NUTZUNG VON CLOUD-DIENSTEN DURCH ÄRZTINNEN UND ÄRZTE

BERUFSGEHEIMNIS UND ANFORDERUNGEN DES DATENSCHUTZES UND DER DATENSICHERHEIT

Baar, 27. März 2019 606-25

Von: Rechtsanwalt Lukas Fässler

/Volumes/DISKs-Public/04-1 Laufende Mandate/606 FMH - HIN AG/606-25 Beratung Standardverträge /Zusammenfassung Nutzung von Cloud-Diensten durch Ärzte - 27-03-2019.docx

1. Ausgangslage

Der Schweizerische Anwaltsverband SAV hat von der Universität Zürich (Prof. Dr. Christian Schwarzenegger, Prof. Dr. Florent Thouvenin, Prof. Dr. Burkhard Stiller) im November 2018 ein Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte erstellen lassen[1]. Dieses Gutachten lässt sich aufgrund der gleichermassen ausgestalteten Voraussetzungen und Bedingungen des Berufsgeheimnisses ohne Abstriche auf die Berufsausübung von Ärztinnen und Ärzten übertragen.

Im Vordergrund stehen dabei zwei Fragestellungen:

- Zum einen ist zu prüfen, ob die Nutzung von Cloud-Diensten eine Verletzung des Berufsgeheimnisses der Ärztin oder des Arztes darstellt;
- Zum anderen ist zu prüfen, ob und unter welchen Bedingungen die Nutzung von Cloud-Diensten durch Ärztinnen und Ärzte mit den Vorgaben des Datenschutzrechtes überhaupt vereinbar ist.

Wir fassen die wesentlichen Aussagen dieses Gutachtens an dieser Stelle für die Ärztinnen und Ärzte zusammen.

[1] Gutachen zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbandes (SAV), Zürich 1. November 2018; https://www.sav-fsa.ch/en/aktuell/gutachten-zur-nutzung-von-cloud-diensten-durch-anwaeltinnen-und-anwaelte-46.html

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin
sekretariat@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Partnerkanzleien:

de la cruz beranek Rechtsanwälte AG
Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin
delacruz@delacruzberanek.com

Nicole Beranek Zanon
Rechtsanwältin und Notarin[1,2]
beranek@delacruzberanek.com

Industriestrasse 7
CH-6300 Zug
Tel.: ++41 41 710 28 50
Fax: ++41 41 710 90 76
www.delacruzberanek.com
UID: CHE-389.928.945 MWST

Lichtsteiner Rechtsanwälte und Notare
Urs Lichtsteiner
lic. iur. Rechtsanwalt[1,2], MSc (Stanford)
lichtsteiner@lilaw.ch

Baarerstrasse 10, Postfach 7517
CH-6302 Zug
Tel.: +41 41 726 90 00
Fax: +41 41 726 90 05
www.lilaw.ch
info@lilaw.ch
UID: CHE-404.805.335 MWST

Anwaltskanzlei Dr. Weltert
Hans M. Weltert
Dr. iur. Rechtsanwalt[1,4]
hans.weltert@raweltert.ch

Matthias Heim
lic.iur. Rechtsanwalt[1,4]
matthias.heim@raweltert.ch

Michael Heim
lic.iur. Rechtsanwalt[1,4]
michael.heim@raweltert.ch

Bahnhofstrasse 10
CH-5001 Aarau
Tel.: +41 62 832 77 33
Fax: +41 62 832 77 34
www.raweltert.ch
info@raweltert.ch
UID: CHE-100.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug
[3] Eingetragen im Anwaltsregister des Kantons Zürich
[4] Eingetragen im Anwaltsregister des Kantons Aargau

2. Übersicht

Im Kapitel B (ab Seite 5-12) werden die technischen Grundlagen des Cloud-Computing im Allgemeinen, Cloud-Dienstmodelle (SaaS, IaaS, PaaS) und Szenarien zu den Sicherheitsmassnahmen dieser Modelle erörtert.

Im Kapitel C (ab Seite 13-38) wird der strafrechtliche Tatbestand der Verletzung des Berufsgeheimnisses nach Art. 321 StGB dargestellt. Es werden Ausführungen zum geschützten Geheimnis, zum möglichen Täterkreis (Geheimnisherr und Hilfspersonen) und zum objektiven Tatbestandsmerkmal des «Offenbarens», zu den subjektiven Tatbestandselementen (Vorsatz und Eventualvorsatz auf Seiten des Geheimnisherrn und der Hilfspersonen), Rechtswidrigkeit, Strafantrag und zur Frage der internationalen Sachverhalte und Strafanwendung gemacht.

Im Kapitel D (ab Seite 39-56) wird der Datenschutz abgehandelt. Dabei werden Fragen des anwendbaren Rechts (Schweizerisches Datenschutzgesetz und der DSGVO), das Bearbeiten von Personendaten und die Auftragsdatenverarbeitung in der Schweiz oder im Ausland dargestellt.

Im Kapitel E (ab Seite 57-58) werden die Erkenntnisse zusammengefasst.

Von Interesse für diese analog auf die Ärztinnen und Ärzte anzuwendende Zusammenfassung sind die Erkenntnisse und Schlussfolgerungen. Wer an der Herleitung der Aussagen in den Erkenntnissen interessiert ist, wird auf das detaillierte Studium des gesamten Gutachtens verwiesen.

3. Erkenntnisse

Aus dem Gutachten ergeben sich für Ärztinnen und Ärzte – analog zu den Feststellungen für Anwältinnen und Anwälte – folgende Schlussfolgerungen:

3.1. Besonders schützenswerte Patientendaten

Bei der Bearbeitung von Patientendaten muss die Ärztin oder der Arzt erhöhte (organisatorische und technische) Anforderungen des Datenschutzes nach DSG (Schweiz) oder DSGVO (europäische Datenschutz-Grundverordnung) einhalten. Es sind spezifische Schutz- und Sicherheitsmassnahmen zu erfüllen, unabhängig davon, ob diese Daten ausschliesslich in der eigenen Praxis oder in der Cloud bearbeitet werden.

Spezifisch für den Fall der Bearbeitung der Patientendaten in Softwareapplikationen, welche in der Cloud zur Verfügung gestellt werden, ist Folgendes zu beachten:

3.2. Verschlüsselung der bearbeiteten Personendaten durch Ärztinnen und Ärzte vor der Übertragung an Cloud-Provider

- **Keine Offenbarung von Geheimnissen i.S.v. Art. 321 StGB**
  Sofern die durch die Ärztinnen und Ärzte erhobenen Daten vor der Übertragung an den Cloud-Provider verschlüsselt werden und der Cloud-Provider keinen zur Entschlüsselung erforderlichen Schlüssel besitzt, liegt keine Offenbarung von Geheimnissen im Sinne von Art. 321 StGB vor. Das Berufsgeheimnis wird nicht verletzt.

- **Keine Verletzung von Datenschutzbestimmungen**
  Da verschlüsselte Daten nicht als Personendaten zu qualifizieren sind, liegt auch keine Bearbeitung von Personendaten durch den Cloud-Provider vor. Es braucht diesfalls auf Seiten des Cloud-Providers keine zusätzlichen technischen oder organisatorischen Sicherheitsmassnahmen. Jedoch ist in jedem Fall zu empfehlen, dass die Ärztin oder der Arzt mit dem Cloud-Provider einen Betriebsvertrag mit Service Level Agreement abschliesst, in welchem die vertraglichen Leistungen des Cloud-Providers sauber geregelt werden. Die von der FMH dazu ausgearbeiteten Allgemeinen Vertragsbedingungen und Mustervorlagen für Cloudservices können dabei sehr gute Dienste leisten.

In dieser Konstellation ist die Nutzung von Cloud-Services durch Ärztinnen und Ärzte strafrechtlich wie auch datenschutzrechtlich unbedenklich. Die Nutzung von Cloud-Services für die Bearbeitung von (vom Arzt vorverschlüsselten) Patientendaten ist erlaubt.

3.3. Verschlüsselung der bearbeiteten Patientendaten durch den Cloud-Provider

- Der Cloud-Provider ist als Hilfsperson der Ärztin oder des Arztes zu qualifizieren.
- Die Möglichkeit der Kenntnisnahme von Patientendaten durch Hilfspersonen bei der Auslagerung und Bearbeitung von Patientendaten in der Cloud stellt kein «Offenbaren» eines Geheimnisses i.S.v. Art. 321 StGB, weil der Cloud-Provider als Hilfsperson zum sogenannten inneren Kreis der Organisation der Ärztinnen und Ärzte gehört.
- Die Nutzung von Cloud-Services durch Ärztinnen und Ärzte führt damit nicht zu einer Verletzung des Berufsgeheimnisses nach Art. 321 StGB.
- Der Arzt oder die Ärztin haben mit dem Cloud-Serviceprovider (wie anderen internen Mitarbeitenden wie z.B. Praxisassistentinnen) die Verpflichtung zur Einhaltung des Berufsgeheimnisses jedoch schriftlich (z.B. in einem **Datenverarbeitungsvertrag**) festzuschreiben und unterzeichnen zu lassen.
- Ärztinnen und Ärzte müssen den Cloud-Serviceprovider mit der notwendigen Sorgfalt auswählen und vertragliche Mindestanforderungen erfüllen.
- In einem schriftlichen **Datenverarbeitungsvertrag** zwischen Arzt, Ärztin oder Arztpraxis und dem Vertragspartner, welcher die Cloud-Services anbietet, müssen mindestens folgende Punkte schriftlich geregelt werden:
  - die Pflicht zur Wahrung des Berufsgeheimnisses (vgl. oben);
  - Vereinbarung, dass die Patientendaten durch den Cloud-Serviceprovider nicht genutzt, bearbeitet oder an Dritte weitergegeben werden dürfen;
  - Die Überwachung der Einhaltung der für den Arzt gegenüber dem Cloud-Serviceprovider ermöglicht und zugelassen wird;
  - Dem Arzt oder der Ärztin oder einem beigezogenen, unabhängigen Dritten die Möglichkeit eingeräumt wird, die Einhaltung der Datenschutz- und Datensicherheitspflichten zu überprüfen oder überprüfen zu lassen;
  - Regelung zum Eigentum an den in der Cloud bearbeiteten und gespeicherten Personendaten (ausschliesslich beim Arzt resp. dem Patienten) ;
  - Die Herausgabe der Patientendaten resp. das Recht zum Download der Patientendaten bei Vertragsauflösung ohne Obstruktionen seitens des Cloud-Serviceproviders;

- Regelung eines regelmässigen Datenbackups (in einem separaten SLA) und Recht auf Speicherung dieser Backup-Daten bei einem Drittanbieter oder beim Arzt oder der Ärztin selber zur Sicherstellung des Datenzugriffs im Falle eines Totalausfalles der IT-Infrastrukturen beim Cloud-Serviceprovider.

Die von der FMH entwickelten Vertragsklauseln nehmen diesbezüglich die notwendigen Definitionen vor und können gegenüber dem Softwareanbieter und den von ihm beigezogenen Cloud-Serviceprovider (sofern der Softwareanbieter nicht gleichzeitig auch Cloud-Serviceprovider ist) vollumfänglich eingesetzt und zur Anwendung verlangt werden.

In dieser Konstellation ist die Nutzung von Cloud-Services durch Ärztinnen und Ärzte ebenfalls strafrechtlich und datenschutzrechtlich erlaubt. Aber die Nutzung von Cloud-Services muss durch vertragliche Abmachungen (**Datenverarbeitungsvertrag**) in den oben angeführten wesentlichen Fragen geregelt werden. Und der Arzt oder die Ärztin hat sicherzustellen, dass die vertraglichen Vereinbarungen periodisch auf deren Einhaltung überprüfbar sind und auch tatsächlich überprüft werden.

4. Ausblick auf einen gesetzeskonformen Eintrittsprozess des Patienten

In Zukunft wird vom Patienten oder von der Patientin beim Ersteintritt in eine neue Arztpraxis (Erstaufnahmeprozess) wohl zwingend eine schriftliche **Einwilligungserklärung zur Bearbeitung der Patientendaten in der Cloud** verlangt werden müssen, sofern nicht eine Vorabverschlüsselung (Konstellation 1; Ziffer 3.2.) sichergestellt ist. In dieser Einwilligungserklärung ist vom Patienten oder der Patientin bestätigen zu lassen, dass er oder sie:

- einer Auslagerung seiner/ihrer Patientendaten durch den Arzt oder die Ärztin in die Cloud ausdrücklich zustimmt;
- Angaben über alle in der Cloud gespeicherten oder ausgetauschten Patientendaten erfolgen;
- Angaben über alle in der Cloud in Anspruch genommenen Services (Applikationen) bekannt gemacht werden;
- Der Zweck und die Rechtsgrundlage (Rechtfertigungsgrund) für die Patientendatenbearbeitung in der Cloud genannt werden;
- Auf das jederzeitige Widerrufsrecht des Patienten oder der Patientin zur erteilten Einwilligung der Datenbearbeitung in der Cloud unter Angabe der Adresse für die Widerrufserklärung (z.B. E-Mailadresse der Praxis) aufmerksam gemacht wird;
- Auf die datenschutzrechtlichen Grundrechte der Auskunftserteilung, Berichtigung oder Löschung hingewiesen wird;
- Die mit dem Cloud-Serviceprovider vertraglich vereinbarten organisatorischen und technischen Massnahmen offengelegt werden.

Die digitale Transformation, welche in allen Lebensbereichen sehr stark im Gange ist, macht somit auch vor der Praxistüre des Arztes oder der Ärztin keinen Halt mehr. Die FMH hat mit ihren Grundsätzen zur gesetzeskonformen Bearbeitung von Patientendaten durch den Arzt oder die

Ärztin einen «Berufskodex» erlassen, an den sich Arzt oder Ärztin unbedingt halten sollten. Damit die Realisierung von cloudbasierten Patienten-Administrationslösungen oder anderen Software- oder Datenaustauschlösungen in Zukunft realisiert werden können, sind aber neue Mindestanforderungen umzusetzen. Der Arzt und die Ärztin sollten daher konsequent von den Mustervorlagen der FMH Gebrauch machen und diese gegenüber den Software- oder Cloud-Serviceanbietern konsequent durchsetzen.

März 2019