Was für Bankdaten gilt, gilt auch für Gesundheitsdaten

Immer mehr Informationen über unsere Gesundheit sind digital verfügbar. Wie steht es um deren Schutz, wenn sich das Gesundheitswesen vernetzt? Die Technik dafür ist vorhanden. Oft fehlt es aber an Know-how für den Betrieb von sicheren E-Health-Systemen. Kaspar Geiser

Patienten wollen effiziente und unkomplizierte Behandlungen. Und sie haben ein Recht auf die Wahrung ihrer Privatsphäre. Krankenversicherer möchten möglichst viele und detaillierte Angaben über die Versicherten. Ärzte sind auf den schnellen Austausch von Krankengeschichten angewiesen und möchten ihre Diagnosen anhand von Fällen abstützen können. Die Interessen der Akteure im Gesundheitswesen sind vielfältig und manchmal widersprüchlich. Die Anforderungen an Entwicklung und Betrieb von E-Health-Systemen wird oft unterschätzt.

Das Gesundheitswesen im Rückstand

Ein Patient kommuniziert meist direkt mit seinem Arzt, klassischerweise per Telefon oder in der Praxis. Doch immer mehr Leistungserbringer und nahestehende Organisationen bieten Onlineportale. Krankenversicherer stellen gewisse medizinische Auskünfte via Internet zur Verfügung. Doch anders als beim Onlinebanking fehlen bei Gesundheitsportalen häufig sichere Mechanismen für die Übertragung von schützenswerten Daten. Was bei den Banken bereits seit mehreren Jahren state-of-the-art ist, ist im Gesundheitswesen noch immer nicht die Regel. Mit einer Ausnahme: Unter Ärzten und zwischen Ärzten und Spitälern gibt es bereits heute etablierte Standards. Hier haben sich starke Authentisierung sowie die sichere Übertragung von Daten etabliert. Eine Schwäche besteht hier, im Unterschied zu den Informatiksystemen von Banken, einzig bei der staatlichen Kontrolle. Handfeste Vorgaben, wie jene der Finma für das Finanzwesen, fehlen. Auch gibt es in der Schweiz nach wie vor eine Vielzahl verwendeter Standards, was die Zusammenarbeit erschweren kann.

Kaspar Geiser ist Geschäftsführer und Inhaber der Aspectra AG.

Technische Schranken allein reichen nicht

Ein weiteres Problem in der Kommunikation unter Fachpersonen ist die Abgrenzung des Aktionsradius. Darf ein Physiotherapeut beispielsweise alle Informationen zu einem Patienten erhalten oder nur die für die Therapie notwendigen? Wie kann sichergestellt werden, dass bei der Weiterreichung von Daten eines Patienten auch dessen Einwilligung eingeholt wurde?

Die IT kann technische Schranken setzen. Weil der Mensch aber der am schwersten zu kontrollierende Faktor ist, sind Bau, Betrieb und Überwachung solcher Schranken kompliziert und höchst aufwendig. Ein Beispiel: Ein Arzt erfasst Informationen über einen Patienten in einer E-Health-Anwendung. Er darf diese auch nachträglich einsehen und verändern. Sein Kollege aber darf diese Daten nur lesen – nach dem Einholen der Erlaubnis beim Patienten. Schützenswerte Daten stellen also hohe Anforderungen an alle Beteiligten: An den Hersteller der E-Health-Anwendung, den Betreiber und an die Anwender, die die Informationen erfassen.

Sicher gebaut – und sicher betrieben?

Die Voraussetzungen für den Bau einer E-Health Anwendung sind komplex: Welche Systeme eines Spitals beispielsweise sind für die Erbringung der E-Health-Funktionen nötig? Was sind die Betriebszeiten dieser beteiligten Systeme? Wie sicher sind sie? Wer betreut sie? Wie verläuft der Informationsfluss zwischen Leistungsnehmer- und Leistungserbringer-Systemen? Welche Risiken bestehen, wenn Teile einer Anwendung online zur Verfügung stehen? Die Entwicklung einer sicheren Anwendung ist dabei nur der Anfang, der sichere Betrieb stellt eigene Anforderungen. Bei der Entwicklung stellen sich Fragen zu Funktionen, Layout und Testing. Für den sicheren Betrieb sind Verfügbarkeit, Sicherheit und Performance entscheidend. Insbesondere die Frage nach möglichen Sicherheitsmechanismen sollte keinesfalls nur von der Entwicklung gestellt und beantwortet werden, sondern auch nach der Umsetzung – und dies permanent. Sicherheitsrelevante Elemente einer E-Health-Anwendung sollen also vom Betreiber realisiert und betreut werden.

E-Health: Mindestanforderungen für den sicheren Betrieb

Was zählt beim Betrieb einer E-Health-Anwendung zu den sicherheitsrelevanten Aufgaben und Komponenten? Die folgenden drei Punkte umreissen die Mindestanforderungen: Erstens müssen die Firewalls und die Verbindungen zu allen involvierten Systemen und deren Daten aktiv und permanent betreut werden, also auch ausserhalb der Öffnungs- und Betriebszeiten. Zweitens müssen die Systeme und Standardapplikationen aktiv überwacht und im Bedarfsfall mit den nötigen Updates versehen werden. Dazu zählen das Betriebssystem, die Datenbank und die vom Entwickler eingesetzten Applikationsserver. Drittens verfügen viele E-Health-Anwendungen über sogenannte starke Authentifizierungsmechanismen. Dies sind neben Benutzername und Passwort Streichlisten, Zertifikate oder dynamische Ein-Mal-Passwörter. Auch diese Komponenten muss der Betreiber zur Verfügung stellen.

Diese Aufgaben stellen hohe Anforderungen an das Betriebspersonal und die eingesetzten Schutz- und Sicherheitssysteme. Aber kleinere und mittlere Unternehmen verfügen in der Regel nicht über genügend qualifiziertes Personal für den sicheren Betrieb einer E-Health-Applikation.

Betreiber von E-Health-Anwendungen müssen Sicherheit und Verfügbarkeit ihrer Systeme und zugleich den Schutz von Patientendaten garantieren können. Die technischen Möglichkeiten dafür bestehen. Der Einsatz erfordert aber viel Erfahrung und Know-how – nicht nur bei den Entwicklern, sondern auch bei den Betreibern und den Anwendern. Banken und Finanzportale haben hier wichtige Erfahrungen gemacht. Anbieter von E-Health-Plattformen können und sollten sich daran orientieren. <