Veraltete Infrastruktur

Technische Probleme bei der Einführung der elektronischen Patientenakte

Obwohl die rechtlichen Anforderungen an die elektronische Patientenakte nach wie vor ungeklärt sind, müssen sich die Ärzte bereits an die dafür vorgesehene Infrastruktur anschließen und kämpfen mit Sicherheitsproblemen und veralteten Konzepten.

Von Jochen Brüggemann und Alexander Wilms

Begonnen hat das Projekt der elektronischen Vernetzung von Leistungserbringern und Patienten vor fast zwanzig Jahren als Folge eines Arzneimittelskandals. Details dazu erklären wir in einem Artikel auf Seite 54. Die ursprüngliche Idee war, Daten einfach auf der damals neuen elektronischen Gesundheitskarte zu speichern, die Patienten ohnehin von Arzt zu Arzt tragen müssen. Das Konzept wurde jedoch bald abgelöst durch die Planung einer umfassenden IT-Infrastruktur.

Zum einen war relativ schnell klar, dass nicht alle Daten einer ganzen Patientenakte auf die Karte passen würden. Zum anderen soll die Vernetzung von Arztpraxen, Apotheken, Krankenhäusern, Krankenkassen et cetera eine ganze Reihe neuer Anwendungen ermöglichen.

Von der Zeit überholt

Das Telematik-Infrastruktur genannte System wurde in den 2000er-Jahren als virtuelles privates Netz (VPN) konzipiert, in dem die Patientendaten verschlüsselt auf den zentralen Servern einiger weniger Anbieter gespeichert werden. Die Gesundheitskarte dient dabei der Authentifizierung. Um an das Netz angeschlossen zu werden, benötigen alle Teilnehmer einen speziellen VPN-Router, den sogenannten Konnektor, der unter anderem einen „Sicherheits-Chip“ mit Zertifikatsinformationen enthält. Nicht vorgesehen war die Möglichkeit, ohne diese besondere Hardware zum Beispiel über mobile Geräte auf die Telematik-Infrastruktur zuzugreifen. Patienten sollten Daten lediglich über ein „Patientenfach“ austauschen können, wobei ihr Zugang stets durch einen Arzt freigegeben werden musste.

Durch die jahrelangen Verzögerungen bei der Einführung wurde dieses Konzept von der technischen Entwicklung irgendwann überholt. Der in den Arztpraxen vorgesehene Konnektor spiegelt das praxiszentrierte Weltbild von vor 15 Jahren wider. Telemedizin, mobile Ärzte, mündige Patienten, Smartphones und Tablets kommen in diesem Ansatz überhaupt nicht vor. Infolgedessen wurde von der zuständigen Gesellschaft für Telematik-Anwendungen der Gesundheitskarte (Gematik) mehrfach nachgebessert, allerdings mit durchwachsenem Ergebnis. So ist nach aktuellen Plänen zwar durchaus ein privates Frontend für Versicherte vorgesehen, aber es ist offen, wie die Authentifizierung des Versicherten dort stattfinden soll.

Das könnte wie beim Arzt durch die elektronische Gesundheitskarte geschehen, mit der ein geeignetes Smartphone per NFC drahtlos kommunizieren würde. Allerdings ist das Verfahren bislang weder spezifiziert noch gibt es geeignete Gesundheitskarten mit eingebautem Funk-Chip. Ersatzweise soll die Authentifizierung über eine sogenannte „alternative Versichertenidentität“ möglich sein, die einen hardwareunabhängigen Zugriff auf die Patientenakte böte. Wie genau diese Versichertenidentität aussieht, ist aber ebenso wenig spezifiziert.

Die Politik wollte solche Ausarbeitungen und Nachbesserungen ohnehin nicht abwarten, um im europäischen Vergleich nicht zurückzustehen. Man entschloss

Bild: Jens Kalaene / dpa

Gesundheitskarten sollten erst die Patientendaten selbst speichern, dann doch nur die Schlüssel zu den Daten und mittlerweile sollen sie nur noch zum Zugriff auf die Schlüssel berechtigen.

sich schon 2015, mit dem Health-Gesetz die Telematik-Infrastruktur verbindlich einzuführen. Damals wurde festgelegt, dass bis Mitte 2019 alle niedergelassenen Ärzte per Konnektor an die Infrastruktur angeschlossen sein müssen. Dieses Ziel wurde allerdings schon aufgrund von Lieferengpässen verfehlt. Zudem haben viele Praxen den Anschluss aus grundsätzlichen (Datenschutz-)Bedenken verweigert – ihnen drohen nun Honorarkürzungen.

Anschlussprobleme

Praxen, die mitgemacht haben, kämpfen mit technischen Problemen: Wie der Systemadministrator Jens Ernst aufdeckte, wurden die Telematik-Konnektoren in vielen Praxen unsachgemäß installiert. Bestehende Schutzmechanismen wie Firewalls oder Virenscanner seien im Zuge der Installation abgeschaltet oder Praxen ohne Schutzmaßnahmen erstmals ans Internet angeschlossen worden. Eigentlich sollte dies der sogenannte Reihenbetrieb verhindern, bei dem eine eingebaute Firewall des Konnektors das Praxisnetz schützt. Da in dieser Betriebsart der Zugang zum Internet nicht oder nur über einen zusätzlichen, kostenpflichtigen Secure-Internet-Service möglich ist, wurde sie aber in den allerwenigsten Praxen umgesetzt.

Wegen solcher Installations- und Sicherheitsprobleme gibt es in der Zwischenzeit die ersten Anbieter, die den Konnektor im Rechenzentrum hosten. Diese von der Gematik zertifizierte Variante verringert die Betriebsaufwände der Ärzte und bietet eine höhere Verfügbarkeit, weil bei einem Ausfall einfach auf einen anderen Konnektor umgeschaltet werden kann. Allerdings stellt sich die Frage, warum überhaupt dezentrale Konnektoren in die Arztpraxen sollen, wenn man seitens der Gematik auch damit zufrieden ist, diese Endpunkte der Infrastruktur in Rechenzentren zu konsolidieren.

Zudem ist ein mindestens ebenso wichtiges Detail zurzeit gänzlich außerhalb der Diskussion: Das Zertifikat auf dem fest in den Konnektoren verbauten Sicherheits-Chip läuft in spätestens fünf Jahren ab. Ein kompletter Austausch der entsprechenden Hardware wird dann unausweichlich.

Eventuell wird dieser Zeitpunkt dann aber auch dafür genutzt, auf eine rein in Software umgesetzte Variante umzustellen. Genaueres weiß man darüber im Moment jedenfalls nicht. *(syt@ct.de)* c't

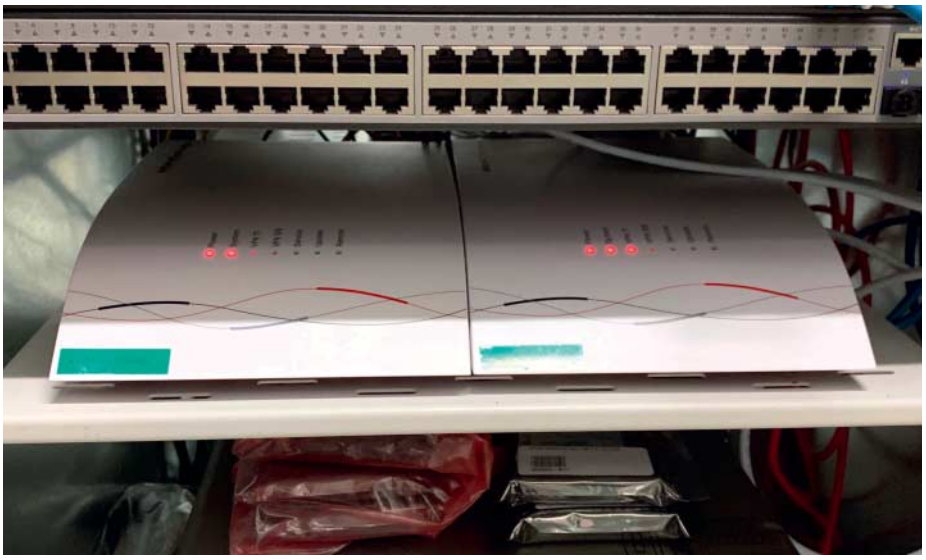

Bild: RED Medical Systems GmbH

Optisch eher Fritzbox als Big Iron: zwei Konnektoren, hier im Rechenzentrum gehostet

Konzepte und Spezifikationen der Telematik-Infrastruktur: ct.de/ytsz

Verschlusssache

Die Patientendaten werden in der Telematik-Infrastruktur auf zentralen Servern abgelegt. Um zu verhindern, dass irgendwelche Parteien – insbesondere auch die Serverbetreiber – unzulässig Patientendaten einsehen (oder gar verändern), werden diese verschlüsselt gespeichert. Die Gesundheitskarte dient dabei der Authentifizierung, damit innerhalb der zentralen Infrastruktur kein Zugriff auf die Daten möglich ist.

Allerdings enthält die Karte die benötigten Schlüssel nicht selbst, sondern erlaubt nur deren Nutzung. Abgelegt werden die Schlüssel – getrennt von den Dokumenten – in der Infrastruktur selbst, was das System verkompliziert und sicherheitstechnisch verwässert.

Diese sogenannte Ende-zu-Ende-Verschlüsselung betrifft zudem nur die eigentlichen Dokumente, etwa Befunde oder Diagnosen. Metadaten, wie sie zum Suchen und Finden der Dokumente benötigt werden, dürfen zwar auch nur verschlüsselt gespeichert werden, können aber beim Betreiber entschlüsselt werden. Das ist problematisch, weil auch solche Metadaten Informationen preisgeben können, die die Betroffenen lieber geheim hielten. Ein Beispiel sind Metadaten, die die bloße Existenz von Dokumenten eines Psychotherapeuten verraten. Zudem ist eine Entschlüsselung von Metadaten nicht zwingend erforderlich, es gibt technische Lösungen, um in verschlüsselten Daten zu suchen, ohne sie zu entschlüsseln.

Die Gematik schreibt aber nichts dergleichen vor, sondern setzt stattdessen auf „vertrauenswürdige Ausführungsumgebungen“ (VAU). Nur in diesen dürfen Metadaten entschlüsselt werden. An die VAUs stellt die Spezifikation, die frei zugänglich ist (siehe ct.de/ytsz), relativ hohe Anforderungen, was ihre Integrität, logische und physische Isolation und Vertrauenswürdigkeit betrifft. Überprüfen kann das auch der technisch versierte Nutzer aber höchstens teilweise. Ausschlaggebend ist deshalb, wie rigide die Spezifikation interpretiert und ihre Einhaltung überprüft wird. Letztlich muss man also der Gematik vertrauen, schon weil die Systeme weder Open Source noch Open Hardware sind.