Inhalt

SANEXIO Verwaltungs GmbH | Meisebacherstraße 25 | 36251 Bad Hersfeld | info@sanexio.de | www.sanexio.de |Tel.: +49 6621 51098 50 | Fax: +49 6621 51098

SANEXIO Verwaltungs GmbH | Meisebacherstraße 25 | 36251 Bad Hersfeld | info@sanexio.de | www.sanexio.de |Tel.: +49 6621 51098 50 | Fax: +49 6621 51098

Einleitung

Vorwort von Frithjof Ebert

Einen Großteil meiner beruflichen Laufbahn habe ich damit verbracht, mich um IT Systeme in Arztpraxen zu kümmern. Dabei ist mir sehr häufig aufgefallen, dass es große Unterschiede in der Wahrnehmung von technischen Problemen und Umsetzungen zwischen IT-lern und Medizinern gibt.

Als Arzt haben sie schon mit vielen Arten von Netzwerken gearbeitet. Bei Netzwerken handelt es sich im Grunde genommen immer nur um einen Zusammenschluss von vielen Computern. Sie als Anwender sehen meistens nur die Benutzeroberfläche. Dies kann nun das KIS (Krankenhausinformations-system) sein, dass Sie im Krankenhaus kennengelernt haben oder Ihre eigene Praxis-Software. Insbesondere als niedergelassener Arzt sind Sie aber nicht nur einfacher Anwender dieser Dienstleistung sondern auch Entscheider, der über die strategische Ausrichtung seiner IT für die Praxis entscheiden muss.

Das Problem hierbei: Die Entscheidung für oder gegen ein bestimmtes IT-System hat grundsätzlich weitreichende Folgen: Dies umfasst zum einen den unternehmerischen Standpunkt und hierbei insbesondere die Kosten, zum anderen aber auch den ergonomischen Aspekt, also wie einfach oder schwierig sich die Software für Sie und Ihre Mitarbeiter bedienen lässt. Welchen Schulungsaufwand und welche Frustration eine falsche Entscheidung nach sich ziehen kann, habe ich in meiner Tätigkeit als Berater und Systemadministrator häufig erlebt.

Sie müssen als Arzt natürlich nicht detaillierte Kenntnisse der IT erwerben, um die richtigen Entscheidungen zu treffen. Die richtige Beratung und ein Grundwissen über die wichtigsten Prozesse reichen aus, um beim nächsten Gespräch mit dem Techniker oder dem Support Ihrer beauftragten

Softwarefirma die richtigen Fragen zu stellen, die Antworten zu verstehen und hiervon abhängig die richtigen Entscheidungen zu treffen.
Aus diesem Grund haben wir uns entschlossen, hier eine kleine Sammlung zu entwickeln, die Ihnen bei Ihren zukünftigen Entscheidungen helfen soll.

Der vernetzte Arzt

Netzwerke haben immer eine Primär-Aufgabe, nämlich Sie mit anderen Mitgliedern oder Teilnehmern des Netzes zu verbinden oder auf gemeinsame Informationen zuzugreifen. Mit welchen informationstechnischen Strukturen dies nun abgebildet wird, macht erst mal keinen Unterschied. Die Informationstechnologie hilft Ihnen, Ihre Kommunikation so effizient wie möglich zu gestalten, um die einzelnen Teilnehmer eines Netzwerks gezielt zu verbinden. Es geht letztendlich bei jeder Art von Netzwerk immer nur um den Informationsaustausch.
Sie werden in Ihrer Praxis sicher auch schon entsprechende IT-Strukturen einsetzen. Ihre Mitarbeiten kommunizieren hierüber untereinander oder mit den Patienten, der KV oder den Krankenkassen. Hinter diesen Systemen stecken aufwändige Strukturen. Diese möchten wir uns zunächst einmal etwas genauer anschauen.

Über die Autoren

Herr Dr. Siegbert Stracke ist Gründer und Geschäftsführer der Sanexio GmbH & Co.KG. Durch die langjährige klinische Erfahrung an einer Uniklinik sowie durch die anhaltende Tätigkeit als freiberuflicher Arzt und Berater kennt Herr Dr. Stracke die problembehaftete Versorgungswirklichkeit vieler medizinischer Einrichtungen.

Herr Frithjof Ebert ist technischer Leiter der Sanexio-GmbH und hat als Fachinformatiker für Systemintegration lange Zeit Netzwerke von Ärzten betreut. Zudem beschäftigt er sich gemeinsam mit Herrn Dr. Stracke mit der Etablierung von modernen vernetzten Onlinesystemen im Gesundheitswesen. Dabei nutzt er teils in anderen Bereichen etablierte Verfahren, um Lösungen auf die entsprechenden Probleme in der Medizin zu übertragen.

Was erwartet Sie hier?

In diesem Dokument werden wir einige Themen der IT aufarbeiten. Sie werden einen Überblick bekommen, was sich hinter den Begriffen wie Cloud, soziales Netzwerk oder Webseite überhaupt verbirgt.

Dieses Dokument gibt Ihnen einen Überblick über die technischen sowie einen kleinen Ausschnitt über die rechtlichen Aspekte, welche Anwendung bei Nutzung moderner Kommunikationssysteme finden. Dieses Dokument erhebt keinen Anspruch auf Vollständigkeit oder formal juristische Gültigkeit. Alle Informationen sind nach bestem Wissen zusammengetragen. Für Schäden, die aus der Anwendung der hier aufgeführten Informationen entstehen, können wir keine Haftung übernehmen.

Grundlegendes zu Technik und Recht

Das Client Server Prinzip

In den meisten Fällen haben Sie in Ihrer Praxis viele unterschiedliche Geräte miteinander vernetzt. Diese werden auch als Clients bezeichnet. Zudem werden Sie wahrscheinlich auch einen Server haben. Dieses Gerät spielt für Ihr Netz eine entscheidende Rolle. Der Server stellt Ihnen nämlich verschiedene wichtige Dienste zur Verfügung. Diese Dienste können sehr vielfältig sein. Beispiele hierfür sind Patienten-verwaltung, Speicherung von Röntgen-bildern,

automatisches Erstellen von Datensicherungen und vieles mehr. In dem nebenstehenden Bild sehen Sie eine Darstellung eines Netzwerkes. Der Internetzugang wird über Ihren Router realisiert. Eine Firewall schützt Sie gegen Angriffe von außen. Hinter dieser Firewall sind dann die einzelnen Clients und der Server angeordnet.

Die Einstellungen, die Sie an der Firewall sowie an dem Server oder den Clients vornehmen, haben weitreichende Folgen für Ihre Datensicherheit. Hier treffen rechtliche und technisch/praktische Aspekte aufeinander.

Alle Daten und Informationen, die Sie generieren, werden normalerweise nicht auf den einzelnen Computern abgespeichert, sondern auf dem Server. Hierbei gibt der Server einen bestimmten Ordner frei, auf welchen der Benutzer Daten ablegen kann. Dies hat den Vorteil, dass alle Anwender auf diese Daten prinzipiell zugreifen können. Die Zugriffsrechte werden hierbei von dem Systemadministrator vergeben. Mit Zugriffsrechten auf Dateiebene ist gemeint, wer in welchem Ordner lesen und schreiben kann.

Ein Beispiel für geteilte Dateien und Zugriffsrechte:

Auf Ihrem Server liegen beispielsweise folgende Verzeichnisse:

- Arztbriefe,
  - in diesem Ordner hinterlegen Sie fertig erstellte Arztbriefe zur weiteren Bearbeitung durch Ihr Praxispersonal.
- Geschäftsführung
  - in diesem Ordner speichern Sie alles, was mit der Organisation Ihrer Praxis zu tun hat. Mitarbeitervereinbarungen, Bewerbungen und andere Dokumente, die nur für Ihre Augen bestimmt sind
- Gescannte Laborwerte

- in diesem Ordner werden von Ihrem Personal Laborwerte gespeichert, die Sie durchsehen sollen.

- Buchhaltung
  - in diesem Ordner speichern Sie alles, was mit Ihrer Buchhaltung zu tun hat.

Sie haben nun die Benutzer:

- Arzt
  - Dr. Netz
- Helferinnen
  - Susi Müller
  - Claudia Machtfix
- Büro
  - Tina Tippschnell

Generell haben wir mehrere Stufen der Berechtigung, die wir vergeben können. So können Sie zum Beispiel nur Leserechte vergeben, wenn ein Benutzer Dateien nur lesen aber nicht ändern oder abspeichern darf. Sie können nur Schreibrechte vergeben, wenn ein Benutzer in diesem Ordner nur schreiben soll. Dies kann beispielsweise dann der Fall sein, wenn er zwar erstellte Dateien abspeichern soll, die restlichen auf dem Ordner liegenden Dateien aber nicht einsehen darf.

SANEXIO Verwaltungs GmbH | Meisebacherstraße 25 | 36251 Bad Hersfeld | info@sanexio.de | www.sanexio.de |Tel.: +49 6621 51098 50 | Fax: +49 6621 51098

In unserem Beispiel würden jetzt die Dateirechte so aussehen:

Benutzer\Ordner	Arztbriefe	Geschäftsführung	Gescannte Laborwerte	Buchhaltung
Dr. Netz	lesen/schreiben	lesen/schreiben	lesen/schreiben	lesen/schreiben
Susi Müller	lesen		lesen/schreiben	
Claudia Machtfix	lesen		lesen/schreiben	
Tina Tippschnell				lesen/schreiben

Wie Sie aus der oben stehenden Tabelle sehen können, haben nun die Benutzer Ihrer Praxis verschiedene Rechte auf verschiedene Ordner. So können Ihr Personal zum Beispiel die Arztbriefe lesen, also auch ausdrucken, aber nicht verändern. Für diesen Ordner dürfen das nur Sie.

Sie können die verschiedenen Teilnehmer in so genannte Benutzergruppen einteilen:

- Ärzte
- Med. Personal
- Abrechnungskräfte

Ein Benutzer kann immer mehreren Benutzergruppen angehören. Benutzergruppen ermöglichen es, für eine bestimmte Personengruppe immer dieselben Rechte einzustellen. Sie müssen daher nicht für jeden einzelnen Benutzer Rechte vergeben sondern tun dies einmalig für eine Gruppe.

Das Beispiel würde nun so aussehen:

Benutzer\Ordner	Arztbriefe	Geschäftsführung	Gescannte Laborwerte	Buchhaltung
Ärzte	lesen/schreiben	lesen/schreiben	lesen/schreiben	lesen/schreiben
Med. Personal	lesen		lesen/schreiben	
Buchhaltung				lesen/schreiben

Der Vorteil wird dann deutlich, wenn man sich überlegt, dass im weiteren Verlauf immer wieder neue Benutzer hinzukommen oder alte Benutzer wegfallen können.

Außerdem können Sie über eine solche Informationsstruktur alle Geräte im Netz wie zum Beispiel Scanner, Drucker, Telefone, etc. miteinander teilen.
Ob nun der Server in Ihren Praxisräumen steht oder in einem Rechenzentrum, unterscheidet letztendlich die klassische Praxis-IT von „Cloud"-gestützten Systemen.

Datenübertragung

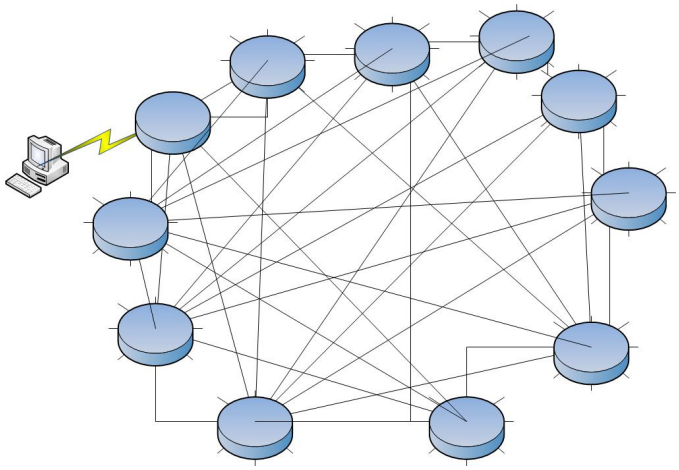


Abbildung 1 Beispielhafte Darstellung des WAN Netzes

Natürlich ist es auch interessant zu erfahren, wie die Daten geschützt sind. Wenn Sie lokale Daten, also innerhalb ihres Netzwerks Daten übertragen, sind diese in der Regel nicht verschlüsselt. Da das eigene Netzwerk zumeist ein vertrauens-würdiger Ort ist. Zudem kostet

Verschlüsselung Rechenaufwand, was die Geschwindigkeit des Netzwerks behindern würde. Durch sogenannte Serverrichtlinien können Sie aber auch die Kommunikation innerhalb ihres Netzwerks verschlüsseln. (Abhängig vom verwendeten Betriebssystem, der Clients und der Server.)

Sie übertragen aber nicht nur Daten innerhalb ihres Netzwerkes. Wie sieht nun eine Kommunikation über das Internet aus? Das Internet ist in erster Linie ein wahllos zusammengewürfelter Haufen aus Verbindungen (siehe Abbildung oben). Jeder blaue Kreis steht für ein eigenes Netzwerk und ist über verschiedene Verbindungen mit anderen Netzwerken verbunden. Welchen Weg ihre Daten nehmen, ist hierbei nicht unbedingt der kürzeste Weg sondern der effizienteste. Ihr Computer legt dabei lediglich das Ziel eines Datenpaketes fest. Den Weg, den es nimmt, bestimmen die so genannten Router. Router möchten ein Paket immer auf einen möglichst effizienten Weg transportieren. Hierbei berechnet der Router den Verkehr auf den einzelnen Verbindungsstellen und errechnet dann für sich den günstigsten Weg. Dies kann dazu führen, dass ein Datenpaket einmal um die Welt läuft, bevor es bei ihren Nachbarn ankommt.

Dieser Vorgang nennt sich Routing. Übertragen wir unsere Informationen im Klartext, kann es sein, dass diese Informationen für viele Netzwerkteilnehmer !!!theoretisch!!! einsehbar sind.

Fax

Ein sehr häufig genutztes Kommunikationsmittel ist das Faxgerät. Viele Anwender vergessen hierbei die enormen Risiken, die ein Faxgerät bietet. Nicht nur das Vertippen bei dem Empfänger kann dafür sorgen, dass vertrauliche Informationen an der falschen Adresse landen sondern auch die Übertragung an sich ist hoch fehleranfällig. Ein Fall, der für viel Aufsehen gesorgt hatte, war das

Fax des Anwalts von Michel Friedman-, welches er versehentlich an eine Pizzeria gefaxt hatte:
http://www.spiegel.de/panorama/ermittlungsakten-panne-friedman-verteidiger-schickte-fax-an-pizzabaecker-a-255449.html
Normalerweise ist die Faxübertragung nicht verschlüsselt. Das bedeutet, jeder der in der Lage ist, an die Telekommunikationsverbindung zu kommen, ist in der Lage, das Fax mit zu lesen.

E-Mail

Eine E-Mail wird grundlegend im Klartext übertragen. Das bedeutet, dass alle Stellen auf dem Vermittlungsweg die E-Mail auslesen können. Aus der oben stehenden Abbildung können Sie ersehen, dass eine Verbindung niemals direkt funktioniert. Verbindungen im Internet sind nur virtuell.
Wir reden hier bei von verbindungsloser Kommunikation. Ihnen kommt es war so vor, als ob sie direkt mit dem Server verbunden sind. Welchen Weg aber die einzelnen Daten dabei nehmen, liegt dabei bei der Netzwerkübertragung.
Die Standard E-Mail - Kommunikation ist also nicht abhörsicher.

Möchten Sie nun dafür sorgen, dass die Kommunikation - also der Nachrichteninhalt zwischen Sender und Empfänger - geheim bleibt, müssen Sie die E-Mail verschlüsseln. Das bedeutet, dass der Textanteil Ihrer E-Mail durch verschiedene Verfahren so verschleiert wird, dass eine mithörende Station nichts mit diesen Daten anfangen kann.

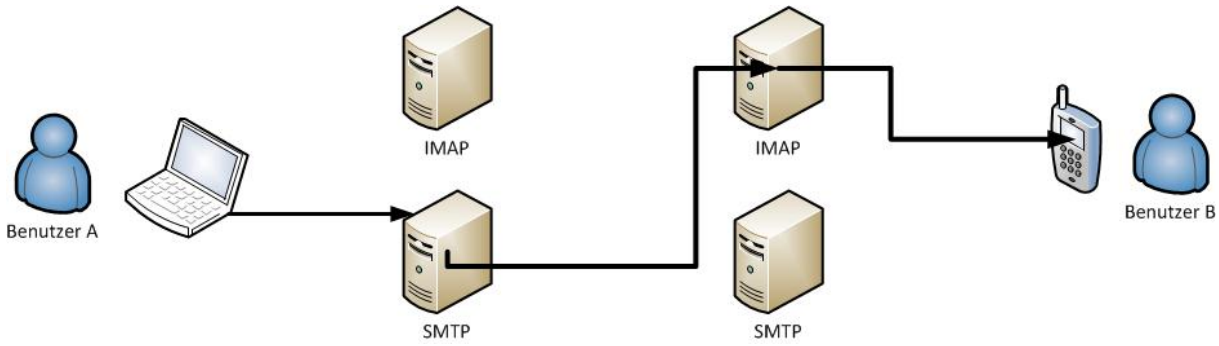


Abbildung 2 Prinzip der E-Mail Übertragung

Die Grafik zeigt, was eigentlich bei der Übertragung von E-Mails passiert. Sie haben Ihr E-Mail Konto bei einem Anbieter. Dieser Anbieter stellt Ihnen zwei Server zu Verfügung. Einen Server, der für das Versenden von E-Mails zuständig ist (SMTP) und einen, in dem Ihre E-Mails abgelegt werden (häufig: IMAP).

Wenn Sie E-Mails versenden, dann werden sie über das Internet an den E-Mail Provider übertragen. Dort kümmert der betreffende Server darum, die E-Mail an den empfangenden Server zu übertragen. Der empfangende Server legt sie daraufhin in die Postbox des Benutzers. Der Benutzer ruft seine E-Mail dann zum Beispiel mit einem Smartphone ab.

Rufen Sie nun Ihre E-Mails in einem Internetcafé ab oder einem anderen öffentlich zugänglichen WLAN Netzwerk, könnte jeder der ebenfalls in diesem Netzwerk ist, Ihre E-Mails mitlesen.

Um hier einen Grundschutz zu bieten, kann man die Verbindung zwischen E-Mail-Programm (Thunderbird, Outlook, Mail ect.) und dem eigenen E-Mail Server verschlüsseln (SSL). Ob dies möglich ist oder nicht, hängt von Ihrem E-Mail Anbieter ab. In der Regel kommunizieren die E-Mail-Server verschlüsselt miteinander.

Verschlüsselung des Nachrichteninhalts

Sender und Empfänger müssen bei Verschlüsselung des Nachrichteninhaltes dieselbe Verschlüsselungsmethode unterstützen!

Möchten Sie nun sicherstellen, dass die Verbindung zwischen ihnen und dem Empfänger nicht auslesbar ist, müssen Sie den Inhalt der Nachricht verschlüsseln. Hier gibt es einige Verfahren, die sich in den letzten Jahren etabliert haben.

Ein kostenloses und weit verbreitetes Verfahren ist das so genannte PGP (Pretty Good Privacy Verfahren:

http://de.wikipedia.org/wiki/Pretty_Good_Privacy

Hierbei wird eine so genannte asymmetrische Verschlüsselung eingesetzt. Das heißt, der Schlüssel, der zum Verschlüsseln einer Nachricht notwendig ist, unterscheidet sich von dem Schlüssel, der zum Decodieren notwendig ist. Man hat also ein Schlüsselpaar. Der Empfänger gibt Ihnen seinen öffentlichen Schlüssel, mit dem jeder E-Mails an ihn verschlüsseln kann. Der öffentliche Schlüssel ist auch nicht weiter bedenklich. Der geheime und wichtige Schlüssel zum Entschlüsseln bleibt bei dem Empfänger. Nur ihm ist es damit möglich, den Text zu entschlüsseln.

Eine gängige Methode, die sich in der Praxis bewährt hat, ist der so genannte Einsatz von E-Mail Zertifikaten. Ein Zertifikat ist eine Datei, die von einer Prüfungsstelle ausgestellt wird und hiermit bestätigt, dass sie auch die Person sind, für die Sie sich ausgeben. Der Empfänger muss ihr Zertifikat in seinem E-Mail-Programm hinterlegen, damit er diese Nachrichten von Ihnen lesen kann.

Webseiten

Die Problematik bei Webseiten ist nicht nur die Sicherheit der Server der Webseitenbetreiber sondern auch der Übertragungsweg. Hier gibt es drei problematische Stellen. Der Computer des Anwenders, der zumeist nicht gut gesichert ist, der Übertragungsweg an sich und der Zielserver. Ein Computer der durch Viren oder ähnliches befallen ist, stellt natürlich eine große Sicherheitslücke dar. Da ein Virus, das Daten ausspähen will, nicht auffallen möchte, wird der Benutzer erst sehr spät oder gar nicht merken, wenn sein Rechner davon befallen ist. Der Übertragungsweg im Internet ist in der Regel nicht verschlüsselt. Alle Daten, die man aus dem Internet empfängt und in das Internet überträgt, sind unverschlüsselt. Wenn nun sensible Informationen wie zum Beispiel persönliche Daten an einen Server übermittelt werden, ist eine der grundlegenden Maßnahmen, die Verbindung zu verschlüsseln. Hier hat sich das Verfahren HTTPS etabliert. Dieses Verbindungsprotokoll ermöglicht die verschlüsselte Übertragung. Hierzu werden Zertifikate eingesetzt. welche die verschlüsselte Übertragung ermöglichen.

Der Nachteil hierbei ist, dass die Rechenleistungen auf beiden Seiten größer werden, die ein Computer zur Ver- und Entschlüsselung aufbringen muss. Beim Onlinebanking ist Ihnen dieses Verbindungsprotokoll bestimmt schon anhand des grünen Balken begegnet. Diese Anzeige wird dadurch hervorgerufen, dass die Verbindung besonders gesichert ist. Gerade bei Webseiten, die mit sensiblen Daten umgehen, ist es zwingend notwendig, darauf zu achten, dass der Betreiber ein sicheres und gültiges Zertifikat einsetzt, um die Verbindung zu verschlüsseln. Bei einem gut konfigurierten Server ist das Eindringen in die Datenbank nicht einfach und gewährleistet daher schon einen guten Schutz.

VPN

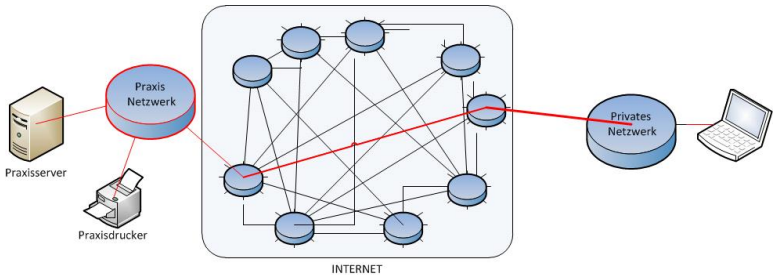


Abbildung 3 Beispiel eines VPNs

Das virtuelle private Netzwerke, kurz VPN genannt, bietet die Möglichkeit, zwei lokale Netzwerke miteinander zu verbinden. Nehmen wir an, Sie haben eine moderne Praxis IT und möchten am Wochenende von zu Hause darauf zugreifen. VPN bietet Ihnen die Möglichkeit, sich einen sicheren Tunnel durch das Internet zu erstellen und ihren Computer zu Hause mit denen in Ihrer Praxis virtuell zu verbinden. Die Daten werden durch das VPN verschlüsselt übertragen. Es gibt generell zwei Typen von VPN-Netzwerken. Einerseits gibt es VPN-Netzwerke, die zwei Standorte miteinander verbinden, andererseits gibt es VPN-Netzwerke, die innerhalb eines zweiten Netzwerks einen einzelnen Computer verbinden.

Ein klassischer Anwendungsfall für die Verbindung eines Computers innerhalb des heimischen Netzwerks oder innerhalb eines Hotels zu einem Praxisnetzwerk ist der, dass ein Arzt von zu Hause mit seinem Computer auf das gesicherte Praxisnetzwerk zugreifen möchte. Dabei ist entscheidend, an welcher Stelle der Tunnel aufgebaut wird. Bei der ersten Methode wird der Tunnel am Eingang also für das gesamte zweite Netzwerk aufgebaut und gilt damit für alle Computer innerhalb des Netzwerks. Bei der zweiten Methode wird der Tunnel direkt an

dem sich einwählenden Computer aufgebaut und gewährleistet damit auch innerhalb des zweiten Netzwerks eine Abwehrsicherheit.

Datenschutz

Datenschutzbeauftragter

Für die Einhaltung der Datenschutzbestimmungen ist generell die Unternehmensleitung verantwortlich. Da aber der Datenschutz ein sehr technisches Thema ist, ist ein Unternehmen ab einer bestimmten Größe verpflichtet, eine Person zu benennen, die der Unternehmensleitung dabei hilft, die Datenschutzbestimmungen umzusetzen.

> „[…] in nicht-öffentlichen Stellen (beispielsweise Unternehmen, Vereine), wenn mehr als 9 Personen (§ 4f Abs. 1 Satz 1 und 4 BDSG) mit der Verarbeitung dieser Daten beschäftigt sind oder Zugriff auf diese Daten haben. Diese Grenze entfällt, wenn ein bestimmtes Risiko vermutet wird, welches eine sofortige Bestellung erforderlich macht oder Verfahren eingesetzt werden, die der Vorabkontrolle unterliegen (§ 4d Abs. 5, § 3 Abs. 9, § 4e, § 4f Abs. 1 Satz 6 BDSG), oder wenn sie personenbezogene Daten geschäftsmäßig verarbeitet, um diese an dritte Personen weiterzugeben (z. B. Adressdatenhandel). Weiter entfällt diese Grenze auch, wenn eine volle Automatisierung der Erfassung beispielsweise für Statistik (z. B. Markt- und Meinungsforschung) oder Forschungszwecke eingesetzt wird. […]“
>
> Quelle http://de.wikipedia.org/wiki/Datenschutzbeauftragter Stand: 20.11.13

Ein Datenschutzbeauftragter hat die Aufgabe, die Unternehmensleitung bei der Einhaltung der Datenschutzbestimmungen zu unterstützen. Er ist ein Kontroll- und Überwachungsorgan. In der Regel benötigt ein Datenschutzbeauftragter hohe technische Sachkenntnis, um die Vorgänge zu verstehen und umsetzen zu

können. Er ist nicht weisungsbefugt, kann aber auch nicht durch Weisungen an der Ausübung seiner Tätigkeit gehindert werden. Er stellt für die Unternehmensleitung wie auch für die Mitarbeiter den Ansprechpartner dar, der in allen Fragen des Datenschutzes konsultiert werden muss. Zudem schult er die Mitarbeiter auf die Einhaltung des Datenschutzes.

Ein Unternehmen kann eine interne Kraft aber auch eine externe Kraft als Datenschutzbeauftragten stellen.

Technischer Datenschutz

In der Regel werden Ihre Patientendaten auf einem Server gespeichert. Die von Ihnen verwendete Praxis-Software regelt nun, in welcher Form die Daten gespeichert werden.

Bei der Speicherung der Daten gibt es zwei grundlegende Verfahren:

Die Speicherung der Daten im Klartext oder die verschlüsselte Speicherung. Je nachdem welche Praxissoftware Sie einsetzen, können die Daten durch die Software selbst verschlüsselt werden.

Aber auch der Server kann seine Festplatten und damit auch die Daten, verschlüsseln. Durch die Verschlüsselung auf Seiten des Servers ist sichergestellt, dass jemand der Zugang zu den Festplatten hat, diese nicht auslesen kann.

Sind Ihre Daten nun im Klartext durch die verwendete Software gespeichert und gleichzeitig die Festplatten des Servers nicht verschlüsselt, erhält man relativ leicht Zugang zu diesen Daten.

Der offensichtliche Nachteil bei Verschlüsselung ist natürlich der, dass für den Fall, dass der Schlüssel verloren geht, kein Zugang zu den Daten mehr besteht.

Wann sollte nun eine Verschlüsselung der Daten erfolgen?

1. Speicherung der Daten

a. Verschlüsselung durch den Server
b. Verschlüsselung durch die Software

2. Übertragung der Daten zwischen Server und PC

Dem Anwender fällt in der Regel nicht auf, ob und wie die Daten geschützt sind. Er kann nicht sehen, ob die Daten verschlüsselt oder im Klartext gespeichert werden. Der einzige, der dem Anwender erklären kann, wo und wie verschlüsselt wird, ist der System Administrator.

Der Vorteil einer Verschlüsselung ist, dass jemand der unbefugt Zugang zu den Daten erhält, diese Daten nur sehr erschwert auslesen kann. Es gibt keine Verschlüsselung, die nicht theoretisch entschlüsselt bar wäre. Je komplexer eine Verschlüsselung ist, desto höher wird der Aufwand sein, den richtigen Schlüssel herauszufinden. Praktisch kann dies bedeuten, dass bei komplexen Verschlüsselungsverfahren Großrechner viele Jahre rechnen müssten, um einen Schlüssel zu decodieren. Je höher ein Verschlüsselungsalgorithmus ist, desto sicherer sind die Daten vor dem Zugriff Unbefugter geschützt.

Der große Nachteil von Verschlüsselung ist, dass im Schadensfall der Schlüssel verloren gehen kann. Dies kann dazu führen, dass die Daten nicht mehr auslesbar sind. Zudem muss man sicherstellen, dass die Datensicherungen auch mit verschlüsselten Daten funktionieren. Zudem kann es passieren, dass Daten nicht wieder herstellbar sind.

Ein weiterer Aspekt ist die benötigte Rechenleistung. Verschlüsselung beruht auf komplexen mathematischen Verfahren. Auch mit den heutigen hohen

Rechenleistungen stellt eine Verschlüsselung für einen Computer oder auch einen Server immer einen hohen Aufwand dar.

In der Praxis hat der Netzwerkbetreiber (der Administrator) ein Sicherheitskonzept erstellt. Nach diesem Konzept werden die relevanten Bereiche abgesichert. Dies stellt dann auch die technische Seite des Datenschutzes dar.

Dies erfordert ein hohes Vertrauen in den Administrator. Da häufig ein Praxisnetzwerk in die IT ausgelagert wird, sollte man hier verstärkt auf Spezialisten achten. Gerade für Praxisnetzwerke empfiehlt es sich, ein renommiertes Systemhaus für Netzwerktechnik zu engagieren.

Organisatorischer Datenschutz

Eine sehr anschauliches Szenario, warum organisatorischer Datenschutz wichtig ist, finden sie unter:

https://www.datenschutzzentrum.de/material/themen/gesund/patient.htm

Zudem finden Sie dort weitere Informationen zu den rechtlichen Aspekten.

Datenschutz im Internet

Betreiben Sie eine Internetseite, sind Sie verpflichtet, Informationen nach dem deutschen Recht weiterzugeben. Sie müssen das Impressum auf jeder Seite klar erkennen können. Es darf nicht versteckt werden und hat fast immer denselben Aufbau. Dies resultiert daraus, dass die Impressumspflicht im Telemediengesetz sowie in anderen Gesetzen geregelt ist. Ausländische Seiten haben zumeist kein

Impressum. Viele Anbieter sind auch ganz froh darum, kein Impressum angeben zu müssen.

Sie sind in der Regel dazu verpflichtet, nach den Bestimmungen der Bundesrepublik Deutschland ihre Webdienste zu betreiben. Insbesondere der Umgang mit personenbezogenen Daten spielt hier eine große Rolle. Auf welche Art Sie diese Daten speichern und verwenden und wann Sie diese Daten löschen müssen, ist genauso klar geregelt wie die sicherheitsrelevanten Aspekte.

SANEXIO Verwaltungs GmbH | Meisebacherstraße 25 | 36251 Bad Hersfeld | info@sanexio.de | www.sanexio.de |Tel.: +49 6621 51098 50 | Fax: +49 6621 51098

Grundlegende Datenschutz-Rechte

Nachfolgend werden die wichtigsten Punkte kurz umrissen. Zur Vereinfachung werden einige Aspekte weggelassen. Hierbei soll Ihnen nur ein grober Überblick über die verschiedenen Rechte und Pflichten gegeben werden. Eine ausführliche Beschreibung würde den Rahmen dieses Papiers sprengen. Ich bitte daher um Ihr Verständnis, dass einige Teile stark vereinfacht ausgedrückt werden. Für die Experten unter ihnen habe ich weitere Quellen eingefügt sowie einige interessante Artikel verlinkt.

Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist ein „Bundesrecht“. Es gewährt jedem einzelnen das Recht, selbst zu entscheiden, welche Informationen er preisgibt und was mit seinen persönlichen Daten gemacht werden darf.

In vielen Verträgen finden Sie Klauseln, dass sie mit der Verarbeitung der Daten einverstanden sind. Dies sind Auswirkungen des Rechts auf informationelle Selbstbestimmung.

Merke: Sie sind verpflichtet, Daten zweckgebunden zu erheben und die Daten nur dann zu erheben, wenn Sie diese auch benötigen. Sie benötigen nicht nur eine klare Ermächtigungsgrundlage, in der Sie genau mitteilen, warum und wieso Sie diese Daten erheben sondern müssen dem Bürger auf Verlangen auch Auskunft darüber erteilen, welche Daten sie von ihm gespeichert haben..

Vergleiche Dazu: http://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung

Recht auf Selbstauskunft

Abgeleitet aus dem Grundrecht auf informationelle Selbstbestimmung hat jeder Bürger das Recht, Auskunft darüber zu erlangen, was über ihn gespeichert wird.

Quelle: http://de.wikipedia.org/wiki/Recht_auf_Selbstauskunft Stand 20.11.13

Das Recht ist in § 19 (betreffend Datenverarbeitung öffentlicher Stellen) und § 34 (betreffend Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen) Bundesdatenschutzgesetz (BDSG) festgelegt:

§ 19 BDSG – Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

[...]

§ 34 BDSG – Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

[...]

Vertraulichkeit und Integrität informationstechnischer Systeme

Das umgangssprachlich als „IT-Grundrecht“ bezeichnete Recht dient vornehmlich dem Schutz persönlicher Daten. Nach dem Urteil des Bundesverfassungsgerichtes vom 27. Februar 2008 wurde es neu formuliert. Das allgemeine Persönlichkeitsrecht umfasst nach Maßgabe des Bundesverfassungsgerichtes

auch die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Nähere Informationen hierzu finden Sie unter: http://de.wikipedia.org/wiki/Grundrecht_auf_Gew%C3%A4hrleistung_der_Vertraulichkeit_und_Integrit%C3%A4t_informationstechnischer_Systeme

Für die ärztliche Praxis sind die berufsständischen Einschränkungen und Bestimmungen zur Aufklärungs- und Informationspflicht für Sie natürlich maßgebend. Nicht nur eine Behandlung bedarf der ausdrücklichen Einwilligung des Patienten, auch die Datenerhebung bedarf einer Zustimmung ihres Patienten. Selbstverständlich besteht eine Schweigepflicht über alles, was mit diesen Daten zu tun hat.

Auf der Webseite des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein steht:

> „Grundsätzlich gilt bei der Erhebung der Daten genauso wie bei der Nutzung und der weiteren Verarbeitung, dass der Einzelne davor zu schützen ist, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt ist (vgl. Wortlaut des § 1 Abs. 1 Bundesdatenschutzgesetz - BDSG). Der Verstoß hiergegen in unserer Gemeinschaftspraxis liegt auf der Hand: Die Bildschirme sind so zu stellen, dass sie nur vom befugten Personal einzusehen sind. Personenbezogene Daten sind vor unbefugten Zuhörern geschützt zu erheben. Gegebenenfalls ist demjenigen, der die Daten zur Verfügung stellen muss, ein Blatt Papier zu reichen, auf dem die Daten unbeobachtet notiert werden können. Und selbstverständlich ist ein gehöriges Maß an Diskretion am Telefon zu wahren, wenn schon Telefongespräche von Umstehenden mitgehört werden können.“ Quelle: https://www.datenschutzzentrum.de/material/themen/gesund/patient.htm
>
> Stand: 18.11.13

Datenschutz in der ärztlichen Praxis

Der nachfolgende Abschnitt bezieht sich auf „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer in der Veröffentlichung vom 09.Mai 2008. http://www.bundesaerztekammer.de/page.asp?his=0.7.47.6188

Zitat: „[...]

> Unabhängig vom gewählten Medium der Datenverarbeitung und
>
> Nutzung muss der Arzt beim Umgang mit Patientendaten folgende Grundsätze beachten:
>
> – das Persönlichkeitsrecht des Patienten in der Ausprägung des
>
> informationellen Selbstbestimmungsrechts
>
> – die Wahrung des Patientengeheimnisses
>
> – die Dokumentation der Behandlungsabläufe und -ergebnisse
>
> – das Recht des Patienten, in der Regel Einsicht in die objektiven Teile der ärztlichen Aufzeichnungen zu nehmen
>
> – subjektive Einschätzungen können, müssen aber nicht offenbart werden[...]“
>
> Quelle:
> http://www.bundesaerztekammer.de/downloads/Empfehlung_Schweigepflicht_Datenschutz.pdf
>
> Stand: 20.11.13

SANEXIO Verwaltungs GmbH | Meisebacherstraße 25 | 36251 Bad Hersfeld | info@sanexio.de | www.sanexio.de |Tel.: +49 6621 51098 50 | Fax: +49 6621 51098

Die ärztliche Schweigepflicht ist Ihnen bestens vertraut, gemäß § 203 Abs. 1 Strafgesetzbuch, und §9 MBO .

> Auszug aus dem § 203 StGB:
>
> „[...] (1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als
>
> 1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
>
> [...]
>
> anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. [...]“
>
> Quelle: http://dejure.org/gesetze/StGB/203.html Stand: 20.11.13

Die ärztliche Schweigepflicht bezieht sich natürlich auch auf die Art, wie sie kommuniziert wird. Da die Technik - insbesondere die Kommunikationstechnik - hier einen maßgebenden Einfluss hat, müssen Sie als Arzt heutzutage natürlich auch diese Kommunikationswege schützen.

Gesetzliche Vorschriften oder die Einwilligung des Patienten können Ausnahmen von der Schweigepflicht herbeiführen. Auf Grundlage des Bundesdaten-schutzgesetzes ergibt sich eine Zulässigkeit der Datenerhebung, der Verarbeitung und der Nutzung durch ihre ärztliche Tätigkeit. Weiterhin müssen Sie beachten, in welcher Form Sie die Daten bearbeiten oder übertragen dürfen.

Auch der oben bereits erwähnte Datenschutzbeauftragte wird für Sie spätestens dann Vorschrift, wenn mehr als neun Personen Zugang zu personenbezogenen Daten haben.

Aus dem Recht auf informationelle Selbstbestimmung wissen wir, dass ein Patient die Sperrung, die Berichtigung oder das Recht auf Datenauskunft hat.

Solange ein Behandlungsvertrag oder eine Aufbewahrungspflicht besteht, brauchen Daten nicht gelöscht zu werden. Diesen Rechten muss auch dadurch Rechnung getragen werden, dass durch organisatorische Maßnahmen kein Einblick in Patientendaten gegeben werden darf. So darf ein Patient zum Beispiel nicht an einen nicht gesperrten EDV Arbeitsplatz gelangen oder den Bildschirm einsehen können.

Nach Paragraph 10 Abs. 5 der Musterberufsordnung dürfen Sie elektronische Aufzeichnungen anfertigen. Hierbei müssen allerdings Schutzmaßnahmen bestehen, um die unrechtmäßige Verwendung auszuschließen. Dies ist Aufgabe der eingesetzten Praxissoftware. Zusätzlich spielt hier natürlich die Server- und Netzwerksicherheit eine zentrale Rolle. Die Daten müssen elektronisch signiert werden.

Auch bei der Übernahme externer Daten, muss sichergestellt werden, dass die Daten authentisch sind. Wird ein Arztbrief elektronisch signiert, kann angenommen werden, dass dieser Brief authentisch ist. Möchte man seine Praxis natürlich nun papierlos gestalten, muss sichergestellt werden, dass die Scans der Dokumente ebenfalls authentisch sind. Hier gibt es mehrere Möglichkeiten der revisionssicheren Datenerfassung.

Zusammenfassend:

Sie müssen die Bestimmungen des Bundesdatenschutzgesetzes genauso einhalten wie die Bestimmungen der entsprechenden ärztlichen Berufsordnung. Datenschutz erstreckt sich nicht nur auf die technische Seite sondern auch auf die organisatorische. Sie sind für den Schutz ihrer Daten verantwortlich. Sie müssen technisch dafür sorgen, dass niemand an die Daten kommt, der hierfür nicht autorisiert ist. Sie müssen spätestens dann einen Datenschutzbeauftragten für Ihre Organisation stellen, wenn mehr als neun Personen Zugang zu den Daten besitzen.

Web 2.0

„Soziale Netzwerke“

Soziale Netzwerke bilden Strukturen der wirklichen Welt ab. In den letzten Jahren haben soziale Netzwerke immer weiter an Bedeutung gewonnen. Gerade der Boom von Webseiten wie Facebook spiegelt hier wider, wie wichtig soziale Netzwerke für Menschen sind. Soziale Netzwerke ermöglichen aber auch den schnellen Zugang zu seinen Patienten.

Als Arzt muss man hier jedoch stark aufpassen. Sowohl Standesrecht, das Arzt-Werberecht oder der Datenschutz, um nur einige zu nennen, machen einem hier das Leben schwer.

Sie haben prinzipiell die Möglichkeit, ihre Praxis auf sozialen Netzwerken zu präsentieren.

Sie können soziale Netzwerke nutzen, um sich bekannt zu machen. Sie können auf einer freieren Ebene mit ihren Patienten oder potentiellen Kunden kommunizieren als sie dies durch klassische Medien wie den Praxisflyer machen können.

Sie müssen hierbei insbesondere auf Ihre Kommentare achten. Insbesondere anpreisende, irreführende oder vergleichende Werbung ist Ärzten untersagt. Aktuell sind dem Autor keine genauen rechtlichen Vorschriften für Ärzte bei sozialen Netzwerken bekannt.

Insbesondere möchte ich darauf hinweisen, dass sie als Arzt zum Datenschutz verpflichtet sind. Wenn Sie ein Netzwerk benutzen, müssen Sie also sicherstellen, dass der Datenschutz eingehalten wird. Dies können Sie bei Netzwerken wie zum Beispiel Facebook allerdings nicht. Anders ist dies bei spezialisierten Netzwerken, die von vornherein den Datenschutzaspekt entsprechend beachten.

Cloud - Was ist das?

Unter dem in letzter Zeit immer wieder kursierenden Begriff des Cloud-Computing versteht man das Auslagern von Diensten an zentrale Server. Ein Beispiel dafür ist die Online-Terminverwaltung. Hierbei gibt es eine zentrale Stelle, einen Server, der diese Dienstleistung anbietet. Die einzelnen Benutzer greifen dabei auf den Server zu und benutzen die dort hinterlegte Software. Diese Software ist häufig eine Art Weboberfläche. Der Internetdienstanbieter Google bietet zum Beispiel die Textverarbeitung online an. Der Benutzer loggt sich dabei mit einem beliebigen Computer auf der Webseite ein und kann dort seine Texte bearbeiten und speichern. Der Dienstanbieter sorgt dafür, dass die Daten von anderen Kundendaten getrennt bleiben.

Einige Firmen haben sich darauf spezialisiert, für Arztpraxen Cloud-Computing anzubieten. Dabei wird der Server der normalerweise in der Praxis steht, durch den Dienstanbieter in einem Rechenzentrum bereitgestellt. Über das Internet greift dann der Arzt auf diese Dienste zu. Das hat den Vorteil, dass ein Arzt

keinen eigenen Server unterhalten muss und sich damit die Kosten für die Hardware wie auch die Betriebskosten reduzieren. Hier ist allerdings der geographische Standort des Servers wichtig. Problematisch wird es, wenn die Server oder die Firma im Ausland angesiedelt sind.

Die Daten werden also nicht mehr in der Praxis gespeichert sondern in einem Rechenzentrum. Sie als Arzt müssen ihren Patienten gegenüber allerdings sicherstellen, dass alle rechtlichen Aspekte bei der Wahl des Anbieters und des Servers beachtet wurden. Aus diesem Grund sollten Sie vor Entscheidung für oder gegen ein Cloudsystem besondere Sorgfalt in die Wahl des richtigen Anbieters legen. Insbesondere Anbieter, die sich auf den ärztlichen Sektor spezialisiert haben, können Ihnen dabei helfen. Im Zweifelsfall sollten Sie auch einen Fachanwalt konsultieren und die rechtlichen Aspekte abklären zu lassen.

Was bringt mir die Cloud?

Generell bringt Ihnen die Cloud eine Einsparung an Hardwarekosten und Betriebskosten. Sie sind allerdings von einem Dienstanbieter abhängig, der die gesamte technische Infrastruktur bereitstellt. Zudem teilen sich häufig verschiedene Praxen einen physikalischen Server. Durch verschiedene technische Konzepte ist es möglich, die Daten dennoch voneinander virtuell zu trennen.

Onlineberatung

Das Internet bietet natürlich auch interessante Möglichkeiten zur Beratung. Im Internet gibt es zahlreiche Plattformen, auf denen sich Laien beispielsweise von Fachanwälten Rat einholen können. Diese Plattformen ermöglichen einen schnellen Informationsaustausch und der Gedanke liegt nahe, Online-Beratung

auch durch Ärzte anzubieten. Dieses Thema ist allerdings deutlich umstritten wie das Urteil des Oberlandesgerichts Köln vom 10. August 2012 zeigt.

Unter dem Aktenzeichen 6 U 235/11 findet sich der Fall einer Gynäkologin, die sich an einer Plattform beteiligt hat, auf welcher Patienten online beraten wurden. Dieses Urteil kann unter http://openjur.de/u/462481.html eingesehen werden.

Der Fachanwalt für Medizinrecht Philip Christmann schreibt zu diesem Urteil auf seiner Internetseite: http://www.christmann-law.de/neuigkeiten-mainmenu-66/336-urteil-zur-onlinewerbung-des-arztes-medizinische-beratung-im-internet-ist-nicht-erlaubt.html

> „[...]Die Onlinepräsenz einer Arztpraxis wird für die Patientenakquise immer wichtiger. Aber mit einer medizinischen Beratung per Internet darf ein Arzt nicht werben, wie das OLG Köln am 10.08.2012 entschied (Az.: 6 U 235/11).[...]"
>
> Stand: 18.11.13

Insbesondere ging das Gericht darauf ein, dass die Werbung unzulässig sei, da die Empfehlung des Arztes nicht durch die eigene Wahrnehmung entstanden war. Dies schließt jedoch nicht allgemeine Gesundheitstipps und Gesundheitsratschläge aus. Sondern bezieht sich auf die individuelle Behandlungsempfehlung.

Allgemeingültige medizinische Informationen und Aussagen über Themen, die sich nicht auf einen bestimmten Patienten und Fall beziehen, können durchaus von einem Arzt online geäußert werden.

> **In der Berufsordnung für die Ärzte Bayerns in der Bekanntmachung vom 9. Januar 2012** heißt es dazu:

> „[…] (4) Der Arzt darf individuelle ärztliche Behandlung, insbesondere auch Beratung, nicht ausschließlich über Print- und Kommunikationsmedien durchführen. Auch bei telemedizinischen Verfahren ist zu gewährleisten, dass ein Arzt den Patienten unmittelbar behandelt […]". Quelle: http://byds.juris.de/byds/035_4.5_BOArzt_BY_P7.html
>
> Stand 18.11.13

Demnach ist es also möglich, Teile der Beratung auch über moderne Kommunikationsmedien durchzuführen, sofern der Patient unmittelbar von diesem Arzt behandelt wird. Insbesondere bei sehr beratungsintensiven Erkrankungen und Patientengruppen bietet sich hier auch die Möglichkeit, mit seinen Patienten moderne Kommunikationswege zu benutzen. Wichtig ist dabei vor allem, dass der Kommunikationsweg geschützt ist. Dies kann durch verschlüsselte Verbindungen aber auch durch den Einsatz von verschlüsselten Nachrichten gewährleistet werden.

Die Webseite

Webseiten und das Arztwerberecht

Bei der Entwicklung einer eigenen Webseite gilt es das Arzt-Werberecht zu beachten. Die Landesärztekammer Hessen hat die Informationspflichten für Ärzte in folgendem Dokument zur Verfügung gestellt.
http://www.laekh.de/upload/Aerzte/Rund_ums_Recht/Publikationen_Merkblaetter/Merkblatt_Telemediengesetz.pdf
Als Inhaber einer Webseite sind sie Dienstanbieter im Sinne des §2 Telemediengesetz (TMG) und somit gelten für Sie die Informationspflichten

gemäß §5 TMG. Arztwerberecht, Standesrecht, TMG und Datenschutz sind weitere wichtige Punkte für eine rechtssichere Arztwebseite. Insbesondere die Impressumspflichten sind hierbei möglichst genau zu beachten. Ein falsches oder ein unvollständiges Impressum kann Abmahnungen nach sich ziehen. Gleiches gilt für eine falsche Darstellung von Inhalten auf ihrer Webseite.

Die Pflichtangaben nach dem Telemediengesetz

- das Impressum sollte von jeder Seite Ihrer Homepage aus gut erreichbar sein. Sie dürfen den Link nicht „verstecken".
- Kontaktaufnahme
    - Angaben für eine schnelle elektronische Kontaktaufnahme. (E-Mail)
    - Angaben für eine telefonische Kontaktaufnahme
    - Angaben für eine schriftliche Kontaktaufnahme
- Ihre Berufsbezeichnung sowie den Staat indem sie sie erworben haben. (Inklusive Bundesland)
- ihre kassenärztliche Vereinigung und ihre Ärztekammer
- Berufsordnungen sowie das hessische Heilberufsgesetz

ein Muster Impressum finden Sie unter dem oben genannten Link.

(Keine Vollständige Aufzählung!)

Werbung

Für Ärzte gilt das Arzt Werberecht. Die online Enzyklopädie Wikipedia definiert das Arbeitsrecht:

> „[...]Das **Arztwerberecht** in Deutschland ist die Gesamtheit der Bestimmungen, die die Möglichkeiten und Grenzen der Werbung von Ärzten und Zahnärzten regeln. Gesetzliche Grundlagen des Arztwerberechts sind die jeweiligen Berufsordnungen der Landes(zahn)ärztekammern in den einzelnen Bundesländern,

das Heilmittelwerbegesetz(HWG) und das Gesetz gegen den unlauteren Wettbewerb (UWG).[...]“ http://de.wikipedia.org/wiki/Arztwerberecht Stand: 18.11.13

Da sie mit ihrer Webseite immer den Patienten oder auch neue Patienten informieren möchten, sind die nachfolgenden Informationen für alle Webseiten gültig.

Sie können auf ihrer Webseite Informationen über den Praxisinhaber, die Praxis und das Team, die Fachgebiete und die Spezialisierungen aufführen.

Alle Informationen müssen sachlich sein. Sie dürfen nicht anpreisend oder irreführend sein. Außerdem sollten Sie vermeiden mit einem Alleinstellungsmerkmal zu werben.

Sie können auch Ihre Sprachkenntnisse sowie Ihr Praxisteam und ihre Praxis präsentieren.

Das Web 2.0 zeichnet sich durch die Interaktion mit seinen Benutzern aus. So könnten sie Foren, Gästebücher, Patientenbewertungen oder ähnliches auf ihrer Webseite publizieren. Richtig? Nein!

Sie bieten zwar anderen, nämlich den Benutzern ihrer Webseite an, Ihre Meinung dort zu hinterlassen, aber in Anbetracht der rechtlichen Rahmenbedingungen sollten Sie dies mit Vorsicht tun!

Hier könnten ihre Patienten nämlich oben beschriebene anpreisende oder irreführende Aussagen tätigen. Es ist rechtlich unklar, unter welchen Umständen Sie diese Inhalte zuvor hätten prüfen müssen. Aussagen Ihrer Patienten könnten als wettbewerbswidrige Aussagen aufgefasst werden.

Das Oberlandesgericht Koblenz hat in seinem Urteil (Urteil vom 13.02.1997 - Az.:6U1500/96) 1997 entschieden, dass ein Arzt kein Forum oder Gästebuch betreiben darf. Dieser Punkt ist allerdings umstritten. Es existiert keine gefestigte Rechtsprechung. (Zumindest ist dem Autor keine solche bekannt.)

In der Praxis rate ich deswegen lieber von einem Gästebuch oder einem eigenen Forum ab.

Domain

Insbesondere beim Domainnamen kann es Probleme geben. Ein Domainname kann werbenden Charakter besitzen. Domains wie „Bester-Kinderarzt.de“ oder „Kinderarzt-Musterstadt.de“ lassen den Verdacht einer Bewerbung von Alleinstellungsmerkmalen zu.

Außerdem müssen Sie bei Domainnamen die Rechte anderer bedenken, zum Beispiel Markenrechte.

Inhalte der Webseite

- Inhalte müssen sachlich sein und sich auf die Erbringung von ärztlichen Leistungen beziehen.
- Organisatorische Informationen sind OK.
- Keine anpreisende Werbung!
- Keine Bewerbung von Alleinstellungsmerkmalen
- Keine exzessiven Suchmaschinenoptimierungsmaßnahmen
- Die Webseite sollte dem aktuellen Stand der Technik entsprechen.

Virtuelle regionale Gesundheitsnetze

Load balancing

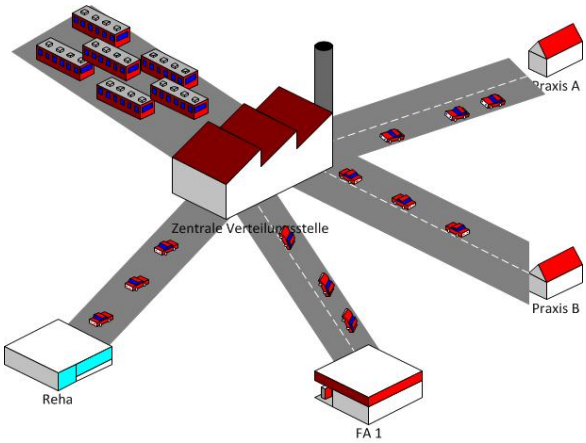
Ein Begriff aus der IT. Er beschreibt, dass die Datenlast (Load) auf mehrere Stellen verteilt werden kann. Hierfür gibt es eine Stelle, die die Anfragen zunächst annimmt und dann an andere Stellen verteilt. Sie sorgt für eine gleichmäßige Auslastung.

Das Prinzip lässt sich auf alle Modelle übertragen, in denen es um eine intelligente Steuerung von Informationen oder Ressourcen geht.

In der untenstehenden Grafik sehen Sie exemplarisch zwei Praxen. In der einen Praxis herrscht zu einem gegebenen Zeitpunkt ein recht hoher Andrang. In der zweiten Praxis sowie in der Facharzt-Praxis herrscht ein moderater Andrang. Die Aufgabe des Loadbalancing wäre es nun dafür zu sorgen, dass der Patientenstrom so delegiert wird, dass eine möglichst gleichmäßige Auslastung entsteht. In diesem Fall kann die IT helfen, die Delegation und die Kommunikation zu vereinfachen.

Im Folgenden kreiere ich ein Beispielszenario, das zeigen soll, wie es technisch möglich wäre, ein Netzwerk regional aufzubauen, um den Patientenandrang zu steuern und die Kommunikationswege standardisiert zu vereinfachen.

Beispiel für eine onlinegestützte Verwaltung



Beispiel Loadbalancing

Wenn es nun ein System gibt, in dem Ärzte ihre verfügbaren Zeiten, Vertretungen und Kapazitäten hinterlegen können, wäre es möglich, den Ansturm von Patienten auf die verfügbaren Plätze zu verteilen.

Terminreservierungen über ein zentrales System würden zudem die Möglichkeit bieten, den notwendigen Arbeitsaufwand, den beispielsweise das Assistenzpersonal durch Terminvergabe hat, zu minimieren. In diesem Beispiel melden die beteiligten Praxen ihre verfügbaren Kapazitäten der zentralen Verwaltungsstelle. Deren Aufgabe ist es nun, die Patienten nach Bedarf auf die verschiedenen Praxen zu verteilen. Dieses sternförmige System ist beliebig erweiterbar. Es könnte zum Beispiel so aussehen:

Alle Praxen melden ihre Kapazitäten an eine für die Region zentrale Plattform. Diese Plattform bietet gleichzeitig eine Schnittstelle für den Patienten, über die er sich einen Termin reservieren könnte.

Die Plattform entscheidet nun je nach Auslastung und Entfernung, welcher Termin für den Patienten der optimale wäre. Der Arbeitsaufwand für Organisation im gesamten Netz sinkt dadurch. Solch eine Plattform lässt sich natürlich auch mit Hilfe weiterer Funktionen ausbauen. Es könnten beispielsweise Erinnerungsfunktionen für Patienten implementiert werden, die sie daran erinnern können zur nächsten Kontrolle zu gehen. Eine Online-Rezeptvergabe ist ebenso möglich. Die einzelnen Leistungserbringer müssen somit nicht mehr selbstständig die Eingabe übernehmen, die Verarbeitung sowie die Ausgabe, da dieser Teil vollständig automatisiert abläuft. Das solch ein System für alle Beteiligten transparent bleiben muss, versteht sich von selbst. Nur wenn alle Mitglieder des Netzes einen Mehrwert durch dieses System erfahren, wird es sich durchsetzen können.

Eine weitere Erweiterung des Netzes kann beispielsweise über die Erfassung und Auswertung relevanter medizinischer Daten im Sinne eines Telemedizinnetzwerkes sein.

Realisiert werden könnte dies durch ein regionales Internetportal, auf das Ärzte und Patienten entsprechenden Zugriff haben. Durch eine benutzerfreundliche Realisierung wären Einarbeitungsaufwand sowie Betreuungsaufwand relativ gering.

SANEXIO Verwaltungs GmbH | Meisebacherstraße 25 | 36251 Bad Hersfeld | info@sanexio.de | www.sanexio.de |Tel.: +49 6621 51098 50 | Fax: +49 6621 51098