Datenschutz und Datensicherheit

Autor_Johannes Oberhuber

© StockLite

Sobald Sie in Ihrer Praxis mittels elektronischer Datenverarbeitung Patientendaten aufnehmen und bearbeiten beziehungsweise ein digitales Röntgenbild vorliegen oder dieses zu erstellen haben, gibt es eine Reihe von Gesetzen und Verordnungen, die es zu beachten gilt. Bei den immens wachsenden Datenvolumina ist die Beachtung der einschlägigen Vorschriften von Beginn an mit einzuplanen.

_Der Arzt in der modernen Praxis sollte außer Mediziner am besten noch Rechtsanwalt, Betriebswirt und Computerspezialist sein. Der Einsatz EDV-gestützter Systeme bringt bestimmt mannigfaltige Vorteile im täglichen Betrieb, aber mit dem Ansammeln von immer mehr Daten wird die Beherrschung der Datenberge zunehmend schwieriger. In der Praxis sind unter anderem folgende Gesetze und Richtlinien einzuhalten, bzw. sind diese Verordnungen von Relevanz: StGB (Strafgesetzbuch), BDSG (Bundesdatenschutzgesetz), EG-Richtlinie, DIN-Normen, VDE, RöV mit QS-RL und GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen).
Die Digitalisierung geht in großen Schritten voran. Untersuchungen der IDC Central Europe im Auftrag von EMC Deutschland kamen zu dem Schluss, dass wohl bis Ende 2010 circa 1,2 Zettabyte Daten auf den Speichersystemen abgespeichert sind. Um sich das zu versinnbildlichen: das sind 1,2 Billionen Gigabyte oder 37,5 Mrd. Apple iPad mit je 32 GB Speicher. Diese iPad aneinandergereiht könnten den Äquator 227-mal umrunden. Die Tendenz ist ganz klar: die Datenvolumen werden weiter in großem Maße steigen, sodass die Herausforderung sein wird, mit diesen Daten verantwortungsvoll und gesetzmäßig umzugehen.

_Das A und O – der Datenschutz

Bereits in der Vergangenheit haben wir immer öfter von Datenskandalen, Datenlecks und den daraus resultierenden Problemen gehört und gelesen. Die Veröffentlichung habhaft gewordener Daten betrifft heutzutage nicht nur Regierungen, sondern in vermehrtem Maße auch den normalen Bürger und Patient. Es ist von großer Wichtigkeit, den Datenschutz und die Datensicherheit noch mehr als bisher in den Fokus der Aktivitäten zu lenken. Der Datenschutz beinhaltet vor allem, dass personenbezogene oder andere persönliche Daten (auch Unternehmensdaten) nicht unberechtigt weitergegeben werden bzw. vor sonstigem Missbrauch geschützt sind. Der zweite Punkt, die Sicherheit der Daten, resultiert aus dem Datenschutz bzw. ist dessen logische Konsequenz.
Wie wichtig beide Punkte sind, wird in § 203 StGB (Strafgesetzbuch) deutlich. Dort heißt es: „Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als (...) Arzt, Zahnarzt (...) anvertraut worden oder sonst bekannt geworden ist, wird mit einer Freiheitsstrafe von bis zu einem Jahr oder mit einer Geldstrafe bestraft."
Das Verbot der Weitergabe von Daten stellt jedoch nur einen Aspekt innerhalb des Datenschutzes dar, welcher unter gewissen Umständen auch durch die schriftliche Zustimmung des betroffenen Patienten aufgeweicht werden könnte. Unberührt davon bleibt jedoch das Recht des Patienten auf Auskunftserteilung, das sich z.B. bei Verwendung einer digitalen Röntgenanlage auch auf die „Auskunft über den logischen Aufbau der automatisierten Verarbeitung" usw. erstreckt. Es ist wichtig, diese Punkte in das Praxisqualitätsmanagement mit aufzunehmen. Sie als Arzt sind aber nicht nur dafür verantwortlich, was Sie speichern, sondern auch für den Umstand, wer, wo und wie Zugriff auf das Gespeicherte hat. Hinzu kommt noch, dass dies alles lückenlos dokumentierbar und nachvollziehbar sein muss.

Hierbei reicht keinesfalls der Fakt aus, dass die Daten einfach nicht weitergegeben werden. Sie bedürfen einer zusätzlichen ordentlichen wie zuverlässigen Sicherung, sodass sie bei Bedarf jederzeit wiederhergestellt werden können bzw. auch nach Jahren noch verfügbar sind.
Mit dem Einsatz bildgebender Verfahren wachsen die zu verwaltenden Datenvolumen auch in der Praxis um ein vielfaches schneller als dies bisher der Fall war. Die Verantwortlichen und die Administratoren müssen sich darauf einstellen und Strategien für die Datenhaltung, die Datensicherung und den Datenschutz vorbereiten. Oft werden aufgrund von mangelndem Wissen, aus Zeitnot oder einfach nur durch schlechte Beratung Risiken eingegangen, die nicht nur unkontrollierbar sind, sondern im extremen Gegensatz zu geltenden Rechtsvorschriften stehen (siehe erwähnten § 203 StGB). Die Datenschutzbeauftragten der Länder haben in ihren Beratungen grundlegende Sicherheitsziele definiert, die von Systemen zur medizinischen Datenverarbeitung gewährleistet werden müssen. Die Ziele sind: 1. Vertraulichkeit, 2. Authentizität (Zurechenbarkeit), 3. Integrität, 4. Verfügbarkeit, 5. Revisionsfähigkeit, 6. Validität, 7. Rechtssicherheit, 8. Nicht-Abstreitbarkeit von Datenübermittlungen, 9. Nutzungsfestlegung.
Wie weit die Vorschriften und der tatsächliche Umgang mit Daten deckungsgleich sind, das muss jeder für sich selbst beantworten. Die Tendenz ist aber leider nicht von der Hand zu weisen. Es gibt hier so etwas wie einen Gewöhnungseffekt zu beobachten. Immer mehr User geben in Internetforen und Social Networks in erheblichen Umfängen persönliche Daten von sich preis. Dadurch, dass es im persönlichen Bereich zur Normalität wird Informationen auszutauschen, ist auch die Hemmschwelle im Arbeitsalltag gesunken. Was vor einigen Jahren noch undenkbar war, ist heute Normalität.
So passiert es durchaus, dass eine unverschlüsselte Mail mit Röntgenbildern oder ganze Patientenstammdaten an einen Kollegen verschickt werden, um diese fachlich mit ihm zu besprechen bzw. eine Behandlungsstrategie festzulegen. Oder es werden die Daten auf einem fremden FTP-Server zum Download geparkt. Auch die Datensicherung auf Speichersystemen im Internet ist zur Normalität geworden und es wird nicht mehr überprüft, ob die einschlägigen Vorschriften erfüllt werden können.
Diese Verhaltensweisen mögen sehr praktisch und einfach sein, sie sind aber im direkten Widerspruch mit den Gesetzen. Ganz klar: wer so handelt, befindet sich nicht in einer Grauzone, sondern im Unrecht.

_Das größte Sicherheitsrisiko ist der Bediener

Ebenfalls nicht vernachlässigt werden darf die Datenhaltung in den eigenen Räumen. In der erwähnten Studie von IDC wird auch die Problematik der Datensicherheit aufgezeigt. Der Anteil der schützenswürdigen Daten wird im Jahr 2020 einen Anteil von 50 Prozent haben. In einer Praxis sind es allerdings über 90 Prozent! Mitarbeitern sollten nur so viele Rechte im System gewährt werden, wie diese minimal benötigen, um arbeiten zu können. Das größte Sicherheitsrisiko ist nach wie vor der Bediener.
Der Datenschutz fängt bei der IT mit der Erfassung der Daten an. So sollte genau definiert sein, wer welche Daten eingeben oder ändern darf. Das unberechtigte Weitergeben oder Löschen von Daten muss prinzipiell unterbunden werden. Zudem sollte jede Datenbewegung dokumentiert nachvollzogen werden können. Kommt es aus gutem Grund zur Weitergabe von Daten, müssen diese verschlüsselt werden, wobei lediglich der rechtmäßige Empfänger über den entsprechenden Schlüssel verfügt. Nur wenn sichergestellt werden kann, dass die richtige Person der Datenempfänger ist, stehen Sie selbst nicht in der Verantwortung. Wie die Arbeitsabläufe zur Datenweitergabe gestaltet sind, sollte im Qualitätsmanagement dokumentiert sein.
Nicht selten sind ganze Netzwerke nach außen hin (Internet) nur sehr unzureichend geschützt oder verfügen noch nicht einmal über eine funktionierende Virenprüfung. Auch die Öffnung der hausinternen Netze wegen des Betriebes von modernen Kommunikationsmitteln wie Smartphones kann durchaus problematisch werden. Sind solche Lücken vorhanden und werden diese Lücken von Angreifern ausgenutzt, dann geht die Rechtsprechung regelmäßig wenigstens von Fahrlässigkeit aus.

_Achtung auch bei der Datensicherung

Von großer – weil ggf. existenzsichernder – Bedeutung ist die Datensicherung. Bezogen auf die Speicherkapazität ist eine der preiswertesten Methoden, um Daten zu sichern, die externe Festplatte. Die Schreibgeschwindigkeiten sind gut und die Transportierbarkeit ist mittlerweile durch die geringen Größen und Gewichte auch annehmbar. Allerdings muss auch hier darauf geachtet werden, dass die Daten auf der Sicherungsplatte verschlüsselt sind. Nur dann kann bei einem eventuellen Verlust davon ausgegangen werden, dass die Daten sicher vor dem Zugriff eines fremden Dritten sind. Hinsichtlich der Datensicherung muss ein Plan mit Verantwortlichkeiten existieren. Zudem müssen turnusgemäß Medien zur Verfügung stehen, die nur ein einziges Mal beschrieben werden und danach nur noch lesbar sein können. Dieser Fakt ist für die revisionssichere Datenablage von Belang.
Ein weiteres Problem stellen die Vorschriften bezüglich Aufbewahrungsdauer von Unterlagen dar. Diese gelten für elektronische Systeme übrigens ge-

nauso wie für herkömmliche Patientenakten oder Röntgenbilder.

Um zu erkennen, welche Probleme auf uns alle, die wir moderne IT in unseren Unternehmen und Praxen einsetzen, zukommen können, müssen wir erst einmal einen kurzen Blick zurückwerfen.

Kennen Sie beispielsweise noch die 8-Zoll-Diskette, die mit etwas mehr als 200 mm Seitenlänge aus heutiger Sicht riesig erscheint? Nein? Oder die 5¼-Zoll-Diskette mit ihrer für damalige Verhältnisse enormen Speicherkapazität von 110 KB (ca. 0,1 MB)? Sicher haben Sie auch noch ein passendes, funktionierendes Laufwerk parat, um die auf solchen Disketten befindlichen Daten zu lesen. Oder müssen Sie etwa auch hier mit „Nein" antworten?

So wie Ihnen wird es wohl 99,9 Prozent aller Leser dieses Beitrags gehen. So wird diese „alten" Speichermedien heute so gut wie keiner mehr auslesen können, und das, obwohl die Einführung der 5¼-Zoll-Diskette gerade einmal rund 30 Jahre zurückliegt.

Dennoch vertrauen wir wie selbstverständlich darauf, dass wir im Jahr 2041 ganz automatisch imstande sein werden, die ausgelagerten Daten von heute bzw. die Datensicherung von morgen wieder einzulesen. Ohne ein sinnvolles Datensicherungskonzept und ohne eine entsprechende Migrationsstrategie für die Archivierung wird es Ihnen jedoch nicht möglich sein, Patientenakten und ggf. Röntgenbilder bis dahin aufzubewahren bzw. sie dann auch noch lesen zu können.

Mit der steigenden Datenmenge nimmt auch das Problem der Datenmigration zu. Daten auf USB-Sticks sind nach maximal zehn Jahren verschwunden. Festplatten sind da sogar noch „vergesslicher" – dort ist bereits nach rund fünf Jahren mit ersten Ausfallerscheinungen zu rechnen.

So gibt es momentan eigentlich nur zwei wirklich sinnvolle Alternativen, große Datenmengen über lange Zeiträume zu speichern und auch abrufen zu können. Das gilt zum einen für das Magnetband im LTO-Ultrium5-Standard (bis zu 3.000 GB) und zum anderen für ein Hochsicherheitsrechenzentrum, auf dem die Daten komplett verschlüsselt übertragen und gespeichert werden. Beim Magnetband stellt sich allerdings die Frage nach der Hardware in 30 Jahren.

Die Infrastrukturen für die gesicherte, verschlüsselte externe Datenspeicherung befinden sich gerade im Aufbau. Hier wird sich in naher Zukunft einiges tun. Zu den Neuerungen wird auch die verschlüsselte Speicherung in zukünftigen Strukturen, den sogenannten Clouds, gehören.

Aus heutiger Sicht sind diese beiden Wege die einzigen zukunftssicheren Möglichkeiten, um gegebene Vorschriften zu erfüllen und die Daten auch in vielen Jahren noch lesen zu können._

_Kontakt

digital dentistry

Johannes Oberhuber
Senior-Consultant it-netconsult GmbH
Neuling 4
83278 Traunstein
Tel.: 08756 96999-90
E-Mail: kontakt@itntc.de
www.itntc.de

Autor