Zusammenschluss von IT Systemen im Gesundheitswesen

In diesem Serienteil zum Thema Informationstechnik-Sicherheit für Ärztinnen und Ärzte beleuchten wir jene Sicherheitsaspekte, die sich durch eine Übertragung von Daten über Ordinationsgrenzen hinweg ergeben.

Eine Serie von DI Michael Nöhammer

Aus rechtlicher Sicht sind, vereinfacht gesagt, Ärztinnen und Ärzte für die Datensicherheit innerhalb der Ordination verantwortlich. Werden sensible persönliche Daten aus der Ordination an andere Systeme übertragen, muss der „Datenbereitsteller" sicherstellen, dass die entsprechenden Gesetze eingehalten werden. Aus dieser Verpflichtung heraus wird man sicherstellen müssen, dass Daten nur auf wohldefinierten Wegen übertragen werden. Eine Übertragung von sensiblen persönlichen Daten per Mail oder ungesichertem Webformular ist nicht zulässig.

Befundübertragung

Unter „gerichteter Befundübertragung" versteht man die Übertragung eines Befundes an einen bestimmten Empfänger. Diese Form des Datenaustausches ist seit Mitte der 1990er Jahre unter den Produktnamen „Dame" (A1 Telekom) und „medical net" (HCS) sowie „GNV" (Ärztekammer Vorarlberg) bekannt. Grundsätzlich ist diese Datenübertragung gesetzlich und technisch als datensicher anzusehen. Das Verfahren hat sich in der täglichen Praxis bewährt, allerdings sind diese Befunde bei einem Patientenerstkontakt üblicherweise nicht verfügbar. Die Dokumente werden als signierte und verschlüsselte Mails übertragen und können von dritter Seite aus nicht eingesehen werden.

ELGA

ELGA ist ein ungerichtetes System, Dokumente werden also auf einem Dokumentenserver aufbewahrt und können dort jederzeit von berechtigten Personen abgerufen werden. Der Absender kann nicht festlegen, welche Empfänger das Dokument einsehen werden, das wird durch ELGA selbst entschieden. ELGA ist seit 2012 gesetzlich geregelt, die Datensicherheit wird bis zum Einsatz von ELGA (Anfang 2015 für Krankenhäuser, Mitte 2016 für den niedergelassenen Vertragsarztbereich) noch im Detail festzulegen sein.

Sichere Netze

Neben der Behandlung der Daten selbst – Fälschungssicherheit durch Signierung, Verwehren unbefugter Einsicht durch Verschlüsselung – kann auch der Übertragungsweg abgesichert werden. Mittels elektronischer Verfahren (VPN, Kanaltrennung, etc.) werden Datenströme getrennt geführt. Dadurch kann die Möglichkeit minimiert bzw. ausgeschaltet werden, überhaupt die Leitung „anzuzapfen" und damit Daten abrufen zu können.

Ein bewährter Vertreter dieser Gattung ist das „GIN", über das u. a. die ecard-Informationen laufen. Im Gesundheits-Informations-Netz (GIN) werden durch spezielle Router in den Ordinationen die Datenströme getrennt von eventuell vorhandenen Internetleitungen zum „Peeringpoint" (Netzwerkknoten) geführt, um dort in die weiteren Netze (Sozialversicherung, Mehrwertdienste) weitergleitet zu werden. Damit wird ein Zugriff aus dem Internet auf diese Datenströme ausgeschlossen und die Datensicherheit erhöht.

Lokale und regionale Zusammenarbeit

In manchen Regionen bieten Krankenhäuser bereits Services an, damit niedergelassene Ordinationen die Daten „ihrer“ Patienten einsehen können. Dagegen ist nichts einzuwenden, solange die Datensicherheit gewährleistet ist und z. B. die Identität der Ärzte und die Zuordnung Patient-Zuweiser genau und sorgfältig geregelt sind.

Praxistipps	
√	Nur bewährte Methoden zur Datenübertragung verwenden
√	Vom Anbieter Datenschutzerklärungen verlangen
√	Niemals Daten per Mail versenden