

Rechtsgutachten analysiert Online-Risiken: Heilberufs-Portale - sicher nur mit Smartcard!

Wie riskant ist es eigentlich für den Arzt, am wachsenden Online-Geschehen im Gesundheitswesen teilzuhaben? Das erste ausführliche Gutachten zu den Rechtsaspekten solcher Prozesse gibt jetzt eine erstaunliche einfache Antwort: Wenn die richtige Technik zum Einsatz kommt, geht eine ganze Menge.

In der Diskussion um die Online-Vernetzung im deutschen Gesundheitswesen setzt der Bochumer Rechtsprofessor Dr. Georg Borges mit seinem Gutachten „Rechtliche Aspekte der Internetportale für Heilberufler“ jetzt zum ersten Mal ein verlässliches Orientierungslicht. Sein zunächst wichtigster Verdienst ist dabei die klare Identifikation der rechtsrelevanten Sensibilitäten heutiger Online-Angebote und der dahinter liegenden Prozesse. Aus Sicht des Arztes als Nutzer muss demnach das Augenmerk insbesondere folgenden Fragen gelten:

- Wie kann ich beweisen, dass ich eine Nachricht versandt habe?
- Wie kann ich sicher stellen, dass meine Nachricht nicht manipuliert wird?
- Wie kann ich verhindern, dass ein Dritter Nachrichten in meinem Namen versendet?

Wie kann ich vermeiden, dass meine Nachricht Unbefugten zugänglich wird? Bei der Analyse dieser Fragen konzentriert sich das Gutachten auf Online-Prozesse, bei denen rechtswirksame Handlungen im Rahmen von Online-Portalen realisiert sind. Typische Anwendungssituationen hierfür sind z.B. die Einweisung des Patienten zur stationären Weiterbehandlung am Online-Portal des Krankenhauses oder der Austausch der Abrechnungsdaten im Online-Portal der KV/KZV bzw. PVS.

(Rechts-)sichere Online-Prozesse

Für solche Zusammenhänge weist das Gutachten nach, dass der Einsatz angemessener technischer Hilfsmittel geeignet ist, die notwendige Rechtsverbindlichkeit für den Arzt herzustellen. Konkret: Nur die eingesetzte Technik bestimmt, ob Online-Prozesse mindestens genauso rechtssicher funktionieren wie tradierte papiergebundene Abläufe via Postversand oder persönlicher Übergabe.

Gleichzeitig macht die Studie deutlich, dass die Verantwortung für die Realisierung des angemessenen technischen Umfeldes im Kern bei den Portal-Betreibern liegt. Die Gründe hierfür liegen einerseits in der wesentlich komplexeren Beweislage der Betreiberseite: Selbstverständlich ist es die

medisign gmbh

Richard-Oskar-Mattern-Str. 6 | 40547 Düsseldorf

Tel.: 02 11 / 53 82 230 | Fax: 02 11 / 53 82 232

info@medisign.de | www.medisign.de

Geschäftsführer

Uwe Meyer-Vogelgesang | Peter Gabriel

Pflicht des Portal-Eigentümers, für die Unverfälschbarkeit und eindeutige Zuordbarkeit der dort gespeicherten Daten zu sorgen.

Andererseits folgt aus der physischen (Zwischen-)Speicherung der ärztlichen Nachricht auf dem Server des Portal-Betreibers auch seine haftungsrechtliche Verantwortung. Nicht der Arzt sondern der Portal-Betreiber hat dafür zu sorgen, dass die Anforderungen des Datenschutzes erfüllt sind – und das setzt, sobald Patientendaten ins Spiel kommen, sehr hohe Maßstäbe.

Risiken für den Arzt

Trotz der somit klar verteilten Rollen – der Arzt kann sich nicht einfach zurücklehnen und einfach alles die Betreiberseite machen lassen. Rechtlich riskante Online-Portale bergen auch für den einzelnen Nutzer Gefährdungspotenziale. Und wenn es nur ein möglicher Streit darüber ist, ob der Arzt seinen Mitwirkungspflichten fristgerecht nachgekommen ist.

Insofern bietet die Studie dem Arzt eine zweite ganz wichtige Entscheidungshilfe, indem sie ihm klare Kriterien an die Hand gibt, was ein rechtssicheres Online-Portal ausmacht und was nicht. Als zentrales technisches Unterscheidungsmerkmal identifiziert sie dazu die so genannte Authentisierung. Einfach ausgedrückt, meint das die Antwort auf die Frage: „Wer bist du?“ Im normalen Leben gibt es hierfür den persönlichen Anschein, den Personalausweis und/oder die persönliche Unterschrift. Keine Rezept, kein Befund, keine Abrechnung dürfte ohne eine entsprechende Bestätigung und sichere Kenntnis akzeptiert werden.

Und bei Online-Prozessen? Genau an dieser Stelle trifft die Studie nun erstmals eine klare Aussage, welches elektronische Äquivalent zur Authentisierung im Gesundheitswesen „angemessen“ ist. Dazu unterscheidet sie nach verfügbarer Technologie in drei Authentisierungsklassen und stellt fest: Weil sich die immer noch weit verbreitete Authentisierung mit dem sicher jedem Internet-Nutzer bekannten Verfahren „Benutzername/Passwort“ durch relativ einfache Angriffe schnell überwinden lässt, kann auf diese Weise kein rechtsverbindlicher Nachweis geführt werden.

Authentisierung via Smartcard/PIN

Schon deutlich vertrauenswürdiger verhält sich die Authentisierung mit Softzertifikaten (= Datei und Programm zur Identifikation sind auf dem Computer gespeichert). Das Gutachten argumentiert, dass eine solche Technik zumindest nahe legt, wer der Urheber bestimmter Handlungen im Portal gewesen ist. Dieser für den Arzt völlig ausreichende Anscheinsbeweis hilft dem Portalbetreiber im Streitfall allerdings nur wenig, da Softzertifikate

medisign gmbh

Richard-Oskar-Mattern-Str. 6 | 40547 Düsseldorf

Tel.: 02 11 / 53 82 230 | Fax: 02 11 / 53 82 232

info@medisign.de | www.medisign.de

Geschäftsführer

Uwe Meyer-Vogelgesang | Peter Gabriel

z.B. durch Trojaner angegriffen und somit Urheberrechtsverletzung nicht zweifelsfrei ausgeschlossen werden können.

Bleibt als dritte technische Möglichkeit die Authentisierung mit Smartcard (= eine nicht kopierbare Chipkarte regelt die komplette Identifikation). Diese erfüllt aus Sicht des Gutachtens derzeit alleinstehend die Voraussetzungen, um in Kombination mit portal-internen Funktionen eine rechtssichere Online-Portal-Kommunikation zu realisieren. Rechtlich relevant ist dabei zum Ersten die Fähigkeit eines per Smartcard/PIN geschützten Online-Portals, jede Handlung im Portal mit einer verantwortlichen Person eindeutig in Verbindung zu bringen. Daten im Portal können nicht unbemerkt verfälscht oder verschoben werden.

Für den Arzt besonders bedeutsam: Genauso wenig können Daten in einem Smartcard/PIN-geschützten Portal von Unbefugten eingesehen werden. Diese Authentisierung gewährleistet damit auch die zweite Rechtsvoraussetzung ganz im Sinne der vom Gesetzgeber für den Gesundheitsbereich geforderten Datenschutzvorgaben. Das Gutachten bewertet die mit diesem Verfahren verbundenen leicht erhöhten Anforderungen und Aufwendungen sogar als verhältnismäßig – mit der nachdrücklichen Konsequenz, dass die anderen Authentisierungsklassen im Missbrauchsfall eine Haftung der Betreiber nach sich ziehen.

Fazit

Die Nutzung von Online-Techniken ist ein wesentlicher Schlüssel, damit Ärzte sich im Zuge zunehmender Kommunikationsanforderungen wieder mehr auf die eigene Kernkompetenz konzentrieren und behandlungsfremden Aufwand reduzieren können. Damit sich diese großen Vorteilspotenziale durch Rechtsrisiken nicht ins Gegenteil verkehren, sind ärztliche Nutzer allerdings auf verantwortungsbewusst handelnde Online-Service-Anbieter angewiesen.

Zuverlässigste Anzeige für ein derartiges Verhalten ist derzeit vor allem das eingesetzte Authentisierungsverfahren: Betreiber von Online-Portalen, die alle Zugänge mit Smartcard/PIN-Techniken absichern, schützen den Arzt zuverlässig davor, dass (auch) er haftbar gemacht werden kann für Fehler und Manipulationen, die er gar nicht selbst gemacht zu haben braucht.

medisign gmbh

Richard-Oskar-Mattern-Str. 6 | 40547 Düsseldorf

Tel.: 02 11 / 53 82 230 | Fax: 02 11 / 53 82 232

info@medisign.de | www.medisign.de

Geschäftsführer

Uwe Meyer-Vogelgesang | Peter Gabriel