Foto: © Fotolia/ra2 studio

HEITER BIS WOLKIG:

Cloud-Computing

PRAXISDATENSCHUTZ & DATENSICHERHEIT im Netz

Papick G. Taboada

Selbstständige Heilpraktiker stehen heute vor der z. T. undankbaren Aufgabe, sich mit modernen Netzwerken auseinandersetzen zu müssen. Doch die rasante Entwicklung der IT-Branche hat auch eine Menge Erleichterungen mit sich gebracht: Der Computer, einst eine Einzelplatzlösung, fand dank Miniaturisierung den Weg in die Hosentasche. Damit ist Datenverarbeitung und Kommunikation von jedem Standort aus möglich. Das Internet hat uns neue Welten der Datenbeschaffung, -verbreitung und -übermittlung eröffnet.

Ende der Insellösungen – Siegeszug der Web-Anwendungen

Google, Facebook und andere Online-Dienstleister konnten zeigen, dass Software durchaus bedienbar, stabil und sinnvoll auf unterschiedlichen Geräten laufen kann. Hierbei handelt es sich meist um Web-Anwendungen (Anwendungen, die in einem Browser wie Firefox, Safari, Google Chrome oder Internet Explorer angezeigt werden). Die im Browser dargestellten Seiten werden durch ein Programm auf einem Web-Server erzeugt und über das Internet übertragen. Der Nutzer wird somit nicht mehr mit technischen Details wie Installation, Updates, Betrieb von Servern oder Backups konfrontiert. Noch nie war IT daher so einfach, niederschwellig und effizient wie heute.

In diesem Zuge ist es mittlerweile selbstverständlich, dass Daten auf mehreren Geräten verfügbar sind. Vernetzung ist damit kein Bonus mehr, sondern Voraussetzung für funktionierende Hardware. Programme werden über das Internet installiert – von Updates bis zu ganzen Betriebssystemen. CDs und Insellösungen gehören der Vergangenheit an, Rechner funktionieren nur noch vernetzt. Wir haben uns an Facebook, WhatsApp, Dropbox und Google-Dienste gewöhnt, die allesamt nicht im Einklang mit un-

Taboada PG: Heiter bis wolkig: Cloud-Computing. DHZ – Deutsche Heilpraktiker Zeitschrift, 2015; 1: 64–67

serem Datenschutzgesetz stehen, aber im privaten Bereich gerne genutzt werden und für eine hohe Erwartungshaltung sorgen.

Top Secret: Patienteninformationen als besondere Personendaten

In einer Praxis werden laufend besondere Personendaten elektronisch erhoben und verarbeitet, von der Terminplanung über Diagnostik und Therapie bis hin zur Rechnungsstellung. Das sind sog. besonders schützenswerte Daten mit einer hohen Gefahr der Grundrechtsverletzung. Wie mit diesen umzugehen ist, regelt umfassend das Bundesdatenschutzgesetz (BDSG). Zu den besonderen Personendaten zählen laut § 3 Abs. 9 BDSG Angaben wie ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, sexuelle Neigungen oder Angaben über die Gesundheit. Letztere schließen z. B. Krankheiten (Diagnose, Verlauf, Schwere, Dauer), Ablauf und Inhalt medizinischer Behandlungen und Medikamente ein.

Merke: Prinzipiell zählen alle im Zusammenhang einer Therapie erhobenen Informationen zu den besonderen Personendaten.

Auch Angaben, die indirekt Informationen vermitteln, sind eingeschlossen. So liefert der Vermerk „Max Mustermann, osteopathische Behandlung des Rückens“ im Terminkalender eines Heilpraktikers indirekt Informationen über die Gesundheit.

Die Erfassung besonderer Personendaten ist im Rahmen der therapeutischen Tätigkeit zweckgebunden zulässig sowie notwendig und erfordert daher keine explizite Zustimmung des Patienten (§ 28 BDSG). Diese wird erst dann erforderlich, wenn Daten an Dritte übermittelt werden. Als Übermitteln definiert § 3 Abs. 4 Nr. 3 BDSG die Bekanntgabe personenbezogener Daten an Dritte. Dritter ist gemäß § 8 Abs. 2 BDSG jeder andere, mit Ausnahme des eigentlichen Betroffenen, meist des Patienten, und derjenigen, die die personenbezogenen Daten nur im Auftrag erheben, verarbeiten oder nutzen. Es kommt somit darauf an, ob der Heilpraktiker noch selbst die Kontrolle über die personenbezogenen Daten behält oder ob andere die personenbezogenen Daten eigenverantwortlich und weisungsfrei verwenden können, wie dies bei Abrechnungszentren der Fall ist.

KURZ GEFASST

1 *Zum modernen Praxis-Datenmanagement zählt die Nutzung von Online-Anwendungen, auch als SaaS- oder Cloud-Dienste bezeichnet.*

2 *Das Bundesdatenschutzgesetz setzt hinsichtlich der Speicherung und Weitergabe von Patientendaten enge Grenzen. Dies gilt insbesondere für besondere Personendaten, zu denen auch Information über die Gesundheit zählen.*

3 *Beliebte kostenlose Dienste, z. B. von Google, Apple, Yahoo oder Dropbox scheiden für die therapeutische Arbeit weitgehend aus, da sich die Server außerhalb Europas befinden und ein Vertrag über eine Auftragsdatenverarbeitung sowie besondere Datenschutzvorkehrungen erforderlich wären.*

INFORMATION

Grundregeln zum Datenschutz: Anlage zu § 9 S. 1 BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Taboada PG: Heiter bis wolkig: Cloud-Computing. DHZ – Deutsche Heilpraktiker Zeitschrift, 2015; 1: 64–67

Foto: © Fotolia/momius

Beispiel: Datenübermittlung durch Wechsel der Datenkontrolle

Ein Beispiel verdeutlicht den Wechsel der Datenkontrolle: Ein Heilpraktiker speichert Abrechnungsinformationen auf einem USB-Stick, den ein Fahrradkurier zu einem Abrechnungsdienstleister transportiert.

Der Fahrradkurier transportiert lediglich die Daten. Hier findet keine Datenverarbeitung statt. Damit wurden auch keine Daten an ihn übermittelt.

Der Abrechnungsdienstleister muss die Daten aus dem Stick auslesen und für seine Tätigkeit übernehmen. Rechnungen werden nicht im Namen des Heilpraktikers, sondern im Namen der Abrechnungsstelle gestellt. Somit findet ein Wechsel der Kontrolle über die personenbezogenen Daten und damit eine Datenübermittlung statt.

Daher erfordert die Beauftragung des Abrechnungszentrums die Zustimmung des Patienten. Denn hier geht die Kontrolle besonderer Personendaten auf Dritte über, ohne dass dies für die Durchführung der Therapie automatisch erforderlich wäre.

Jede Verarbeitung personenbezogener Daten bedarf eines besonderen Schutzes. Dieser wird durch technische oder organisatorische Maßnahmen ermöglicht (s. Grundregeln zum Datenschutz), die unabhängig von der Praxisgröße umgesetzt werden müssen. So schließt z. B. die Zutrittskontrolle die Festlegung von Sicherungsbereichen, befugten Personen (Mitarbeiter, Fremdbehörden, Fremdfirmen, Wartungsdienste, Anwendungsbetreuung), Besucherregelungen, Sicherung von Gebäuden und Räumen sowie Anwesenheitsaufzeichnungen ein.

Auftragsdatenverarbeitung: Dürfen Daten(-Dienste) ausgelagert werden?

Viele EDV-Aufgaben können unter Effizienzgesichtspunkten ausgelagert werden, man spricht auch von Outsourcing. Externe Experten können in diesem Rahmen beraten, technische und organisatorische Maßnahmen umsetzen oder die Infrastruktur betreuen. Sie unterliegen allerdings weder der ärztlichen Schweigepflicht, noch sind sie naturgemäß und nachvollziehbar am therapeutischen Geschehen beteiligt. Damit dürfen sie nicht ohne weiteres Zugriff auf besondere Personendaten erhalten. Dies gilt z. B. für die Reparatur des Praxis-Rechners. Findet diese in Anwesenheit des Heilpraktikers statt, kann er einen unerlaubten Zugriff ausschließen, nicht jedoch bei Überlassung des Rechners!

Für diese und weitere Fälle im Sinne eines Outsourcings wurde im Zuge der BDSG-Novellierung im Jahr 2009 in § 11 BDSG die sog. Auftragsdatenverarbeitung oder ADV definiert. Diese beruht auf einem Vertrag zwischen Heilpraktiker (Auftraggeber) und Dienstleister (Auftragnehmer), der u. a. den Umgang mit besonderen Personendaten regelt. Da der Heilpraktiker hierbei Herr der Daten bleibt, liegt keine Übermittlung von Daten an Dritte und damit keine Einwilligungspflicht vor. Denn der Vertrag regelt, aus und zu welchem Zweck die Daten durch den Dienstleister verarbeitet werden sollen und beinhaltet als Anlage eine Auflistung von Datenschutzmaßnahmen des Dienstleisters, die durch den Auftraggeber überprüft werden können. Die Beauftragung eines Abrechnungsdienstleisters fällt hingegen nicht unter die ADV, da dieser selbst die Rechnungen stellt und damit die Kontrolle über die Daten übernimmt, was die Zustimmung des Patienten erfordert. Vorlagen für ADV-Verträge sind z. B. bei den Verbänden und im Internet erhältlich.

Auch die Nutzung einer „Online-Software“ wird im Rahmen der ADV rechtssicher geregelt. Hierbei handelt es sich um die Datenverarbeitung im SaaS-Modell (Software as a service), auch als Cloud(-Dienste), in der IT-Branche als Cloud-Computing, bezeichnet. In diesem Modell werden Aufgaben, Umsetzung, Infrastruktur, Anwendungsbetrieb, Wartung und Datensicherung an einen Dienstleister ausgelagert. Über das Internet kann aber auch auf angemietete Infrastruktur wie Rechner oder Netzwerke zugegriffen werden – hier spricht man von IaaS (infrastructure as a service), im Fall angemieteter Datenbanken von PaaS (platform as a service). Endanwender nutzen jedoch fast ausschließlich SaaS-Angebote.

Cloud-Dienste für Patientendaten: Nur mit ADV-Vertrag

Die Cloud zählt zu den ältesten Sinnbildern der Informationstechnik und steht in Schaubildern für Netzwerke zwischen Computern. Daher kann man ohne Kontext nicht verstehen, was genau gemeint ist – ob Onlinespeicher, Kalender, Synchronisierung, Kontakte oder sogar Fotobearbeitung. Denn Cloud ist praktisch alles, was man über das Internet nutzen kann, einschließlich aller SaaS-Angebote wie Web-Anwendungen, Google-Dienste und Facebook. Diese basieren auf dem Grundsatz, dass die genutzte Software und zugehörige Infrastruktur bei einem externen IT-Dienstleister betrieben und vom Kunden – meist über einen Webbrowser oder eine App – genutzt wird.

Taboada PG: Heiter bis wolkig: Cloud-Computing. DHZ – Deutsche Heilpraktiker Zeitschrift, 2015; 1: 64–67

SaaS beschreibt somit ein erfolgreiches Modell des Softwarevertriebs: Der Endanwender erhält ein Produkt, das nahezu wartungsfrei genutzt werden kann. Der Anbieter ist für Updates, Backups, die Weiterentwicklung und die Verfügbarkeit im Allgemeinen zuständig.

Ein Heilpraktiker darf allerdings streng genommen einen Cloud-Dienst nur dann nutzen, wenn ein ADV-Vertrag mit dem Anbieter abgeschlossen wurde, und er muss sicherstellen, dass die Daten nicht außerhalb der EU abgelegt werden. Dort ist ein angemessener Schutz personenbezogener Daten laut § 4b Abs. 2 S. 2 BDSG nicht gegeben. Somit dürfen z. B. weder Google- noch iCloud-Kalender für die Terminplanung von Behandlungen verwendet werden, sobald auch nur indirekt auf besondere Personendaten geschlossen werden kann. Dies gilt auch für Dropbox als Synchronisierung von Dateien zwischen mehreren Computern sowie für Tabellenkalkulationen mit Abrechnungsdaten über Dropbox oder Google Docs: Abrechnungsinformationen enthalten üblicherweise Anschrift, Geburtsdatum, Diagnose und eine Auflistung der erbrachten Leistungen!

Merke: Google, iCloud, Dropbox und viele weitere Cloud-Dienste laufen über Server außerhalb Europas. Damit verstößt deren Nutzung für die Verarbeitung besonderer Personendaten gegen das Bundesdatenschutzgesetz.

Das erste Problem der ursprünglich genialen Idee des Cloud-Computing besteht in der Nutzung zu nicht vorgesehenen oder unzulässigen Zwecken. Zum Zweiten finanzieren viele SaaS-Anbieter ihr Angebot über Werbung oder das Sammeln und gewerbliche Nutzen werbetechnisch relevanter Daten. Zahlt man nicht für einen Dienst, dann ist man nicht der Kunde, sondern das Produkt.

Somit kommen viele Anbieter cloudbasierter Lösungen für den Einsatz in Praxen nicht infrage. Erst durch die BDSG-Novelle von 2009 können Patientendaten überhaupt rechtssicher in der Cloud gespeichert werden, wenn

- die gespeicherten Daten den europäischen Raum nicht verlassen,
- ein schriftlicher Vertrag über eine Auftragsdatenverarbeitung zwischen Heilpraktiker und Anbieter abgeschlossen wurde,
- der Dienstleister über eine ausreichende Verschlüsselung verfügt. Ansonsten kann es zu datenschutzrechtlichen oder sogar strafrechtlichen Konsequenzen kommen.

Wichtig ist in dem Zusammenhang, dass der Heilpraktiker in keinem Moment die Kontrolle und Verantwortung über die Daten abgibt. Somit sind Heilberufen für die Verwendung von Cloud-Diensten deutlich engere Grenzen gesetzt als Privatnutzern, die ihre eigenen Daten oder allgemeine Personendaten erfassen.

Perspektivenwechsel: Datenspeicher als Aktenschrank

Betrachten Sie als Heilpraktiker die elektronisch erfassten Daten wie die Unterlagen in einem Aktenschrank: Dieser sollte sicher abschließbar sein und dritten Personen nur dann Zugriff erlauben, wenn die Patienten zugestimmt haben. Wo der Aktenschrank steht, spielt hingegen keine Rolle, ob angemietet in einem Lagerraum, in eigenen oder angemieteten Räumlichkeiten – solange nur Sie Zugriff darauf haben. Sobald eine Firma allerdings Reparatur- und Wartungsarbeiten daran durchführt, müssen Sie mit dieser vertraglich u. a. vereinbaren, dass sie in Ihrem Auftrag arbeiten, die Akten jedoch nicht öffnen darf. Im Vertrag wird zudem festgehalten, welche technischen und organisatorischen Maßnahmen ergriffen werden, damit die Daten in den Akten geschützt sind, und dass die Firma nicht unbefugt Kenntnis von den personenbezogenen Daten und damit faktisch auch die Verfügungsmacht darüber erhalten darf. Sie können die Reparatur- und Wartungsarbeiten auch selbst überwachen und somit den Schutz der Akten sicherstellen. Oder Sie leeren einfach zuvor Ihren Aktenschrank: Wo keine Daten enthalten sind, gibt es auch keine Datenschutzregelungen zu beachten. ▪

Dieser Artikel ist online zu finden:
http://dx.doi.org/10.1055/s-0035-1546454

Internet

Weitere Informationen erhalten Sie unter:

https://www.hzdr.de/db/Cms?pNid=420

www.bfdi.bund.de/bfdi_wiki/index.php/3_BDSG_Kommentar_Absatz_9_Beispiele

Dipl.-Wi.-Ing. Papick G. Taboada

Bachstr. 11
76185 Karlsruhe
E-Mail: info@pgt.de
Internet: http://lemniscus.de

Papick G. Taboada ist Geschäftsführer der pgt technology scouting GmbH und Betreiber der online Praxisverwaltung Lemniscus. Er war maßgeblich an der datenschutztechnischen Umsetzung beteiligt. Die Rechtsberatung bei Erstellung und Durchführung von Lemniscus wird von der Kanzlei Dr. Bechtold & Kollegen in Karlsruhe durchgeführt, federführend durch die Rechtsanwältin und zertifizierte Datenschutzbeauftragte Christa Hagen. Ihr gilt auch der Dank des Autors für das juristische Lektorat und die wertvollen Ergänzungen des Artikels.