Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 13. Jahrgang, Heft 3, November 2013

Schwerpunkt:

Informed Consent für Biobanken

fokus: Biobanken: Entwicklungen und Trends
report: Mobile Medical Apps: Patient Datenschutz
report: Verdeckte Kommunikation für Whistleblowers

Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

inhalt

fokus

Schwerpunkt:
Informed Consent für Biobanken

auftakt
Die Schweiz braucht mehr Biobank
von Peter Meier-Abt Seite 81

Einwilligen in heute noch Unbestimmtes?
von Beat Rudin Seite 84

Biobanken: Entwicklungen und Trends
von Michelle Salathé Seite 86

«Generaleinwilligung» bei Biobanken
von Bruno Baeriswyl Seite 90

«Generaleinwilligung» braucht Einbettung
von Beat Rudin Seite 94

Biobank-Regelwerke im Vergleich
von Thomas Gruberski Seite 102

Biobanken: Entwicklungen und Trends

2006 veröffentlichte die SAMW medizinisch-ethische Richtlinien zu «Biobanken». Haben sie sich bewährt? Werden die darin geforderterten Standards umgesetzt? Und wie entwickelt sich die «Biobanken-Landschaft» in der Schweiz?

«Generaleinwilligung» bei Biobanken

Die Aufbewahrung von Proben und Daten in einer Biobank für noch nicht bestimmte Forschungsprojekten ist datenschutzrechtlich nicht unproblematisch. Inwieweit erscheint eine «Generaleinwilligung» der betroffenen Person zulässig?

«Generaleinwilligung» braucht Einbettung

Eine Biobank braucht ein Reglement, wenn sie mit einer knappen, übersichtlichen Einwilligung der Spender(innen) auskommen will. Es muss dem Betrieb der Biobank einen klaren Rahmen geben. Was muss in diesem Reglement geregelt werden?

Biobank-Regelwerke im Vergleich

Inwieweit sind die SAMW-Richtlinien zu Biobanken und die Vorschläge für eine «Generaleinwilligung» und die Musterreglemente kompatibel mit den auf dem 1. Januar 2014 in Kraft tretenden Humanforschungsrecht des Bundes?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktorin: Dr. iur. Sandra Husi-Stämpfli

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Verdeckte Kommunikation für Whistleblower

Im letzten halben Jahr ist die ausufernde Überwachungspraxis der NSA und anderer Geheimdienste publik geworden. Der Autor ist überzeugt, dass eine freiheitlich demokratische Gesellschaft durch das wichtige Regulativ, das Whistleblower darstellen, gewinnt. Dann stellt sich allerdings die Frage, wie Whistleblower Informationen anonym und vor allem unbeobachtbar weiterleiten können.

Mobile Medical Apps: Patient Datenschutz

Mobile Gesundheits-Apps sind längst auf Smartphones und Tablet präsent.
Die Ubiquität und Mobilität von Gesundheitsdaten wecken datenschutzrechtliche Bedenken. Ein im Heilmittelrecht verankerter technischer Systemdatenschutz wäre wünschbar.

Mehr Datenschutz in Europa

Die Anpassung des Datenschutzrechts an die technologischen Fortschritte der letzten Jahrzehnte ist in der Schweiz, im Europarat und in der EU in vollem Gange. Wohin geht die Reise im Europarat und in der Schweiz?

Aus den Datenschutzbehörden

Wer tritt als Datenschutzbeauftragte nicht wieder zur Wahl an – und warum? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzszene.

report

Kommunikationsüberwachung
Verdeckte Kommunikation für Whistleblower
von Volker Roth Seite 106

agenda Seite 109

Mobile Anwendungen
Mobile Medical Apps: Patient Datenschutz
von Michael Isler Seite 110

Rechtsentwicklung
Mehr Datenschutz in Europa
von Robert Baumann Seite 116

forum

privatim
Aus den Datenschutzbehörden
von Sandra Husi-Stämpfli Seite 122

schlusstakt
Schlooff, Kindli, schlooff!
von Beat Rudin Seite 124

cartoon
von Reto Fontana

Mobile Anwendungen

Mobile Medical Apps: Patient Datenschutz

Michael Isler, Dr., Rechtsanwalt, Wenger Plattner, Küsnacht-Zürich michael.isler@ wenger-plattner.ch

Mobile Softwareanwendungen für Smartphones und Tablets (sog. Apps) sind längst in den Gesundheitsbereich vorgedrungen. Nicht nur Patienten, sondern auch Ärzte und Pflegepersonal greifen immer häufiger zu mobilen Gesundheits-Apps («Medical Apps»), um Patienteninformationen zu erheben, zu visualisieren, zu übermitteln und zu analysieren[1].

Der eigentliche Paradigmenwechsel in der verbreiteten Nutzung von Medical Apps liegt weniger in den gebotenen Mess-, Analyse- und Diagnosemöglichkeiten, sondern in der Allverfügbarkeit und Mobilität der medizinischen Daten über drahtlose Kommunikationsnetze. Anstatt Patienteninformationen stationär zu erheben und zu bearbeiten, können diese kontinuierlich verfügbar und für vielfältige Zwecke wie Diagnose, Behandlung, Überwachung, Lehre und Forschung oder Patientenadministration nutzbar gemacht werden. An die Stelle der herkömmlichen Arztbesuche wird in manchen Fällen die Selbstbehandlung und -fürsorge treten. Mit der damit verbundenen Reduktion der Konsultationen ist die Erwartung einer spürbaren Kostenreduktion verbunden.

Sensoren als Treiber

Mobile medizinische Anwendungen, die auf dedizierten PDAs (Personal Digital Assistants) ablaufen, waren schon vor über 15 Jahren erhältlich, blieben aber ein Nischenprodukt. Ihren eigentlichen Aufschwung erlebten die Medical Apps mit der exponentiellen Verbreitung der mobilen Smartphones und Tablets («mobile Geräte»), wobei die wachsende mobile Breitbanddurchdringung zusätzlich als Katalysator wirkte. Aktuell sind im iTunes® app store in den Rubriken Medizin und Gesundheit rund 15 000 Apps erhältlich, was ungefähr vier Prozent der gesamten App-Population entspricht[2].

Die marktgängigen mobilen Geräte verfügen standardmässig über eine Vielzahl von Sensoren zur Aufnahme von Bildern und Ton oder für die Registrierung von Bewegungen. Diese können auch für medizinische Zwecke genutzt werden. Durch die Anbindung weiterer externer Sensoren mutiert das mobile Gerät in eine einfach bedienbare und leistungsfähige multifunktionale Plattform für alle denkbaren medizinischen Mess-, Diagnose- und Überwachungsanwendungen. So gibt es beispielsweise einen EKG-Monitor, der auf ein iPhone® gesteckt werden kann. Blutzuckermessgeräte, die über eine Medical App bedient werden und eine kontinuierliche Patientenüberwachung ermöglichen, stellen einen weiteren Anwendungsfall dar. Die Entwicklung ist noch nicht am Ende. Aktuell zeichnet sich ein Trend zu Lösungen ab, die Medical Apps in eine zentrale Plattform einbinden, über die medizinische Daten unterschiedlicher Provenienz aggregiert und für Medizinalpersonen wie Patienten gleichermassen zugänglich gemacht werden[3].

Geteilte Verantwortung

Die «App-Economy» hat zahlreichen kleinen und mittleren Unternehmen, ja selbst kreativen Einzelpersonen, einen niederschwelligen Marktzutritt in für sie bislang unerreichbare Geschäftsfelder ermöglicht. Ganz besonders gilt dies für den Medizinproduktebereich, der traditionell von hoch spezialisierten Unternehmen beherrscht wird. Die Verbreiterung des Anbietermarktes lässt sich hauptsächlich dadurch erklären, dass Entwicklung und Vertrieb einer Medical App nicht aus einer Hand aufgezogen werden müssen, sondern die Lasten auf mehrere unabhängige Akteure verteilt sind:

- Der App-Entwickler trägt die Verantwortung für die Programmierung der App. Als App-Entwickler gelten auch Organisationen, welche die Entwicklung an Spezialisten auslagern und die anschliessend die App unter ihrer eigenen Marke anbieten. Häufig hängt der Betrieb der App von einer externen Cloud-Plattform ab, auf der die programmierten Funktionen ablaufen. Diese Plattformen unterliegen ebenfalls der Verantwortung des App-Entwicklers.
- Der App-Distributor (app store) stellt die App über eine

Download-Plattform den Nutzern zur Verfügung. Er besorgt somit den Vertrieb.

- Der Gerätehersteller liefert das mobile Gerät samt zugehörigem Betriebssystem, auf dem die App installiert werden kann. Hersteller externer Sensoren fallen in dieselbe Kategorie.
- Der Netzwerkbetreiber stellt die Infrastruktur und Dienste zur mobilen Datenübertragung zur Verfügung.

Regulatorisches Umfeld

Medizinprodukterecht

Viele App-Entwickler sind nicht oder nur unzureichend vertraut mit den regulatorischen Anforderungen, die das Gesundheitswesen durchdringen. Am meisten unter den Nägeln brennt die Frage, ob und in welchem Umfang Medical Apps der Medizinprodukteregulierung unterliegen[4]. Die Legaldefinition des Medizinprodukts lässt keinen Zweifel: Sofern ein Computerprogramm nach der Zweckbestimmung des Herstellers für die medizinische Verwendung bestimmt ist oder entsprechend als Zubehör eines Medizinprodukts verwendet werden soll, gilt es als Medizinprodukt (Art. 4 HMG[5]; Art. 1 und 3 MepV[6]). Von der Medizinprodukteregulierung ausgenommen sind somit lediglich Gesundheits-Apps ohne ausdrückliche oder implizite medizinische Zweckbestimmung, wie beispielsweise Nachschlagewerke, Trainingshilfen oder allgemeine Gesundheits- und Fitnessberater[7].

Die Unterstellung von Medical Apps unter das Heilmittelgesetz bringt sowohl in der Phase vor als auch nach der Markteinführung eine Reihe von Verpflichtungen für die App-Entwickler mit sich. Im Vordergrund steht bei der Software-Entwicklung die Einhaltung technischer Normen, einschliesslich Programmierstandards. Im Nachmarktstadium sind insbesondere Instandhaltungs- und Produktbeobachtungspflichten zu erwähnen[8].

Das Schweizerische Heilmittelinstitut (Swissmedic) und europäische Aufsichtsbehörden haben die Entwicklung auf dem Markt der Medical Apps bislang eher passiv beobachtet. Demgegenüber veranlasste die US-amerikanische Zulassungs- und Aufsichtsbehörde Food & Drug Administration (FDA) einen regelrechten Regulierungsschub, indem sie im Juli 2011 die Kriterien für die Unterstellung der Medical Apps unter ihre Aufsicht in einem Richtlinienentwurf festlegte. Die definitive Fassung dieser Richtlinie wurde am 25. September 2013 verabschiedet[9].

Datenschutzrecht

Im Gegensatz zur Frage der Unterstellung unter die Medizinprodukteregulierung wurden die datenschutzrechtlichen Problemstellungen bei Medical Apps bislang mit erstaunlich wenig Aufmerksamkeit bedacht. Dabei führt gerade die dargestellte Zersplitterung der Verantwortung in der App-Entwicklungs- und Vertriebslandschaft zu komplexen Datenströmen und entsprechend risikobehafteten Datenübermittlungsschnittstellen. Die Gratis-Kultur der «App-Economy» nährt die Versuchung, Nutzerdaten im Gegenzug für die kostenlose Softwareanwendung als Währung zu betrachten und Datenschutzaspekte im Zuge der App-Programmierung bewusst oder unbewusst zu vernachlässigen.

Vor dem Hintergrund der dargestellten Risiken haben bereits mehrere behördliche und private Initiativen stattgefunden, die den Datenschutz bei mobilen Apps generell ins Licht rückten. So nahm die Art.-29-Datenschutzgruppe der Europäischen Union im Februar 2013 in einem Gutachten über Apps auf mobilen Kommunikationsgeräten die Datenschutzaspekte detailliert unter die Lupe und gab Handlungsanweisungen und -empfehlungen ab[10]. Fast zeitgleich erschien ein Bericht der US-amerikanischen Federal Trade Commission, welcher ebenfalls datenschutzrechtliche Anforderungen an mobile Apps und die dahinterstehende Vertriebsorganisation stellte[11]. Eine spezifisch auf Medical Apps bezogene deutsche Studie, die eine kleine Stichprobe von acht Medical Apps untersuchte, stellte schliesslich zahlreiche Verstösse gegen das Transparenzgebot und die Datensicherheit fest[12].

Zielkonflikte

Nicht mit jeder Medical App werden Personendaten bearbeitet. Sofern aber die bearbeiteten Daten einer bestimmten Person zugeordnet sind oder eine solche sich in Kombination mit zusätzlichen Identifikatoren wie IP- oder MAC-Adresse eruieren lässt, handelt es sich um Personendaten im Sinne von Art. 3 lit. a DSG[13].

Aus der Perspektive des Datenschutzes wäre es wünschbar, eine Identifizierung der Nutzer von Medical

Kurz&bündig

Mobile Gesundheits-Apps für Smartphones und Tablets sind längst in den Bereich der professionellen medizinischen Leistungserbringung vorgedrungen. Die damit verbundene Ubiquität und Mobilität von Gesundheitsdaten wecken datenschutzrechtliche Bedenken. Die geltenden Normen schützen insbesondere nur unzureichend gegen sicherheitsanfällige Medical Apps. Ein im Heilmittelrecht verankerter technischer Systemdatenschutz wäre wünschbar. Die junge App-Innovationskultur ist aber auch vor Überregulierung zu schützen.

Apps zu verunmöglichen oder wenigstens zu erschweren. Die Erwartungen des Datenschutzes geraten diesbezüglich jedoch in einen Zielkonflikt mit der Medizinprodukteregulierung. Der App-Entwickler kann die Compliance mit den gesetzlichen Nachmarktpflichten ab einer gewissen Risikoneigung nur dann effektiv sicherstellen, wenn sich die Nutzer zur Aktivierung der App bei ihm registrieren müssen. Dies ermöglicht es dem App-Entwickler, die Nutzer zeitgerecht und zuverlässig über allfällige Produktverbesserungen oder -warnungen zu informieren. Je besser die App-Entwickler ihre Kunden kennen und aus den erhobenen Daten eigentliche Gesundheitsprofile ableiten können, desto mehr dringen Datenschutzfragen in den Vordergrund.

Anwendbares Recht

Zivilrecht

Die Rechtsverhältnisse zwischen den Nutzern und den am Vertrieb einer App beteiligten Akteure sind in der Regel grenzüberschreitender Natur. Folglich stellt sich als erstes die Frage, ob die schweizerische Datenschutzordnung überhaupt anwendbar ist.

Privatrechtliche Verletzungs- und Auskunftsansprüche von betroffenen Personen gegen Datenbearbeiter unterliegen der Sonderverweisung von Art. 139 Abs. 3 i.V.m Abs. 1 IPRG[14]. Eine akzessorische Anknüpfung an ein vorbestehendes Vertragsverhältnis im Sinne von Art. 133 Abs. 3 IPRG, die bei allenfalls unmittelbarer Vertragsbeziehung zwischen den Beteiligten denkbar wäre, findet nicht statt. Die datenschutzspezifische Sonderverweisungsnorm sieht einen Strauss von möglichen Anknüpfungen vor:

- Gewöhnlicher Aufenthalt des Geschädigten,
- Niederlassung oder gewöhnlicher Aufenthalt des Verletzers,
- Ort, an dem die Persönlichkeitsverletzung vorgenommen wird oder deren Erfolg eintritt. Befindet sich dieser Ort in der Schweiz, kann daselbst auch geklagt werden (Art. 129 IPRG; Art. 5 Nr. 3 LugÜ[15]).

Ein Anknüpfungspunkt für die Berufung des privatrechtlichen schweizerischen Datenschutzrahmens ist somit in der Regel gegeben.

Öffentliches Recht

Für die Anwendung der öffentlich-rechtlichen Bestimmungen des Datenschutzgesetzes, insbesondere die Prüfungszuständigkeit des EDÖB gemäss Art. 29 DSG, gilt das Territorialitätsprinzip. Das DSG ist somit auf die Bearbeitung von Personendaten in der Schweiz anwendbar, wobei die Erhebung von Personendaten oder der Eintritt einer Persönlichkeitsverletzung in der Schweiz auch dann als Anknüpfungspunkt genügen, wenn die Daten ins Ausland übermittelt und überwiegend dort bearbeitet werden[16].

Pflichten der Beteiligten

Unter materiellrechtlichen Gesichtspunkten besteht die herausragende Besonderheit bei Medical Apps darin, dass Gesundheitsdaten als besonders schützenswerte Personendaten im Sinne von Art. 3 lit. c Ziff. 2 DSG gelten. Entsprechend darf die Bekanntgabe an Dritte – unter Vorbehalt einer zulässigen Auftragsdatenbearbeitung (Art. 10a DSG) – nur erfolgen, wenn ein Rechtfertigungsgrund, in der Regel in Form einer ausdrücklichen Zustimmung der betroffenen Person, vorliegt (Art. 12 Abs. 2 lit. c i.V.m. Art. 13 Abs. 1 und Art. 4 Abs. 5 DSG).

Die zersplitterte Entwicklungs- und Vertriebsumgebung des App-Angebots wirft sodann die Frage auf, wer welche datenschutzrechtliche Verantwortung trägt.

Im schweizerischen Recht ist – anders als im gemeineuropäischen Kontext[17] – jeder Bearbeiter von Personendaten gleichermassen zur Einhaltung der allgemeinen Bearbeitungsgrundsätze gemäss Art. 4 ff. DSG verpflichtet. Den Inhaber einer Datensammlung im Sinne von Art. 3 lit. i DSG treffen sodann zusätzliche Pflichten[18]. Man wird sich also auch der Aufgabe stellen müssen, im Mosaik der Akteure den oder die Inhaber einer Datensammlung zu eruieren.

App-Entwickler

Die App-Entwickler stehen zuvorderst an der Datenschutz-Schaltstelle. Sie entscheiden, welche Daten erhoben und wie sie bearbeitet werden können. Es ginge jedoch zu weit, dem App-Entwickler per se eine Funktion als Datenbearbeiter zuzuschreiben, wie dies die Art. 29 Datenschutzgruppe propagiert[19]. Datenbearbeitung setzt gemäss der Legaldefinition von Art. 3 lit. e DSG einen «Umgang mit Personendaten» voraus. Dies impliziert, dass der Bearbeiter direkt oder indirekt eine Möglichkeit zur Kenntnisnahme der erhobenen Personendaten haben muss[20]. Wenn die erhobenen Gesundheitsdaten zusätzlich auf einer externen Serverplattform zusammengeführt werden oder der App-Entwickler anderweitig systematisch auf die gespeicherten Daten zugreifen kann, dürfte er regelmässig auch als Inhaber einer Datensammlung gemäss Art. 3 lit. i DSG zu qualifizieren sein.

Dies ist jedoch nicht bei allen Medical Apps der Fall.

So gibt es beispielsweise pädiatrische Apps, mit denen sich Arzneimitteldosierungen für Kleinkinder anhand Alter, Gewicht und Grösse der Patienten berechnen lassen. Solche Programme sind lokal auf dem mobilen Gerät installiert und sehen keine Möglichkeit der Kenntnisnahme von Personendaten durch den App-Entwickler vor. Sofern die App sicherheitsanfällig ist und Daten über Schnittstellen zum Betriebssystem unbemerkt oder ohne ausreichende Verschlüsselung abgeführt werden können, liegt die Verantwortung für solches Handeln bei den Personen, welche diese Datenerhebungen veranlassen. Dasselbe gilt, wenn die App es einem Arzt ermöglicht, auf die Messdaten seiner Patienten über den Umfang der ihm erteilen Berechtigungen hinaus zuzugreifen, der App-Entwickler selbst aber keinerlei Zugriffsmöglichkeit auf die Daten hat. Den App-Entwickler trifft mit anderen Worten keine Pflicht, einen technischen Systemdatenschutz («privacy by design») zu gewährleisten.

Diese allgemeine Aussage wird allerdings durch das fernmelderechtlich verankerte Transparenzgebot gemäss Art. 45c FMG[21] relativiert. Nach dieser Bestimmung, die als «Cookie-Regel» bekannt ist, dürfen Daten auf fremden Geräten nur dann durch fernmeldetechnische Übertragung bearbeitet werden, wenn dies entweder für die Erbringung der Fernmeldedienste oder ihre Abrechnung erforderlich ist oder die betroffenen Personen über die Bearbeitung und ihren Zweck informiert und darauf hingewiesen werden, dass sie die Bearbeitung ablehnen können.

Art. 45c FMG ist von Art. 5 Abs. 3 der europäischen Datenschutzrichtlinie für elektronische Kommunikation[22] inspiriert. Deren ursprüngliche Fassung sah eine entsprechende Informationspflicht vor bei der Speicherung von Informationen oder dem Zugriff auf Informationen auf dem Endgerät eines Teilnehmers oder Nutzers. Die Richtlinie wurde allerdings im Jahr 2009 revidiert[23]. Im Zuge dieser Revision wich das in Art. 5 Abs. 3 verankerte Transparenzgebot einem eigentlichen Zustimmungserfordernis.

Die Regelung des europäischen Richtliniengebers und ihr helvetisches Spiegelbild divergieren in vielerlei weiteren Facetten. Im vorliegenden Kontext fällt diesbezüglich insbesondere auf, dass auch die Frage, in welchem Umfang der App-Entwickler Adressat der fernmelderechtlichen Informationspflicht ist, von den beiden verwandten Regelungskomplexen auf unterschiedliche Weise angegangen wird. Art. 45c FMG spricht lediglich den «Bearbeiter» an. Ein App-Entwickler, der ein System zur Verfügung stellt, welches eine Datenbearbeitung entgegen den fernmelderechtlichen Vorgaben zulässt, kann somit nicht belangt werden, wenn er selbst nicht als Bearbeiter agiert. Damit ist gegenüber der allgemeinen Datenschutzregelung nichts gewonnen.

Die gemeineuropäische Richtlinienvorgabe ist demgegenüber offener formuliert, indem allgemein die Speicherung von oder der Zugriff auf Informationen als gestattungspflichtig erklärt wird. Sie könnte daher als Nukleus einer «privacy by design»-Verpflichtung ausgelegt werden und die App-Entwickler in eine generelle Systemverantwortung nehmen. Die App-Entwickler hätten nach dieser Massgabe sicherzustellen, dass die technischen Möglichkeiten vorhanden sind, damit von der betroffenen Person nicht gewollte Datenbearbeitungen auf ihrem Endgerät unterbunden werden können. In diesem Sinne sollte an sich auch Art. 45c FMG ausgelegt werden, um ihm überhaupt einen gegenüber den Vorgaben des DSG eigenständigen Regelungsgehalt zu geben. De lege ferenda wäre die Einführung einer heilmittelrechtlich verankerten Datenschutzvorgabe für das Design von Medizinprodukte-Software wünschbar, wie sie für Telekommunikationsgeräte bereits Realität ist.

Geräte- und Betriebssystemhersteller

Im Gegensatz zu den App-Entwicklern gilt für die Gerätehersteller ein Systemdatenschutz: Sie müssen dafür sorgen, dass die Fernmeldeanlagen über taugliche Sicherheitsvorrichtungen zum Schutz personenbezogener Daten und der Privatsphäre der Benutzer und Teilnehmer verfügen[24]. Den Herstellern der mobilen Geräte, in die sie ihr eigenes oder ein fremdes Betriebssystem implementieren, kommt bei der Sicherstellung des Datenschutzes eine entscheidende Rolle zu, weil sie die Konfigurationsmöglichkeiten der Schnittstellen programmieren, über die eine App die auf dem mobilen Gerät gespeicherten Daten bearbeiten kann[25].

Leistungserbringer im Gesundheitswesen

Es wurde bereits erwähnt, dass immer häufiger auch Medizinalpersonen und andere Anspruchsgruppen im Gesundheitswesen Medical Apps im Rahmen ihrer dienstlichen Tätigkeit einsetzen. Je nach Rechtsgrundlage der ausgeübten Tätigkeit ist der Datenschutz für sie kantonal (z.B. bei öffentlichen Spitälern) oder durch das eidgenössische Datenschutzgesetz (z.B. bei

frei praktizierenden Ärzten) geregelt. In jedem Fall unterstehen diese Bearbeiter einer beruflichen Schweigepflicht (Art. 321 StGB[26]) und sind daher in besonderem Masse aufgerufen, sich über den Umfang der Datenbekanntgabe und Einhaltung der Datensicherheitsstandards der von ihnen beruflich eingesetzten Apps zu vergewissern.

Fernmeldedienstanbieter

Die Fernmeldedienstanbieter, welche Gesundheitsdaten übermitteln, unterstehen in erster Linie dem Fernmeldegeheimnis (Art. 43 ff. FMG); das DSG ist subsidiär anwendbar (Art. 89 FDV[27]). Es ergeben sich keine spezifischen Besonderheiten im Zusammenhang mit dem Transport von durch Medical Apps bearbeiteten Gesundheitsdaten.

Weitere Beteiligte

Zahlreiche weitere Akteure können potenziell in den Besitz von Gesundheitsdaten gelangen, die über eine Medical App bearbeitet werden. Zu denken ist etwa an App-Distributoren oder Service-Plattformen, welche Gesundheitsdaten zusammenführen und den verschiedenen Anspruchsgruppen für deren Bedürfnisse zur Verfügung stellen. Für diese gelten die Bestimmungen des Datenschutzgesetzes. Die fernmelderechtlichen Datenschutznormen sind für sie mangels Zuordnung der Speichergeräte zu den von der betroffenen Person beanspruchten Diensten nicht anwendbar.

Ein Blick über den Atlantik…

Ähnlich wie im Bereich der Medizinprodukteregulierung dürfte die regulatorische Vor-

Fussnoten

1 Vgl. O.I. Franko, / T.F. Tirrel, Smartphone App Use Among Medical Providers in ACGME training programs, J Med Systems 2012, 3135–3139; Henning Düwert / Mathias Klümper, Gesundheits-Apps: Ein neuer Trend und seine rechtlichen Herausforderungen, in: MPJ – Medizinprodukte Journal 2013, 23–30, 23 m.w.H.

2 Research2Guidance: Global mHealth Market Report 2011–2015.

3 Vgl. beispielhaft Chris Wiltz, Qualcomm Life and WebMD Partner to Bring mHealth Data to Consumers, DeviceTalk, 5 March 2013, <http://www.mddionline.com/blog/devicetalk/qualcomm-life-and-webmd-partner-bring-mhealth-data-consumers>, zuletzt besucht am 19. Juli 2013.

4 Vgl. Ben Backmann, Gesundheits-Apps im Durchbruch, MPR 2011, 73–75; Henning Düwert / Mathias Klümper (Fn. 1), *passim;* Michael Isler, Risiken und Nebenwirkungen von Gesundheits-Apps, in: NZZ Online 17. Mai 2013, <http://www.nzz.ch/aktuell/digital/medizinische-apps-rechtslage-schweiz-europa-usa-1.18083010>, zuletzt besucht am 19. Juli 2013; Philippe Fuchs/Marco Giovanettoni, Apps als Medizinprodukte – und die Folgen davon, in: Jusletter 27. Mai 2013, *passim.*

5 Bundesgesetz vom 15. Dezember 2000 über Arzneimittel und Medizinprodukte (Heilmittelgesetz, HMG), SR. 812.21.

6 Medizinprodukteverordnung vom 17. Oktober 2001 (MepV), SR 812.213.

7 Ausführlich Fuchs/Giovanettoni (Fn. 4), Rz. 11.

8 Vgl. Art. 45 Abs. 4, Art. 49 und Art. 59 HMG.

9 Mobile Medical Applications – Guidance for Industry and Food and Drug Administration Staff, <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf>, zuletzt besucht am 22. Oktober 2013.

10 Opinion 02/2013 on apps on smart devices, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>, zuletzt besucht am 19. Juli 2013.

11 Report on Mobile Privacy Disclosures, <http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf>, zuletzt besucht am 19. Juli 2013.

12 Urs-Vito Albrecht/Oliver Pramann/Christoph Noll/Tobias Jungnickel/Ute von Jan, Datensicherheit von Medical Apps – eine Stichprobe, 10. Oktober 2012, <http://plrimedapplab.weebly.com/uploads/7/4/0/7/7407163/stichprobe_datensicherheit_von_medical_apps_v17.pdf>, zuletzt besucht am 19. Juli 2013.

13 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

14 Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht (IPRG), SR 291.

15 Übereinkommen vom 30. Oktober 2007 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (Lugano-Übereinkommen, LugÜ), SR 0.275.12.

16 BGE 138 II 346 ff., 352 f, E. 3.2 m.w.H. («Google Street View»).

17 Vgl. Art. 6 Abs. 2 der Richtlinie 94/46/EG vom 24. Oktober 1995, ABl L 281 v. 23. November 1995, wonach der für die Datenverarbeitung verantwortlichen Person die Einhaltung der Datenbearbeitungsgrundsätze obliegt.

18 Z.B. Auskunftspflicht (Art. 8 DSG), Pflicht zur Registrierung von Datensammlungen (Art. 11 Abs. 3 DSG), qualifizierte Informationspflicht bei der Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 14 DSG).

19 Opinion 02/2013 (Fn. 10), 9.

20 Vgl. David Rosenthal, in: Rosenthal / Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 N 67.

21 Fernmeldegesetz vom 30. April 1997 (FMG), SR 784.10.

22 Richtlinie 2002/58/EG vom 12. Juli 2002, ABl L 201 v. 31. Juli 2002, 37.

23 Richtlinie 2009/136/EG vom 25. November 2009, ABl L 337 v. 18. Dezember 2009, 11.

24 Vgl. Art. 7 Abs. 4 lit. c der Verordnung vom 14. Juni 2002 über Fernmeldeanlagen (FAV), SR 784.101.2.

25 Opinion 02/2013 (Fn. 10), 11.

26 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.

27 Verordnung vom 9. März 2007 über Fernmeldedienste (FDV), SR 784.101.1.

28 Aktionsplan für elektronische Gesundheitsdienste 2012–2020 – innovative Gesundheitsfürsorge im 21. Jahrhundert, KOM(2012) 736 endg., 13.

29 Art. 23 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012)11 endg.

30 Aktionsplan für elektronische Gesundheitsdienste 2012–2020 (Fn. 28), 13.

reiterrolle der USA in der Telemedizin auch hinsichtlich der Datenschutzstandards Auswirkungen auf Europa zeitigen. Im Blickpunkt steht der Health Insurance Portability and Accountability Act (HIPAA). Dieses Gesetz war mit dem Hauptziel in Kraft gesetzt worden, die Abhängigkeit der Spitäler von Technologielieferanten durch proprietäre Datenformate zu lindern. Die dadurch bewirkte Datenmobilität machte einen flankierenden Datenschutz notwendig, der sich inzwischen zu einem der Hauptaspekte des Gesetzes gemausert hat. HIPAA enthält strenge Datenschutz-, Datensicherheits- und Meldepflichten bei Verstössen, welche in erster Linie von den Leistungserbringern im Gesundheitswesen (sog. «covered entities») zu beachten sind, soweit sie Gesundheitsdaten fernmeldetechnisch übermitteln. Die Auftragsdatenbearbeiter (sog. «business associates»), welche die hierfür notwendige Technologie zur Verfügung stellen, waren HIPAA ursprünglich nicht unterstellt. Dies änderte sich jedoch mit dem kürzlich erfolgten vollständigen Inkrafttreten des Health Information Technology for Economic and Clinical Health (HITECH) Act. Dieser Erlass bindet nun auch die App-Entwickler in das Datenschutzregime ein, wenn die App von Medizinalpersonen dazu benutzt wird, Patientendaten zu bearbeiten.

… und ein Ausblick

Die Förderung mobiler Gesundheitsdienste gehört in zahlreichen Staaten zum festen Kern der Gesundheitspolitik. So wird die Europäische Kommission im Rahmen des Aktionsplans für elektronische Gesundheitsdienste 2012–2020 im Laufe des Jahres 2014 ein Grünbuch herausgeben, welches sich spezifisch den mobilen Gesundheitsanwendungen widmen wird[28]. Dabei wird auch die Befassung mit dem Datenschutz nicht zu kurz kommen.

Die Art.-29-Datenschutzgruppe hat diesbezüglich bereits Leitplanken gesetzt und für die verschiedenen Akteure Verhaltensregeln und Empfehlungen aufgestellt. Oft bleibt allerdings der Wunsch Vater des Gedankens; die Realität des App-Ökosystems ist von den geäusserten Vorstellungen weit entfernt. Der Regulierungsschub aus den USA dürfte allerdings dazu führen, dass mehr denn je die Spreu vom Weizen getrennt wird, indem App-Entwickler zunehmend die Medizinprodukte- und HIPAA-Compliance als Wettbewerbsvorteil wahrnehmen. Die Entwickler gesetzeskonformer Apps werden gleich lange Spiesse fordern und mittels Anzeigen bei den zuständigen Aufsichtsbehörden den Druck auf jene Konkurrenten erhöhen, die sich nicht an die regulatorischen Vorgaben halten. Eine weitere Verschärfung dürfte die Datenschutzverordnung der EU bringen, welche insbesondere Vorgaben bezüglich Datenschutz durch Technik («privacy by design») und durch Voreinstellungen («privacy by default») verspricht[29]. Die schiere Menge der erhältlichen Medical Apps wird allerdings die Vollzugsdefizite bestehen lassen.

Trotz aller Problematik ist auch der Innovationskraft, die von mobilen App-Technologien ausgeht, Respekt zu zollen. Die aktuelle Herausforderung besteht darin, den zentralen Sicherheits- und Persönlichkeitsschutzanliegen Nachachtung zu verschaffen, ohne die neue niederschwellige Innovationskultur abzuwürgen. «All dies muss ohne Überregulierung bewältigt werden, denn es handelt sich um ein neu entstehendes Technologiecluster, das zwar geringere Kosten und Risiken birgt, aber auch geringere Renditen verspricht»[30]. ■

Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §