



Digitalisierung
im Schweizer
Gesundheitswesen



Big Data und Healthcare – wie die Digitalisierung das Schweizer Gesundheitswesen verändert

Die digitale Transformation schreitet in vielen Bereichen des öffentlichen und privaten Lebens sowie in der Wirtschaft kontinuierlich voran. So auch im Gesundheitswesen: Seit April 2017 regelt das Bundesgesetz über das elektronische Patientendossier (EPD) die Rahmenbedingungen für dessen Einführung und Verbreitung. Die Möglichkeiten der Digitalisierung nutzend, soll das EPD die Qualität der medizinischen Behandlung stärken, Behandlungsprozesse verbessern und das Gesundheitssystem insgesamt effizienter machen.

Dabei hat das EPD allerdings noch einige Hürden zu überwinden, denn gerade in Sachen Digitalisierung hat die Gesundheitsbranche noch viel aufzuholen. Eine Untersuchung des [Health Tech Clusters Switzerland](#) im Rahmen der Studie «digital.swiss» zeigt, dass die Digitalisierung des Gesundheitswesens in der Schweiz erst zu 39 Prozent vollzogen ist. Das gilt vor allem für die administrativen Bereiche in den Arztpraxen und Spitälern. Hier beherrschen immer noch Papier-basierte Vorgänge das Bild, steckt die Digitalisierung noch in den Kinderschuhen. Anders sieht es in den medizinischen und pflegerischen Disziplinen aus. Bei der Behandlung von Patienten, im Operationssaal oder in der Nachsorge sowie in der pflegerischen Arbeit gehört der Kollege Computer häufig zum festen Bestandteil vieler Teams. Das Cluster konstatiert: „Obwohl der Umsatz mit digitalen Lösungen im Gesundheitsbereich wächst, schlägt sich die Nutzung und der Einsatz von eHealth Lösungen noch nicht in der Breite nieder.“

Sicherheitsbedenken hemmen Digitalisierung

Für diese prekäre Situation im administrativen Umfeld des Gesundheitswesens sind gleich mehrere Faktoren verantwortlich. Der grösste Hemmschuh liegt wohl in der Sicherheit und der Furcht vor der zunehmenden Cyber-Kriminalität. Patientendaten enthalten sehr sensible Informationen, die nicht in unbefugte Hände geraten dürfen. Hier müssen Arztpraxen und Spitäler mit entsprechenden Sicherheitsmassnahmen dafür sorgen, dass die Daten ihrer Patienten bestmöglich gegen Attacken geschützt sind. Auch Gesetze rund um die Gesundheit sowie die strengen Bestimmungen zum Datenschutz sind derzeit noch ein Stolperstein auf dem Weg zur Digitalisierung, da sie strenge Auflagen und Sicherheitsmechanismen für den Umgang mit sensiblen Daten einfordern.

Es sind also die besonderen Ansprüche der Branche, die den Digitalisierungsprozess derart komplex werden lassen. Abgesehen von den zahlreichen gesetzlichen Anforderungen sorgt die Diversifizierung des Industriezweiges für weitere Herausforderungen. Viele Brüche im Behandlungsprozess und die Einbeziehung verschiedenster Akteure machen eine übergreifende Vernetzung bisher schwierig. Allerdings verursacht genau dieser Status quo hohe Kosten, die sich durch eine effizientere Ausgestaltung der Prozesse erheblich reduzieren liessen. Hinzu kommt, dass Branchen der Wettbewerbsdruck verglichen mit anderen recht gering ist – für die Unternehmen, Spitäler und andere Beteiligte besteht kein zwingender extrinsischer Anreiz, digitale Strategien umzusetzen.



Elektronisches Patientendossier kommt

Dabei liegt die Digitalisierung im Interesse aller Branchenakteure. Neben den Arztpraxen und Spitälern profitieren auch Apotheken, Versicherungen, Rehakliniken, Gesundheitsinteressenvertreter oder Gesundheitsplattformen. Und nicht zuletzt natürlich die Patienten. Denn die aus einem standardisierten, digitalisierten Gesundheitswesen resultierenden Innovationen unterstützen mittel- und langfristige die Verbesserung und Effizienzsteigerung in der Gesundheitsversorgung.

Allen Hindernissen zum Trotz sind digitalisierte Vorgänge im Schweizer Gesundheitswesen auf dem Vormarsch. So ist zu erwarten, dass in den kommenden Jahren das elektronische Patientendossier (EPD) flächendeckend umgesetzt wird. Spitäler müssen es bis spätestens 2020 einführen – genau der extrinsische Anreiz, der der Branche bisher fehlte. Dafür werden medizinische Daten dezentral gespeichert und sind unabhängig von Zeit und Ort durch autorisierte Personen abrufbar. Einheitliche Standards sollen dafür sorgen, dass Systeme zum Einsatz kommen, die kompatibel sind, sich problemlos vernetzen lassen und ohne Medienbrüche miteinander kommunizieren können.

Bevor es so weit ist, dass von einer flächendeckenden Digitalisierung die Rede sein kann, müssen die Ausgangsvoraussetzungen auf den Prüfstand gestellt werden. Denn selbst wenn mit dem EPD ein initialer Schritt getan ist – noch immer ist viel zu tun. Beim Aufbau einer nationalen, digitalen Gesundheitsstruktur sind zudem die spezifischen Schweizer Rahmenbedingungen in Betracht zu ziehen: So spielen Datenschutzbestimmungen eine zentrale Rolle für die Digitalisierung im Gesundheitsschutz. Die Verarbeitung von personenbezogenen Daten unterliegt den strengen gesetzlichen Bestimmungen des Schweizer Datenschutzgesetzes. Kontrolliert wird dessen Einhaltung im Bund durch den „Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten“. Für die Kontrolle der Einhaltung kantonaler Datenschutzgesetze sind die Kantone selbst zuständig. In der Schweiz besteht zusätzlich zur Auskunftspflicht auch eine Informationspflicht (Art. 14 und Art. 18a). Werden Personendaten von Bundesorganen bearbeitet oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile von privaten Personen bearbeitet, müssen die betroffenen Personen grundsätzlich aktiv durch den Inhaber der Datensammlung informiert werden. Alle Daten, die eine Profilbildung erlauben (Art. 3d), sind den besonders schützenswerten Daten gleichgestellt. In die Kategorie der persönlichen Daten fallen auch Patientendaten, die sehr sensible Informationen enthalten und daher besonders geschützt werden müssen.

Nicht zuletzt dürfen bei all den Bemühungen um digitale Strukturen jene Patienten nicht aus dem Raster fallen, die aus verschiedenlichen Gründen nicht online partizipieren können – gerade im Gesundheitswesen ein Faktor, der nicht ausser Acht gelassen werden darf.

Digitalisierung baut Brücken

Problematisch für den zügigen Aufbau digitaler Prozesse im Gesundheitswesen sind zudem die mangelnde Zusammenarbeit von Arztpraxen, Spitälern, Apotheken und Versicherungen sowie das veraltete Tarif-Abrechnungssystem. Hier soll die Digitalisierung in Zukunft eine Brücke zwischen den Gesundheitsinseln bauen. Für den Zugriff auf das EPD müssen sich Gesundheitsfachpersonen darum in Zukunft zu einer so genannten Stammgemeinschaft zusammenschliessen. Spitäler müssen innerhalb von drei Jahren beitreten, für Pflegeheime gilt eine Übergangsfrist von fünf Jahren. Wer nicht teilnimmt, darf nicht mehr auf der Spitalliste geführt werden. Für Apotheken, Ärzte mit eigener Praxis und Spitexorganisationen ist der Beitritt freiwillig. Dennoch wird sich der Aufbau einheitlicher Strukturen mittelfristig für alle Beteiligten rechnen, auch wenn zuerst Investitionen in E-Health-Lösungen getätigt werden müssen. Der Bund stellt den Kantonen für den Aufbau rund 30 Millionen Franken zu Verfügung, damit sie ein standardisiertes, übergreifendes System realisieren können. Der Aufbau einer einheitlichen IT-Infrastruktur für das Gesundheitswesen soll durch das [Swiss Personalized Health Network \(SPHN\)](#) gefördert werden. Diese nationale Initiative will die Entwicklung der personalisierten Medizin und personalisierten Gesundheit in der Schweiz vorantreiben. Mit der Umsetzung der Initiative hat der Bund die Schweizer Akademie der Medizinischen Wissenschaften (SAMW) beauftragt.

Mehr Effizienz und Transparenz für Patienten

Bei all den komplexen Anforderungen und Schweiz-spezifischen Herausforderungen ist eines gewiss: Wenn es gelingt, dringende Fragen in Bezug auf die Sicherheit der Daten in den Griff zu bekommen, ist das Potenzial immens. Durch die Digitalisierung entsteht ein elektronischer Informationskreislauf von Aufnahme, Übermittlung, Verarbeitung und Interpretation von Gesundheitsdaten. Arztbriefe, Labordaten, Röntgenbilder, Diagnose- und Medikationslisten stehen in digitalisierter Form zur Verfügung und können jederzeit abgerufen werden. Das schafft Transparenz und beschleunigt Abläufe. Gesundheitsdienstleister erhalten einen schnelleren Überblick über den Zustand des Patienten und können notwendige Behandlungsschritte schneller einleiten. Davon profitiert nicht zuletzt der Patient. Die engere Vernetzung und Abstimmung der verschiedenen Leistungserbringer vereinfacht die gesamtheitliche Betrachtung der Gesundheit eines Patienten.



Individuell abgestimmte Ansätze in der Prävention, bei der Diagnostik oder dem Einsatz von Hilfsmitteln werden durch die digitalen Prozesse erleichtert. Gesammelt und bereitgestellt werden sämtliche Gesundheitsdaten in dem geschützten elektronischen Patientendossier, auf das Gesundheitsdienstleister und Mediziner autorisierten Zugang erhalten, wenn es die Behandlung erfordert.

Patienten haben schon heute Zugriff auf eine Vielzahl an Informationsquellen, die sich mit gesundheitlichen Themen befassen. Die Zeiten, als Ärzte als „Halbgötter in Weiss“ galten, gehören der Vergangenheit an. Der moderne Patient ist informiert, fragt nach. Durch digitale Technologien kann der medizinische Laie verschiedene Quellen nutzen, um sich über seine Gesundheit sowie über Behandlungsmethoden zu informieren, falls sich Symptome zeigen. Ein noch vergleichsweise neues Instrument sind die populären Fitness-Armbänder, mit denen sich das gesundheitliche Befinden aktiv überwachen lässt. Die digitalen Armbänder registrieren permanent die Herzfrequenz, die Hauttemperatur und die Bewegungsaktivitäten. Weichen die Werte ab oder zeigen sich verdächtige Entwicklungen, schlagen sie sofort Alarm.

Besser informierte Patienten helfen auch dem medizinischen Personal bei seiner Arbeit. Die Beschreibungen der Beschwerden sind meist anschaulicher und vereinfachen die Diagnose. In Foren und Interessengruppen haben die Patienten zudem die Möglichkeit, sich auszutauschen, ihre Erfahrungen zu teilen und sich mit Tipps gegenseitig zu helfen.

Für die Patienten bringt das zusammengefasst einen wesentlichen Vorteil: Sie emanzipieren sich vom passiven Leistungsempfänger hin zu aktiven Akteuren, die selbstbestimmt und vollumfänglich informiert am eigenen Behandlungsmanagement partizipieren und darauf einwirken. Gerade wenn es um die eigene Gesundheit geht, entspricht genau diese Entwicklung den Wünschen und Vorstellungen vieler Patienten.

Digitale Revolution im Gesundheitswesen

Neben den Patienten profitieren auch alle anderen Beteiligten von digitalen Strukturen. So haben beispielsweise Big-Data-Technologien das Potenzial, tiefgreifende Veränderungen in den Behandlungsmethoden zu bewirken. Die bestehenden Datenmengen stellen eine wertvolle Basis dar, um aus ihnen neue wissenschaftliche Erkenntnisse zu ziehen oder in schwierigen und komplexen Gemengelagen zu schnellen Entscheidungen zu finden – die richtigen Analysetools vorausgesetzt. Im Gesundheitswesen verspricht man sich davon eine bessere Diagnostik sowie vielfältigere Ansätze für die Therapie, da Mediziner auf eine breitere und spezifischere Informationsgrundlage zurückgreifen können. Therapien können zielgerichteter und wirksamer sowie meist auch preiswerter eingesetzt werden. Big Data soll aber auch die Prozesse in Spitälern und Arztpraxen verbessern helfen. Daten stehen an zentraler Stelle zur Verfügung und können per Mausklick abgerufen werden. Mehrfach-Recherchen in unterschiedlichen Datenbanken oder Informationsquellen werden damit überflüssig. Laut einer [Umfrage von PWC unter Schweizer Spitaldirektoren](#) erwarten sich dementsprechend 33 Prozent der Führungskräfte einen grossen Nutzen für effektivere Behandlungen. Abgesehen davon schafft die Digitalisierung schlichtweg mehr Zeit für Menschen. Mit sinkenden Prozesskosten und einer verbesserten Ressourcenzuteilung, wenn es zum Beispiel um die Wahl des richtigen Arztes geht, können sich Angestellte im Gesundheitswesen auf das Wesentliche konzentrieren: Heilung und Vorsorge.

Nicht zuletzt schafft die Digitalisierung ein steigendes Attraktivitätspotenzial für neue Mitarbeitende; das erwarten auch 43 Prozent der von PWC befragten Direktoren. Mobile und flexible Arbeitsmöglichkeiten sind schliesslich nicht nur der Wunsch bei Wissensarbeitern, auch Pflegekräften, Apothekern und vielen anderen wird der Arbeitsalltag so erheblich erleichtert.

Europäische Datensicherheit für das Gesundheitswesen

Nach wie vor ist das Thema Sicherheit ein nicht wegzudiskutierender Faktor, wenn wir über die Digitalisierung sensibler Bereiche wie dem Gesundheitswesen sprechen. In diesem Zusammenhang lohnt sich zudem ein Blick über die Ländergrenzen hinweg. Ab 2018 tritt in der Europäischen Union die Datenschutzgrundverordnung in Kraft, eine einheitliche rechtliche Grundlage zum Datenschutz in den beteiligten Staaten. Personenbezogene Daten werden in der Verordnung präzise definiert. Sie sind durch das Regelwerk nachhaltig geschützt, unabhängig davon, wo sie hingesendet, verarbeitet oder gespeichert werden. Information darüber, welche Daten von Betroffenen verarbeitet werden, müssen bei Bedarf verfügbar gemacht, die Zustimmung der Betroffenen eingeholt werden. Auch die Verarbeitung von Daten durch Dritte (Auftragsdatenverarbeitung) muss transparent und vertraglich geregelt sein. Die Verordnung gilt unabhängig vom Standort einer Niederlassung.

Mit der Verordnung liegt erstmals ein einheitliches Regelwerk für die Datenschutzbestimmungen in allen EU-Mitgliedsländern vor. Die Schweiz verbindet mit der EU enge Kontakte und Verträge. Aus diesem Grund wird sich das Schweizer Datenschutzrecht an der Datenschutzgrundverordnung orientieren und mit dieser konform gehen.

Microsoft sieht die Datenschutzgrundverordnung als einen wichtigen Schritt für den Schutz der Privatsphäre Einzelner. Sie gewährt in der EU ansässigen Personen mehr Kontrolle über ihre personenbezogenen Daten, was besonders für Patientendaten von grosser Bedeutung ist. Die neue Datenschutzgrundverordnung geht auch auf aktuelle Technologien ein, die bei der Generierung und Verarbeitung persönlicher Daten zum Einsatz kommen. Bis Mai 2018 hat es sich Microsoft daher zur Aufgabe gemacht, all seine Produkte und Dienstleistungen mit der Verordnung in Einklang zu bringen. Damit unterstützt das Unternehmen seine Kunden und Partner bei der umfassenden Änderung der Datenerfassung sowie deren Verwaltung und stellt gleichzeitig intelligente Technologien, Innovationen und Tools für eine effiziente Zusammenarbeit zur Verfügung. Eine entscheidende Rolle bei diesen Anpassungen spielen unter anderem Cloud-Dienste, denn diese stellen beim Lokalisieren und Kategorisieren personenbezogener Daten sowie deren Verwaltung und Überwachung eine effiziente Unterstützung dar. Mit individuellen Lösungen, beispielsweise Hybrid-Angeboten, die On-Premise mit klassischen Cloud Services kombinieren, lassen sich sichere Umgebungen auch für sensible Daten schaffen. Darüber hinaus können sich Akteure im Gesundheitswesen bereits in fünf Schritten auf die kommenden Änderungen vorbereiten und den Grundstein für eine strategische Neuausrichtung der eigenen IT-Sicherheit legen:

1. **Ermitteln:** Wo lagern personenbezogene Daten?
2. **Kontrollieren:** Wie werden diese Daten aktuell verwaltet?
3. **Schützen:** Wie können Sie Datenschutzverletzungen und Risiken verhindern, erkennen und im Fall der Fälle darauf reagieren?
4. **Berichten:** Etablieren Sie ein Dokumentations- und Berichtswesen.
5. **Überprüfen:** Unterziehen Sie Ihre Strukturen und Strategien regelmässigen Audits und überprüfen Sie sie auf Ihre Aktualität hin.

Mobiles und flexibles Pflegemanagement

Der branchenübergreifende Wunsch nach optimierten Möglichkeiten für ein flexibles Arbeiten ist kein Geheimnis. Zu stark drängen Gewohnheiten aus der privaten Nutzung in den Arbeitsalltag. Für Arbeitgeber natürlich immer ein potenzielles Sicherheitsrisiko, gerade wenn eine fehlende Strategie den Wildwuchs genutzter Geräte oder Apps begünstigt. Damit die Branche dem begründeten Wunsch der Mitarbeitenden dennoch nachkommen kann, ist auch hier Grundlagenarbeit gefragt. Mit den richtigen Lösungen lassen sich Flexibilität und Anforderungen an Sicherheit und Compliance durchaus unter einen Hut bringen – natürlich immer vorausgesetzt, dass die Mitarbeitenden entsprechend für die potenziellen Gefahren sensibilisiert und regelmässig geschult werden.

Im Übrigen müssen sich Akteure der Gesundheitsbranche nicht allein auf ihr eigenes Urteilsvermögen in Sachen Sicherheit verlassen: Ihre IT können sie beruhigt in professionelle Hände legen. Die Schweizer IT-Landschaft bietet starke Partner, die die Anforderungen des Gesundheitswesens verstehen und wissen, wie Projekte geplant, implementiert und gepflegt werden müssen. Zahlreiche erfolgreich umgesetzte Projekte beweisen die Expertise und das hohe IT-Fachwissen von Schweizer Experten.

Identitäts- und Zugriffsverwaltung

Sie kann das Risiko eines unberechtigten Zugriffs auf sensible Daten verringern und vereinfacht Anmeldeprozeduren, die im Arbeitsalltag viel Zeit kosten können. Dabei ersetzt eine einzige Identität mehrere Anmeldeinformationen für den Zugriff auf lokale und Cloud-Ressourcen. Nicht jeder Mitarbeitende benötigt den Zugriff auf die kompletten Daten einer Arztpraxis oder eines Spitals. Deshalb ist es ratsam, den Zugriff eines Benutzers auf die Ressourcen zu beschränken, die er tatsächlich für seinen Aufgabenbereich benötigt. Ändern sich die Aufgaben eines Mitarbeitenden oder verlässt er das Unternehmen, müssen Zugriffsrechte sofort entzogen werden, um Manipulationen, Diebstahl oder Beschädigungen zu vermeiden. Ein mehrstufiges Authentifizierungsverfahren mit zusätzlichen Optionen wie PIN oder Schlüsselkarte schützt zusätzlich.

Verwaltung mobiler Geräte und Anwendungen

Der Trend zu BYOD und die Nutzung von Software as a Service (SaaS) erhöht das Risiko für die Daten. Gehen Geräte verloren oder werden gestohlen, sind die Daten Angriffen ausgesetzt. Darum müssen mobile Geräte und Anwendungen besonders geschützt werden. Zugriffsrichtlinien für mobile Geräte sowie deren Anwendungen sollten in den Spielregeln für die IT daher fest verankert werden. Eine Multi-Faktor-Authentifizierung schafft eine zusätzliche Schutzebene.

Schutz von Unternehmensdaten

BYOD erhöht leider das Risiko für das versehentliche Offenlegen von Daten durch Apps und Dienste wie E-Mail, soziale Medien und die Cloud. Abhilfe schafft der Unternehmensdatenschutz (Enterprise Data Protection, EDP). Er verwaltet und reglementiert in sensiblen Datenumgebungen die Tätigkeiten von Apps, damit keine unerwünschten Änderungen der Daten vorgenommen werden können.

Datenverluste verhindern

Der Verlust von Daten ist nicht nur ärgerlich, sondern kann auch teuer werden. Mit Funktionen zur Verhinderung von Datenverlust (Data Loss Protection – DLP) lassen sich Daten beim Speichern, Verschieben und Teilen schützen. So kann beispielsweise die Verteilung einer E-Mail auf eine bestimmte Organisation beschränkt werden. Eine digitale Rechteverwaltungsqualifizierung regelt, wer eine Nachricht öffnen darf. Auch Microsoft Office 365 bietet Optionen, um zu verhindern, dass nicht autorisierte Benutzer Dokumente öffnen können.

Sichere Zusammenarbeit

Bequemlichkeit geht beim Datenaustausch häufig vor Sicherheit. Mitarbeitenden ist häufig nicht bewusst, dass sie durch ihr Verhalten Unternehmensdaten gefährden oder sogar verlieren können.

Sichere Tools für den Austausch von Daten sind ein probates Mittel für mehr Schutz. Gleichzeitig muss sichergestellt werden, dass immer nur autorisierte Mitarbeitende Zugriff haben. Eine sichere Lösung zum Teilen von Dokumenten ist beispielsweise Microsoft SharePoint. Eine Netzwerkfreigabe mit eingeschränktem Zugriff oder eine Cloud-basierte Lösung sind eine weitere Schutzmassnahme. Eine digitale Rechteverwaltungssoftware oder eine sichere Lösung für den Versand sensiblen Materials per E-Mail sind weitere Optionen. Ein einfacher und sicherer Workflow für den Austausch von Daten vereinfacht die interne und externe Zusammenarbeit.

Schadcode abfangen

Kontinuierliche Sicherheitsschulungen stärken und vertiefen das Bewusstsein für Sicherheitsaspekte und die Gefahren der Cyber-Kriminalität. Regelmässige Erinnerungen an grundlegende Sicherheitsempfehlungen sowie die Teilnahme an Weiterbildungen informieren über häufige Angriffsmethoden durch Schadsoftware und neue Formen von Cyber-Angriffen. URLs in E-Mails sollten nur geöffnet werden, wenn sie relevant, korrekt und legitim sind. Apps sollten nur aus vertrauenswürdigen Quellen heruntergeladen werden, um digitale Schädlinge im Netz zu verhindern. Hier ist viel und kontinuierliche Aufklärungsarbeit notwendig, um das Bewusstsein der Mitarbeitenden zu schärfen und das Unternehmen zu schützen.



Soziale Arbeit in der Cloud – mit Microsoft Office 365 und Microsoft Azure

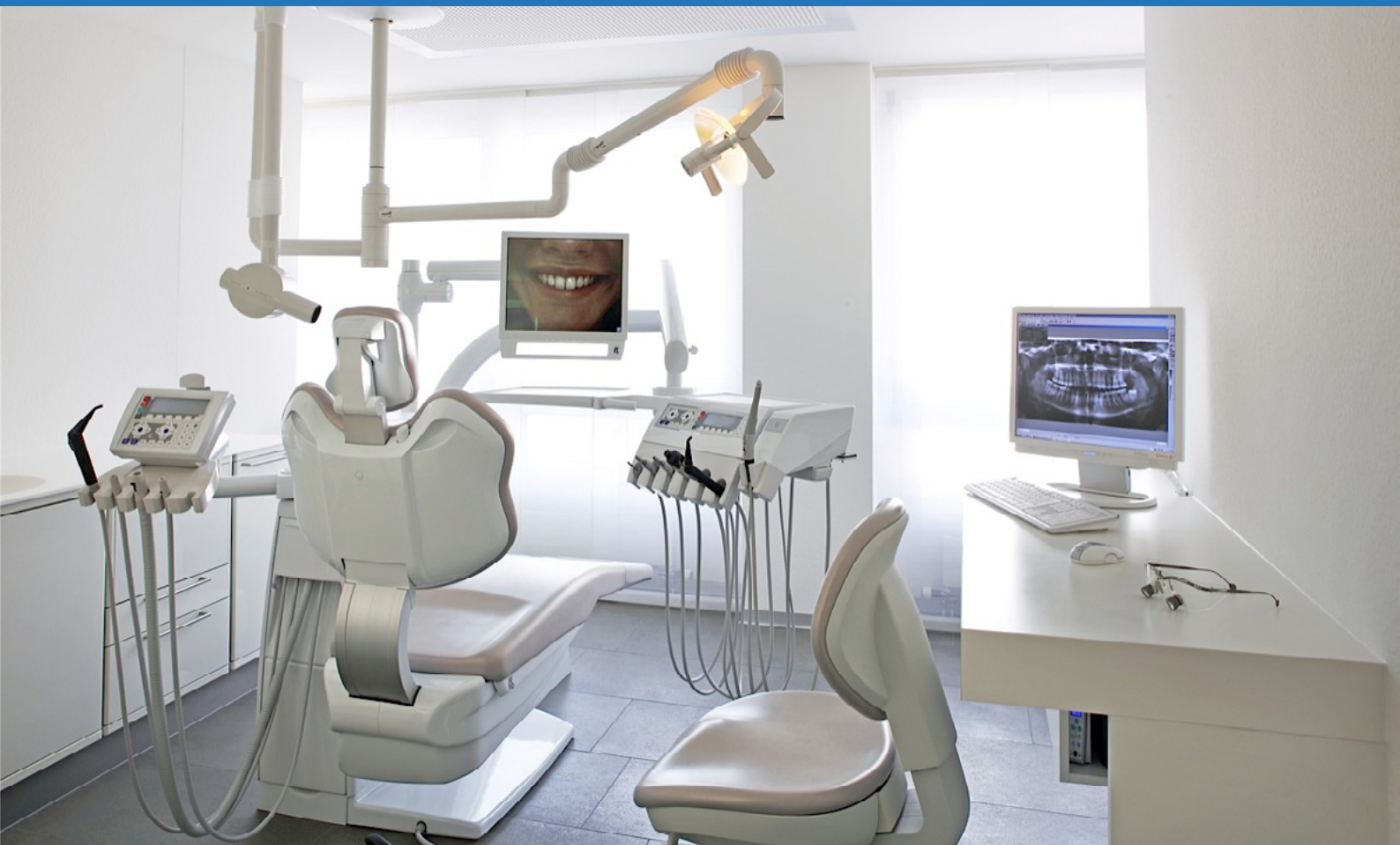


Die Kommunität Diakonissenhaus Riehen (KDR) ist in der sozialen Jugendarbeit, in Gemeinnützigkeitsfonds oder in der Pflege älterer Menschen tätig. Ziel ist es, Menschen im gesellschaftlichen Zusammenhang zu unterstützen.

Die IT-gestützte Administration hilft, die vorhandenen Ressourcen möglichst effizient zu verwalten. Um den Herausforderungen der Digitalisierung gewachsen zu sein, setzte das Diakonissenhaus Riehen auf eine Erneuerung der veralteten Infrastruktur. Damit wollte man die Soziale Arbeit moderner gestalten. Dazu zählt ebenso eine funktionierende Infrastruktur, denn die Digitalisierung macht vor sozialen Branchen nicht halt.

Die alte, heterogene IT-Infrastruktur sollte vereinheitlicht und standardisiert werden. Gleichzeitig wünschte sich das KDR eine flexiblere Lösung für die Mitarbeiter, denn soziale Tätigkeiten erfordern eine hohe Mobilität. Dementsprechend muss die IT gewährleisten, dass Mitarbeiter jederzeit und von überall Zugriff auf die Strukturen, Daten und Anwendungen haben. Gleichzeitig ist selbstverständlich Vorsicht hinsichtlich der Datensicherheit geboten – gerade bei sensiblen Daten. Die Lösung: eine hybride Cloud-Lösung kombiniert mit Microsoft Azure Backup. Die hybride Cloud-Lösung schaffte auch neue Kommunikationswege für die Angestellten. Der E-Mail-Verkehr läuft über Microsoft Outlook. Der Einsatz von Microsoft Office 365 sowie von Cloud-basierten Dateiablagensystemen wie OneDrive und SharePoint schafft neue Möglichkeiten zur Zusammenarbeit. Das gemeinsame Arbeiten an Dateien, problemloser Austausch und vor allem die Möglichkeit, jederzeit alle Beteiligten auf dem gleichen Stand zu halten, erleichtern die tägliche Arbeit um ein Vielfaches. Das Ergebnis ist eine auf allen Ebenen optimierte Organisation des KDR-Aufgabengebietes, die ein zielorientiertes und soziales Arbeiten effizient unterstützt.


Microsoft Office 365: Volldigitalisierte Zahnarztpraxis mit Cloud-Lösung



Die Praxis Schwerzmann hat sich auf zahlreiche unterschiedliche Bereiche der Zahnmedizin spezialisiert. Neue Herausforderungen und vor allem die steigenden Anforderungen an ein modernes Patientenmanagement konnte das in die Jahre gekommenen Netzwerk nicht mehr bewältigen. Deshalb suchte die Praxis nach einer adäquaten Lösung. Sie sollte die Sicherheit der sensiblen Patientendaten gewährleisten und gleichzeitig die bestehenden Abläufe optimieren. Wegen sensibler Daten sowie gewissen Schnittstellen zu anderen Systemen stand von Anfang an fest, dass Dr. Schwerzmann seinen lokalen Server behalten sollte. Zentral war nun die Frage, wo die sensiblen Daten künftig gesichert werden sollen. Mit dem redCLOUD Backup, welches sich in der Schweiz befindet, fiel die Entscheidung schliesslich auf redIT. Der Schutz der Praxis nach aussen erfolgt über den redCLOUD Firewall Service.

Mit Microsoft Office 365 Booking will die Zahnarztpraxis die internen Aufwände minimieren und die Terminplanung vereinfachen. Durch den Einsatz dreier Komponenten wird die Verwaltung künftig optimiert. Patienten können über die Buchungsseite ihre Termine planen. Die Praxis-Administration hat jetzt die Option, Mitarbeiterlisten und Dienstpläne flexibel zu verwalten. Über eine mobile App haben Berechtigte Zugriff auf alle wichtigen Daten wie Kundenlisten und Kontaktinformationen oder können manuelle Buchungen vornehmen. Zeitgleich wurde mit Office 365 Business Premium die neue E-Mail-Lösung zur vereinfachten Kommunikation ausgerollt.

Virtualisiertes Gesamtpaket: Outsourcing in die publiccloud



Das Zentrum bietet umfassende Abklärungen und integrative Behandlungen nach dem neusten Stand der psychiatrischen und psychotherapeutischen Forschung. Das Team mit rund 40 Mitarbeitenden führt an zwei Standorten jährlich über 25'000 Konsultationen durch.

Für die ZADZ AG hat das Einhalten von Richtlinien und Vorschriften der Gesundheitsbranche, der Datenschutz und das tadellose Funktionieren der IT höchste Priorität. Zudem war der Zugang zu den Daten von extern inklusive Bearbeitungsmöglichkeit ein grosses Bedürfnis der Unternehmensführung. Deshalb empfahl Scheuss & Partner das Outsourcing der Infrastruktur in das eigene Rechenzentrum der Schweiz: die publiccloud. Aktuelle Softwarelösungen wie Windows 10 oder Microsoft Office 365 sollen die Mitarbeiter dabei unterstützen, effizient und effektiv zu arbeiten.

Die Arbeitsplätze der ZADZ AG erfüllen modernste Ansprüche. Unter Windows 10 laufen die Office Suite sowie Branchenapplikationen. Die elektronische Kommunikation erfolgt verschlüsselt mittels HIN Secure Mail, dem Standard im Schweizer Gesundheitswesen. Die Therapeuten könnten sich an einem der beiden Standorte, unterwegs mit mobilen Geräten oder von zu Hause sicher in die Systeme einloggen. Selbst in einem WorstCase-Szenario, bei dem die eigenen Räumlichkeiten nicht mehr zugänglich sind, wäre trotzdem ein laufender Betrieb möglich, denn das Unternehmen könnte sich dank dieser IT-Lösung entsprechend organisieren, sodass die Betreuung der Patienten unabhängig vom Betriebsstandort geführt werden kann. Alle Applikationen und Daten liegen dazu geschützt in der publiccloud und sind jederzeit zuverlässig und ohne Umbruch verfügbar.

Auf dediziert zugeteilten Systemen arbeitet die ZADZ AG daher heute mit modernster Hard- und Software zu kostengünstigen Konditionen.

© 2017 Microsoft Corporation. All rights reserved. This document is for informational purposes only. Microsoft makes no warranties, express or implied, with respect to the information presented here.