MEDletter

> Ausgabe 1 / 2026
> Informationen für Ärzte und medizinische Fachberufe

Digitalisierung in Arztpraxen – zwischen Effizienzgewinn und neuen Risiken

Digitalisierung ist längst im Alltag der Arztpraxen angekommen. Spätestens mit der verpflichtenden Einführung der Telematikinfrastruktur (TI), dem E–Rezept und der elektronischen Gesundheitskarte (eGK) gehört der digitale Austausch sensibler Gesundheitsdaten zum Normalbetrieb. Doch je stärker Prozesse digitalisiert werden, desto größer wird auch die Verantwortung, Daten sicher und zuverlässig zu verarbeiten.

Die eGK ist weit mehr als ein Versicherungsnachweis. Über sie wird der Zugriff auf sensible Versichertendaten ermöglicht: Medikationspläne, Notfalldaten, E–Patientenakte (ePA). Damit ist die eGK ein zentrales Element der modernen Patientenversorgung – aber auch ein potenzieller Angriffspunkt.

Technisch basiert die eGK auf einer Kombination aus:

- Kryptografischen Schlüsseln,
- Zugriffsschutz durch VPN,
- Verbindung über die Telematikinfrastruktur

In der Theorie ein robustes Konzept – in der Praxis jedoch stark abhängig vom verantwortungsvollen Umgang der beteiligten Systeme und Mitarbeitenden.
Für die Nutzung der elektronischen Gesundheitskarte ist es nicht erforderlich, die dahinterliegenden kryptografischen Verfahren oder die Funktionsweise der Telematikinfrastruktur im Detail zu verstehen. Genau dafür wurden diese Systeme entwickelt: damit Ärzte und medizinisches Personal sich auf die Versorgung der Patienten konzentrieren können, während die technischen Prozesse im Hintergrund stabil und sicher ablaufen.

Wichtig ist jedoch ein anderes Verständnis – nämlich warum diese Systeme geschützt werden müssen. Digitale Gesundheitsdienste verarbeiten äußerst sensible Daten: Diagnosen, Medikationspläne, Befunde und Notfalldaten. Egal wie einfach die Anwendung gestaltet ist, der Schutzbedarf dieser Informationen bleibt hoch.

Die eGK transportiert nicht „irgendeine" Information, sondern hochvertrauliche medizinische Details. Und weil diese Informationen so wertvoll sind, sind sie auch ein attraktives Ziel für Cyberkriminelle.
Der entscheidende Punkt lautet daher:

Man muss die Technik nicht beherrschen, aber man muss wissen, dass sie nur dann zuverlässig funktioniert, wenn sie geschützt wird – durch sichere Passwörter, geschulte Mitarbeitende und eine stabile, aktuelle IT–Umgebung. Dieses Bewusstsein ist kein technisches Verständnis, sondern Teil der professionellen Verantwortung im Umgang mit Patientendaten. Die Sicherheit entsteht nicht allein durch Verschlüsselung und Konnektoren – sie entsteht durch das Zusammenspiel von Technik und verantwortungsvollem Handeln der Menschen, die täglich damit arbeiten.

Wo liegen die Risiken im Praxisalltag?

Trotz hoher technischer Standards gibt es mehrere Einfallstore, die im täglichen Betrieb unterschätzt werden und regelmäßig zu Schäden führen:

1. Ungesicherte Arbeitsplatzrechner
Wenn IT–Konnektoren und eGK–Lesegeräte an veraltete oder unzureichend geschützte Systeme angeschlossen sind, entstehen Sicherheitslücken.
Beispiel: Ein nicht gepatchtes Betriebssystem kann Malware einschleusen, bevor die eGK überhaupt eingelesen wurde.

2. Menschliche Fehleinschätzung
Unachtsame Klicks, gemeinsam genutzte Accounts oder unzulässige Speicherung von Gesundheitsdaten auf lokalen Endgeräten können zu Datenschutzverletzungen führen – oft unbewusst. Ob aus Stress, Routine, Zeitdruck oder schlicht Unaufmerksamkeit – die Erfahrung zeigt, dass sich menschliche Fehlhandlungen niemals vollständig ausschließen lassen. Ein 100%iger Schutz ist illusorisch, weil kein technisches System die letzte Entscheidung des Menschen vollständig kompensieren kann.

Genau deshalb kommt es darauf an, Sicherheit nicht als „Perfektion“, sondern als **Risiko–Reduktion** durch mehrere Schutzschichten zu verstehen: klare Prozesse, Schulungen, Berechtigungskonzepte, technische Barrieren und regelmäßige Sensibilisierung.
Sicherheitsmaßnahmen müssen den unvermeidbaren menschlichen Faktor nicht ausschalten, sondern so abfedern, dass ein einzelner Fehlklick nicht zur Katastrophe wird.

3. Fehlkonfiguration der TI–Komponenten
Die Telematikinfrastruktur ist komplex. Wird ein Konnektor falsch eingebunden, ein Update nicht installiert oder ein Zertifikat nicht rechtzeitig erneuert, kann dies sowohl den Praxisbetrieb stören als auch ein Sicherheitsrisiko darstellen.

4. Ausfall zentraler Systeme
Die zunehmende Abhängigkeit von Cloud–Anwendungen, Online–Diensten und zentralen Servern bringt eine klassische Frage mit sich:

Was passiert, wenn das System ausfällt?
Ob ePA–Zugriff oder e–Rezept – ohne Zugriff auf die TI steht eine Praxis im Zweifel still.

Was bedeutet das für Arztpraxen?

Digitalisierung ist kein Selbstläufer. Damit sie funktioniert, braucht es klare Strukturen.

1. Transparenz schaffen – Praxen müssen wissen:
- Welche Geräte sind angebunden?
- Welche Anwendungen sind aktiv?
- Wer hat welche Zugriffsrechte?

Nur was transparent ist, kann geschützt werden.

2. Sicherheitsgrundlagen ernst nehmen – dazu gehören:
- Regelmäßige Updates
- Starke Passwörter / MFA
- Klare Rollen– und Berechtigungskonzepte
- Verschlüsselte Übertragungswege
- Professionelle Backup–Strategien

Die eGK–Infrastruktur schützt Daten nur so gut, wie das Umfeld es zulässt.

3. Mitarbeitende sensibilisieren
- Schulungen zum Umgang mit Patientendaten
- Erkennen von Social–Engineering–Angriffen
- Bewusstsein für die Bedeutung der TI
- Sicherer Umgang mit mobilen Endgeräten

Ist die Digitalisierung Chance oder Risiko?
Beides.
Die moderne Gesundheitsversorgung profitiert enorm von:
- Schnellerer Verfügbarkeit relevanter Daten
- Besseren Abstimmungsprozessen
- Weniger Papieraufwand
- Verbesserter Dokumentation
- Reduzierter Fehleranfälligkeit

Mit steigender Digitalisierung steigt auch die Angriffsfläche. Ein Ausfall oder eine Datenpanne betrifft nicht nur die Praxis selbst – sondern unmittelbar die Versorgung von Menschen.

Autor

Sönke Glanz, Produktmanagement & Underwriting Cyber, HDI