige Sicherung, wenn diese erworben bzw. eingespielt wurde.

Eine erfolgte Datensicherung ist unbedingt zu dokumentieren. Bei der Rekonstruktion von Daten ist größte Vorsicht geboten, um nicht versehentlich Daten zu überschreiben.

Es ist wichtig, dass alle relevanten Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen eine besondere Herausforderung dar. Sie sollten gegebenenfalls auch mobile Endgeräte wie Notebooks, unvernetzte Einzelplatzrechner und PDAs mit einbeziehen.

Bitte beachten Sie: Die Liste enthält nur die wichtigsten Punkte. Studieren Sie auch die Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Sie helfen Ihnen dabei, Ihre Praxis in puncto Sicherheit richtig einzustellen. Natürlich können und müssen Sie nicht alle technischen Details selbst beherrschen. Sie sind deshalb gut beraten, sich gegebenenfalls professionelle Unterstützung zu holen, vor allem wenn Sie vernetzt arbeiten und Telematikanwendungen nutzen.