Datenschutz in der Praxis

Veranstaltung der LPPKJP Hessen am 24.05.2014 mit Astrid Ackermann, Rechtsanwältin – Medien- und IT-Recht, Frankfurt/Main.

Mit ca. 70 TeilnehmerInnen war das eine erstaunlich gut besuchte Veranstaltung zu dem Thema. Aber in Zeiten von NSA und ständig zunehmender Daten-Sammelwut aller möglichen Internet-Anbieter und Hacker-Angriffen in großem Stil dringend notwendig für uns Psychotherapeuten. Mehr denn je müssen wir uns um die Sicherheit der uns anvertrauten Patientendaten sorgfältig kümmern.

Frau Ackermann begann ihren Vortrag (Folien im Mitgliederbereich unter „Dokumente“) mit Fragen und Problemen rund um den Internet-Auftritt von Psychotherapeuten: Wie sprechen Therapeuten ihre (potentiellen) Patienten im Internet, auf ihrer Praxis-Homepage an? Immerhin sind ca. 78 % der Internetnutzer in den Social Media (z. B. Facebook, Google, Linked in, wer-kennt-wen.de, Xing) angemeldet und 67% von ihnen dort auch aktiv. Die Vorteile der Kommunikation liegen auf der Hand: etwa der niedrigschwellige Zugang, die leichte Erreichbarkeit, die geringen Kosten. Die Gefahren können dabei leicht in den Hintergrund geraten, nämlich ganz besonders die Gefahr von Persönlichkeitsrechtsverletzungen, die schwere Kontrollierbarkeit bzw. der hohe Kontrollaufwand in den Portalen und die teilweise geringe Seriosität. Es liegt nahe, dass auch Patienten-Therapeuten-Kontakte über die sozialen Medien erfolgen können. Unsere Berufsordnung gebietet uns hier jedoch äußerste Zurückhaltung, so dass von der verbreiteten Art der Kommunikation über die sozialen Medien abgeraten werden muss (ganz besonders etwa bei Freundschaftsanfragen von Patienten über Facebook).

Nicht vermeidbar sind im Internet die heute bereits verbreiteten Bewertungsplattformen (jameda, esando, sanega u. a., für Kliniken z. B.: klinikbewertungen.de). Wie funktionieren diese Plattformen? Ein Nutzername und eine E-Mail-Adresse genügen für die generell anonymen Bewertungen, die entweder in Schulnoten oder in Textform erfolgen können. An Mitmachplattformen für Patienten wären Google, yelp, eKomi zu nennen. Man kann sie nutzen mit aktivem Empfehlungsmanagement als Teil eines Online-Reputations-Managements (Sammeln positiver Beurteilungen). Was aber tun bei schlechten Bewertungen? Hier gilt es, sich an den Portalbetreiber zu wenden. Bei offenkundig rechtswidrigen Angaben, bei falschen Tatsachenbehauptungen oder wenn Klarnamen genannt werden, muss gelöscht werden, notfalls mit anwaltlicher oder gerichtlicher Hilfe. Darüber hinaus gibt es für die Bewerteten auch die Möglichkeit zu kommentieren, eine generelle Löschung ist nicht möglich. Vorbeugen kann man jedoch durch regelmäßiges Online-Reputations-Management, durch regelmäßige Eingabe des eigenen Namens in eine Suchmaschine oder etwa mit Google Alert, worüber eine automatische Benachrichtigung erfolgt, wenn im Netz etwas zum eigenen Namen veröffentlicht wird. Nach der Entdeckung falscher, diskriminierender Einträge sollte man Beweise sichern (z. B. mittels Screenshots) – innerhalb von 4 Wochen nach Feststellung ist einstweiliger Rechtsschutz möglich. Generell ist die Rechtslage so, dass das Persönlichkeitsrecht des Bewertenden auf freie Meinungsäußerung über dem Recht des Bewerteten steht. Hier besteht mitunter die Schwierigkeit der Abgrenzung zwischen Tatsachenbehauptung und Meinungsäußerung.

Datenschutz in der Praxis: eine der naheliegenden, einfachsten Kommunikationsmöglichkeiten in der Praxis ist der E-Mail-Kontakt. Hier ist jedoch dringend Zurückhaltung geboten. Der übliche E-Mail-Verkehr ist in keiner Weise als datengeschützt anzusehen. Auch die von T-online neuerdings angebotene E-Mail-Verschlüsselung kann nach Einschätzung der Referentin nicht als genügend sicher einschätzt werden, auch nicht das durch Bundesgesetz geregelte DeMail-Verfahren, es werde auch kaum genutzt. Eine wirklich hinreichend sichere Verschlüsselung allerdings sei aufwendig und umständlich. Links zu geeigneter Verschlüsselungs-Software lassen sich in den Computer-Fachzeitschriften finden. Derzeit kann ansonsten von inhaltlicher Kommunikation mit Patienten über E-Mail nur abgeraten werden. Allenfalls Terminabsprachen über E-Mail, bei Einverständnis des Patienten, können als vertretbar angesehen werden. Falls von Patienten E-Mail-Kontakt gewünscht wird, sollten sie auf jeden Fall ausdrücklich (schriftlich, ggf. schon im Behandlungsvertrag) darauf hingewiesen werden, dass bei unverschlüsseltem E-Mail-Verkehr Unbefugte mitlesen können.

Vorsicht ist auch geboten beim Austausch von Daten/Informationen über Fax. Faxgeräte, wie übrigens auch moderne Kopiergeräte, speichern die übermittelten bzw. kopierten Daten. Dies muss berücksichtigt werden bei der Entsorgung von Fax-Filmrollen, der Weitergabe, Zurückgabe (Leasing) oder Entsorgung dieser Geräte (bei Kopierern z. B. den Gerätechip entnehmen).

Mobile Computer: Hier ist zu bedenken, dass zumindest in ungenügend gesicherten Netzen, besonders im öffentlichen Raum, ein Abfangen der Informationen jederzeit möglich ist. Wichtig im öffentlichen Raum ist entsprechend eine Diebstahlsicherung, Schutz vor Einblick auf den Monitor durch Unbefugte (Screensaver u.a.), ggf. Aufbau eines Virtual Private Network. Für vertrauliche Daten sollte auf dem Laptop ein Security Lock angelegt werden. Bei iPads besteht die Schwierigkeit, dass keine Datenspeicherung auf externen Datenspeichern möglich ist, dies geschieht entweder auf Chip oder in der Dropbox, d. h. in einer Cloud. Analoges gilt für Smartphones. Sensible Daten sollte man nicht auf diesen Geräten speichern. Selbst wenn man meint, alles auf solchen Geräten gelöscht zu haben und den Chip entnommen hat, bleiben weiter Daten auf dem Smartphone gespeichert. Eine Entsorgung dieser Geräte sollte daher am besten sicher auf dem Wertstoffhof erfolgen.

Als besonders unsichere Kommunikationsform ist der Referentin zufolge What's app einzustufen.

Outsourcing von Dienstleistungen in der Praxis: In Frage kommen hier die Fernwartung von Computern, die Nutzung externer Sekretariatsdienste (Schreibarbeiten, Termindienste wie TerminLand, die die Daten auf eigenen Servern speichern, Abrechnung) oder die Nutzung der Speichermöglichkeiten auf externen Servern (Cloud Computing). Hier bestehen erhebliche Probleme in Richtung eines Verrats von Berufsgeheimnissen. Von externen Dienstleistern ist auf jeden Fall eine Verschwiegenheitserklärung zu fordern (schriftlich).

Die Speicherung von Patientendaten in der Cloud ist nicht zulässig, da unbekannt ist, wo, auf welchen Servern die Daten gespeichert werden und man dafür keine Kontroll- und Zugriffsmöglichkeiten hat! Für private Datenspeicherung kommen allenfalls Private Clouds bei deutschen oder wenigstens europäischen Anbietern in Frage. Bei der Speicherung von Patientendaten auf externen Medien, namentlich auch USB-Sticks, ist auf jeden Fall auf eine hinreichend sichere Verschlüsselung zu achten.

Bei der Vernichtung von Papierakten sollte darauf geachtet werden, dass ein Shredder mit cross-cut-Verfahren gewählt wird. Oder die Akten sollten von einem zertifizierten Aktenvernichtungsbetrieb vernichtet werden.

Abschließend einiges zur Gestaltung der Praxis-Homepage: Bei der evtl. Verwendung fremder Texte oder Bilder gilt es, unbedingt das Urheberrecht zu beachten (Urhebername am besten direkt am Bild/Foto mit Namen des Urhebers). Das ©-Zeichen ist nicht erforderlich. Wichtig ist, dass das Impressum auf jeder Seite der Homepage mit höchstens einem Klick erreichbar ist. Für das Impressum sind die Vorgaben von § 5 TMG und der DL-InfoV zu beachten. Die UmsatzsteuerID, bei Bedarf einschließlich Haftpflichtversicherungsangabe wären u. a. zu nennen (für weitere Informationen vgl. das „Merkblatt zu Darstellungsmöglichkeiten im Internet": http://lppkjp.de/recht/datenschutz/). Wenn über die Homepage Daten erhoben werden z. B. über ein Kontaktformular, Aufrufe-Zähler, Einbindung in soziale Netzwerke bedarf es darüber hinaus auch einer Datenschutzerklärung. Bei Nutzung des Aufrufe-Zählers der Google Inc. (Google Analytics) ist zu bedenken, dass die Daten an Google weitergegeben und dort gespeichert werden. Ein Ausweg könnte ein Aufrufe-Zähler ohne Tracking Tool sein. Alle unsere über Facebook oder Google eingegebenen Daten werden gespeichert und in die USA bzw. nach Kanada übermittelt.

Zum Schluss ging Frau Ackermann in Kürze auch auf die Vor- und Nachteile der Online-Beratung und -Therapie ein (über Internet-Blogs, E-Mail, Skype u. a.). Zu erwähnen sei hier nur: Online-Beratung über Skype muss inzwischen als schwierig eingeschätzt werden, da auch Skype inzwischen abgehört werden kann. Hier soll nicht weiter darauf eingegangen werden. Zur Online-Beratung und -Therapie hat es am 9.11.2013 eine eigene Tagung der LPPKJP gegeben. Informationen zu dieser Thematik finden sich auf der Homepage unter http://lppkjp.de/aktuelles/berichte-veranstaltungen/.

Dr. Rainer Doubrawa
(Datenschutzbeauftragter der LPPKJP)