Datensicherheit in der Telemedizin

Anforderungen, MÃ¶glichkeiten und praktische Umsetzung

Martin H. Ludwig
Martin.H.Ludwig@imagmbh.de
IMA Gesellschaft fÃ¼r 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 frÃ¼hen Projektphasen berÃ¼cksichtigt werden muss. Der Aufsatz gibt einen Ãœberblick Ã¼ber die rechtlichen Vorgaben und die technischen MÃ¶glichkeiten der Datensicherheit in der Telemedizin. Er beleuchtet an Hand von Beispielen die sinnvolle Umsetzung und das Zusammenspiel der Bausteine Authentifizierung, Signierung und VerschlÃ¼sselung und legt dar, wie die Kernpunkte der Datensicherheit: Vertraulichkeit, AuthentizitÃ¤t, IntegritÃ¤t, VerfÃ¼gbarkeit, RevisionsfÃ¤higkeit, ValiditÃ¤t und Rechtssicherheit gewÃ¤hrleistet werden kÃ¶nnen.

Einleitung

Datensicherheit steht in der Telemedizin im Zentrum eines Spannungsdreiecks: Auf der einen Seite stehen Mediziner und kurativ TÃ¤tige: Sie mÃ¼ssen auf Krankengeschichte, Befunde, Werte und Bilder der Patienten unverzÃ¼glich zugreifen kÃ¶nnen. Die zweite Seite bilden Verwaltungen und KostentrÃ¤ger. Ihr Ziel ist es, die sich aus den medizinischen Daten ergebenen Verwaltungs- und Abrechnungsdaten zu verwerten. Die dritte Seite des Dreiecks bildet der Patient. Er mÃ¶chte optimal behandelt und bei der Wiederherstellung oder Erhaltung seiner Gesundheit unterstÃ¼tzt werden. Diese drei Seiten bedingen unterschiedliche Anforderungen an die Datenverarbeitung in der Telemedizin. Neben gemeinsamen Interessen, wie hundertprozentige ValiditÃ¤t der Daten, gibt es auch widerstreitende Aspekte: FÃ¼r den Mediziner ist eine schnelle VerfÃ¼gbarkeit von mÃ¶glichst umfassenden Daten im Allgemeinen wichtiger als weitgehender Datenschutz. Er muss dem Patienten, hÃ¤ufig im Kampf gegen die Zeit, helfen. Durch diese Anforderungen erklÃ¤ren sich die AuswÃ¼chse in der aktuellen medizinischen DatenÃ¼bertragung: personalisierte Befunde, die per Fax oder per Email Ã¼bertragen werden. Und dem â€žArgumentâ€œ, der DatenschÃ¼tzer wÃ¤re bei zu hohen Anforderungen fÃ¼r den Tod des Patienten zumindest mitverantwortlich, wenn die medizinischen Daten nicht schnell genug dem kompetenten Arzt zur VerfÃ¼gung stÃ¼nden, kann kaum entgegnet werden.

Der mÃ¼ndige Patient hingegen ist sich der SensibilitÃ¤t seiner medizinischen Daten bewusst. Er weiÃŸ um die Notwendigkeit des Zugriffs durch die Mediziner seines Vertrauens, aber auch um die Gefahren der unautorisierten Verwendung. Beim â€žeinfachen BÃ¼rgerâ€œ ist es im gÃ¼nstigsten Fall nur das ungute GefÃ¼hl, dass die Nachbarin z.B. we dass er zeugungsunfÃ¤hig ist. Schwerer wiegende Aspekte wÃ¤ren Probleme am Arbeitsplatz, beim Versicherungsabschluss etc. Die mÃ¶glichen Szenarien sind in der Ã–ffentlichkeit hinlÃ¤nglich bekannt. Und dies ist ja auch der Hauptgrund dafÃ¼r, dass die gesetzlichen Anforderungen an den Datenschutz in Deutschland extrem streng sind.

Die Interessen der dritten genannten Gruppe sind auf Grund der InhomogenitÃ¤t vielfÃ¤ltig. Krankenhausverwaltungen benÃ¶tigen die medizinischen, patientenbezogenen Daten vor allem zu Abrechnungszwecken. Versicherungen mÃ¶chten Ausgaben auf ihren Sinn hin Ã¼berprÃ¼fen und Risikopersonen aus ihrem Kundenkreis ausschlieÃŸen. Die Ã–ffentlichkeit und die Wissenschaft haben ein Interesse an der Erforschung von Heilungsmethoden und Ursachen von Krankheiten. HierfÃ¼r sind prinzipiell keine personalisierten Daten notwendig. Trotzdem besteht, insbesondere bei seltenen Krankheiten, die Gefahr der RÃ¼ckschlussmÃ¶glicheiten auf Individuen.

Die Datenverarbeitung und die Datensicherheit in der Telemedizin hat nun die Aufgabe, diese widerstreitenden Interessen der Beteiligten unter AbwÃ¤gung eben dieser Interessen zu befriedigen. Hierbei kann es nicht Aufgabe der Informatik sein, die AbwÃ¤gung selbst vorzunehmen. Diese gesellschaftliche Aufgabe muss vom Gesetzgeber gelÃ¶st und kodifiziert werden. Hierdurch tritt jedoch ein weiteres Problem der Informatik an den Tag: die gesellschaftlichen Anforderungen wandeln sich und sind auch in unterschiedlichen LÃ¤ndern stark verschieden. Es mÃ¼ssen also LÃ¶sungen gefunden werden, welche ein HÃ¶chstmaÃŸ an FlexibilitÃ¤t aufweisen.

SchlieÃŸlich werden alle LÃ¶sungen von Menschen benutzt werden. Menschen sind im allgemeinen vergesslich und bequem. Seit der Erfindung des Passwortes gibt es die Notizzettel unter den Tastaturen und AussprÃ¼che wie â€žGib mir Â´mal eben dein Passwort, meines ist noch nicht eingerichtet...â€œ. LÃ¶sungen in der Telemedizin mÃ¼ssen also fÃ¼r alle Beteiligten extrem einfach, logisch und konsistent sein. Das Vorgehen in der Telemedizin sollte sich von bewÃ¤hrten Prinzipien mÃ¶glichst wenig unterscheiden.

Ã„rztliche Schweigepflicht

GrundsÃ¤tzlich gilt, dass der Arzt Garant fÃ¼r die ihm anvertrauten Patientengeheimnisse ist. Neben der moralischen Verpflichtung existiert auch eine ausdrÃ¼ckliche, im Â§ 203 StGB Straf bewehrte Verpflichtung zu Wahrung der Geheimnisse. Deswegen ist er verpflichtet, die Daten vor dem Zugriff Unbefugter zu schÃ¼tzen. [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 unverschlÃ¼sselten Weitergabe einwilligen, denn das Bestimmungsrecht Ã¼ber die Patientendaten liegt beim Patienten. Voraussetzung hierfÃ¼r ist jedoch, dass er Ã¼ber das Risiko der unverschlÃ¼sselten Datenweitergabe informiert wurde und insbesondere auch hinsichtlich Art und Umfang eines Zugriffs Unbefugter und den Verlust der Kontrolle Ã¼ber eine Weiterverbreitung der Daten. Willigt der Patient unter diesen Voraussetzungen ein, erfolgt die DatenÃ¼bermittlung, auch wenn sie unverschlÃ¼sselt ist, befugt. Eine Verantwortung des Arztes â€“ im Bezug auf die Schweigepflicht â€“ fÃ¼r einen weitergehenden Schutz der Daten zu sorgen, notfalls auch gegen den durch die Einwilligung ausdrÃ¼cklich erklÃ¤rten Willen des Patienten, besteht nicht. Willigt z.B. der Patient in eine unverschlÃ¼sselte DatenÃ¼bertragung ein, weil er seine Patientendaten nicht fÃ¼r so sensibel hÃ¤lt, dass er das Risiko eines Zugriffs Unbefugter bei einer unverschlÃ¼sselten Weitergabe eingeht um sich hierfÃ¼r z.B. den Weg zu einem entfernten Spezialisten zu ersparen, verstÃ¶Ÿt der Arzt auch dann nicht gegen das Gebot der Ã¤rztlichen Schweigepflicht, wenn tatsÃ¤chlich ein Zugriff Unbefugter erfolgt. [4] Die Anforderungen an die AufklÃ¤rungspflicht dem Patienten gegenÃ¼ber durch den Arzt sind jedoch sehr hoch anzusetzen. Das Risiko, dass dem Arzt eine nicht genÃ¼gende AufklÃ¤rung Ã¼ber die mÃ¶glichen Risiken einer unverschlÃ¼sselten und ungesicherten Ãœbertragung zur Last gelegt wird, ist demnach sehr hoch. Aus diesem Grunde kann von einer unverschlÃ¼sselten Weitergabe aus arzthaftungsrechtlicher Sicht nur abgeraten werden.

Die Ã¤rztliche Schweigepflicht gilt grundsÃ¤tzlich auch zwischen den Ã„rzten. Eine Ãœbermittlung personenbezogener Daten an einen vor-, mit-, oder nachbehandelnden Arzt bedarf daher der Einwilligung des Patienten. [5]

Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen in der Bundsrepublik Deutschland werden durch

- das Bundesdatenschutzgesetz (BDSG),

- die jeweiligen Landesdatenschutzgesetze sowie

- die datenschutzrechtlichen Bestimmungen der jeweiligen Landeskrankenhausgesetze
gebildet.

FÃ¼r die Verarbeitung von Patientendaten durch niedergelassene Ã„rzte gelten die Vorschriften des BDSG. FÃ¼r die Verarbeitung von Patientendaten durch die KrankenhÃ¤user gelten in Bund und LÃ¤ndern unterschiedliche Rechtsvorschriften. In einzelnen LÃ¤ndern liegen sog. bereichspezifische Regelungen der Verarbeitung personenbezogener Daten in KrankenhÃ¤usern vor. Soweit keine bereichspezifischen Regelungen vorhanden sind, gelten die allgemeinen datenschutzrechtlichen Bestimmungen. [4, 5]

FallabhÃ¤ngig mÃ¼ssen demnach die jeweiligen bestehenden Gesetzesgrundlagen bei der Ãœbertragung patientenbezogener Daten beachtet werden. Findet z.B. ein Datenaustausch zwischen zwei niedergelassenen Ã„rzten statt, gelten hier allein die Bestimmungen des BDSG. Findet hingegen ein Datenaustausch zwischen zwei KrankenhÃ¤usern statt, gelten das BDSG, die jeweiligen Landesdatenschutzgesetze sowie die Landeskrankenhausgesetze fÃ¼r das jeweilige Bundesland...

Dokumentinformationen zum Volltext-Download
Â
Titel:
Datensicherheit in der Telemedizin
ArtikelÂ istÂ erschienenÂ in:
TelemedizinfÃ¼hrer Deutschland, Ausgabe 2004
Kontakt/Autor(en):Martin H. Ludwig
Martin.H.Ludwig@imagmbh.de
IMA Gesellschaft fÃ¼r Informationsmanagement mbH, Dr.-C.-Otto-Str. 133, 44879 Bochum
Seitenzahl:
7,5
Sonstiges

4 Abb., 2 Kasten Dateityp/ -grÃ¶Ÿe: PDF /Â Â 2.210 kBÂ Click&Buy-PreisÂ inÂ Euro: kostenlos

Â