

Radiologie-Ferndiagnose: Sicherheitsrisiken verwalten und optimale Leistung sicherstellen

Informationsschrift

Von:

Jan Dobbenie

CEO DOBCO Medical Systems

 +32 (52)77 01 16

 info@dobcomed.com

 Nachtegaalstraat 6, 9240 Zele, Belgium

 www.pacsonweb.com

Inhalt

1. Einführung	3
2. Die Sicherheitsrisiken der Ferndiagnose	4
2.1 VPN-Verbindungen auf dem PC oder Laptop	4
2.2 Unternehmenseigene und verwaltete Workstations	6
2.3 VPN in Kombination mit virtuellen Desktop-Lösungen	7
3. Software- und Bandbreiten-Herausforderungen: lokal vs. Cloud	8
4. Sicheres und vollständig webbasiertes PACS	9
5. Die Evolution der webbasierten Cloud-Plattform im Gesundheitswesen	11
6. PACSonWEB: Cloud-PACS für die Ferndiagnose und mehr	12
7. Referenzen	14

1. Einführung

Schon seit vielen Jahren lesen Radiologen bildgebende Untersuchungen zu Hause oder an externen Standorten. Der Zugriff auf die Bilder erfolgte zunächst von anderen Standorten im Krankenhaus oder in einer Privatpraxis über ein LAN (Local Area Network), das mit einem PACS (Picture Archiving and Communication System) des Krankenhauses verbunden war. Bis heute haben sich die Möglichkeiten der Ferndiagnose erheblich erweitert, und Radiologen können von zu Hause oder von außerhalb über ein WAN (Wide Area Network) auf Bilder und die volle PACS-Funktionalität zugreifen.

Die Möglichkeit, Bilder von einem beliebigen Ort außerhalb des Krankenhauses zu lesen, hat sich vor allem inmitten der Coronavirus-Pandemie als vorteilhaft erwiesen. Hier hat sich die Ferndiagnose als eine wichtige Möglichkeit angeboten, das "Social Distancing" zu unterstützen und gefährdete Radiologen und andere im Krankenhaus zu schützen. Darüber hinaus gewährleistet die Ferndiagnose nahtlose Interpretationsmöglichkeiten in Notfallszenarios, heißt es in der Vorabveröffentlichung eines frei zugänglichen Artikels im American Journal of Roentgenology (AJR).¹

Um den Anforderungen an die Ferndiagnose gerecht zu werden, stehen Organisationen im Gesundheitswesen jedoch vor zahlreichen Herausforderungen – von der Ausstattung der Radiologen mit den richtigen Werkzeugen zu Hause bis hin zur Bereitstellung einer sicheren Arbeitsumgebung.

In diesem Whitepaper untersuchen wir die verschiedenen Optionen und Sicherheitsbedenken sowie die Software- und Bandbreitenherausforderungen in Bezug auf die Ferndiagnose. Wir betrachten auch die Entwicklung der webbasierten Cloud-Plattform im Gesundheitswesen und prüfen die Vorteile von Cloud-PACS.

„Heute haben sich die Möglichkeiten der Ferndiagnose erheblich erweitert, und Radiologen können von zu Hause oder von außerhalb über ein WAN auf Bilder und die volle PACS-Funktionalität zugreifen.“

2. Die Sicherheitsrisiken der Ferndiagnose

IT-Abteilungen stehen heute vor einer Vielzahl von Herausforderungen. Der Mangel an technischem Sicherheitspersonal, gesetzliche und regulatorische Compliance-Anforderungen und der ständige Ansturm immer neuer Bedrohungen gehören laut den Forschungs- und Analyseexperten von Gartner zu den größten Herausforderungen für die Sicherheit.² Darüber hinaus hat COVID-19 Unternehmen einem enormen Druck ausgesetzt, Digitalisierungsinitiativen auszuweiten und sich Cloud-Computing zu widmen.

Gleichzeitig sind die IT-Abteilungen im Gesundheitswesen schlank und decken ein breites Spektrum an Aufgaben ab. Eine schnelle Skalierung, um medizinisches Personal mit sicheren Firmen-Laptops oder -Geräten auszustatten, ist nicht immer möglich. Dies führt dazu, dass viele Radiologen ihre eigenen Geräte (Laptop, Smartphone, Tablet) nutzen, um remote auf Daten zuzugreifen.

Mit welchem Vorgehen lässt sich die Ferndiagnose schnell und effizient skalieren und gleichzeitig die Sicherheit gewährleisten und den Radiologen ein Höchstmaß an Systemleistung bieten? Zunächst wird die Verwendung einer Virtual Private Network (VPN)-Verbindung in verschiedenen Konfigurationen erläutert.

2.1 VPN-Verbindungen auf dem PC oder Laptop

„Während einige Sicherheitsexperten dies [die Installation eines VPN auf dem Heim-PC eines Mitarbeiters] für eine akzeptable Praxis halten mögen, birgt diese Strategie ein hohes Risiko mit einem unerwünschten Angriffsvektor, wenn sie den Zugriff auf Ihre Umgebung zulässt.“

Morey Haber, „The Dangers Of Using A VPN On Home Computers For Work And What To Do Instead“, Forbes Technology Council ³

„COVID-19 hat Unternehmen einem enormen Druck ausgesetzt, ihre Digitalisierungsinitiativen zu erweitern und sich dem Cloud-Computing zu widmen.“

Ein gängiger Ansatz für die Ferndiagnose besteht darin, Radiologen eine VPN-Verbindung zur Verfügung zu stellen, die sie auf ihrem persönlichen PC zu Hause oder ihrem Laptop nutzen können. Diese Option ist zwar einfach einzurichten, birgt aber mehrere Sicherheitsrisiken. Wie von Morey Haber beschrieben, sind dies einige der wichtigsten Bedenken:

A Mehrere Benutzer erhöhen die Risiken

PCs werden in der Regel von mehreren Familienmitgliedern gemeinsam genutzt. Wenn jemand einem Phishing-Betrug oder einem anderen Angriff zum Opfer fällt, besteht die Möglichkeit, dass ein Virus in das virtuelle Netzwerk der Organisation hochgeladen wird. Techniken wie der schnelle Benutzerwechsel verschlimmern das Problem, da andere Profile im Speicher gehalten werden. Letztendlich könnte ein Benutzer, der nicht zur Organisation gehört, aufgrund der aktiven VPN-Sitzung, die mit der Organisation verbunden ist, leicht das virtuelle Netzwerk einer ganzen Organisation kompromittieren.

A Unfähigkeit, den Host zu sichern und fehlende Befugnisse

Die meisten Unternehmens-VPN-Lösungen betten in der Regel ein Zertifikat in Benutzerprofile oder eine Verbindung ein, um die Verbindung zu validieren. Dies geschieht getrennt von der Authentifizierung, die Benutzer durch Anmeldedaten und eine andere Form der Zwei-Faktor-Authentifizierung vornehmen müssen, um eine sichere Verbindung zu erhalten. Die Sicherheit des Zertifikats und der Anmeldedaten für die Authentifizierung wird nicht viel bringen, da sie nur so sicher sind wie die von der Organisation implementierte Sicherheitswartung. Diese werden zu einem bevorzugten Ziel für Cyberkriminelle, die eigene Verbindungen initiieren oder sogar Sitzungen von remote arbeitenden Mitarbeitern kapern können.

Das ist ein großes Sicherheitsrisiko, denn wenn Sie nicht in der Lage sind, den Host zu sichern, schaffen Sie es auch nicht, die Verbindungssoftware zu sichern.

„PCs werden in der Regel von mehreren Familienmitgliedern gemeinsam genutzt. Wenn jemand einem Phishing-Betrug oder einem anderen Angriff zum Opfer fällt, besteht die Möglichkeit, dass ein Virus in das virtuelle Netzwerk der Organisation hochgeladen wird.“

Darüber hinaus können Lösungen für die Netzwerkzugriffskontrolle zwar Antiviren-Signaturversionen und grundlegende Hardwareeigenschaften validieren, aber sie können keinen Heimcomputer inventarisieren und sicherstellen, dass er wie ein Vermögenswert des Unternehmens gewartet und gehärtet wird. Diese Lücken und fehlenden Befugnisse können Datenlecks durch bildschirmaufzeichnende Malware und Keystroke-Logger ermöglichen.

A Geringere Malware-Abwehr

Die meisten Malware-Angriffe erfordern administrative Rechte, um ein System zu inspizieren. Benutzer persönlicher Geräte sind in der Regel lokale Administratoren für ihre eigenen Computer. Wenn Teammitglieder mit einem älteren Betriebssystem arbeiten, stellt dies ein größeres Risiko für sie dar. Laut dem AV-TEST-Sicherheitsreport 2019/2020 (AV-TEST ist ein unabhängiges Forschungsinstitut für IT-Sicherheit in Deutschland) sind Computer, auf denen Windows läuft, besonders anfällig für Angriffe: Im Jahr 2019 wurden 114 Millionen neue Schadprogramme entwickelt, und 78,64 Prozent aller Angriffe wurden auf Windows-Systemen durchgeführt.⁴

A Keine schützenden Ressourcen

Nicht jeder macht sich zu Hause Gedanken über Antiviren-Software. Es wird geschätzt, dass 25 % der PCs nicht mit Antiviren-Software geschützt sind, und die Wahrscheinlichkeit, dass sie infiziert werden, ist etwa 5,5-mal so hoch.⁵ Obwohl das Bewusstsein der Benutzer von Privatgeräten wächst, sind sich viele Benutzer zusätzlicher Sicherheitstools wie Endpoint, Detection and Response (EDR) oder Endpoint Privilege Management (EPM) nicht bewusst.

2.2 Unternehmenseigene und verwaltete Workstations

Einige Organisationen im Gesundheitswesen haben den Ansatz gewählt, Radiologen unternehmenseigene und verwaltete Workstations zur Verfügung zu stellen. Mit dieser Lösung können Sie sicherstellen, dass Radiologen nicht über herkömmliche (private) Desktop-Computer auf das VPN der Organisation zugreifen.

„Viele Benutzer sind sich zusätzlicher Sicherheitstools wie Endpoint, Detection and response (EDR) oder Endpoint Privilege Management (EPM) nicht bewusst.“

Die unternehmenseigene Workstation arbeitet wie eine reguläre PACS-Workstation und könnte sogar ein verwaltetes Asset sein, das die zuvor geprüften Risiken minimiert.

Diese Lösung hat jedoch ihren Preis: Diese Workstations müssen von der Organisation verwaltet, aktualisiert und unterstützt werden. Vielfach jedoch sind Organisationen im Gesundheitswesen oder ihre IT-Abteilungen nicht dafür organisiert oder strukturiert, Hard- und Software außerhalb der Organisation zu unterstützen, insbesondere wenn es um die spezielle Hard- und Software geht, die Radiologen benötigen. Es sind zusätzliche Ressourcen und Maßnahmen erforderlich, um die Systeme zu aktualisieren und zu verwalten, um Sicherheit, Leistung und den erforderlichen Service-Level zu gewährleisten. Für Radiologen sind diese Workstations das primäre Werkzeug zum Lesen von Studien und daher unverzichtbar.

Darüber hinaus kann die Leistung immer noch ein Thema sein und sollte in mehreren Szenarios bewertet und (Stress-) getestet werden. **In den meisten Fällen laufen VPNs über eine gemeinsam mit der Organisation genutzte Internetverbindung, was bedeutet, dass die erforderliche Leistung aufgrund mangelnder Upload-Bandbreite der Gesundheitsorganisation nicht garantiert werden kann.**

2.3 VPN in Kombination mit virtuellen Desktop-Lösungen

Dies ist eine weit verbreitete Lösung innerhalb von Organisationen im Gesundheitswesen. Diese Lösungen (wie Citrix, VirtualBox, Horizon und andere) erstellen einen virtuellen Desktop auf dem Heimcomputer des Arztes mit Zugriff auf die Anwendungen der Gesundheitsorganisation. Es handelt sich dabei um isolierte Umgebungen, die die zuvor genannten Risiken minimieren. Unter Sicherheitsaspekten sind diese Lösungen (in der Regel) die richtige Wahl und zudem relativ einfach zu implementieren. Obwohl sie für die meisten Krankenhausanwendungen, die vom Arzt zu Hause benötigt werden sehr nützlich sind (z. B. für den Zugriff auf die EMR), sind sie nicht geeignet, um Studien im PACS zu lesen.

„Lösungen (wie Citrix, VirtualBox, Horizon und andere) erstellen einen virtuellen Desktop auf dem Heimcomputer des Arztes mit Zugriff auf die Anwendungen der Gesundheitsorganisation.“

Das Scrollen durch große Datenmengen, die Fensterausrichtung, 3D oder die Spracherkennung funktionieren über diese Art von Lösung einfach nicht gut genug.

Dafür gibt es mehrere Gründe: keine Unterstützung für mehrere Monitore, die Bildwiederholungsrate der Umgebung, die fehlende Unterstützung für Peripheriegeräte usw. Nach allgemeiner Erfahrung fehlt diesen Umgebungen die Leistung, um spezialisierte Anwendungen wie PACS auszuführen. Darüber hinaus stellt die Anzeige verlustfreier DICOM-Bilder über Remote- oder virtuelle Desktop-Techniken ein potenzielles Risiko dar, da das Bild durch die virtuelle Desktop-Software komprimiert oder verzerrt werden kann.

3. Software- und Bandbreiten-Herausforderungen: lokal vs. Cloud

Zusätzlich zu den Sicherheitsbedenken müssen die IT-Teams im Gesundheitswesen mit der Installation mehrerer Softwareanwendungen und den Bandbreiten-Anforderungen für Radiologen umgehen, die Ferndiagnosen von ihren persönlichen Geräten aus durchführen.

Eine Standard-PACS-Workstation besteht aus mehreren Monitoren und erfordert die Installation mehrerer Softwareanwendungen wie der PACS-Software, der Spracherkennungssoftware und der RIS (Radiologie-Informationssystem)-Clientsoftware.

Diese Anwendungen sind typischerweise für LAN-Verbindungen ausgelegt, denn das PACS benötigt aufgrund der großen Datensätze, die insbesondere bei CT- und MR-Untersuchungen für eine reibungslose Bilddarstellung verarbeitet werden, eine Verbindung mit hoher Bandbreite und geringer Latenz zwischen Client und Server. Ein einzelner CT-Scan kann beispielsweise mehrere GB groß sein. Die Bildwiederholungsrate ist auch entscheidend, wenn der Radiologe Manipulationen vornimmt, z. B.

„Webbasierte Cloud-PACS-Lösungen hingegen beseitigen die Sicherheitsrisiken der Verwendung eines VPN, erfordern keine Installation von Software, um hochwertige DICOM-Bilder verlustfrei aus der Ferne zu betrachten, und sind über jeden Browser auf jedem mit dem Internet verbundenen Gerät verfügbar.“

bei der Fensterausrichtung. Radiologen können sich zu Hause für eine Internetverbindung mit höherer Bandbreite entscheiden. Die Verbindung aus dem Krankenhaus muss hingegen auch die Upload-Geschwindigkeit für mehrere Sitzungen verschiedener Anwendungen gleichzeitig bewältigen.

Ein Ansatz, den mehrere PACS-Anbieter zur Überwindung von Bandbreitenproblemen implementiert haben, ist das Zwischenspeichern der Bilder auf der Workstation. In vielen Fällen sind die Inhalte im Cache nicht verschlüsselt, was zu noch größeren Sicherheits- und Datenschutzrisiken für den Patienten führt, da sich die Daten auf den lokalen Festplatten befinden. Außerdem sind Internetverbindungen anfällig für hohe Latenzzeiten und Verbindungsabbrüche, für die die PACS-Workstation-Software nicht ausgelegt ist.

Angesichts dieser Sicherheits Herausforderungen und des Bedarfs an mehreren Softwareanwendungen für die medizinische Bildgebung sowie einer beträchtlichen Bandbreite für Radiologen stellt sich die Frage, welche alternativen Optionen es für die sichere und schnelle Skalierung der radiologischen Ferndiagnose gibt.

4. Sicheres und vollständig webbasiertes PACS

Während die Verwendung eines VPN, die Installation lokaler Software und die Bereitstellung eines dedizierten PCs für Radiologen einige der Sicherheits- und Leistungsprobleme im Zusammenhang mit der Ferndiagnose lösen können, bleibt dieser Ansatz risikobehaftet und erfordert erhebliche Unterstützung durch die IT-Abteilung.

„Ein einzelner CT-Scan kann mehrere GB groß sein.“

Webbasierte Cloud-PACS-Lösungen hingegen beseitigen die Sicherheitsrisiken der Verwendung eines VPN, erfordern keine Installation von Software, um hochwertige DICOM-Bilder verlustfrei aus der Ferne zu betrachten, und sind über jeden Browser auf jedem mit dem Internet verbundenen Gerät verfügbar.

Der Client ist lediglich ein Browser, der über HTTPS mit der Cloud-Umgebung kommuniziert, um die Sicherheit zu gewährleisten. Er hinterlässt keine Daten auf dem lokalen PC oder der Workstation und benötigt keine Client-Verwaltung. Bei diesen sicheren Weblösungen kommen Multi-Faktor-Authentifizierungstechniken sowie eine umfangreiche Protokollierung zum Einsatz. Upgrades sind auf die Cloud-Umgebung beschränkt und die Software kann auf jedem Gerät oder Betriebssystem laufen. Von der Cloud aus lassen sich Bandbreiten skaliert und Verbindungen duplizieren, um eine hohe Verfügbarkeit zu gewährleisten.

Die Ferndiagnose wird vollständig unterstützt, und Radiologen können:

A (Vorläufige) Berichte außerhalb des Krankenhauses, von zu Hause oder einem anderen Büro aus vorbereiten.

A problemlos mit anderen Diagnostikgruppen und Radiologen zusammenarbeiten.

A auf die volle PACS-Funktionalität zugreifen, ohne dass sie ein VPN oder eine komplexe IT-Infrastruktur benötigen.

Darüber hinaus werden Bilder und Befunde in Echtzeit verknüpft und der diktierte Text gleichzeitig auf dem Bildschirm angezeigt. Der Befund wird nach Fertigstellung in das lokale Radiologie-Informationssystem (RIS) oder in die elektronische Patientenakte (EMR) übernommen.

5. Die Evolution der webbasierten Cloud-Plattform im Gesundheitswesen

Obwohl das Konzept einer webbasierten Cloud-Plattform in anderen Bereichen (wie z. B. Homebanking, Office-Anwendungen, Customer Relationship Management [CRM] usw.) weithin akzeptiert und im Einsatz ist, verlief die Einführung im Bereich der IT-Software für das Gesundheitswesen und insbesondere der Software für die medizinische Bildgebung etwas langsamer (obwohl sie jetzt deutlich an Boden gewinnt). Hierfür gibt es mehrere Gründe:

A Altsystem: Softwareanwendungen für die medizinische Bildgebung sind traditionell Thick-Client-Anwendungen, die lokale Ressourcen benötigen und spezifische Anforderungen an die Workstation stellen. Die aktuellen Systeme sind auf einer veralteten Architektur und Softwaretechnik aufgebaut.

A Für eine Implementierung jeder Funktion in einer Web-Umgebung liegt die technische Messlatte hoch:

Von der Anzeige großer CT/MR-Datensätze über komplexe Bildgebungswerkzeuge mit hohen Anforderungen an die Rechenleistung (MIP/MPR), bis hin zur Spracherkennung wird jede Funktion benötigt, um den Arbeitsablauf des Radiologen zu unterstützen, ist aber in einer Web-Umgebung nur schwer zu implementieren. Diese Funktionen in einem reinen HTML-Kontext zu erstellen, erfordert einen großen Forschungs und Entwicklungsaufwand (von Grund auf) sowie mehr (Design-) Entscheidungen als zuvor.

A Multitenant-Cloud: Dieses Konzept ist bei Lösungen für das Gesundheitswesen noch nicht weit verbreitet, da sich die Anbieter auf das einzelne Unternehmen konzentrieren. In manch anderen Bereichen ist dies jedoch durchaus üblich (Salesforce, Google etc.).

„Das Konzept einer webbasierten Cloud-Plattform ist weithin akzeptiert und in anderen Bereichen wie Homebanking, Büro-Anwendungen, Customer Relationship Management (CRM) usw. im Einsatz.“

A Leistung: Dieser web- und cloudbasierte Ansatz erfordert bessere und intelligentere Techniken, um Daten über Verbindungen mit geringerer Bandbreite/hoher Latenz schneller verfügbar zu machen.

Die Vorteile dieser Technologie für das Gesundheitswesen liegen jedoch klar auf der Hand. Reine Web- und Cloud-Technologie wird Organisationen im Gesundheitswesen helfen, ihre aktuelle Infrastruktur beizubehalten und zu vereinfachen, die Verwaltungsaufgaben und Gesamtkosten zu senken und eine Lösung für die Fernarbeit zu bieten, ohne die Sicherheitsrichtlinien zu kompromittieren.

6. PACSonWEB: Cloud-PACS für die Ferndiagnose und mehr

PACSonWEB ist eine sichere, rein webbasierte Multitenant-Cloud-Lösung. Die wichtigsten PACS-Funktionen sind jederzeit, überall und auf jedem Gerät aus der sicheren Cloud-Umgebung verfügbar. Der Client ist der Browser, der nur über HTTPS kommuniziert. PACSonWEB unterstützt Multi-Monitor-Anwendungen und bietet die Funktionen, die Geschwindigkeit und den flüssigen Ablauf, die ein Radiologe von einer PACS-Workstation erwartet, während das Sicherheitsniveau der Gesundheitsorganisation erhalten bleibt. Die Ferndiagnose mit Spracherkennung ist integriert und die Verwaltungsaufgaben der IT-Abteilung werden deutlich reduziert. **Alle Benutzer von PACSonWEB, einschließlich Radiologen, andere Kliniker, Hausärzte und Patienten, werden durch einen zentralen Helpdesk unterstützt, der als zentrale Anlaufstelle für alle PACSonWEB-Anfragen dient.** Dieser Support ist in deutscher, englischer, französischer und niederländischer Sprache verfügbar, über Telefon, E-Mail oder ein Fernverbindungstool wie LogMeIn oder TeamViewer. Dabei sind schnelle Reaktionszeiten garantiert.

Wenn Sie mehr über PACSonWEB für die Ferndiagnose wissen oder mehr über PACSonWEB erfahren möchten, besuchen Sie uns:

www.pacsonweb.com

7. Referenzen

1. Srini Tridandapani, Greg Holl, and Cheri L. Canon, „Rapid Deployment of Home PACS Workstations to Enable Social Distancing in the Coronavirus Disease (COVID-19) Era“, American Journal of Roentgenology 2020 215:6, 1351-1353. Abgerufen von: <https://www.ajronline.org/doi/full/10.2214/AJR.20.23495>

2. Christy Pettey, „Gartner Top 9 Security and Risk Trends for 2020“, September 17/20. Abgerufen von: <https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/>

3. Morey Haber, „The Dangers Of Using A VPN On Home Computers For Work And What To Do Instead“, Forbes, Forbes Technology Council, July 17/20, abgerufen von: <https://www.forbes.com/sites/forbestechcouncil/2020/01/17/the-dangers-of-using-vpn-on-home-computers-for-work-and-what-to-do-instead/?sh=5041735d6349>

4. AV-TEST Security Report 2019/2020, vom unabhängigen Forschungsinstitut für IT-Sicherheit AV-TEST in Deutschland, abgerufen von: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2019-2020.pdf

5. Sophie Anderson, „Antivirus and Cybersecurity Statistics, Trends & Facts 2021“, SafetyDetectives, January 24/20, abgerufen von: [https://www.safetydetectives.com/blog/antivirus-statistics/#:~:text=The%20Threats%20Against%20Regular%20Users&text=However%2C%20an%20estimated%20one%2Dfourth,PUPs%20\(potentially%20unwanted%20programs\).](https://www.safetydetectives.com/blog/antivirus-statistics/#:~:text=The%20Threats%20Against%20Regular%20Users&text=However%2C%20an%20estimated%20one%2Dfourth,PUPs%20(potentially%20unwanted%20programs).)

DOBCO Medical Systems

Das in Belgien ansässige Unternehmen DOBCO Medical Systems ist Spezialist für cloudbasierte medizinische Bildgebungslösungen. Das Unternehmen wurde 2011 von Jan Dobbenie und Kristof Coucke, beides Veteranen der Healthcare-IT-Branche, gegründet und verzeichnete innerhalb von weniger als acht Jahren einen Jahresumsatz von 4 Millionen Euro.





Unsere Vision: Wir glauben, PACS ist Cloud

Wir sind von der Leistungsfähigkeit einer Cloud- und Internettechnologie fest überzeugt, die es uns ermöglicht, Radiologie-Arbeitsabläufe zu verbessern und medizinische Informationen schneller, genauer und sicherer für Ärzte und Patienten bereitzustellen.

Wir möchten Radiologen so unterstützen, dass sie ihre Dienste für Patienten, Hausärzte und Kliniker sowie das Krankenhausmanagement optimieren können.

Wir stehen für Innovation. Unsere Lösungen für medizinische Bildgebungsverfahren sind darauf ausgerichtet, unsere Kunden dabei zu unterstützen, durch besseren Service sowohl in der Patientenversorgung als auch im Geschäft ihre Ziele zu erreichen. Unser Versprechen: Wir gewährleisten allen, die über die PACSonWEB-Lösung auf Bilder zugreifen, über das gesamte Patientenversorgungskontinuum hinweg eine ausgezeichnete Erfahrung und hervorragenden Service.

Kontakt

-  +32 (52)77 01 16
-  info@dobcomed.com
-  Nachtegaalstraat 6, 9240 Zele, Belgium
-  www.pacsonweb.com