Datenschutz und -sicherheit im privaten Krankenversicherungswesen

02. September 2016

Einwilligungserklärungen und transparente Datenschutzhinweise – eine Kunst für sich

Dr. Lutz M. Keppeler

Dr. Stefan Jöster, LL.M.

Steigendes Datenvolumen, steigende Anforderungen

Die Anzahl und Komplexität der personenbezogenen Daten, die eine Krankenversicherung von ihren Kunden erhebt und verarbeitet, hat sich im Laufe der letzten Jahre enorm gesteigert. Durch die Nutzung von Gesundheits-Apps, Wearables und die Verfügbarkeit von Social Media-Daten werden gesundheitsrelevante Daten live übertragen und stehen für Risikoanalyse und eine gezielte Ansprache der Versicherungsnehmer zur Verfügung.

Gesteigerte Anforderungen an Datenschutzsicherheit und Compliance folgen der aktuellen Digitalisierungswelle in der Krankenversicherung auf dem Fuß. Die Risiken die mit der Gemengelage aus anwendbaren Vorschriften – man denke nur an Datenschutzgrundverordnung und die IT-Security Gesetzgebung –, dem neuen Bußgeldrahmen durch die EU-Datenschutz-Grundverordnung (bis zu 20 Millionen €) und die hohen Haftungsrisiken bei IT-Sicherheitslücken einhergehen, werden in Laufe der nächsten Jahre stetig zunehmen.

Transparenz von Datenschutzhinweisen

Aus verschiedenen datenschutzrechtlichen Normen (§ 13 Abs. 1 TMG und § 3 Abs. 3 BDSG) und Art. 8 Abs. 2 der Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft des GDV ergibt sich die **Pflicht, die Betroffenen einer Datenerhebung transparent über die Identität der verantwortlichen Stelle und die Zweckbestimmung der Datenerhebung zu informieren.**

Die Rechtsprechung stellt dabei hohe Anforderungen an die Transparenzpflichten. Der Betroffene soll grundsätzlich verstehen

können, was mit seinen Daten geschieht, in welchem Umfang diese wo gespeichert werden und welche Rechte ihm diesbezüglich zustehen. Soll durch Tracking-Technologien ein Nutzerprofil mit Bezug zu Gesundheitsdaten erstellt werden, so muss dem Nutzer auch mitgeteilt werden, wie das Tracking an sich funktioniert, ob z. B. Cookies, Device-Finger-Prints, IP- oder Mac-Adressen usw. gespeichert werden und ob seine Daten in diesem Rahmen an weitere Dienstleister weitergegeben werden. Auch wenn die Daten für Werbezwecke genutzt werden, muss dies deutlich zum Ausdruck kommen. **Es genügt es heute nicht mehr, den Nutzer nur durch das Anklicken einer Checkbox bestätigen zu lassen, dass er „die Datenschutzerklärung „akzeptiert"**.

Anforderungen an notwendige Einwilligungserklärungen

In vielen Fällen genügen die gesetzlichen Erlaubnistatbestände zur Verarbeitung von personenbezogenen Daten nicht, um die Informationen von Versicherungsnehmern wie gewünscht verarbeiten zu können. Vielmehr bedarf es einer qualifizierten Einwilligungserklärung.

Dies ist eine Kunst für sich, da **auch eine unübersichtliche Datenschutzerklärung als intransparent angesehen werden kann**, zumal die Rechtsprechung hier die Maßstäbe der AGB-Kontrolle anwendet.

Für Gesundheit-Apps sind hierbei noch relativ einfache Lösungen über die Anzeige von Datenschutzerklärungen denkbar. Bei Wearables steht zumeist kein ausreichend großes Display für die Wahrnehmung längerer Datenschutztexte zur Verfügung. Hier sind kreative Lösungen gefragt.

Generell gilt hierbei: **Je komplexer die beabsichtigte Datenanalyse ist**, die unter Zugrundelegung der personenbezogenen Daten des Versicherungsnehmers unternommen werden soll, **umso deutlicher muss diese dem Nutzer erklärt und vor der Abgabe der Einwilligungserklärung vor Augen geführt werden.** Dies gilt besonders bei dem – in Deutschland umstrittenen, wenngleich nicht von vorne herein ausgeschlossen – Zugriff auf Social-Media Daten.

Die „Datenkraken" im Fokus des Verbraucherschutzes

Es liegt auf der Hand, dass die Versicherungsbranche durch den Einzug von Big-Data-Analysen, der Etablierung einer Vielzahl von Gesundheit-Apps und dem Volumen generierter gesundheitsbezogener Daten durch Wearables zunehmend in das Fadenkreuz der Datenschutzaufsichtsbehörden und der Verbraucherschutzverbände gerät. **Hier lohnt es sich, aus den Fehlern der großen IT-Datenkraken (z. B. Google, Facebook, Samsung) zu lernen,** die

ihre Datenschutz- und Einwilligungserklärungen nach Gerichtsurteilen in Deutschland nachbessern mussten.

Verschärfung der Sanktionen und Vertrauensverlust

Transparenzverpflichtungen und **Anforderungen an Einwilligungserklärungen werden sich** mit Art 14a und Art 7 der EU-Datenschutz-Grundverordnung **noch deutlich verschärfen**. Doch auch die möglichen Sanktionen werden eine ganz neue Dimension erlangen:

Wo heutzutage auf Basis des BDSG ein Bußgeld von bis zu Euro 300.000 und im Rahmen des TMG von bis zu Euro 50.000 möglich ist, erhöht die EU-Datenschutz-Grundverordnung den Sanktionsrahmen auf **eine Bußgeldhöhe von bis zu Euro 20 Mio. oder auf 4 % des weltweiten Jahresumsatzes**, wobei der jeweils höhere Wert den Maximalrahmen vorgibt. Die datenschutzrechtlichen Bestimmungen der §§ 12ff. TMG mit ihren milden Bußgeldrahmen, welches für Apps, Wearables und sonstige Treckingtechnologien heute das maßgebliche Regelungsregime enthält, werden aufgrund des Anwendungsvorrangs der EU-Datenschutz-Grundverordnung vollständig unanwendbar.

Im sensiblen Gesundheitswesen dürfte zudem ein Vertrauensverlust durch Berichterstattung über Datenschutzverstöße häufig schwerer wiegen als ein gerichtlicher Unterlassungstenor bezüglich einzelner Klauseln einer Datenschutzerklärung.

IT-Security und Datenschutz

Hand in Hand mit der Entwicklung der datenschutzrechtlichen Vorgaben gehen **die steigenden Haftungsrisiken aufgrund von IT-Sicherheitsvorfällen** insbesondere wegen unautorisierten Zugriffs auf die besonders sensiblen Gesundheitsdaten einher.

Anforderungen an die technischen und organisatorischen Maßnahmen zum Datenschutz nach § 9 BDSG und werden in Zukunft durch eine sich verschärfende IT-Security-Gesetzgebung und die EU-Datenschutz-Grundverordnung weiterentwickelt. Sollte trotz aller Sicherheitsbemühungen ein unautorisierter Zugriff vorliegen, so ergeben sich eine Vielzahl von **Meldepflichten**: Neben der zuständigen Datenschutzaufsichtsbehörde müssen die Betroffenen, der Betriebsrat und das Bundesamt für Sicherheit in der Informationstechnologie („BSI“) benachrichtigt werden.

Fazit

Spätestens bis Mitte 2018, wenn die EU-Datenschutz-Grundverordnung unmittelbar anwendbar wird, sollte jeder Krankenversicherer die Digitalisierung und deren Nutzung durch ein solides Datenschutz-, IT-Sicherheits- und Compliance-Programm abgesichert haben.

Wir beraten Sie gerne – von der Erstellung wirksamer Einwilligungserklärungen über die Implementierung von Präventions- und Bonusprogrammen bis zum vollständigen Datenschutz- und -sicherheits-Audit und in allen weiteren unternehmensrelevanten Fragen.

Sprechen Sie uns gerne an.

Ihre Ansprechpartner zu diesem Thema

Rechtsanwalt
Dr. Lutz Martin Keppeler
T +49 221 20 52-426
F +49 221 20 52-1
l.keppeler@heuking.de

- Datenschutzrecht
- IT-Sicherheitsrecht
- Fachgutachter für die Zeitschrift Datenschutz im Gesundheitswesen
- Regelmäßige Vortrags- und Publikationstätigkeit im Datenschutz- und IT-Recht

Rechtsanwalt / Partner
Dr. Stefan Jöster, LL.M.
T +49 221 20 52-557
F +49 221 20 52-1
s.joester@heuking.de

- Langjährige Erfahrung in allen Bereichen des Versicherungs- und Haftungsrechts
- Beratung von betrieblichen und öffentlich/rechtlichen Pensionsfonds/-kassen und Lebensversicherern (insbesondere aufsichtsrechtliche Vorgaben, Vertriebsmodelle, Internet-Direktvertrieb, Kapitalanlagen)