Rechtliche Aspekte der Internetportale für Heilberufler

Georg Borges

Internetportale für Heilberufler werden zunehmend auch für die Übermittlung rechtsverbindlicher Erklärungen und vertraulicher Inhalte genutzt. Welche technischen Voraussetzungen aus rechtlicher Sicht hierfür zu erfüllen sind, wurde jetzt erstmals durch ein Rechtsgutachten untersucht.

Internetportale für Heilberufler sind derzeit in der Diskussion. Nicht zuletzt berufsständische Organisationen und Dienstleister erwägen die Einführung derartiger Portale, da sich hierdurch bei vielen Verwaltungsvorgängen (z. B. Honorarabrechnungen) deutliche Vorteile für Betreiber und Teilnehmer erreichen lassen.

Internetportale für Heilberufler

Beispielhaft für das Leistungsportefeuille von Internetportalen für Heilberufler stehen die von kassenärztlichen und kassenzahnärztlichen Vereinigungen betriebenen Portale. Neben einem aus rechtlicher Sicht weitestgehend unkritischen öffentlichen Bereich bieten die Portale zunehmend auch einen Teilnehmerbereich für die rechtlich relevante Kommunikation zwischen Arzt/Zahnarzt und Vereinigung, nicht zuletzt Anteile im abrechnungsbezogenen Informationsfluss. Im Rahmen der Abrechnung sind insbesondere die beiden folgenden Abläufe von Bedeutung:

- Direkte Übermittlung von Abrechnungsdaten an das Portal der Berufsorganisation: Dies geschieht indem sich der Teilnehmer am Portal anmeldet und dort
  - in der Regel über ein Formular ausgelöst
  - die entsprechende Datei zur Weiterverarbeitung ablegt.

- Bereitstellung der resultierenden Honorarbescheide nebst Anlagen im Portal: Der Vertragsarzt wird elektronisch über die Verfügbarkeit benachrichtigt. Er kann sodann den Bescheid einsehen, herunterladen und ggf. ausdrucken.

Die hierbei aufgeworfenen Rechtsfragen unterscheiden sich vom Grundsatz her nicht von der Situation in der herkömmlichen Papier- oder Diskettenabrechnung. In allen Fällen geht es vereinfacht ausgedrückt darum, den Nachweis erbringen zu können, dass bestimmte Erklärungen abgegeben wurden und wer der Urheber dieser Erklärungen ist. Außerdem sollten alle Prozesse so gestaltet sein, dass datenschutzrechtlich relevante Inhalte ohne Haftungsrisiken ausgetauscht werden können.

Während allerdings für die klassischen Abrechnungsverfahren verbindlich definierte Anforderungsprofile hinsichtlich rechtssicherer Abläufe bzw. Handlungen existieren und von allen Beteiligten konsequent befolgt werden, bietet sich für den Bereich der Online-Abrechnung derzeit noch ein sehr unklares Bild. Neben der unmittelbaren Gestaltung der Portale macht dabei vor allem das eingesetzte Authentisierungsverfahren den Unterschied aus.

- Passwort: Das zentrale Authentifizierungsmerkmal beim Zugang mittels Benutzername und Passwort ist das Wissen des geheimen Passworts. Dieses Wissen lässt sich sowohl durch gezielte Angriffe als auch durch unsachgemäßen Umgang leicht kompromittieren.
- Softzertifikat: Softzertifikate sind vom Speichermedium unabhängige Zertifikatsdateien, die jeweils eine bestimmte Person/Gruppe als berechtigten Teilnehmer ausweisen. Die Authentisierung erfolgt durch das Wissen des zugehörigen geheimen Passworts und die Herrschaft über das Softzertifikat.
- Signaturkarte: Bei der Signaturkarte sind die persönlichen Zertifikate fest auf genau einem Chipmodul gespeichert, das gleichzeitig über einen internen Mikroprozessor alle Zugriffe auf die Zertifikate steuert. Damit ist der Besitz der Signaturkarte – in der Regel mit einer PIN-Abfrage kombiniert – die einzige Möglichkeit zur Authentisierung.

Vor diesem Hintergrund ist es offensichtlich, dass die weitere rechtliche Untersuchung von Internetportalen für Heilberufler direkt vom jeweils gewählten Authentisierungsverfahren abhängig ist. Die nachfolgend zusammengefassten Ergebnisse berücksichtigen dies durch eine differenzierte Bewertung, die für alle Portalbetreiber zumindest grundsätzliche Rückschlüsse hinsichtlich der für sie geltenden Rechtssicherheit und Haftungsrisiken zulässt.

Sicherer Zugang von Nachrichten in Internetportalen

Für die Betreiber der Internetportale (z. B. Kassenärztliche bzw. Kassenzahnärztliche Vereinigungen) ist es von Bedeutung, den Teilnehmern (hier Vertragsärzte) zugangsbedürftige Erklärungen, etwa den Honorarbescheid, rechtswirksam über das Portal vermitteln zu können. Diese Anforderung kann bei sachgerechter Gestaltung des Portals erreicht werden.

Der Zugang von elektronisch übermittelten Erklärungen setzt die Speicherung der Erklärung in einer Empfangseinrichtung des Teilnehmers voraus. Das Postfach des Teilnehmers im Portal ist eine solche Empfangseinrichtung, da die exklusive organisatorische Zuordnung des Postfachs für die Eigenschaft als Empfangseinrichtung ausreicht. Ebenso liegt die erforderliche Widmung zum Empfang von Erklärungen des Portalbetreibers vor.

Der Zugang erfolgt mit gelungener Speicherung. Das Übermittlungsrisiko, das grundsätzlich der Absender trägt, wird minimiert, da die Übermittlung innerhalb des Datenverarbeitungssystems des Portal-

Autor: Georg Borges
Titel: Rechtliche Aspekte der Internetportale für Heilberufler
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 46-48

betreibers erfolgt. Sofern der Teilnehmer die Speicherung schuldhaft verhindert, wird er nach dem Grundsatz von Treu und Glauben so behandelt, als wäre die Erklärung zugegangen.

Erklärungen, die nicht im Postfach gespeichert, sondern etwa an anderer Stelle des Portals abgebildet sind, werden mit Kenntnisnahme durch den Teilnehmer wirksam.

Die Bereitstellung von Erklärungen zum Herunterladen bewirkt nicht den Zugang. Dieser erfolgt erst, wenn der Teilnehmer die Erklärung tatsächlich heruntergeladen hat. Sofern der Teilnehmer gegenüber dem Portalbetreiber verpflichtet ist, am Zugang der Erklärung durch Herunterladen einer bereitgestellten Erklärung mitzuwirken, kann auf diesem Wege der Zugang gesichert werden. Mit einer Lesebestätigung kann der Nachweis vereinfacht werden, dass der Teilnehmer über die Bereitstellung zum Herunterladen informiert wurde.

Eingriffe Dritter in das Account, z. B. durch das Löschen von Daten, hindern den Zugang der zuvor gespeicherten Erklärung jedenfalls nicht, wenn der Zugriff auf das Account hinreichend gesichert ist.

Nachweise von Handlungen am Account des Teilnehmers

Für Betreiber von Internetportalen kann es wichtig sein, den Nachweis führen zu können, dass der Teilnehmer, und nicht etwa ein unbefugter Dritter, eine bestimmte Handlung am Account vorgenommen hat. Dieser Nachweis erfolgt vor allem über die Authentisierung bei der Anmeldung zum Teilnehmerbereich.

Der Beweis der Urheberschaft einer bestimmten Handlung kann im sozialgerichtlichen Verfahren, wie im Zivilverfahren, mit allen zugelassenen Beweismitteln geführt werden. Beim Nachweis der Urheberschaft aufgrund der Authentisierung erfolgt ein Indizienbeweis aufgrund mehrerer Umstände, insbesondere der Anmeldung am Portal und der Herrschaft des Teilnehmers über das Authentisierungsmedium (z. B. Passwort, Chipkarte).

Der volle Beweis der Urheberschaft wird häufig nicht gelingen, da es nicht nur theoretisch möglich ist, dass ein unbefugter Dritter sich in den Besitz des Authentisierungsmediums gebracht und damit die Anmeldung vorgenommen hat. Umso größere Bedeutung kommt dem sogenannten Anscheinsbeweis zu, durch den der Nachweis der Urheberschaft gleichwohl geführt werden kann. Dieser Anscheinsbeweis setzt voraus, dass nach der Lebenserfahrung davon ausgegangen werden kann, dass der Teilnehmer und nicht ein Dritter sich unter Einsatz des Authentisierungsmediums angemeldet hat. Ein etwa bestehender Anschein kann erschüttert werden, wenn die ernsthafte Möglichkeit eines atypischen Geschehensablaufs besteht.

Bestehen und Erschütterung des Anscheins hängen entscheidend von der Qualität des Authentisierungssystems ab. Für die Authentisierung durch Teilnehmername und Passwort haben die Zivilgerichte bisher ganz überwiegend einen solchen Erfahrungssatz und damit den Anscheinsbeweis abgelehnt, da dieses Authentisierungsverfahren zu unsicher sei. Sofern man einen Anschein annimmt, kann dieser relativ leicht, etwa durch die Möglichkeit von Phishing oder eines Trojaner-Angriffs, erschüttert werden.

Zum Anscheinsbeweis bei Authentisierung durch Passwort und Softzertifikat liegen keine veröffentlichten Gerichtsentscheidungen vor. Man wird aber einen Anschein der Urheberschaft annehmen können. Auch dieser kann aber durch die ernsthafte Möglichkeit eines Trojaner-Angriffs erschüttert werden.

Die Authentisierung durch Chipkarte und PIN begründet den Anschein der Urheberschaft des Karteninhabers. Insoweit kann die Wertung des § 371a ZPO herangezogen werden, wonach die qualifizierte elektronische Signatur, die zur Authentisierung ebenfalls Chipkarte und PIN verwendet, einen Anscheinsbeweis der Urheberschaft begründet. Auch der bei der Verwendung von ec-Karte und PIN anerkannte Anscheinsbeweis spricht für die Annahme der Urheberschaft. Der Anschein wird kaum zu erschüttern sein, da die Authentisierung mittels Chipkarte durch Phishing und herkömmliche Trojaner-Angriffe nicht überwunden werden kann. Etwas anders gilt nur dann, wenn sich künftig die konkrete Möglichkeit aufwendigerer Angriffe zeigen sollte.

Dies rechtfertigt die Erwartung, dass der Nachweis der Urheberschaft des Teilnehmers für eine an seinem Account vorgenommene Handlung bei Authentisierung durch Chipkarte und PIN regelmäßig gelingen, bei weniger sicheren Verfahren häufig scheitern wird.

Anforderungen an die Datensicherheit bei Internetportalen für Heilberufe

Der Betrieb von Internetportalen unterliegt hohen datenschutzrechtlichen Anforderungen. Dazu gehört unter anderem der Schutz gespeicherter, personenbezogener Daten gegenüber unbefugter Verwendung durch Dritte. Dieser Aspekt ist für Internetportale von besonderer Bedeutung, da die Abrechnungsdaten Gesundheitsdaten von Patienten enthalten und auf diese Daten, anders als bei herkömmlicher Abrechnung, über das Internet zugegriffen werden kann. Bei Internetportalen sind auch Phishing und ähnliche Angriffe in Betracht zu ziehen.

Das SGB X und das BDSG fordern für Gesundheitsdaten von Patienten als besonders sensitive Daten einen besonders hohen Schutz gegenüber Angriffen Dritter. Die Authentisierung durch Chipkarte und PIN hat unter den hier betrachteten Authentisierungssystemen die eindeutig beste Eignung, um internetbasierte Angriffe abzuwehren. Dagegen lässt sich die Authentisierung durch Teilnehmername und Passwort schon durch klassisches Phishing, erst recht durch Pharming und Trojaner-Angriffe relativ leicht umgehen. Auch Softzertifikate könne durch Trojaner-Angriffe überwunden werden.

Gemäß § 78a SGB X sind erforderlich und damit rechtlich geboten nur solche Maßnahmen, deren Kosten in einem angemessenen Verhältnis zum erstrebten Schutz stehen. Angesichts der hohen Bedeutung, die das Gesetz dem Schutz von Gesundheitsdaten beimisst, sprechen gute Gründe dafür, dass die mit der Authentisierung durch Chipkarte und PIN verbundenen Kosten nicht unverhältnismäßig sind. Betreiber von Internetportalen für Heilberufler müssen daher damit rechnen, dass das damit erreichte Schutzniveau gesetzlich geboten ist.

Soweit das gesetzlich gebotene Schutzniveau nicht erreicht wird, kommt im Fall eines erfolgreichen Angriffs und des Miss-

brauchs von Patientendaten eine Haftung der Betreiber von Internetportalen in Betracht.

Fazit

Die Untersuchung zeigt, dass zugangsbedürftige Erklärungen, wie zum Beispiel Honorarbescheide, mit Hilfe von Internetportalen rechtswirksam übermittelt werden können. Voraussetzungen hierfür sind eine sachgerechte Gestaltung des Teilnehmerzugangs sowie eine sichere Authentisierung via Smartcard/PIN.

Etwas schwieriger verhält es sich mit dem Nachweis der Urheberschaft. Da nie völlig auszuschließen ist, dass ein Unbefugter sich in den Besitz des Authentisierungsmediums gebracht und damit angemeldet hat, kommt dem Anscheinsbeweis die wesentliche Bedeutung zu. Dieser wird bei Authentisierung durch Benutzername-/ Passwort oder Passwort/Softzertifikat häufig scheitern.

Hinsichtlich der Haftungsrisiken für Betreiber von Internetportalen, die Gesundheitsdaten von Patienten speichern, ist schließlich das gesetzlich gebotene Schutzniveau gegenüber Missbrauch durch Dritte maßgebend. Aufgrund der besonders sensitiven Daten wird dieses Niveau mit einer Authentisierung per Benutzername/Passwort oder Passwort/Softzertifikat nicht erreicht, wohingegen die Authentisierung mittels Smartcard/PIN internetbasierte Angriffe am Besten abzuwehren vermag.

Das Gutachten ist im vollen Wortlaut über die Internetseiten des auftraggebenden TeleTrust Deutschland e. V. erhältlich: http://teletrust.de/fileadmin/files/publikationen/Studien/Gutachten_070308_Rechtl-Asp-Internetportale-f-Heilberufe.pdf.

Kontakt
Prof. Dr. Georg Borges
Juristische Fakultät
Ruhr-Universität Bochum
Universitätsstraße 150
44801 Bochum
georg.borges@rub.de