© NicoElNino/Fotolia.de

Digitaler Workflow in der Cloud

Vorteile nutzen, Datenschutz beachten

Auf der diesjährigen IDS präsentierten Industrie, Handel, Fräszentren und Softwarefirmen ihre neuen und schon eingeführten Angebote zur Nutzung von Cloud-Systemen. Unsere Autoren Hans-Gerd Hebinck und Karsten Schulz klären hier auf: Die Vorteile von Cloud-Computing in Zeiten des CAD/CAM sind bestechend, aber der Umgang mit Patientendaten fordert große Umsicht.

Einfach ausgedrückt bedeutet Cloud (aus dem Englischen = Wolke) bzw. Cloud-Computing, dass Daten auf externen Servern abgelegt werden und von verschiedenen Anwendern über ein Netzwerk wie z. B. das Internet genutzt und verarbeitet werden können. So weit, so gut. Doch wo mehrere Partner aus Praxen, Laboren und Unternehmen – und vielleicht sogar aus unterschiedlichen Ländern – auf Daten zugreifen, da sind auch hohe Anforderungen an den Datenschutz zu beachten.

Die Datenwolke in der modernen Dentalwelt

Bisher nutzt die Dentalbranche Cloud-Systeme noch überwiegend für den reinen Datenaustausch zwischen unterschiedlichen Partnern. So werden Fotos, DVT-Bilder oder Scandaten zwischen Behandler, Dentallabor und Fräszentrum hin- und hergeschickt. Beispielsweise bieten Anbieter von CAD/CAM-Systemen den Austausch von Daten an, die über den Mundscanner gewonnen wurden. Diese Daten werden quasi in der Cloud des Systemanbieters „zwischengeparkt" und dort vom Partner zur Weiterverarbeitung abgeholt. Ebenfalls weitverbreitet ist der Austausch von Daten über spezialisierte Cloud-Anbieter wie die US-amerikanische Dropbox: Hier findet lediglich eine (unverschlüsselte) Online-Datenspeicherung statt, die Teilnehmer laden dorthin Daten hoch und wieder herunter.
Rein technisch kann die Nutzung von Cloud-Lösungen aber noch viel weiter gehen: Auf der IDS 2017 erstmals vorgestellt, gibt es zukünftig eine Praxissoftware als vollständig laufendes Cloud-System. Damit sind Zahnärzte und Praxismitarbeiter in der Lage, mit unterschiedlichen Endgeräten von überall auf die Praxisdaten zuzugreifen und diese zu verarbeiten. Konkret: vom Desktop-Windows-Rechner aus dem Büro, vom Laptop im Behandlungszimmer, vom iPhone oder Android-Smartphone von unterwegs und vom Tablet aus dem Homeoffice. – Und dabei wird auf keinem der Endgeräte eine Softwareinstallation notwendig.

Welche Vorteile hat Cloud-Computing?

Das „Handbuch für Praktiker" von Karsten Schulz [1] nennt bereits 2015 wesentliche wirtschaftliche Vorteile von Cloud-Systemen:

- Geräteunabhängigkeit
- Bessere Planung der Speicherressourcen und Rechenleistungen
- Orts- und zeitunabhängiger Zugriff auf Daten und Software
- Verbesserte Zusammenarbeit zwischen Zahnarztpraxis, Dentallabor, Fräszentren und weiteren Geschäftspartnern
- Steigerung der Effizienz
- Senkung der Ausgaben für IT.

Kein Wunder, dass angesichts solcher Vorteile die Wachstumsraten von Cloud-Anwendungen in den vergangenen

Jahren sowohl im geschäftlichen als auch im privaten Bereich stark gestiegen sind. In den nächsten Jahren ist weiteres starkes Wachstum zu erwarten. Entsprechend werden immer mehr Systemanbieter und Anwender auf den „Cloud"-Zug aufspringen.

Was müssen Sie über Patientendaten wissen, bevor Sie die Cloud nutzen?

Patientendaten sind nach dem Bundesdatenschutzgesetz besonders sensible Daten, die ein hohes Schutzniveau genießen. Das leuchtet ein – zumal der Zahnarzt zusätzlich noch die Paragrafen des Strafgesetzbuches zu beachten hat. Zum „Schutz des Privatgeheimnisses" darf der Zahnarzt ohne die ausdrückliche Einwilligung des Patienten (bis auf Notsituationen) niemals das Patientengeheimnis offenbaren. Konkret bedeutet dies: Will die Zahnarztpraxis dem Labor Patientendaten per Cloud zur Verfügung stellen, braucht sie die ausdrückliche Einwilligung des Patienten. Liegt diese nicht vor, dürfen seine Daten keinesfalls in einer Cloud abgelegt werden. Nur die vollständige Anonymisierung der Daten wäre eine Möglichkeit.
Im Alltag erleben wir allerdings häufig einen sehr laxen Umgang. Da werden Daten inklusive Patientennamen, Geburtsdatum und anderen personenbezogenen Informationen weitergegeben. Vielleicht liegt es an der langjährigen analogen Gewohnheit in der Kommunikation zwischen Zahnarztpraxis und Dentallabor, den Patientennamen als einfaches und effektives Identifikationsmittel zu benutzen. Geht es um die Cloud, müssen nun alle Beteiligten in Sachen Datenschutz sensibilisiert werden – nur so lässt sich der sorglose Automatismus durchbrechen.

Wo werden Daten verarbeitet und/oder gespeichert?

Eine entscheidende Frage lautet: Wo steht der Server? Denn je nachdem, wo der Vertragspartner für die Rechnerwolke seinen Sitz hat und wo die Daten tatsächlich verarbeitet werden, müssen unterschiedliche Dinge beachtet werden. Die Verträge für ein Cloud-Computing mit Gesundheitsdaten sind dadurch je nach Serverstandort sehr komplex. So gibt es beispielsweise Vorschriften, Daten nach der Verarbeitung zu löschen. Diese gelten auch bei einer Verarbeitung im Ausland. Überlegen Sie jetzt einmal: Wie wollen Sie diese erforderliche Löschung jemals bei einem großen Cloud-Anbieter aus den USA wie Amazon, Apple oder Dropbox sicher gewährleisten?
Die Datenschutzaufsichtsbehörde in Schleswig-Holstein lehnt beispielsweise die Nutzung von Microsoft Office 365 ab, weil die Dokumentation von Microsoft nicht ausreicht, um die Datenschutzkonformität festzustellen. Noch drastischer sind die gesetzlichen Vorschriften für die digitale Archivierung von Buchführungsunterlagen jeglicher Art: Nach den steuerrechtlichen Vorschriften in der Abgabenordnung müssen die aufbewahrungspflichtigen Unterlagen grundsätzlich in Deutschland aufbewahrt werden. Ausnahmen sind nicht vorgesehen, sodass die iCloud oder die Dropbox als Rechnungsarchiv ausscheidet. Dies gilt in dieser Schärfe „schon" bei Steuerunterlagen oder Office-Dokumenten aus dem täglichen Geschäftsbetrieb. Die Schutzmaßnahmen für Gesundheitsdaten liegen meist noch höher.
Am einfachsten ist es daher für Sie, wenn der Cloud-Dienst innerhalb der EU oder in einem Staat wie der Schweiz liegt, der von der EU als sicher eingestuft wurde, und wenn die Verarbeitung der Daten auch dort erfolgt. Die USA oder China gelten nach aktueller Rechtslage als sogenannte unsichere Drittstaaten. Nach Ansicht der Autoren ist in naher Zukunft keine Änderung dieser Einstufung zu erwarten. Für Patientendaten empfehlen wir daher, von Anfang an solche Anbieter auszuwählen, die ihre Server innerhalb der EU haben und sich an das europäische Datenschutzrecht halten. Wer dennoch auf einen Anbieter mit Server in den USA zurückgreifen will, benötigt spätestens für diese Entscheidung die Expertise eines externen Datenschutzbeauftragten. Dieser prüft vorab die gewünschte Lösung und berät konkret auf die individuelle Situation zugeschnitten. Der Experte zeigt meistens auch, dass und in welchem Maße der praktische Nutzen durch Einschränkungen oder zusätzliche Verträge und Maßnahmen sinkt.

Wichtig zu wissen!

Die für private Zwecke beliebten Cloud-Dienste von iCloud, Dropbox, GoogleDrive oder WhatsApp scheiden zurzeit für eine geschäftliche Nutzung aus, weil nach deutschem und europäischem Datenschutzrecht aktuell erhebliche Zweifel an einer rechtskonformen Nutzung bestehen.

Datenschutz bei Auslandszahnersatz

Wenn Sie Patientendaten analog oder digital an einen Importeur von Auslandszahnersatz aus China (oder anderen Billiglohnländern) zur Herstellung von Zahnersatz weitergeben, müssen Sie vorab einige Datenschutzvorschriften prüfen und beachten. Immer dann, wenn die Daten nicht garantiert vollständig anonymisiert weitergegeben werden, muss der Techniker seinen Zahnarzt und dieser seinen Patienten über die möglichen Risiken

Cloud-Computing hat viele Vorteile, aber gerade bei sensiblen Daten gilt es einiges zu beachten.
© Martin Bergien/Pixelio.de

umfassend und vollständig aufklären. Das wird kaum ein Zahnarzt fachlich leisten können – bei einer Datenverarbeitung in unsicheren Drittländern wäre dafür umfangreiches Fachwissen über Datenschutz und die Anwendung in fremden Rechtssystemen notwendig. Ohne Anonymisierung müssen der Zahnarzt und das Dentallabor (wenn es als Zwischenhändler tätig würde) einen Datenverarbeitungsvertrag mit dem Importeur abschließen, in dem viele Details geregelt und vor der Datenverarbeitung geprüft werden. Auch hier zeigt sich die Realität anders: Da erfolgen viele Beauftragungen für Auslandszahnersatz einfach so – ohne Vorabüberlegungen, Prüfungen und Maßnahmen für den Datenschutz. Das sind klare Rechtsverstöße. Welche Auswirkungen die neue EU-Datenschutz-Grundverordnung ab dem Jahr 2018 im Hinblick auf rechtliche Konsequenzen haben wird, bleibt abzuwarten.
Ein Tipp: Weiß der Zahntechniker, dass sein Zahnarzt auch Zahnersatzleistungen im Ausland ordert, kann er ihn im Rahmen eines Gesprächs auf die Datenschutzrisiken und mögliche Rechtsverstöße aufmerksam machen.

Aus der Cloud zu anderen Unternehmen – was passiert, wenn Daten „wandern"?

In dem Fall, dass ein Anbieter die Daten an andere Unternehmen weitergibt oder sich das Recht dazu einräumen lässt, wird es richtig kompliziert für eine rechtskonforme Lösung. WhatsApp und Facebook sind ein prominentes Beispiel für dieses Vorgehen. Privat muss jeder Verbraucher für sich selbst entscheiden, ob er diese Dienste nutzen möchte. Für einen Zahnarzt oder den Techniker ist es tabu, wenn sich Geschäftspartner vertraglich das Recht einräumen, Patientendaten an Drittunternehmen weiterzugeben. Eine vertraglich gute und sichere Gestaltung würde in den meisten Fällen so umfangreich und teuer, dass kaum ein Zahnarzt oder Dentallabor noch Interesse an einem solchen Dienst hätte. Beachten Sie: Der praktische Nutzen aus einer Cloud-Lösung kann deutlich sinken, wenn alle notwendigen Maßnahmen im Einzelfall dagegen abgewogen worden sind.

Fazit

Cloud-Computing bietet für Zahnarztpraxen und Dentallabore viele Chancen und kann zu höherer Effektivität, mehr Flexibilität und Kosteneinsparungen führen. Vor der Buchung von Kapazitäten oder dem Kauf eines Systems sollte vorab immer eine ausführliche Prüfung aus Sicht des Datenschutzes erfolgen. Fragen Sie Ihren Cloud-Computing-Anbieter auf jeden Fall vor einem Vertragsabschluss, in welchem Land die Cloud-Dienst-Firma ihren Sitz hat und in welchem Land die Daten verarbeitet und gespeichert werden. Cloud-Anbieter oder Serverstandorte in unsicheren Drittstaaten wie China und USA sollten nach Möglichkeit gemieden werden, weil die Vorteile aus der Cloud-Lösung gegen Rechtsunsicherheit, hohe Beratungskosten und drohende Strafen abgewogen werden müssen. Fragen Sie Ihren Cloud-Computing-Anbieter unbedingt auch, ob und an welche weiteren Unternehmen er die Daten weitergibt oder sich die Möglichkeit der Weitergabe einräumt. Datenschutzbeauftragte bieten Ihnen eine wertvolle Unterstützung bei der Auswahl des Cloud-Dienstes und helfen Ihnen dabei, eine praktikable, kostensparende und rechtssichere Lösung zu finden.

Literaturhinweis unter www.ztm-aktuell.de/literaturlisten

Dipl.-Betriebswirt (FH)
Hans-Gerd Hebinck

Dipl.-Informatiker (FH)
Karsten Schulz

Datenschutz.dental
Metzer Weg 13 · 59494 Soest
Tel.: 0172 2745444
Fax: 03212 1106197
E-Mail: info@godt-hebinck.de
https://datenschutz.dental