DVT – Für & Wider aus Sicht des Anwenders (2)

Während im ersten Teil unserer Artikel-Trilogie (*KN* 1/2-2009) die Anforderungen an die elektronische Archivierung sowie das Versenden von Patientendaten und Röntgenbildern im Mittelpunkt standen, widmet sich Teil 2 nun dem Thema IT-Voraussetzungen. IT-Spezialist Johannes Oberhuber erläutert darin, welche herausragend wichtige Stellung der Datenschutz innerhalb des kieferorthopädischen Praxisalltags einnimmt und wie Daten entsprechend gesichert werden können.

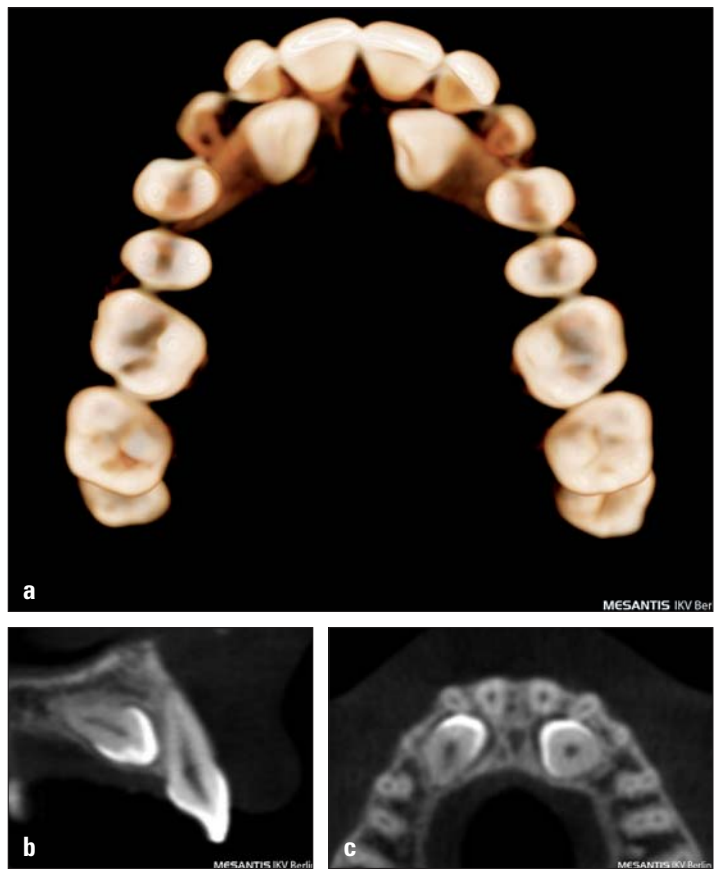

Abb. 1a–c: Eine klassische rechtfertigende Indikation für ein DVT sind verlagerte Zähne. Dabei kommt es – wie häufig angenommen – jedoch nicht nur auf die Topografie der verlagerten Zähne in Relation zu den benachbarten Strukturen an (a), sondern für den kieferorthopädischen Spezialisten vor allen Dingen auf das vestibuläre Knochenangebot in den Cross Sections benachbarter Zähne (b) sowie auf eventuelle Wurzelresorptionen benachbarter Zähne in der Axialebene (c). Erst diese Trias macht ein DVT für einen Kieferorthopäden klinisch wertvoll.

Sobald Sie in Ihrer Praxis mittels elektronischer Datenverarbeitung Patientendaten aufnehmen und bearbeiten bzw. ein digitales Röntgenbild vorliegen oder dieses zu erstellen haben, sollten Ihnen folgende Begriffe unbedingt geläufig sein: StGB, BDSG, EG-Richtlinie, DIN, VDE, RöV und QS-RL. Zwar stellen diese lediglich eine kleine Auswahl an Gesetzen, Verordnungen und Normen dar, dennoch sollten sie in der Praxisroutine unbedingt ihre Berücksichtigung finden. Hinzu kommen weitere Vorschriften hinsichtlich Buchhaltung oder E-Mail-Verkehr, wie beispielsweise die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen" (GDPdU).

Ein Großteil jener Begrifflichkeiten ist im täglichen Arbeitsablauf sehr gut handhabbar – vorausgesetzt, es werden außer den technischen Vorgaben zwei ganz entscheidende, wichtige Punkte beachtet: der Datenschutz und die Datensicherheit. Ersterer 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. Hier jedoch ist bereits äußerste Vorsicht geboten. Denn Sie als Arzt sind nicht nur dafür verantwortlich, was Sie speichern, sondern auch für den Umstand, wer, wo und wie Zugriff auf das Gespeicherte hat. Hinzu kommt der Fakt, dass dies alles noch dokumentierbar 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 verfügbar sind.

Wie sieht nun die Umsetzung all dessen in der realen Arbeitswelt kieferorthopädischer Praxen aus?

Schaut man sich heutzutage Speichermedien an, sind z. B. externe Festplatten sehr preiswert zu haben und daher sehr beliebt, um Patientendaten darauf zu sichern. Schließlich sind sie bequem transportierbar und daher leicht überallhin mitzunehmen. Doch was ist, wenn die Festplatte in der U-Bahn vergessen wird und dadurch eine Kopie der Patientendaten in der Öffentlichkeit kursiert?

Oder aber der E-Mail-Verkehr, mit dessen Hilfe Röntgenbilder oder ganze Patientenstammdaten unverschlüsselt an einen Kollegen verschickt werden, um diese fachlich mit ihm zu besprechen bzw. eine Behandlungsstrategie festzulegen. Was ist, wenn diese wichtigen Daten durch Unbefugte einfach „mitgelesen" werden?

Nicht selten sind ganze Netzwerke nach außen hin (Internet) nur sehr unzureichend geschützt oder verfügen noch nicht einmal über eine funktionierende Virenprüfung. Was ist, wenn Daten korrumpiert werden oder sich gar im Internet wiederfinden?

Leider werden oft Datenbestände nur sporadisch, mangelhaft oder gar nicht gesichert. Was jedoch passiert, wenn diese Daten auf einmal unbrauchbar werden oder gar der Server gestohlen wird?

Ein weiteres Extrem stellen diejenigen dar, die die Datensicherung online bei einem Provider auf einen FTP-Server spielen. Was ist, wenn diese Daten öffentlich würden? Wie stellen Sie sicher, dass nur Befugte den gewünschten Zugriff haben?

Diese fünf Beispiele sollen verdeutlichen, dass es in vielen Praxen oft ganz anders ausschaut, als es eigentlich der Fall sein sollte. Oft werden aufgrund von mangelndem Wissen, aus Zeitnot oder einfach nur durch schlechte Beratung Risiken eingegangen, die nicht nur unkontrollierbar sind, sondern im krassen Gegensatz zu Rechtsvorschriften stehen (siehe erwähnten § 203 StGB).

Zur Erinnerung sollten im Folgenden nochmals die von den Datenschutzbeauftragen der Länder grundlegend definierten Sicherheitsziele genannt sein, die von Systemen zur medizinischen Datenverarbeitung gewährleistet werden müssen:

1. Vertraulichkeit
2. Authentizität (Zurechenbarkeit)
3. Integrität
4. Verfügbarkeit
5. Revisionsfähigkeit
6. Validität
7. Rechtssicherheit
8. Nicht-Abstreitbarkeit von Datenübermittlungen
9. Nutzungsfestlegung.

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 sein. Kommt es aus gutem Grund zur Weitergabe von Daten, müssen diese verschlüsselt werden, wobei lediglich der rechtmäßige Empfänger über den entsprechenden Schlüssel verfügt.

Damit diese Vorgaben eingehalten werden können, sollte die EDV verschiedene Anforderungen erfüllen.

So müssen z. B. alle Daten zentral auf einem Server gelagert werden, um letztlich die Verwaltung und Zugriffsrestriktion zu gewährleisten. Unabhängig davon müssen die Daten permanent verfügbar sein, da ein längerer Ausfall direkten Einfluss auf die tägliche Arbeit hätte. Hierfür sind sogenannte RAID-Systeme zu empfehlen. Serversysteme sollten mindestens über RAID-1, besser jedoch über RAID-5 verfügen.

Bei einigen Betriebssystemen können zusätzlich sogenannte Schattenkopien aktiviert werden, damit zweimal täglich ein „Snapshot" der Festplatten abgelegt werden kann. Würde eine Datei versehentlich gelöscht, könnte diese binnen weniger Minuten wieder hergestellt werden.

Mitarbeitern sollten nur so viele Rechte im System gewährt werden, wie diese minimal benötigen, um arbeiten zu können. 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.

Alle externen Transaktionen müssen sicher verschlüsselt und dokumentiert werden. Nur wenn sichergestellt werden kann, dass die richtige Person der Datenempfänger ist, stehen Sie selbst nicht in der Verantwortung.

Ein weiteres Problem stellen die Vorschriften bezüglich Aufbewahrungsdauer von Unterlagen dar. Diese gelten für elektronische Systeme übrigens genauso wie für herkömmliche Patientenakten oder Röntgenbilder.

Die gesamten Patientendaten einer mittelgroßen Praxis auf einem USB-Stick zu speichern und dann einfach in die Hosentasche zu stecken, ist heute ohne Weiteres möglich. Durch diese moderne, leicht zu handhabende Technik erscheint es uns daher auch abwegig, hier an irgendwelche Fallstricke zu denken. Doch genau darin liegt künftig die Crux. 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 erschient? Nein? Oder die $5^1/_4$-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 % aller Leser dieses Beitrags gehen. So wird diese „alten" Speichermedien heute so gut wie keiner mehr auslesen können und das, obwohl die Einführung der $5^1/_4$-Zoll-Diskette gerade einmal rund 30 Jahre zurückliegt.

Dennoch vertrauen wir wie selbstverständlich darauf, dass wir im Jahr 2039 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.

Denn mit der steigenden Datenmenge nimmt auch das Problem der Datenmigration zu. Daten auf oben erwähnten USB-Stick 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 dann immer noch abrufen zu können: Das gilt zum einen für das Magnetband im LTO-4-Standard (bis zu 1.600 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 den Gerätschaften in 30 Jahren und beim Rechenzentrum die Frage nach dem Datenschutz. Denn diese sichere Infrastruktur ist erst noch im Aufbau. Aus heutiger Sicht allerdings sind diese beiden Wege die einzigen zukunftssicheren Möglichkeiten, um gegebene Vorschriften zu erfüllen und die Daten auch in 30 Jahren noch lesen zu können. KN

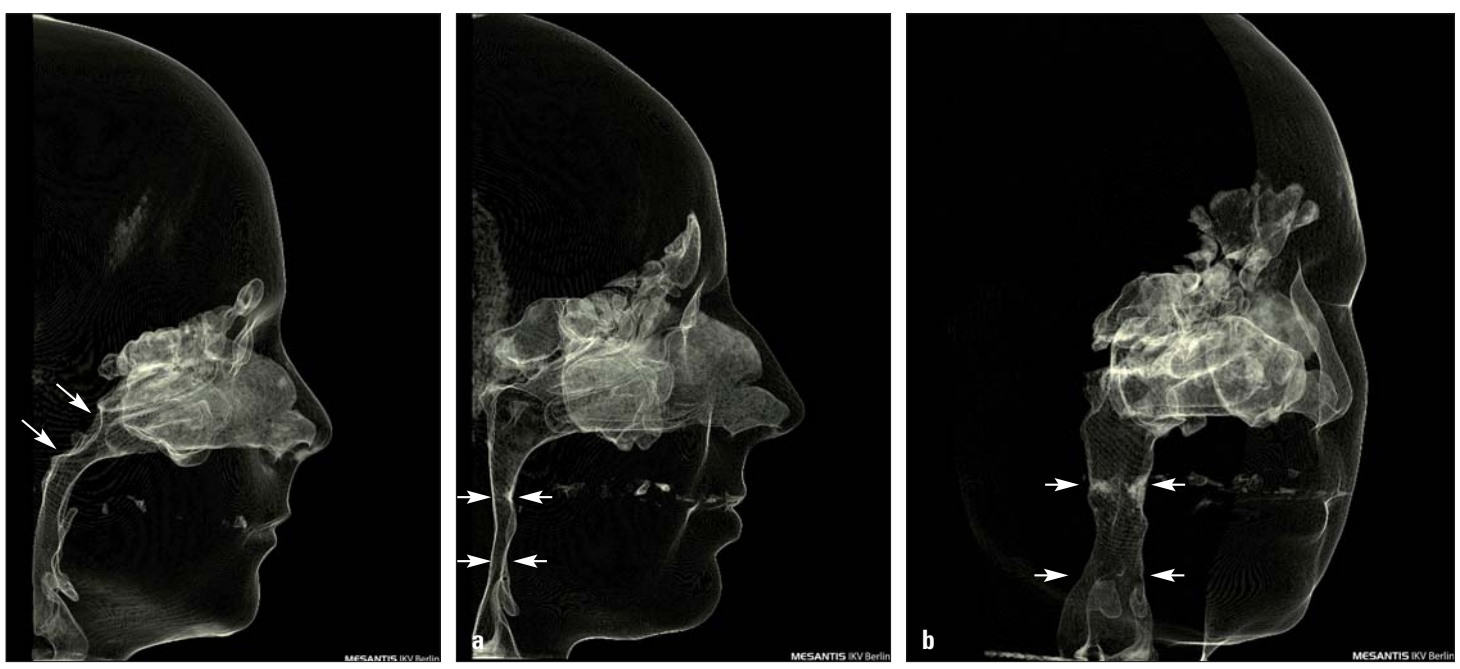

Abb. 2: Darstellung einer Hyperplasie der Tonsilla pharyngea (Pfeile) mithilfe der Spezialsoftware MESANTIS-3D. Derartige Befunde sind insbesondere bei Patienten mit Mundatmung von besonderer Bedeutung und in der interdisziplinären Behandlung mit HNO-Kollegen zu therapieren.

Abb. 3a, b: Darstellung einer Einengung des Oropharynx (Pfeile) in der Sagittalebene (a). Diese Veränderungen sind im Einzelfall nur durch Unterkiefervorverlagerungen – soweit kieferorthopädisch indiziert – zu therapieren. Der 2-D-Querschnitt der oberen Atemwege in der Sagittalebene täuscht in manchen Fällen aber nur ein geringes Volumen der oberen Atemwege vor. Daher sind 3-D-Aufnahmen, in denen man die Breite sowie das Volumen direkt berechnen kann, sehr vorteilhaft (b).

KN Adresse

Johannes Oberhuber
Senior-Consultant
it-netconsult GmbH
Neuling 4
83278 Traunstein
Tel.: 0 94 41/1 74 97-90
E-Mail: kontakt@itntc.de
www.itntc.de

KN Kurzvita

Johannes Oberhuber

- Studium Wirtschaftsingenieurwesen an der TU Berlin, Studienschwerpunkt Informations- und Kommunikationssysteme
- seit 1993 als IT-Consultant im Bereich Security tätig
- seit 2004 Senior Consultant der it-netconsult GmbH, zuständig für die deutschlandweite Betreuung von vorwiegend zahnmedizinisch ausgerichteten Kunden