

3M | **M*Modal**

3M™ M*Modal Spracherkennung

Cloud, Datenschutz und 3M:

**Streng vertraulich –
aber sicher!**



Streng vertraulich – aber sicher!

Digitalisierung im Krankenhaus: Alle wollen sie. Doch die Zukunftswelt der Bits und Bytes wirft auch viele Fragen auf – zuallererst die nach der Datensicherheit. Als einer der führenden Anbieter von Softwarelösungen für Krankenhäuser und Kliniken nimmt 3M Health Information Systems (HIS) diese Fragen sehr ernst. Mit Innovationen und KI-basierter Software arbeitet das Unternehmen mit an der sicheren Zukunft des Gesundheitssystems.

Von der **ärztlich-pflegerischen Dokumentation** über Kodierung und Gruppierung bis hin zur Abrechnung und Analyse bietet 3M bereichsübergreifend umfassende Lösungen an, die den wertschöpfenden Gesamtprozess komplett abdecken. 3M HIS bedient sich dabei modernster KI-Methoden. Das Ziel ist es, über die durchgehende Nutzung vorhandener oder erarbeiteter Daten den größtmöglichen Zusatznutzen für alle Abteilungen zu schaffen – bei zeitgleicher Berücksichtigung der relevanten Datenschutzbestimmungen der Kundenanforderungen. Eine modular angelegte Softwarearchitektur ermöglicht dabei die Nutzung von Einzelösungen ebenso wie den stufenweisen Ausbau nach dem jeweiligen Bedarf.

Insbesondere die **3M Sprachlösungen für die ärztlich-pflegerische Dokumentation** spielen eine wesentliche Rolle, denn nur bei korrekter Dokumentation von Beginn an funktioniert im Anschluss auch die „Automatisierte Kodierung“.

Dank eines mehrstufigen Implementierungsansatzes, der den Weg von **reinen Schreibdienst-basierten Abläufen** zu einer hochmodernen, **KI-basierten Frontend-Spracherkennung** ermöglicht, wird sichergestellt, dass verschiedene Arbeitsabläufe möglich sind und jeder Anwender Unterstützung bei dem für ihn passenden Workflow erhält.

Darüber hinaus sind die 3M Sprachlösungen cloudbasiert. Doch was bedeutet das konkret? Und wie sicher ist die Cloud? Und was ist eigentlich mit dem Datenschutz?

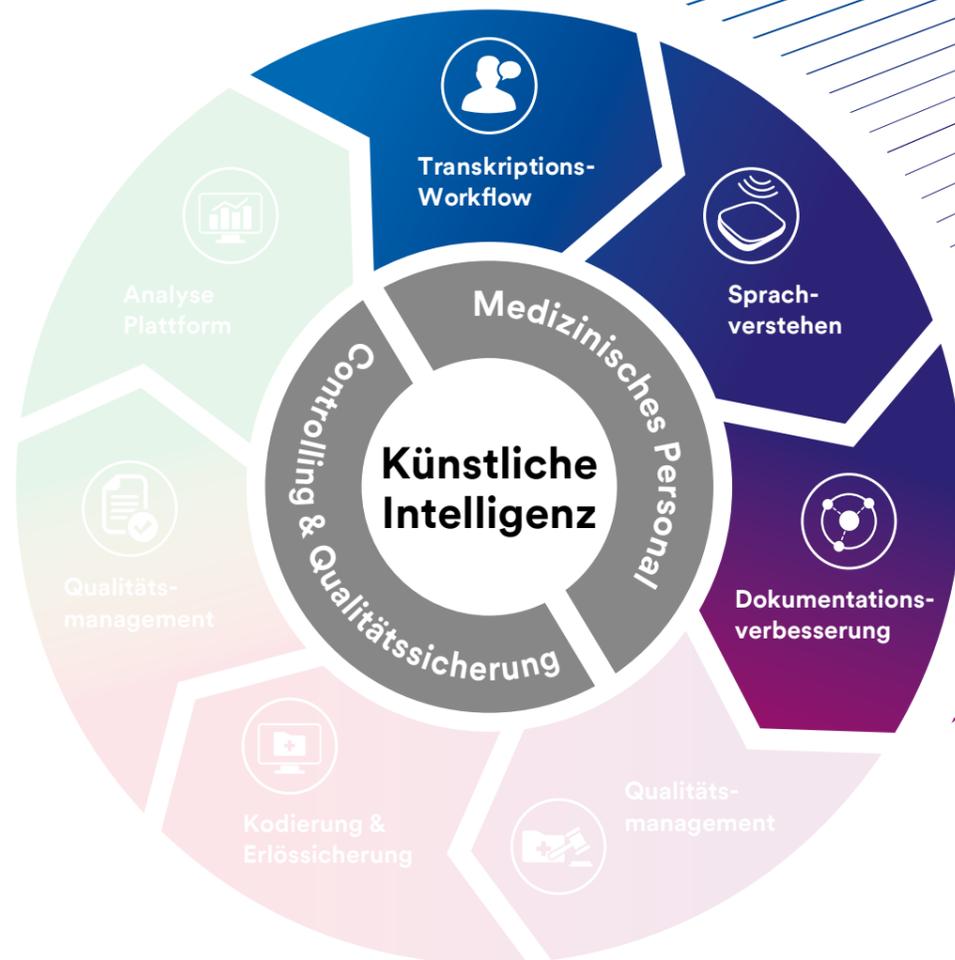
3M™ M*Modal Sprachlösungen in der Cloud

Höchste Verfügbarkeit durch Nutzung cloudbasierter Infrastruktur:

- ▶ Zentrales Releasemanagement
- ▶ Sicherer 24 × 7 × 365 Betrieb
- ▶ Keine On-Premise Kosten
- ▶ Skalierbar
- ▶ Entlastung der IT-Abteilung
- ▶ Kosten planbar durch Abo, ohne Vorinvestition der Lizenzen
- ▶ Optimiert für virtuelle Umgebungen wie Citrix

Jenseits der innovativen Produktlinien und dem Bestreben, den Kunden das Beste zu bieten, sind zwei weitere Elemente die Basis der Unternehmensphilosophie: **Vertrauen und Sicherheit.**

Vertrauen ist der Schlüssel zu jeder Geschäftsbeziehung. Vertrauen ist nicht selbstverständlich, es will erarbeitet werden. Werbesprüche können Werte nicht ersetzen. Das gilt im Alltag ebenso wie in der Frage, wie sensible Daten verarbeitet und gespeichert werden.



Heiter bis wolkig: sicher in der Cloud

Innerhalb der IT-Architektur in Krankenhäusern fallen große Mengen an Daten an, die schnell verarbeitet werden müssen. 3M HIS setzt für diese Prozesse insbesondere im Bereich der Spracherkennung auf Cloudlösungen. Es gibt gute Argumente dafür, die internen Daten in einer externen Cloud zu speichern. So entlastet die Cloud die IT-Ressourcen einzelner Häuser und bietet die Gewähr, in Sachen Software und Datensicherheit immer auf dem neuesten Stand zu sein. Eine Cloud ist ausfallsicherer als der Server im Krankenhaus. Cloud-Computing ist zudem ein wichtiges Element, um den Digitalisierungsprozess in Gesundheitseinrichtungen voranzutreiben. Deshalb nennt auch das Krankenhaus-zukunftsgesetz (KHZG) die Cloud explizit als förderfähiges Tool für das Krankenhaus von morgen.

Zugleich sind mit dem Stichwort „Cloud“ viele Fragen verbunden. Die häufigste lautet: „Sind meine Daten sicher?“ Sie formuliert einen berechtigten Anspruch gegen den Zugriff von außen auf unternehmenseigene Informationen, zumal Krankenhäuser und Kliniken juristisch auch dann für die Daten verantwortlich sind, wenn diese in der Cloud eines Dienstleisters gespeichert werden. Das hat eine erhöhte Sensibilität bei der Abschätzung von Risiken zur Folge. 3M HIS unterstützt diese Haltung, denn Risikominimierung ist für das Unternehmen kein nachgeordneter Bereich, sondern ein wichtiger Ausgangspunkt für alle Produkte.



Dynamische Rahmenbedingungen

Eines der größten Risiken aus Kundensicht ist das Bestreben Dritter, sich Zugang zu den Daten in der Cloud zu verschaffen. In diesem Kontext haben verschiedene Stellen unterschiedliche Interessen an einem solchen Zugriff auf sensible Informationen – von staatlichen Institutionen bis zu Cyberkriminellen. Das Bestreben nach Sicherheit steht dabei immer im Spannungsfeld der Gesetzgebung einzelner Rechtssysteme. Während in den USA der erlaubte Zugriff staatlicher Stellen auf Unternehmensdaten gesetzlich sehr weit ausgelegt wird, sieht es in der EU seit dem Inkrafttreten der DSGVO und dem sogenannten Schrems II-Urteil des Europäischen Gerichtshofs

(EuGH) im Jahr 2020 anders aus. Die Messlatte für das Abfragen von privaten Daten liegt deutlich höher. In der Frage, wie weit staatliche Dienste und Institutionen aus den USA auf Server in Europa zugreifen dürfen, besteht weiterhin Uneinigkeit. Zurzeit dürfen personenbezogene Daten in Drittländer außerhalb der EU nur dann übermittelt werden, wenn das Schutzniveau der DSGVO nicht unterlaufen wird. Was das im Einzelfall in der Konsequenz bedeutet, ist umstritten. Die Interpretation und Auslegung der rechtlichen und politischen Rahmenbedingungen der Cloud-Technologie sind innerhalb der EU aktuell sehr dynamisch.

Mit Recht vertraulich

Umso wichtiger ist Vertrauen und Verlässlichkeit im täglichen Umgang mit Daten. 3M HIS versteht sich in Sachen Datensicherheit als Partner für Krankenhäuser und Kliniken. Das heißt: Das Unternehmen tut alles, um die Datenhoheit in den Händen der Kunden zu belassen und sie gegen Ansprüche von Dritten zu verteidigen. 3M nimmt die Sicherheit seiner (Kunden-) Daten ernst, wird alle Zugriffsanfragen durch Sicherheitsbehörden mit allen verfügbaren juristischen Mitteln prüfen und anfechten und auch von seinen Geschäftspartnern die Einhaltung der Datenschutzgesetze einfordern. Ein europäisches Netzwerk von Fachanwälten stellt sich in Zusammenarbeit mit 3M diesen Herausforderungen. Das gilt auch für die Serverbetreiber, mit denen 3M kooperiert. Zudem schließt die jetzige Gesetzeslage

„Blanko-Anfragen“ zu sensiblen Daten aus. Jeder Wunsch nach Offenlegung von Unternehmensdaten muss schon jetzt begründet werden und darf den Grundsatz der Verhältnismäßigkeit nicht verletzen. 3M verpflichtet sich gegenüber seinen Kunden, Anfragen von Dritten – sofern rechtlich zulässig – offenzulegen und mit dem Kunden eine gemeinsame Antwort zu koordinieren. Der juristische Rahmen der europäischen und US-Gesetzgebung sieht außerdem vor, dass die betroffenen Unternehmen gegen staatliche Versuche der Einsicht in private Daten Rechtsmittel einlegen können. Davon macht 3M HIS Gebrauch, um den Schutz der Daten zu gewährleisten – nicht für das Unternehmen, sondern in erster Linie für die Kunden.

Sichere Sache: Kundendaten bei 3M

3M HIS hat in Übereinstimmung mit den Empfehlungen der Europäischen Datenschutzbehörde Mechanismen etabliert, die dem Datenschutz höchste Priorität einräumen. Alle Aktivitäten, jeder Datentransfer und jeder Zugriff werden dokumentiert. Von einem Team von Datenschutzkoordinatoren wird dieses Protokoll auf dem neuesten Stand gehalten. Standardvertragsklauseln nach § 46 der DSGVO bieten die Garantie auf einen integren Umgang mit personenbezogenen Daten. Zusätzliche technische und organisatorische Maßnahmen gehen zudem darüber hinaus. Zugangsbeschränkungen, Verschlüsselung bei der Übertragung und im Ruhezustand, die bewusste Minimierung der Datenmenge und permanente Mitarbeiterschulungen sowie von 3M HIS formulierte Zusatzklauseln im Verkehr mit Cloudanbietern heben das Schutzniveau weiter an.

Der 3M-Service in Sachen Sicherheit schließt eine fundierte Beratung „im Fall des Falles“ ein. Bei Auskunftersuchen aus bestimmten Zielländern kann 3M den Kunden eine seriöse Folgenabschätzung des Datentransfers liefern, die eine gründliche und umfangreiche Bewertung des Kontexts vornimmt. Dabei werden die Datenschutzgesetze des jeweiligen Landes objektiv rechtlich bewertet, bereits erfolgte Datenabfragen analysiert und eventuelle Vorfälle offengelegt, die Anlass zu Datenschutzbedenken geben können. Bestehen solche Bedenken, kann 3M HIS für die Kunden mit technischen und organisatorischen Mitteln die Datensicherheit steigern – wie zum Beispiel mit einer zusätzlichen Verschlüsselung oder Pseudonymisierung. Die Richtlinien der Europäischen Datenschutzbehörde sehen als weitere Maßnahme die laufende Überprüfung aller Übertragungsvereinbarungen vor. 3M kommt diesem Anspruch mit regelmäßigen internen und externen Audits nach und legt deren Ergebnisse seinen Kunden offen.

Datenschutz von Anfang an

3M HIS sorgt mit langjährigem Know-how und dem detaillierten Wissen von Experten dafür, dass Krankenhaus-Daten in der Cloud sicherer sind als auf einem In-House-Server. Datenschutz als strategisches Thema bedeutet für das Unternehmen mehr als Firewall und Anti-Viren-Programm: Datensicherheit ist der Kern des 3M HIS-Geschäftsmodells. Dafür hat das Unternehmen erfolgreiche Methoden und Prozesse entwickelt, die unberechtigte Zugriffe verhindern oder im Falle von juristisch berechtigten Zugriffen die Daten so verschlüsseln, dass sie nicht rückverfolgbar sind. Der Zugriff auf den „Schlüssel“, der am Ende die Daten entschlüsseln kann, bleibt definitiv im Europäischen Wirtschaftsraum (EWR). 3M bietet zu diesem Zweck maßgeschneiderte Optionen an, um Daten bereits bei der Übermittlung oder auch auf dem Speichermedium zu verschlüsseln.

Das heißt: Selbst wenn 3M HIS oder Cloud-Serverbetreiber juristisch zur Herausgabe von Daten angehalten werden, bleibt der Datenschutz gewährleistet.

3M HIS ist ein zuverlässiger und vertrauensvoller Partner für die Transformation im Gesundheitswesen. Die Interessen der Kunden stehen dabei an erster Stelle. Deshalb ist das Unternehmen bereit für den Dialog und unterstützt seine Kunden gerne bei diesem wichtigen Thema, sei es über Webinare, Informationsdokumente, im direkten Gespräch oder in einem unserer Experten-Talks.

Krankenhäuser und Kliniken können 3M HIS also vertrauen. Mit Sicherheit.



Cloud, Datenschutz und Sicherheit – entscheidende Gründe für 3M.

Datenschutzkonform

3M investiert erheblich in Kundenanliegen und in die Einhaltung der DSGVO und aller Datenschutzgesetze. In enger Zusammenarbeit mit AWS werden Risiken minimiert und internationale und nationale Anforderungen unterstützt:

- ▶ EU-DSGVO & BDSG (neu)
- ▶ In Frankfurt gehostet
- ▶ BSI C5 zertifiziert
- ▶ ISO 9001
- ▶ 27001 Sicherheitsmgmt.kontrollen
- ▶ 27017 Cloudspezifische Kontrollen
- ▶ 27018 Schutz personenbezogener Daten
- ▶ Jährliche Audits

Sicher

Amazon Web Service (AWS) ist Weltmarktführer von Infrastructure as a Service (IaaS) mit höchsten Anforderungen an die Sicherheit:

- ▶ Nutzung von AWS als IaaS
- ▶ Betrieb als Private Cloud, per VPN
- ▶ Verschlüsselte Übertragung und Daten nach TLS bzw. AES-256
- ▶ Striktes Sicherheitsregime/TOMs
- ▶ Next Generation Firewall, sichere Authentisierung, Intrusion Detection System, Log Management System
- ▶ Regelmäßige Risikoanalysen, Penetration Tests und Schulungsmaßnahmen

Ihr Ansprechpartner für Fragen zum Datenschutz und zur Cloudsicherheit

3M HIS Datenschutzkoordinator
Philipp Barschkies
pbarschkies@mmm.com



Mehrwerte

Mehr als Spracherkennung:

- ▶ Qualitätssteigerung in der klinischen Dokumentation durch Echtzeithinweise zur Verbesserung der Prozesse und Abrechnung
- ▶ Effizienzsteigerung im Schreibbüro
- ▶ **Sicherung des Falls gegenüber dem Medizinischen Dienst**

Hochmoderne Technologie

Vorteile durch den Cloud-Einsatz:

- ▶ Zentrales Profil, Nutzung an jedem Arbeitsplatz
- ▶ Mobile Apps
- ▶ Sicherer 24 x 7 x 365-Betrieb
- ▶ Keine On-Premise-Kosten, skalierbar
- ▶ Entlastung der IT-Abteilung

Anwenderfreundlich

Alle Anwender sind eingebunden:

- ▶ Mehrstufiger Ansatz für integrierte Spracherkennung und -diktate
- ▶ Workflow-Unterstützung integriert im KIS, auch mobil
- ▶ Kein explizites Training erforderlich

- ▶ KHZG – förderfähig nach Tatbestand 3 „Digitale Pflege- und Behandlungsdokumentation“. Mit der Förderung Kosten sparen und die Digitalisierung vorantreiben.
- ▶ Ab 2022: Jede Einrichtung muss nach SGB V § 75c KRITIS den neusten Stand der Technik sicherstellen. Die 3M M*Modal Systeme werden jährlich auditiert und permanent aktuell gehalten (in den Bereichen Sicherheit, Technologie und Releasemanagement).



3M Medica
Zweigniederlassung der 3M Deutschland GmbH
Health Information Systems

Standort Neuss
Carl-Schurz-Straße 1 | 41453 Neuss
Telefon 02131 14 - 4241 | Telefax 02131 14 - 4242

Standort Berlin
Sophie-Charlotten-Straße 15 | 14059 Berlin
Telefon 030 326776-0 | Telefax 030 326776-77

drg-info@mmm.com
www.3M.de/HIS

Please recycle. Printed in Germany.
© 3M 2021. All rights reserved.