

Datensicherheit in der Telemedizin

Anforderungen, Möglichkeiten und praktische Umsetzung

Martin H. Ludwig
 Martin.H.Ludwig@imagmbh.de
 IMA Gesellschaft für Informationsmanagement mbH, Dr.-C.-Otto-Str. 133, 44879 Bochum

Datensicherheit ist in der Medizin und insbesondere in der Telemedizin ein grundlegender Faktor, welcher schon in frühen Projektphasen berücksichtigt werden muss. Der Aufsatz gibt einen Überblick über die rechtlichen Vorgaben und die technischen Möglichkeiten der Datensicherheit in der Telemedizin. Er beleuchtet an Hand von Beispielen die sinnvolle Umsetzung und das Zusammenspiel der Bausteine Authentifizierung, Signierung und Verschlüsselung und legt dar, wie die Kernpunkte der Datensicherheit: Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit, Revisionsfähigkeit, Validität und Rechtssicherheit gewährleistet werden können.

Einleitung

Datensicherheit steht in der Telemedizin im Zentrum eines Spannungsdreiecks: Auf der einen Seite stehen Mediziner und kurativ Tätige: Sie müssen auf Krankengeschichte, Befunde, Werte und Bilder der Patienten unverzüglich zugreifen können. Die zweite Seite bilden Verwaltungen und Kostenträger. Ihr Ziel ist es, die sich aus den medizinischen Daten ergebenden Verwaltungs- und Abrechnungsdaten zu verwerten. Die dritte Seite des Dreiecks bildet der Patient. Er möchte optimal behandelt und bei der Wiederherstellung oder Erhaltung seiner Gesundheit unterstützt werden. Diese drei Seiten bedingen unterschiedliche Anforderungen an die Datenverarbeitung in der Telemedizin. Neben gemeinsamen Interessen, wie hundertprozentige Validität der Daten, gibt es auch widerstreitende Aspekte: Für den Mediziner ist eine schnelle Verfügbarkeit von möglichst umfassenden Daten im Allgemeinen wichtiger als weitgehender Datenschutz. Er muss dem Patienten, häufig im Kampf gegen die Zeit, helfen. Durch diese Anforderungen erklären sich die Auswahl in der aktuellen medizinischen Datenübertragung: personalisierte Befunde, die per Fax oder per Email übertragen werden. Und dem Argument, der Datenschützer wäre bei zu hohen Anforderungen für den Tod des Patienten zumindest mitverantwortlich, wenn die medizinischen Daten nicht schnell genug dem kompetenten Arzt zur Verfügung ständen, kann kaum entgegnet werden.

Der mündige Patient hingegen ist sich der Sensibilität seiner medizinischen Daten bewusst. Er weiß um die Notwendigkeit des Zugriffs durch die Mediziner seines Vertrauens, aber auch um die Gefahren der unautorisierten Verwendung. Beim einfachen Bürger ist es im günstigsten Fall nur das ungute Gefühl, dass die Nachbarin z.B. weiß, dass er zeugungsunfähig ist. Schwerer wiegende Aspekte wären Probleme am Arbeitsplatz, beim Versicherungsabschluss etc. Die möglichen Szenarien sind in der Öffentlichkeit hinlänglich bekannt. Und dies ist ja auch der Hauptgrund dafür, dass die gesetzlichen Anforderungen an den Datenschutz in Deutschland extrem streng sind.

Die Interessen der dritten genannten Gruppe sind auf Grund der Inhomogenität vielfältig. Krankenhausverwaltungen benötigen die medizinischen, patientenbezogenen Daten vor allem zu Abrechnungszwecken. Versicherungen möchten Ausgaben auf ihren Sinn hin überprüfen und Risikopersonen aus ihrem Kundenkreis ausschließen. Die Öffentlichkeit und die Wissenschaft haben ein Interesse an der Erforschung von Heilungsmethoden und Ursachen von Krankheiten. Hierfür sind prinzipiell keine personalisierten Daten notwendig. Trotzdem besteht, insbesondere bei seltenen Krankheiten, die Gefahr der Rückschlussmöglichkeiten auf Individuen.

Die Datenverarbeitung und die Datensicherheit in der Telemedizin hat nun die Aufgabe, diese widerstreitenden Interessen der Beteiligten unter Abwägung eben dieser Interessen zu befriedigen. Hierbei kann es nicht Aufgabe der Informatik sein, die Abwägung selbst vorzunehmen. Diese gesellschaftliche Aufgabe muss vom Gesetzgeber gelöst und kodifiziert werden. Hierdurch tritt jedoch ein weiteres Problem der Informatik an den Tag: die gesellschaftlichen Anforderungen wandeln sich und sind auch in unterschiedlichen Ländern stark verschieden. Es müssen also Lösungen gefunden werden, welche ein Höchstmaß an Flexibilität aufweisen.

Schließlich werden alle Lösungen von Menschen benutzt werden. Menschen sind im allgemeinen vergesslich und bequem. Seit der Erfindung des Passwortes gibt es die Notizzettel unter den Tastaturen und Aussprüche wie "Gib mir 'mal eben dein Passwort, meines ist noch nicht eingerichtet...". Lösungen in der Telemedizin müssen also für alle Beteiligten extrem einfach, logisch und konsistent sein. Das Vorgehen in der Telemedizin sollte sich von bewährten Prinzipien möglichst wenig unterscheiden.

Ärztliche Schweigepflicht

Grundsätzlich gilt, dass der Arzt Garant für die ihm anvertrauten Patientengeheimnisse ist. Neben der moralischen Verpflichtung existiert auch eine ausdrückliche, im § 203 StGB strafbewehrte Verpflichtung zur Wahrung der Geheimnisse. Deswegen ist er verpflichtet, die Daten vor dem Zugriff Unbefugter zu schützen. [4, 5]

Die Weitergabe der Patientendaten erfolgt nicht unbefugt, wenn der Patient seine Einwilligung erteilt hat. Hierbei kann der Patient auch in das Risiko einer unverschlüsselten Weitergabe einwilligen, denn das Bestimmungsrecht über die Patientendaten liegt beim Patienten. Voraussetzung hierfür ist jedoch, dass er über das Risiko der unverschlüsselten Datenweitergabe informiert wurde und insbesondere auch hinsichtlich Art und Umfang eines Zugriffs Unbefugter und den Verlust der Kontrolle über eine Weiterverbreitung der Daten. Willigt der Patient unter diesen Voraussetzungen ein, erfolgt die Datenübermittlung, auch wenn sie unverschlüsselt ist, befugt. Eine Verantwortung des Arztes – im Bezug auf die Schweigepflicht – für einen weitergehenden Schutz der Daten zu sorgen, notfalls auch gegen den durch die Einwilligung ausdrücklich erklärten Willen des Patienten, besteht nicht. Willigt z.B. der Patient in eine unverschlüsselte Datenübertragung ein, weil er seine Patientendaten nicht für so sensibel hält, dass er das Risiko eines Zugriffs Unbefugter bei einer unverschlüsselten Weitergabe eingeht um sich hierfür z.B. den Weg zu einem entfernten Spezialisten zu ersparen, verstößt der Arzt auch dann nicht gegen das Gebot der ärztlichen Schweigepflicht, wenn tatsächlich ein Zugriff Unbefugter erfolgt. [4] Die Anforderungen an die Aufklärungspflicht dem Patienten gegenüber durch den Arzt sind jedoch sehr hoch anzusetzen. Das Risiko, dass dem Arzt eine nicht genügende Aufklärung über die möglichen Risiken einer unverschlüsselten und ungesicherten Übertragung zur Last gelegt wird, ist demnach sehr hoch. Aus diesem Grunde kann von einer unverschlüsselten Weitergabe aus arzt Haftungsrechtlicher Sicht nur abgeraten werden.

Die ärztliche Schweigepflicht gilt grundsätzlich auch zwischen den Ärzten. Eine Übermittlung personenbezogener Daten an einen vor-, mit-, oder nachbehandelnden Arzt bedarf daher der Einwilligung des Patienten. [5]

Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen in der Bundesrepublik Deutschland werden durch

- das Bundesdatenschutzgesetz (BDSG),
- die jeweiligen Landesdatenschutzgesetze sowie
- die datenschutzrechtlichen Bestimmungen der jeweiligen Landeskrankenhausgesetze gebildet.

Für die Verarbeitung von Patientendaten durch niedergelassene Ärzte gelten die Vorschriften des BDSG. Für die Verarbeitung von Patientendaten durch die Krankenhäuser gelten in Bund und Ländern unterschiedliche Rechtsvorschriften. In einzelnen Ländern liegen sog. bereichsspezifische Regelungen der Verarbeitung personenbezogener Daten in Krankenhäusern vor. Soweit keine bereichsspezifischen Regelungen vorhanden sind, gelten die allgemeinen datenschutzrechtlichen Bestimmungen. [4, 5]

Fallabhängig müssen demnach die jeweiligen bestehenden Gesetzesgrundlagen bei der Übertragung patientenbezogener Daten beachtet werden. Findet z.B. ein Datenaustausch zwischen zwei niedergelassenen Ärzten statt, gelten hier allein die Bestimmungen des BDSG. Findet hingegen ein Datenaustausch zwischen zwei Krankenhäusern statt, gelten das BDSG, die jeweiligen Landesdatenschutzgesetze sowie die Landeskrankenhausgesetze für das jeweilige Bundesland...

Dokumentinformationen zum Volltext-Download

Ä

Titel:

Datensicherheit in der Telemedizin

Artikel ist erschienen in:

Telemedizinführer Deutschland, Ausgabe 2004

Kontakt/Autor(en): Martin H. Ludwig

Martin.H.Ludwig@imagmbh.de

IMA Gesellschaft für Informationsmanagement mbH, Dr.-C.-Otto-Str. 133, 44879 Bochum

Seitenzahl:

7,5

Sonstiges

4 Abb., 2 Kasten Dateityp/ -größe: PDF / 2.210 kB Click&Buy-Preis in Euro: kostenlos

Ä

Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt. [Hier gehts zum freien PDF Download...](#)