

MEDletter

- > Ausgabe 2 / 2024
- > Informationen für Ärzte und medizinische Fachberufe

Datenschutz in der (Arzt-)Praxis

Datenschutzverletzungen sind in der heutigen digitalen Welt ein ernstzunehmendes Problem, das auch vor der medizinischen Praxis nicht haltmacht. Ärzte sehen sich mit einer Vielzahl von Herausforderungen konfrontiert, wenn es darum geht, die Vertraulichkeit und Integrität von Daten zu gewährleisten. Die zunehmende Digitalisierung der medizinischen Unterlagen und die Nutzung moderner Technologien haben einerseits die Effizienz und Qualität der medizinischen Versorgung verbessert, aber andererseits auch neue Risiken in Bezug auf den Datenschutz geschaffen.

Der Schutz von Patientendaten ist von größter Bedeutung, da es sich um äußerst vertrauliche und sensible Informationen handelt. Ärzte sind berufen, diese Daten sicher aufzubewahren und nur autorisierten Personen den Zugriff zu gewähren. Doch bei dieser Aufgabe stehen sie vor zahlreichen Herausforderungen. Eine der größten Herausforderungen besteht darin, die Verantwortung für die Sicherung der Daten zu tragen, während gleichzeitig eine effektive und umfassende medizinische Versorgung gewährleistet werden muss.

Für eine umfassende Bewertung des Risikos und möglicher Maßnahmen und Umsetzungsfelder ist es unerlässlich, sich mit den Risiken auseinander zu setzen.

Die 5 wesentlichen Herausforderungen sind:

✓ Verantwortung für Patientendaten

Ärzte tragen die Verantwortung, die Vertraulichkeit der medizinischen Daten ihrer Patienten zu wahren. Dies bedeutet, dass sie angemessene Sicherheitsvorkehrungen treffen müssen, um den unbefugten Zugriff, Verlust oder Missbrauch von sensiblen Informationen zu verhindern. Die zunehmende Digitalisierung und Vernetzung medizinischer Daten erschwert diese Aufgabe, da die Anfälligkeit für Datenschutzverletzungen steigt.

✓ Technologischer Fortschritt und Datenschutz

Die Nutzung elektronischer Gesundheitsakten (EHRs) und anderer digitaler Technologien erleichtert den Ärzten die Patientenversorgung. Gleichzeitig ergeben sich jedoch neue Risiken in Bezug auf Datenschutzverletzungen. Cyberkriminalität, Hacking und Datenlecks können sensible Patientendaten gefährden. Ärzte müssen sicherstellen, dass ihre Systeme gut geschützt sind und aktuelle Sicherheitsstandards erfüllen.

✓ Nutzung von Cloud-Services

Die Integration von Cloud-Services in die medizinische Praxis bietet Vorteile wie einen einfachen Zugriff auf medizinische Daten und die Möglichkeit der Zusammenarbeit. Allerdings ergeben sich hierbei auch Datenschutzfragen. Ärzte müssen genau prüfen, welche Daten in der Cloud gespeichert werden und welche Sicherheitsmaßnahmen der Cloud-Anbieter implementiert hat. Ein Herstellerwechsel oder eine unsachgemäße Konfiguration können zu Datenschutzverletzungen führen.

✓ Sensibilisierung und Schulung der Mitarbeiter

Ein wichtiger Aspekt des Datenschutzes ist die Sensibilisierung und Schulung aller Mitarbeitenden. Ärzte müssen sicherstellen, dass sie und ihr Team über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um den Umgang mit sensiblen Patientendaten zu verstehen und angemessen darauf zu reagieren. Regelmäßige Schulungen helfen dabei, das Bewusstsein für Datenschutzverletzungen zu schärfen und Mitarbeiter über die aktuellen Anforderungen auf dem Laufenden zu halten.

✓ Rechtlicher Anforderungskatalog

Ärzte müssen sich mit den rechtlichen Anforderungen in Bezug auf den Datenschutz vertraut machen und sicherstellen, dass sie diese erfüllen. Das bedeutet, dass sie etwaige Verletzungen von Patientendaten der zu-

zuständigen Datenschutzbehörde melden müssen und die erforderlichen Sicherheitsmaßnahmen ergreifen, um zukünftige Datenschutzverletzungen zu verhindern. Die Einhaltung der gesetzlichen Bestimmungen dient nicht nur dem Schutz der Patienten, sondern auch dem Schutz des medizinischen Personals.

Durch die Umsetzung geeigneter Maßnahmen können Ärzte den Datenschutz in ihrer Praxis gewährleisten und das Vertrauen der Patienten in den Umgang mit ihren sensiblen Daten stärken. Daher sollten Ärzte sich über die spezifischen gesetzlichen Bestimmungen und Vorschriften informieren, die für ihre Praxis gelten.

Als erste Einschätzung kann der HDI Datenschutz Quickcheck zur Seite stehen. Dieser bewertet den Stand datenschutzrechtlicher Anforderungen und ist für HDI Cyberkunden kostenlos nutzbar.

Was muss von einer Praxis beachtet werden, um sich möglichst rechtssicher und datenschutzkonform zu verhalten?

Ärzte müssen sicherstellen, dass sie die geltenden Datenschutzgesetze, wie beispielsweise die Datenschutz-Grundverordnung (DSGVO), einhalten.

- Dies umfasst die Meldung von Datenschutzverletzungen an die zuständigen Behörden, die Erstellung von Datenschutzrichtlinien und -verfahren, die Dokumentation von Verarbeitungstätigkeiten und die Gewährleistung der Betroffenenrechte.
- Es ist entscheidend, dass das gesamte medizinische Team über die Bedeutung des Datenschutzes informiert ist und die geltenden Datenschutzrichtlinien und -verfahren versteht. Regelmäßige Schulungen und Schulungsmaterialien können dazu beitragen, das Bewusstsein für Datenschutzverletzungen zu schärfen und das Wissen und die Fähigkeiten des Teams in Bezug auf den Umgang mit sensiblen Patientendaten zu verbessern.
- Zudem sollten angemessene technische und organisatorische Sicherheitsmaßnahmen implementiert werden, um den Schutz sensibler Daten zu gewährleisten. Dies kann die Verwendung von starken Passwörtern, die Verschlüsselung von Daten, die regelmäßige Aktualisierung von Sicherheitssoftware und die Zugangsbeschränkung zu Patientendaten umfassen.
- Die Auswahl sicherer IT-Systeme und die Zusammenarbeit mit zuverlässigen IT-Dienstleistern sind ebenfalls von großer Bedeutung. Auch die Definition von Zuständigkeiten für z. B. die Umsetzung von Sicherheitsmechanismen durch die IT-Dienstleister sollte klar geregelt und transparent in den Verträgen erfasst sein.
- Ärzte sollten klare Richtlinien und Verfahren für den Umgang mit Patientendaten entwickeln und sicherstellen, dass sie von allen Mitarbeitern in der Praxis befolgt werden. Dies umfasst Richtlinien zur Datenverarbeitung, Zugriffsrechte, Datenfreigabe, den

Umgang mit mobilen Geräten und den Einsatz von Cloud-Services. Alle Mitarbeiter sollten über diese Richtlinien informiert werden. Eine regelmäßige Überprüfung und Aktualisierung ist unerlässlich, um den aktuellen Best Practices zu entsprechen.

- Eine regelmäßige Bewertung der Datenschutzrisiken in der Praxis kann dazu beitragen, potenzielle Schwachstellen zu identifizieren und Maßnahmen zur Risikominimierung zu ergreifen. Hierbei sollten alle Bereiche der Praxis, wie die elektronische Datenspeicherung, die Kommunikation, die Datenübertragung und die physische Sicherheit der Räumlichkeiten, berücksichtigt werden. Eine angemessene Risikobewertung kann helfen, Sicherheitslücken zu schließen und den Schutz von Patientendaten zu stärken.
- Ärzte sollten sicherstellen, dass sie eine wirksame Einwilligung von Patienten einholen, bevor sie deren Daten sammeln, speichern oder teilen. Regelmäßige Kommunikation mit den Patienten über den Umgang mit ihren Daten und die Offenlegung von Datenschutzpraktiken kann das Vertrauen stärken und die Transparenz verbessern. Weiter sollte sichergestellt werden, dass angemessene Verfahren zur Freigabe von Patientendaten mit anderen medizinischen Fachkräften, Laboren oder Einrichtungen bestehen, um einen sicheren und geschützten Informationsaustausch zu gewährleisten.

Praxistipp

Die HDI Cyberversicherung unterstützt im Falle von Datenschutzverstößen mit einem umfassenden Experten-Netzwerk. Unter anderem ist auch eine rechtliche Bewertung des Sachverhaltes umfasst, wodurch schnell erste nötige Schritte eingeleitet werden können, um den gesetzlichen Anforderungen zu entsprechen.

Prävention ist besser als Reaktion. HDI Cyberkunden erhalten kostenlosen Zugang zum Perseus Präventionsangebot, dies beinhaltet u.a. eine kostenlose Unterstützung in den Bereichen Mitarbeiterschulungen, Sicherheitsrichtlinien oder auch einem Notfallplan.

Die Bewältigung der Herausforderungen im Bereich Datenschutz erfordert eine ganzheitliche Herangehensweise, bei der Technologie, Organisation, Schulung und Compliance gleichzeitig berücksichtigt werden. Mit einer sorgfältigen Planung und Umsetzung geeigneter Maßnahmen können Ärzte Patienten und deren Daten umfassend schützen und gleichzeitig eine hochwertige, sichere und effektive medizinische Versorgung bieten.

Autoren

Sönke Glanz & Peter Bertram,
Produktmanagement & Underwriting
Cyber, HDI

