www.jusletter.ch

Christophe Schneble / Andrea Martani / David Shaw / Bernice Elger

Social-Media und Social-Messaging im Spital

Ethische und Rechtliche Leitlinien

Social-Messaging hat unser Kommunikationsverhalten stark geprägt. Kaum jemand nutzt heute diese Kommunikationsform nicht, sei es aufgrund der Einfachheit oder der Möglichkeit zur schnellen Interaktion. Besonders im Spital wo sensitive Daten betroffen sind, ist der Gebrauch solcher Tools sorgfältig zu planen oder soll auf klaren Richtlinien basieren. Dieser Beitrag beleuchtet einerseits den rechtlichen Kontext und gibt anderseits die Erkenntnisse aus unserer qualitativen Befragung von kantonalen Datenschutzbeauftragten und SpitaljuristInnen wieder, um schliesslich die ethischen Aspekte herauszuarbeiten und Best Practices zu formulieren.

Beitragsart: Beiträge
Rechtsgebiete: Gesundheitsrecht; Datenschutz; Informatik und Recht

Zitiervorschlag: Christophe Schneble / Andrea Martani / David Shaw / Bernice Elger, Social-Media und Social-Messaging im Spital, in: Jusletter 16. November 2020

Inhaltsübersicht

1. Einleitung

[1] Wie jüngst eine Studie von CommonTime mit 823 Teilnehmenden gezeigt hat nutzen 43% der ÄrztInnen WhatsApp und andere consumer-orientierte Plattformen, bei Ihrer täglichen Arbeit[1]. Sei es um eine(n) KollegIn um Rat bei einer Wundinfektion zu bitten oder auch um eine konsiliarische Meinung zu einem Röntgenbild einzuholen, ÄrztInnen nutzen Social-Messaging Apps vielfältig. Schon 2015 wurde in einer anderen Studie aus dem Vereinigten Königreich aufgezeigt, dass Social-Messaging Apps in der klinischen Arbeit von ÄrztInnen verbreitet sind, auch, um patientenbezogene Daten zu senden[2]. Eine weitere Untersuchung aus Irland zeigte, dass die Gesundheitsfachpersonen eines Spitales sehr oft WhatsApp für ihre Arbeit nutzten, obwohl sie sich bewusst waren, dass der Informationsaustausch durch solche Apps eine Gefahr für die Privatsphäre der Patienten darstellt[3]. Obwohl solche Untersuchungen zum Gebrauch von WhatsApp in der Schweiz nicht vorhanden sind, ist die Vermutung gross, dass aufgrund der Einfachheit und Schnelligkeit solche Tools auch in Schweizer Spitälern verbreitet sind. Dies ist problematisch, weil die Verwendung von online Dienstleistungen wie WhatsApp möglicherweise eine Datenschutzverletzung verursachen können, da personenbezogene Daten der PatientInnen ausserhalb des sicheren IT-Systems des Spitales verarbeitet werden[4].

[2] Richtlinien von Berufsverbänden, namentlich die Empfehlungen[5] der FMH, beschreiben extensiv wie der Umgang von ÄrztInnen mit Social-Media erfolgen sollte. In diesen Richtlinien wird umschrieben, wie ÄrztInnen Facebook nutzen sollen, beispielsweise im Rahmen der Arzt-

1 Martin Christopher (Ed.), Instant Messaging in the NHS – Healthcare provider responses to the NHS consumer messaging & unsanctioned data sharing crisis, https://alertiveworkforce.com/uploads/webpage-documents/5a9b043c-fa3b-4d6c-9a7c-39b7901dddbc.pdf, 2015.

2 M. H. Mobasheri et al., The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study. BMJ Innov, 2015, S. 174–181.

3 D. M. O'Sullivan et al., WhatsApp doc?. BMJ Innov, 3(4), S. 238–239.

4 Henning Kropp/Uwe Günther, Deutsches Ärzteblatt, l 2017; S. 114 ff.

5 Fmh Verbindung der Schweizer Ärztinnen und Ärzte, Umgang mit Sozialen Medien – Empfehlungen für Arztinnen und Arzte, 2016, S 15 ff.

Patienten-Beziehung oder in der Kommunikation mit Arbeits- und BerufskollegInnen. In der Schweiz fehlen jedoch spezifische Richtlinien zum Umgang mit Social-Messaging, wie sie jüngst der National Health Service (NHS) in England herausgegeben hat[6]. Diese Richtlinien gehen intensiv auf den Umgang mit Social-Messaging ein und geben auch Sicherheitsempfehlungen für den Einsatz der gängigen Social-Messaging Apps wie z.B. «WhatsApp» oder «Telegram». Die Empfehlungen der FMH fokussieren sich, im Gegensatz, auf soziale Medien, und, obwohl sie WhatsApp nennen, enthalten sie keine Empfehlungen für den Umgang mit Social-Messaging.[7]

[3] Im Rahmen unseres qualitativen Forschungsprojekts «Big Data Research Ethics»[8], führten wir Interviews mit SpitaljuristInnen und kantonalen Datenschutzbeauftragten durch. Ein Fokus der Interviews lag auf der Verknüpfung von verschiedenen Spitaldaten miteinander. In diesem Zusammenhang wurde auch der Gebrauch von Social-Media und Social-Messaging von mehreren Interviewten angesprochen. Zusätzlich zu den qualitativen Experteninterviews wurden auch die rechtlichen Rahmenbedingungen analysiert; diese spielen gerade im Umgang mit sensiblen Daten, wie es Gesundheitsdaten sind, eine entscheidende Rolle.

[4] Der vorliegende Beitrag hat zwei Ziele: Zum einen werden die wichtigsten Erkenntnisse aus den Interviews bezüglich des Themas Social-Messaging/Social-Media im Spital analysiert und eingeordnet. In einem zweiten Schritt soll aufgezeigt werden, wie der Einsatz solcher Instrumente aus ethischer und rechtlicher Sicht gerechtfertigt werden kann.

2. Methode

2.1. Sampling

[5] Die Studie ist Teil des Forschungsprojekts «Big Data Research Ethics». Im Rahmen des Projekts wurden Interviews mit Forschenden, kantonalen Datenschutzbeauftragten und SpitaljuristInnen in der Schweiz und in den USA im Zeitraum von 2017 bis 2019 durchgeführt. Für die vorliegende Studie wurden alle 20 in der Schweiz getätigten Experteninterviews mit Datenschutzbeauftragten und SpitaljuristInnen ausgewertet, jeweils zur Hälfte kantonale Datenschutzbeauftragte (n=10) und SpitaljuristInnen/Datenschutzverantwortliche (n=10). Bei der Rekrutierung wurde Sorge getragen, dass ExpertInnen aus den unterschiedlichen Sprachregionen der Schweiz und Kantone vertreten sind, damit die interviewten Personen ihre Erfahrungen mit kantonal unterschiedlichen Datenschutzgesetzen einbringen konnten, die für die öffentlichen Institutionen inklusive Universitäts- und Lehrspitälern relevant sind.

[6] Da es sich beim vorliegenden Projekt um eine nationale Studie handelt, wurde die Zuständigkeit via Ethikkommission Zentral- und Nordwestschweiz (EKNZ) abgeklärt. Diese erklärte sich als «nicht zuständig», was bedeutet, dass die Studie nicht unter das Humanforschungsgesetz fällt und in allen Kantonen ohne weitere Auflagen durchgeführt werden konnte.

---

6 NHS England, Information governance considerations for staff on the use of instant messaging Software in acute clinical settings, 2018.

7 In der Liste der Kategorien sozialer Medien, worauf sich die Empfehlungen richten (S. 8), fehlen Social-Messaging Apps wie WhatsApp oder Telegram. Fmh Verbindung der Schweizer Ärztinnen und Ärzte, Umgang mit Sozialen Medien – Empfehlungen für Arztinnen und Arzte, 2016.

8 NFP 75, Big Data, http://www.nfp75.ch/de/projekte/modul-2-gesellschaftliche-und-regulatorische-herausforderungen/projekt-elger.

2.2. Interviews

[7] Bei den Interviews handelte es sich um offene semistrukturierte Interviews, die im Durchschnitt ca. eine Stunde dauerten. Sie umfassten Fragen zum Thema Dateneigentum, zur Unterscheidung Bio-Samples versus reine Daten, zum Umgang mit Social-Media Daten in der Forschung sowie diversen Fragen zum Thema Datenschutz und zu Big Data.

2.3. Datenanalyse

[8] Die Interviews wurden mittels der Software MAXQDA codiert und mittels thematischer Inhaltsanalyse[9] ausgewertet. Hierzu wurden die Interviews gelesen, in verschiedene Teile unterteilt und mit verschiedenen Codes versehen, um Ähnlichkeiten in den Interviews hervorzuheben. Ein weiterer Forscher (D.S.) überprüfte die Codes, um sie zu präzisieren und zu verfeinern. Falls es Unterschiede in der Codierung gab, wurden diese diskutiert und ein Konsens gesucht. Für den vorliegenden Beitrag wurden nur die Abschnitte der Interviews untersucht, welche zum Themenkomplex Social-Messaging und Social-Media im Spital gehören. Das Thema Social-Messaging wurde nicht von allen Teilnehmenden angesprochen. Die vorliegende Analyse wurde durchgeführt aufgrund der erheblichen ethisch-rechtlichen Relevanz des Themas. Um die Aussagen in den Kontext der gängigen Praxis zu stellen, wurde zudem eine Analyse der gängigen Richtlinien und des rechtlichen Kontexts durchgeführt (siehe Diskussion).

3. Resultate

[9] Nachfolgend werden die Resultate der thematischen Analyse des Themenkomplexes Social-Messaging und Social-Media im Spital detailliert vorgestellt.

3.1. Nutzung von Social-Messaging / Datenaustausch im Spital

[10] Die Nutzung von Social-Messaging in der täglichen Arbeit ist nach Ansicht der interviewten ExpertInnen auch im klinischen Bereich ein Bedürfnis für ÄrztInnen. Insbesondere für die Terminplanung und für den unkomplizierten Tausch von Diensten sei Social-Messaging sehr beliebt. Hierbei seien in der Regel keine besonders schützenswerten Patientendaten involviert und der Einsatz wird daher von den im Spital tätigen ExpertInnen als wenig heikel angesehen. Kritischer war die Sicht der Datenschutzbeauftragten beim Einsatz von Social-Messaging auch zu Konsiliarzwecken:

> «*Ich bin jetzt gerade daran, eine Weisung zu schreiben über Social-Media und sage im Patientenkontext im Arbeitskontext: No WhatsApp. Jetzt sagen die [Anmerkung: die Ärzte] aber um Dienste abzutauschen muss das aber möglich sein und so. Jetzt hat dann die Diskussion angefangen, dass es sowieso gang und gäbe ist, dass man Röntgenbilder … [dass]*

[9] Virginia Braun/Victoria Clarke, Using thematic analysis in psychology, Qualitative Research in Psychology, 2006, S. 77 ff.

mit dem Handy einen Screenshot macht – und es dem Kollegen schnell weiterschickt. Und ähhh, das ist dann wirklich datenschutzmässig heikel. (CHLR07)[10]»

[11] Einer der Teilnehmenden weist jedoch darauf hin, dass das Teilen von Daten, wenn nicht zumindest mit WhatsApp, dann aber lokal möglich sein müsse. Insbesondere erwähnt er den Gesichtspunkt, dass Vertrauen eine wichtige Rolle im Arzt-Patienten-Verhältnis spielt und dem Arzt a priori auch ein besonnener Umgang mit Daten attestiert werden sollte, ähnlich wie das Vertrauen des Patienten in den Chirurgen anlässlich eines Eingriffs:

«Wir müssen sicherstellen, dass unsere Ärzte nicht missbräuchlich mit diesen [Daten umgehen], einerseits, dass Sie damit sorgfältig umgehen. WhatsApp ist wirklich ausser Diskussion, aber wir müssen dem Arzt vertrauen, dass er bei Bedarf einmal eine Datei extern abspeichern darf und er das nicht irgendwo verhökert und so. Wir vertrauen dem Chirurgen ja auch, dass er den Patienten in der Operation ja auch nicht umbringt. Also muss ich Ihm auch vertrauen, dass er mit den Daten allfällige missbräuchliche Sachen eben nicht macht. (CHLR07)»

[12] In welche Richtung die künftige Nutzung von Social-Messaging gehen könnte, beschreibt ein weiterer Teilnehmer. Er schlägt die Integration von Third-Party Apps in den Klinik-Alltag vor, weil der Einsatz von eigenen Geräten der Angestellten (BYOD; Bring Your Own Device) eine Herausforderung darstelle. Durch die Bereitstellung von dedizierten Applikationen, die durch die Klinik zur Verfügung gestellt würden, könnten Risiken minimiert und mit den dadurch erhöhten Sicherheits-Mechanismen die Privatsphäre garantiert werden:

«Wir haben einige von denen, die wir managen können. Aber es ist die Realität, dass jeder ein Handy in der Tasche hat. Wir schreiben gerade eine Richtlinie, die besagt das man nur Apps nutzen darf, die von uns autorisiert sind. (. . .) Bei uns, ist es illegal, es zu benutzen, aber die Leute haben es auf ihrem Handy. So haben wir unsere eigene Version eines Krankenhaus WhatsApp, aber es ist eine App. Und wir können dort alles kontrollieren. Ich meine, wir kontrollieren, wir überwachen, dass der Schutz und die Privatsphäre des Patienten und der Mitarbeitenden respektiert wird. (CHLR36).»

3.2. Codes of Conducts

[13] Klare Regeln, insbesondere im Umgang mit Gesundheitsdaten, spielen in den Augen der interviewten ExpertInnen eine wichtige Rolle. Neben den rechtlichen Regularien spielen auch zusätzliche institutionsspezifische Richtlinien (Soft Law) eine entscheidende Rolle für einen ethisch verantwortungsvollen Umgang mit Social-Media. Es erstaunt somit nicht, dass viele der Befragten institutionelle «Codes of Conducts» entwickelt haben. Diese sind oftmals sehr breit angelegt und umfassen Vorschriften von der Kleidung bis zu Social-Media.

[10] Die Pseudonymisierung der Teilnehmer erfolgt nach dem folgenden Schema <Land><Sample Gruppe><Fortlaufende Nummer> – Im Falle von CHLR07. Bedeutet dies Schweizer Gruppe, Juristen, Interview7.

> «*Ja. Auf jeden Fall. Wir haben Verhaltensregeln, sagen wir mal, die von der Kleidung über den Umgang mit Patienten bis hin zum Fotografieren reichen.... Social-Media und so weiter. (CHLR10.)*»

[14] Gleichzeitig wird festgehalten, dass die Umsetzung einer (Informatik-/Social-Media-) Richtlinie von zentraler Bedeutung wäre, aber dass in einem restriktiven finanziellen Umfeld oftmals die Ressourcen, und auch die Weisungsbefugnisse und Sanktionsmassnahmen fehlen, um die Richtlinie optimal umzusetzen und sicherzustellen, dass die darin enthaltenen Regeln auch befolgt werden.

> «*Wir haben auch eine Social-Media Richtlinie, wo wir darlegen was man sollte oder eben nicht sollte. Aber eine Richtlinie haben, heisst noch lange nicht, dass diese gelebt wird. Und dort fehlt es dann eben an den Ressourcen, um diese gut zu implementieren im Unternehmen und auch an Massnahmen wenn dies nicht eingehalten wird. (CHLR08).*»

4. Diskussion

[15] Die Resultate der Interviews zeigen, dass die befragten SpitaljuristInnen und Datenschutzbeauftragten sich über die Verbreitung von Social-Messaging Apps im Klinikalltag und der damit verbundenen Risiken bewusst sind. Sie nehmen es als ein Bedürfnis der ÄrztInnen war, Social-Messaging nicht nur zur Planung der Dienste und zum Abtauschen derselbigen zu nutzen, sondern auch im Umgang mit schützenswerten Daten wie zum Beispiel zu Konsiliarzwecken. Im Nachfolgenden werden die Resultate aus unserer Untersuchung nochmals Punkt für Punkt aufgegriffen und in den Kontext der bestehenden Verbandsrichtlinien und den rechtlichen Kontext gesetzt. Schlussendlich werden ethische Aspekte diskutiert um dann mögliche «Best Practices» im Umgang mit Social-Messaging im Spitalkontext zu formulieren.

4.1. Richtlinien

[16] Richtlinien spielen, wie auch die Teilnehmenden der Studie festgestellt haben, eine wichtige Rolle für den verantwortungsvollen Umgang mit Social-Media/-Messaging Technologien. Neben den in den Interviews angesprochenen institutionellen Richtlinien haben auch Berufsverbände Richtlinien im Umgang mit den sozialen Medien veröffentlicht, z.B. der Berufsverband der Schweizer Ärztinnen und Ärzte (FMH). Diese Richtlinien zielen in die gleiche Richtung, wie die von den Teilnehmenden angesprochenen institutionellen Richtlinien und es sind drei Stossrichtungen auszumachen: 1) Allgemeine Verhaltensempfehlungen, 2) Technisch/organisatorische Massnahmen 3) Kontakt zu Patienten. Die Richtlinien der FMH gehen sehr detailliert auf den Gebrauch von Social-Media ein und liefern den ÄrztInnen auch konkrete Modellbeispiele, an welchen sie sich orientieren können. Auf der anderen Seite sind Richtlinien, wie Sie der NHS zum Thema Social-Messaging in sehr detaillierter Weise entwickelt hat und die insbesondere auf die Vor- und Nachteile der einzelnen Lösungen fokussieren, in der Schweiz bislang nicht auszu-

machen[11]. Die Empfehlungen zum Umgang mit Sozialen Medien der FMH sind ein guter Start, sind aber eher generell gehalten und nur schwer auf die den speziellen Fall des Social-Messaging anzuwenden, des Weiteren lassen sie auch praktische Hinweise vermissen. Die Richtlinie des NHS bieten im Gegenteil eine Liste von konkreten Kriterien, welche den Gesundheitsfachpersonen helfen können, die sicherste Social-Messaging App auszuwählen[12]. Darüber hinaus gibt die englische Richtlinie auch zusätzliche praktikable Vorschläge, wie die App vom Fotoarchiv des Handys zu trennen (*unlink*), oder die Teilnehmer einer beruflichen Messaging-Gruppe regulär zu kontrollieren/prüfen, vor allem wenn man Administrator der Gruppe ist[13].

4.2. Sicherstellung der Einhaltung der Richtlinien

[17] Eine grosse Problematik, die sich im gesamten Datenschutzumfeld stellt, ist die Frage der Sicherstellung der Einhaltung solcher Richtlinien. Limitierend sind häufig die fehlenden Ressourcen, dies wird von den interviewten ExpertInnen mehrfach erwähnt. Die Problematik wird vor allem auf der kantonalen Ebene von den Datenschutzbeauftragten mit Besorgnis wahrgenommen, die für die öffentliche Verwaltung zuständig sind und somit auch die Oberaufsicht über Datenschutz im Spital haben. Die Zunahme der Datenmenge und der damit gekoppelte Einsatz neuer Technologien (wie im vorliegenden Beispiel Social-Messaging, aber auch maschinelles Lernen) wird zukünftig einen vermehrten Einbezug von Datenschutzbeauftragten erfordern.

[18] Gerade aber auf der Ebene der kantonalen Datenschutzbeauftragten die letztendlich eine Kontrollfunktion über die öffentlichen Institutionen haben, hat sich gezeigt, dass diese oftmals personell schlecht ausgestattet sind, und dass ihnen die notwendigen Ressourcen oft fehlen[14]. Die Ausstattung reicht jeweils von einer Person in Teilzeit bis hin zu grösseren Teams. Erschwerend kommt hinzu, dass Spitäler aufgrund ihrer juristischen Form jeweils auch dem eidgenössischen Datenschutzbeauftragten unterstellt sein können.

4.3. Gesundheitsdaten

[19] Gesundheitsdaten sind besonders schützenswerte Daten im Sinne des Datenschutzgesetzes (DSG, Art. 3)[15]. Das DSG bezeichnet die folgenden Kategorien als besonders schützenswert 1) die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, 2) die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, 3) Massnahmen der sozialen Hilfe und 4) administrative oder strafrechtliche Verfolgungen und Sanktionen[16]. Dies steht im

11 DigitalHealth, NHS issues guidance on use of instant messaging apps, 2018, https://www.digitalhealth.net/2018/11/nhs-issues-guidance-use-of-instant-messaging-apps/.

12 Die fünf Kriterien sind konkrete Eigenschaften, die Sicherheit (oder Unsicherheit) einer Social-Messaging App bestimmen: 1) End-to-End Encryption; 2) End User Verification; 3) Passcode Protection; 4) Remote-wipe; 5) Message retention. Eine Tabelle ist auch Verfügbar, die zeigt, welche der meistverwendeten Social-Messaging App (Whatsapp, Viber, Telegram und Signal) die Eigenschaften darbietet. Siehe NHS England, Fussnote 1, Seite 3–4.

13 Siehe NHS England, Fussnote 1, Seite 5.

14 Privatim, Digitaler Staat braucht Datenschutz, 2018, https://www.privatim.ch/de/digitaler-staat-braucht-datenschutz/.

15 Bundesgesetz über den Datenschutz vom 19. Juni 1992, Stand am 1. Januar 2014 (DSG; SR 235.1).

16 Die revidierte Fassung des Datenschutzgesetzes, welche am 25. September 2020 gutgeheissen wurde (die 100-tägige Referendumsfrist läuft), fügt zusätzliche Kategorien von besonders schützenswerten Personendaten hinzu,

Einklang mit den meisten kantonalen Datenschutzgesetzen, die ähnliche Normen enthalten. So definiert zum Beispiel das Gesetz über die Information und den Datenschutz (IDG)[17] des Kantons Zürich in § 3. ebenfalls Gesundheitsdaten als besondere Personendaten. Dies gilt ebenfalls für das IDG[18] des Kantons Basel-Stadt (§3 Abs. 4), sowie das Genfer Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD, Art. 4)[19]. Eine Ausnahme bildet das Datenschutzgesetz des Kantons Bern (KDG)[20] das in Artikel 3 lit. b indirekt Gesundheitsdaten unter dem Begriff «geistigen oder körperlichen Zustand» subsumiert.

[20] Zur Bearbeitung dieser Daten verlangt das DSG in manchen Fällen eine Rechtfertigung, zum Beispiel in Form einer ausdrücklichen Bewilligung des Datensubjekts (DSG, Art. 4 Abs. 5). Überdies regelt das DSG in Art. 12 die Weitergabe von Daten durch private Personen und vermerkt, ein Datenbearbeiter «darf nicht: (...) ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben». Im Fall von Social-Messaging wäre WhatsApp (bzw. sein Besitzer Facebook) als Dritter anzusehen, und wenn eine private Person die Daten einer anderen bekanntgeben wollte, müsste ein Rechtfertigungsgrund vorliegen. Wenn ein Arzt/Ärztin als private Person die Daten eines Patienten durch eine Social-Messaging App weitergeben wollte, müsste er z.B. die Einwilligung des Patienten einholen. In einem öffentlichen Spital kann aber der Arzt/Ärztin nicht als private Person agieren, sondern handelt als Teil des öffentlichen Organs[21], d.h. der Arzt/Ärztin untersteht in diesem Fall dem kantonalen Datenschutzgesetz. Im Kanton Basel-Stadt würde das zum Beispiel heissen, dass die Bekanntgabe der Gesundheitsdaten eines Patienten durch den Arzt/Ärztin einer der folgenden Anforderungen entsprechen müsste: 1) der Arzt/Ärztin ist durch ein Gesetz dazu ermächtigt; 2) die Bekanntgabe ist notwendig zur Erfüllung einer in einem Gesetz klar umschriebenen Aufgabe; 3) der Patient hat zugestimmt oder 4) der Patient ist nicht in der Lage seine Zustimmung zu geben, aber die Bekanntgabe liegt in seinem Interesse und seine Zustimmung darf in guten Treuen vorausgesetzt werden (§ 22 IDG BS).

[21] In Art. 35 regelt das DSG zudem die Verletzung der beruflichen Schweigepflicht, welche insbesondere im Arzt-Patienten-Kontext von Relevanz ist. Ein Verstoss gegen die berufliche Schweigepflicht wird auf Antrag mit Busse bestraft. Aufgrund der kantonalen Leistungsaufträge, die ein Spital erhält – und dies gilt auch für privat-rechtliche Körperschaften – sind zudem die entsprechenden kantonalen Datenschutzgesetze zu berücksichtigen[22].

4.4. Arztgeheimnis

[22] Neben dem Datenschutzgesetz spielt, wie bereits erwähnt, auch die berufliche Schweigepflicht gemäss Art. 321 StGB eine Rolle. Während Daten an Dritte nur weitergegeben werden

wie z.B. genetische Personendaten (Art. 5 lit. C Abs. 3). Ein Text des neuen Datenschutzgesetzes ist hier verfügbar: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059.

17 Gesetz über die Information und den Datenschutz (IDG), Kanton Zürich (ZH).

18 Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG), Kanton Basel Stadt (BS).

19 Loi sur l'information du public, l'accès aux documents et la protection des données personnelles(2) (LIPAD), Etat de Genève.

20 Datenschutzgesetz (KDSG), Bern.

21 Bernhard Rütsche, Datenschutzrechtliche Aufsicht über Spitäler, digma. Schriften zum Datenrecht, 6, 2012.

22 Ebd.

dürfen, wenn dazu ein Rechtfertigungsgrund vorliegt – z.B. hier die Einwilligung des Patienten (oder bei dessen Urteilsunfähigkeit einer berechtigten Vertretungsperson) – darf bei der Betreuung eines Patienten durch ein Ärzteteam (was in der Klinik der Fall ist) davon ausgegangen werden, dass eine stillschweigende Einwilligung für den Informationsaustausch innerhalb des Teams besteht[23]. Diese Regelung, so wie sie der eidgenössische Datenschützer formulierte, lässt demnach einen Interpretationsspielraum für den Gebrauch solcher Apps im Klinik-Alltag offen. Dies steht im Widerspruch zum DSG da im Falle von Social-Messaging der Anbieter als «Dritter» angesehen werden könnte, da dieser die Daten bearbeiten könnte. Das Einholen einer Zweitmeinung bei einem/r KollegIn ausserhalb des Betreuungsteams stellt allerdings eine Weitergabe von Daten dar, zu welcher der Patient einwilligen muss[24], sofern die Anfrage nicht anonymisiert wird.

4.5. Daten in der Cloud

[23] Bei Social-Messaging Apps[25] werden die Daten oftmals im Ausland gespeichert und verarbeitet. Die Haftung zwischen dem Anwender und dem Anbieter wird in den allgemeinen Geschäftsbedingungen geregelt, oftmals auch nach ausländischem Recht. Dieser Umstand erschwert eine Durchsetzung allfälliger Haftungsansprüche. Teilweise stehen die Regelungen auch im Konflikt zu den lokalen Regeln[26]. Anders sieht es beim Datenaustausch durch das geplante elektronische Patientendossier (EPD) aus; hier wird die Infrastruktur der Implementation von Patientendossiers durch verschiedene Stamm-Gemeinschaften betrieben, welche dem Schweizer Recht unterstehen[27]. Mögliche Haftungsgrundlagen im Fall eines rechtswidrigen Datenspeicherns in der Cloud sind gemäss Tag[28] Art. 97 des Obligationenrechts (OR), die Deliktshaftung nach Art. 41 OR sowie die Produkthaftung gemäss dem Bundesgesetz über die Produkthaftpflicht (PrHG) vom 18. Juni.

4.6. Ethische Aspekte

[24] Neben der in den vorangehenden Paragraphen dargelegten rechtlichen Situation spielen auch ethische Überlegungen beim Einsatz von Social-Messaging für den Austausch von Patientendaten eine wichtige Rolle. Abgeleitet von der in der modernen Bioethik weitverbreiteten Prinzipienethik[29] sind die wichtigsten ethischen Grundprinzipen für den verantwortungsvollen Umgang mit sensiblen Gesundheitsdaten: a) Respektierung der Autonomie eines Menschen, b) Rechenschaftspflicht, c) Datenschutz und d) Datenfairness[30]. Diese werden im Nachfolgenden

23 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Schweigepflicht, 2019, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/schweigepflicht.html.

24 Vgl. vorherigen Paragraf.

25 Social-Messaging Apps werden definiert als Apps welche den Austausch von Text aber auch andern Dokumenten zwischen einer oder mehreren Personen erlauben.

26 Brigitte Tag, Gesundheitsdaten für die klinische Forschung und «Datenökonomie» in der Zukunft, Thema im Fokus, Ausgabe 137-August 2018.

27 Vgl. Bundesgesetz über das elektronische Patientendossier vom 19. Juni 2015 (EPGD), SR 816.1.

28 Ebd.

29 Andreas Vieth, Tom L. Beauchamp, James F. Childress, Principles of Biomedical Ethics, 6. Auflage, 2009.

30 Effy Vayena, Ein ethischer Rahmen für den Austausch von Gesundheitsdaten, Schweizerische Ärztezeitung, 2017, 98(36), S. 1138–1140.

kurz mit einem spezifischen Fokus auf ihre Umsetzung in Bezug auf das Teilen von Daten durch Social-Messaging Apps vertieft.

[25] Der *Respekt vor der Patientenautonomie*, eines der wichtigsten Prinzipen der modernen biomedizinischen Ethik[31], verlangt, dass die Wünsche des Patienten respektiert und die Würde der Person im Behandlungskontext oder in der Forschung geachtet werden. In Bezug auf den Umgang mit Daten bedeutet dies, dass die Datenbearbeitung und ein späteres data-sharing nur mit Einwilligung des Betroffenen erfolgen kann, solange es nicht gesetzlich definierte Ausnahmen, wie z.B. die obligatorische Weitergabe von Daten, z.B. wegen Meldepflichten im Rahmen des Epidemiengesetzes (Art. 12 EpG)[32], gibt. Im Forschungskontext ist immer eine informierte Einwilligung (Informed Consent)[33] für die Teilnahme an einem Forschungsprojekt erforderlich, die verlangt, dass Studienteilnehmende genügend und mit grösstmöglicher Sorgfalt aufgeklärt werden. Eine Einwilligung des Probanden ist auch oft dazu erforderlich, um die Bearbeitung seiner Daten in Bezug auf das Forschungsprojekt zu rechtfertigen. Ausgenommen sind Studien in Notfallsituationen, wo spezifische Regelungen gelten und Studien mit bereits gesammelten Daten (Sekundärdaten), wo eine explizite Einwilligung nicht immer erforderlich ist (HFG Art. 32–34). Im Behandlungskontext gilt ebenfalls das Erfordernis der informierten Einwilligung, wobei auch hier für dringliche Situationen (Intensiv-, Notfall- und Rettungsmedizin) spezifische Regelungen gelten.

[26] Das Prinzip der *Rechenschaftspflicht* verlangt, dass die Daten fair, transparent und gesetzesgemäss verarbeitet werden. Gerade im Behandlungskontext spielt dieses Prinzip eine wichtige Rolle. Behandlungen müssen im Rahmen eines Behandlungsprozesses aber besonders im Falle eines Schadens nachvollziehbar sein.

[27] Der *Datenschutz* umfasst die Vertraulichkeit und den *Schutz der Privatsphäre*. Die rechtliche Umsetzung des Datenschutzes lehnt sich eng an den Begriff der Freiheit und somit an die Grundrechte an. Ebenfalls ist dieses Prinzip eng mit der Datensicherheit und Anonymisierung verbunden, somit sind vor allem Fragen technischer Natur oder der Governance der Institutionen verbunden.

[28] *Datenfairness* wird aus dem Gerechtigkeitsprinzip[34] abgeleitet und umfasst die Nutzung von Daten für die Forschung und die Nutzung von Sekundärdaten für weitere Forschung.

[29] Alle diese Prinzipien geben den Rahmen vor, in welchem sich ein verantwortungsvoller Einsatz von datenintensiven Technologien, wie zum Beispiel der Einsatz von Big Data und Social-Messaging, bewegen sollte. Denn oftmals können solche Technologien den Arbeitsalltag in der Klinik verbessern. Die Evidenzen für den hier diskutierten Fall, den Einsatz von Social-Messaging, lassen sich durch diverse Untersuchungen zum Beispiel im Umfeld der Notfallmedi-

31 Andreas Vieth, Tom L. Beauchamp, James F. Childress, Principles of Biomedical Ethics, 6. Auflage, 2009.

32 Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz, EPG) vom 28. September 2020, SR 818.101.

33 Mit dem von der SAMW entworfenen Generalkonsent, steht ein von der SAMW entwickeltes Instrument zur Verfügung, dass den Gebrauch von Forschungsdaten und die Weiterverwendung (data sharing) schweizweit vereinheitlicht werden soll. Eine einheitliche Regelung ist schlussendlich wichtig, da eine solche das Vertrauen eines professionellen Patienten- /Arztverhältnis stärkt.

34 Andreas Vieth, Tom L. Beauchamp, James F. Childress, Principles of Biomedical Ethics, 6. Auflage, 2009.

zin[35] oder als Zusatz in der Telemedizin[36] untermauern. Eine Abwägung für oder gegen einen Einsatz hat auch immer die ebengenannten ethischen Aspekte zu berücksichtigen.

4.7. Empfehlungen für einen bewussten Einsatz von Social-Messaging im Spital-Kontext

[30] Eine zentrale Rolle beim Einsatz von Social-Messaging im Spital-Kontext spielen Transparenz und eine klare Governance. Dies bedeutet, dass die grundlegenden ethischen Regeln wie Vertrautheit, Datenschutz, Einwilligung und Sicherheit eingehalten werden müssen. Gegen einen Einsatz von Social-Messaging im Spitalkontext gibt es somit aus rechtlicher und ethischer Sicht wenig Einwände. Im Gegenteil, durch die Verkürzung der Kommunikationswege und die Einfachheit der Handhabung solcher Tools können Verbesserungen für die Pflege resultieren, wie einzelne Studien bereits belegen[37,38]. Ein Einsatz solcher Tools sollte deshalb nach den untenstehenden formulierten Best Practices erfolgen. Hier schlagen wir eine vorläufige Liste vor, die auf den Resultaten unserer Studie basiert.

1) Es soll so weit wie möglich auf Inhouse Lösungen gesetzt werden, die für Spitäler bereits existieren. Der Einsatz von «consumer» Tools wie WhatsApp, Telegram u.a. ist mit zu vielen, auch rechtlichen, Unsicherheiten belastet. WhatsApp und nicht speziell für diese Zwecke konzipierte Social-Messaging Apps bieten hierfür keinen genügenden Schutz und die Nachverfolgbarkeit aus Sicht der Institution kann mit diesen Tools nicht gewährleistet werden.
2) Nachverfolgbarkeit ist im Spital-Kontext von grösster Bedeutung zum Schutz der Patienten und zur Vermeidung von Schäden.
3) Der Einsatz von Social-Messaging sollte klar in Richtlinien geregelt werden. Richtlinien sollen sich hierbei nicht nur auf die Technik beschränken, sondern müssen auch Community Regeln definieren, so zum Beispiel wie die Kommunikation untereinander erfolgen soll oder in welchen Fällen es im Klinik-Alltag besser ist konventionelle Kommunikationsmittel zu nutzen.
4) Die ethischen Prinzipen müssen beachtet werden. Der Patient muss so oft wie möglich seine *Einwilligung* gegeben haben, Daten müssen *vertraulich* behandelt werden und dürfen den Spitalkontext nicht verlassen. *Transparenz* im täglichen Umgang steht an oberster Stelle.
5) Institutionelle Datenschützer müssen über genügend Ressourcen und Befugnisse verfügen, um Richtlinien durchzusetzen. Dies bedeutet, dass sie auch organisatorisch direkt der Spital-Leitung unterstellt sein sollten, damit die Unabhängigkeit innerhalb der Institution gewährleistet ist.

35 Maximilan J. Johnston et al., Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams, The American Journal of Surgery, Vol 209, Issue 1, 2015.

36 Vincenzo Giordano V. et al., WhatsApp Messenger as an adjunctive Tool for Telemedicine: An Overview, Interactive Journal of Medical Research Vol 6 No 2. Iinteractive of Medical Research.

37 Kaliyadan Feroze et al., What's up dermatology? A pilot survey of the use of WhatsApp in dermatology practice and case discussion among members of WhatsApp dermatology groups, Indian Journal of Dermatology, 2017, Vol 82, Issue, S. 67–69.

38 Maged N. Kamel Boulos/Dean M. Giustini/Steve Wheeler, Instagram and WhatsApp in Health and Healthcare: An Overview, Future Internet, 2016.

4.8. Limitationen

[31] Da es sich um eine explorative qualitative Untersuchung handelt ist die Datenlage aufgrund der Methodik auf ein sogenanntes *purposive sample* beschränkt und stellt keine repräsentative Stichprobe dar[39]. Ziel und Vorteil dieses methodischen Ansatzes ist, eine möglichst grosse Bandbreite verschiedener Sichtweisen abzubilden, u.a. dadurch, dass ExpertInnen aus verschiedenen Regionen und Kontexten der Schweiz herangezogen wurden. Im Interview wurde der Gebrauch von Social-Media spontan nicht von allen Befragten angesprochen, so dass uns nicht von allen Beteiligten eine ausführliche Stellungnahme vorliegt. Aufgrund der ethischen Relevanz erachten wir es aber als sinnvoll diese Thematik sowohl aus ethischer aber auch aus rechtlicher Sicht in diesem Artikel eingehender zu beleuchten mit dem Ziel, eine breitere Diskussion und Lösungsfindung, z.B. durch schweizerische Richtlinien, anzuregen.

Christophe Schneble, MSc, CAS Computer Science ETH, Doktorand am Institut für Bio- und Medizinethik der Universität Basel.

Andrea Martani, Master in European and Transnational Comparative Law, Doktorand am Institut für Bio- und Medizinethik der Universität Basel.

Dr. David Shaw, Master in Medical Law, Senior Scientist am Institut für Bio- und Medizinethik der Universität Basel.

Prof. Dr. med Bernice Elger, Institutsvorsteherin des Instituts für Bio- und Medizinethik der Universität Basel.

39 Virginia Braun/Victoria Clarke, Using thematic analysis in psychology, Qualitative Research in Psychology, 2006, S. 77 ff.