DIGITALISIERUNG

Wie Kliniken digitale Patientendaten am besten schützen

Die Digitalisierung bietet viele Möglichkeiten, Prozesse effizienter zu gestalten und Kosten zu sparen. Doch damit gehen Risiken in IT-Sicherheit und Datenschutz einher. Wägen die Kliniken diese kritisch ab, können sie die neuen Chancen sicher nutzen.

In den Krankenhäusern sorgen die zunehmende IT-Durchdringung und die Einführung der elektronischen Patientenakte (EPA) dafür, dass die Verfügbarkeit von Patientendaten stetig wächst. Zugleich geht der Trend seit einigen Jahren in Richtung vernetzte Strukturen und mobile Endgeräte. Diese Entwicklung bringt viele neue Risiken und Anforderungen mit sich, vor allem in der IT-Sicherheit und im Datenschutz. Da insbesondere der Datenschutz einen hohen Stellenwert im Gesundheitswesen einnimmt, gilt es, die neuen technologischen Möglichkeiten zwingend datenschutzrechtlich zu bewerten und entsprechend auszugestalten. Das Augenmerk liegt dabei hauptsächlich auf den technologischen Aspekten, da für die digitale Datenverarbeitung, -nutzung und -übertragung die gleichen datenschutzrechtlichen Rahmenbedingungen gelten wie beim Einsatz von Papier.

Visite, interne Audits: Nutzung mobiler Endgeräte

Um die Vorteile der EPA und der Digitalisierung auszuschöpfen, setzen viele Krankenhäuser bereits verstärkt mobile Endgeräte wie PDAs (Personal Digital Assistants) und Tablets ein, zum Beispiel in der mobilen Visite, in der Patientenaufklärung, internen Audits, für die Terminkoordination oder zum einfachen und schnellen Informationsaustausch. Ein besonderes Risiko entsteht dadurch, dass Mitarbeiter diese Geräte verlieren oder die Geräte gestohlen werden können. Dann ist ein Zugriff auf darauf gespeicherte Daten, wie E-Mails, Fotos, Kontakt- oder Standortdaten nicht auszuschließen. Außerdem können Angreifer die Geräte manipulieren und unbemerkt zurückgeben, um sich so unberechtigten Zugang zu sensiblen Informationen zu verschaffen. Dabei ist das Gefährdungspotenzial unterschiedlich, je nachdem, ob Mitarbeiter mobile Endgeräte ausschließlich einrichtungsintern nutzen oder sie private Endgeräte auch in der Einrichtung nutzen.

Betriebseigene Geräte: relativ geringes Risiko

Werden betriebseigene Geräte einrichtungsintern verwendet, können die Mitarbeiter der IT diese effektiv verwalten und problemlos in das geschützte WLAN integrieren, zum Beispiel mit einer Device-Management-Software. Dann greifen alle Nutzer über ihre jeweilige Benutzerkennung auf das System zu, wobei das System am Rollenberechtigungskonzept gemäß der OH-KIS auszurichten ist. Dabei unterbleibt das Speichern sensibler Daten auf dem mobilen Endgerät. Halten die Nutzer die regulären IT-Sicherheitsmaßnahmen ein, ist das Risiko des Datenmissbrauchs relativ gering.

Verwenden Mitarbeiter ihre privaten Mobiltelefone oder Smartphones auch dienstlich (Mischnutzung), sind die Gefahren deutlich höher einzustufen, da diese meist nicht in gleichem Maße geschützt sind wie betriebseigene Geräte. Zudem trennen die Nutzer meist nicht zwischen privaten und dienstlichen Daten oder Programmen (Apps). Das ist problematisch, da viele Apps Zugriff auf personenbezogene Daten wie Kontaktlisten, E-Mail-Verkehr oder Fotos haben oder direkt auf Gerätesensoren, Kameras oder das Mikrofon zugreifen. Daher kommt es vor, dass Daten unbemerkt

Foto: Alex/stock.adobe.com

gespeichert und an Dritte übermittelt werden, beispielsweise Anbieter der Apps oder soziale Netzwerke. Zudem nutzen oft unbefugte Dritte, wie Familienangehörige, die privaten Geräte. Bei dieser Mischnutzung sind also neben technischen Sicherungsmaßnahmen auch organisatorische Maßnahmen angezeigt. Dazu zählt, die Mitarbeiter zu sensibilisieren und zu verpflichten, sicherheitsrelevante Verhaltensregeln strikt einzuhalten.

Intersektorale Kommunikation: sichere Wege

Die zunehmende Vernetzung aller an einer digitalisierten intersektoralen Kommunikation Beteiligten wird für die Geschäftsprozesse im Gesundheitswesen immer wichtiger. Sowohl der digitale Datenaustausch mit den Kostenträgern als auch der zwischen stationären Einrichtungen und niedergelassenen Ärzten rücken in den Fokus. Um den Datenschutz zu gewährleisten ist es notwendig, die Inhalte der Kommunikation vor Unbefugten und vor unberechtigter Nutzung zu schützen. Entscheidend ist, sichere Kommunikationswege einzusetzen, zum Beispiel mithilfe von Verschlüsselungstechnologien. Eine Variante ist, die Daten mittels VPN-Tunnel zu übertragen, wie im Fall des KV-SafeNet. Eine weitere Möglichkeit bietet künftig auch die Telematik-Infrastruktur. Dabei können Daten, wie elektronische Arztbriefe, in einem geschlossenen Netz übermittelt werden, indem die Nutzer Verschlüsselungstechnologien verwenden.

Beide Kommunikationswege hat der Gesetzgeber freigegeben, sie können somit bedenkenlos genutzt werden. Das Verwenden von E-Mails ist hingegen ohne eine zusätzliche Ende-zu-Ende-Verschlüsselung nicht geeignet, Patientendaten zu übertragen. Für telemedizinische Anwendungen, wie das Telekonsil, gibt es derzeit noch keine vom Gesetzgeber freigegebenen Kommunikationswege, sodass die Nutzer jeweils individuelle technische Lösungen finden müssen.

Internetdienste und Messenger: hohes Risiko

Inzwischen nutzen auch immer mehr Menschen geräteunabhängig diverse Internet- und Cloud-Dienste, über die sie personenbezogene Daten übermitteln und verarbeiten. Neben der unkomplizierten Handhabung, hoher Geschwindigkeit und leichter Vernetzung ermöglicht das eine nahezu unbegrenzte Verfügbarkeit von Daten. So kommt es vor, dass Laborbefunde oder Röntgenbilder mit dem Smartphone abfotografiert und mittels Messenger an einen Kollegen gesendet werden, um dessen Rat einzuholen.

Mit dem hohen Nutzungskomfort von Diensten wie Dropbox, Skype oder WhatsApp geht jedoch ein extrem hohes datenschutzrechtliches Risiko einher. Wer solche Dienste nutzt, büßt die alleinige Verfügungsgewalt über die Daten ein, da diese außerhalb der eigenen IT-Systeme gespeichert und verarbeitet werden. Vielmehr herrscht völlige Intransparenz darüber, wo und wie die Daten gespeichert werden, wer Zugriff darauf hat und ob die Daten für unrechtmäßige Zwecke missbraucht werden. Zudem bieten diese Dienste meist keine ausreichende Verschlüsselung, auch ein versehentliches Übermitteln an einen unberechtigten Empfänger aus der eigenen Kontaktliste ist nicht auszuschließen. Deshalb ist davon abzuraten, solche Internet- und Cloud-Dienste dienstlich zu nutzen.

Dr. Henning Kropp, Senior-Berater
Dr. Uwe Günther, Geschäftsführer
Sanovis GmbH
81679 München

NACHGEFRAGT

„Flexible Lösungen auf dem Karriereweg“

Frau Dr. Güthlin, warum sollten sich Ärzte für eine wissenschaftliche Karriere an der Uni entscheiden?
Wissenschaftliche Karrieren eröffnen viele Optionen, insbesondere die Möglichkeit zu habilitieren, und zwar in einem Umfeld, das die Bedürfnisse von Wissenschaftlern genau kennt. Jeder Arzt identifiziert früher oder später Versorgungsprobleme im Umfeld seines Handelns. In der Wissenschaft hat man Zeit und Ressourcen, diese genauer zu untersuchen – auch wenn man als wissenschaftlicher Mitarbeiter weniger verdient als ein klinisch tätiger Arzt.

Was tun Sie ganz konkret, um Ärzte für die Arbeit an Ihrem Institut zu begeistern?
Zum einen bieten wir Ärzten in Weiterbildung zum Facharzt für Allgemeinmedizin die Möglichkeit, sich Zeiten bei uns auf ihre Weiterbildung anrechnen zu lassen. Zum anderen helfen wir den Mitarbeitern, effektiv und schnell zu publizieren und bieten Hilfestellungen, Projekte zu konzipieren und alle Schritte wissenschaftlichen Arbeitens zu lernen.

Welche Vorteile bieten Sie als Arbeitgeber?
Wir bieten individuelle Karriereberatung an und wir bemühen uns immer um flexible Lösungen, sodass jeder Einzelne auch klinische Tätigkeiten, Weiterbildung und Familiengründung mit wissenschaftlichem Arbeiten verbinden kann. Als wissenschaftlich arbeitendes Institut sind wir besser als Kliniken oder niedergelassene Praxen darauf vorbereitet, unseren Mitarbeitern die Freiheiten zu lassen, die sie auf dem Karriereweg manchmal brauchen.

Interview mit Dr. Corina Güthlin, Leiterin des Arbeitsbereichs Forschungsmethodik und Projektmanagement am Institut für Allgemeinmedizin an der Johann Wolfgang Goethe-Universität Frankfurt am Main

Wie geht das alles zusammen?
Man sollte klinisches Arbeiten in Verbindung mit wissenschaftlichem Arbeiten so aufteilen, dass kein Umfeld mit dem anderen um Zeit konkurriert, am besten ist ein Wechsel im Wochenrhythmus. Auch Kliniken und niedergelassene Ärzte als Arbeitgeber machen diese Lösungen mit. Doch solche Hybridlösungen sind noch zu wenig bekannt.