ENTSCHEIDERFABRIK

Academy of Health Information Management Executives

Sichere und Datenschutz konforme Messaging-Strategien für das Gesundheitswesen

Autoren

Dr. Pierre-Michael Meier

Dr. Pierre-Michael Meier ist hauptamtlicher Geschäftsführer und Dozent der Academy of Health Information Management Executives AHIME, Generalbevollmächtigter der Hospitalgemeinschaft Hosp.Do.IT und Geschäftsführer des Eco Systems ENTSCHEIDERFABRIK – der eHealth Inkubator.
In der Hospitalgemeinschaft und der ENTSCHEIDERFABRIK ist seine Aufgabe die Mitgliederbetreuung mit dem Fokus auf Digitalisierungs- und IT-Strategie.

Pierre-Michael Meier hält aufgrund seiner Erfahrung und Expertise von der Deutschen Gesellschaft für Informatik (GI) und der Deutschen Gesellschaft für Medizinische Informatik (GMDS) das Zertifikat „Medizinische Informatik", vom College of Health Information Management Executives (CHiME) das Zertifikat „Certified Healthcare CIO (CHCIO)" und von der AHIME das Zertifikat „Strategic Health-Information-Management Executive (SH-I-ME).
Der in Public Health promovierte Diplomkaufmann für internationales Krankenhaus-Management und Betriebsinformatik blickt auf eine leitende internationale Karriere bei Deloitte, Thyssen-Krupp, Siemens, Richard Wolf und März Internetwork Services zurück.
Seine beruflichen Schwerpunkte liegen in der Digitalisierungs- und IT-Strategie. Ferner ist er Lehrbeauftragter am Alfried Krupp von Bohlen und Halbach Stiftungslehrstuhl für Medizinmanagement von Prof. Dr. J. Wasem an der Universität Duisburg-Essen.
Pierre-Michael Meier engagiert sich ehrenamtlich für die Digitalisierung im deutschen Gesundheitswesen. Er ist EVP und CFO der Association of Health Information Management e.V., MarCom Chair und Vorstand von IHE Europe, Secretary der IT Gruppe des Europäischen Verbandes der Krankenhausmanager und Mitglied in weiteren Verbänden wie BVMI, GMDS, etc.

Impressum

Herausgeber

AHIME Academy of Health Information Management Executives

Rochusweg 8
41516 Grevenbroich

Tel: +49(0)21 82 - 88 65 06 6
Fax: +49(0)21 82 - 88 65 38 2

pierre-michael.meier@ahime.eu
www.ahime.eu

Redaktion

Dr. Pierre-Michael Meier (V.i.S.d.P),
pierre-michael.meier@ahime.eu

Prof. Dr. Gregor Hülsken,
gregor.huelsken@terraconnect.de

Flynn Herbst,
flynn.herbst@terraconnect.de

Anzeigen
Ines Grube, ines.grube@guig.org

Layout

DTP-Büro, Holzmann Medien GmbH & Co. KG, Gewerbestraße 2,
86825 Bad Wörishofen

Druck
Silber Druck oHG, Otto-Hahn-Straße 25,
34253 Lohfelden

Bildnachweise
Titel: Michael Traitov – adobestock.com

Prof. Dr. Gregor Hülsken

Prof. Dr. Gregor Hülsken ist hauptamtlicher Dozent für Wirtschafts- und Medizininformatik an der FOM Hochschule für Oekonomie & Management in Essen, Geschäftsführer und Dozent der Academy of Health Information Management Executives (AHIME) AUIG GmbH. Er ist Gesellschafter der terraconnect GmbH & Co. KG, fungiert dort als Unternehmensberater im Gesundheitswesen mit dem Spezialbereich Digitalisierungs- und IT-Strategie.

Der gebürtige Dorstener ist seit 2001 Mitglied der Deutschen Gesellschaft für Medizinische Informatik (GMDS). Er qualifizierte sich weiter in der medizinischen Informatik und erwarb dort Zertifikate und Zusatzqualifikationen im Bereich der Krankenhaus-IT. Nach Studium und Promotion war er bis zum Wechsel an die FOM am Universitätsklinikum Münster zunächst als Arzt, später im IT-Management als Leiter der klinischen IT-Systeme tätig.

Seine beruflichen Schwerpunkte liegen in der strategischen Unternehmensberatung in der Gesundheitswirtschaft. Seine wissenschaftlichen Schwerpunkte liegen im Bereich E-Health, klinische Informationstechnologien, IT-Management und Digitalisierung im Gesundheitswesen.

Gregor Hülsken engagiert sich ehrenamtlich für die Digitalisierung im deutschen Gesundheitswesen. Er ist Vorsitzender der CCeSigG e.V., stellv. Leiter der AG KIS der GMDS und Mitglied im Akademiebeirat der DMEA.

Flynn Herbst

Flynn Herbst, B. Sc. verantwortet das Projektmanagment des Unternehmens terraconnect GmbH & Co. KG. Nach seinem Betriebswirtschaftsstudium an der Hochschule für angewandte Wissenschaften in Hamburg qualifizierte er sich für das Projektmanagement und erwarb 2023 das Prince-II-Foundation-Zertifikat. Er absolviert derzeit im dualen Studium seinen Masterstudiengang im IT-Management an der FOM in Münster.

AHIME Studie

Kommunikation im digitalen Zeitalter

Sichere Messaging-Strategien für das Gesundheitswesen

Im digitalen Zeitalter hat sich die Kommunikation im Gesundheitswesen grundlegend gewandelt, wobei sich sichere Messaging-Strategien als entscheidende Faktoren für eine effektive Zusammenarbeit und den Datenschutz herauskristallisiert haben. Vor dem Hintergrund einer zunehmenden Vernetzung von medizinischem Personal, Patienten und externen Partnern ist der Bedarf an schnellen, vertraulichen und zuverlässigen Kommunikationslösungen stetig gewachsen. Secure-Messenger-Dienste spielen daher eine zentrale Rolle, um die Qualität der Patientenversorgung sicherzustellen und gleichzeitig den Schutz sensibler Informationen zu gewährleisten.

Secure-Messenger-Dienste als Schlüssel zur beschleunigten Kommunikation und verbesserten Patientenversorgung im digitalen Zeitalter

Verschiedene Secure-Messenger-Dienste, die auf die Bedürfnisse von medizinischem Personal, Patienten und Partnern zugeschnitten sind, haben sich in den letzten Jahren im Gesundheitswesen etabliert. Ihre Bedeutung liegt in der Fähigkeit, den Informationsaustausch zu beschleunigen, ohne die Vertraulichkeit sensibler Daten zu gefährden – insbesondere angesichts der zunehmenden Digitalisierung von Patientenakten und dem vermehrten Einsatz elektronischer Kommunikationsmittel. Die Nutzung von Secure-Messenger-Diensten ermöglicht es medizinischen Fachkräften, schnell und unkompliziert wichtige Informationen wie Röntgenbilder und Laborergebnisse zu teilen, was letztendlich zu einer verbesserten Patientenversorgung führt, während gleichzeitig Datenschutz durch autorisierten Zugang und Ende-zu-Ende-Verschlüsselung gewährleistet wird.

Doch wie gestaltet sich die gegenwärtige Situation in den Krankenhäusern?

Im Kontext dieser Fragestellung präsentiert die AHIME Academy ihre aktuellen Forschungsergebnisse. Dabei wurden Umfragedaten von 180 Teilnehmern aus dem Gesundheitssektor gesammelt und ausgewertet, um ein umfassendes Bild über den Stand der Secure-Messenger-Dienste in Krankenhäusern zu erhalten. Die Umfrageergebnisse geben interessante Einblicke in die aktuelle Nutzung von Secure-Messenger-Diensten in Krankenhäusern und Gesundheitseinrichtungen. Es zeigt sich, dass nur 22 % der Mitarbeiter in Krankenhäusern daran gehindert werden, ihre persönlichen Geräte für die Kommunikation am Arbeitsplatz zu nutzen. Besonders das persönliche Smartphone wird von zwei Dritteln der Mitarbeiter für berufliche Aufgaben genutzt.

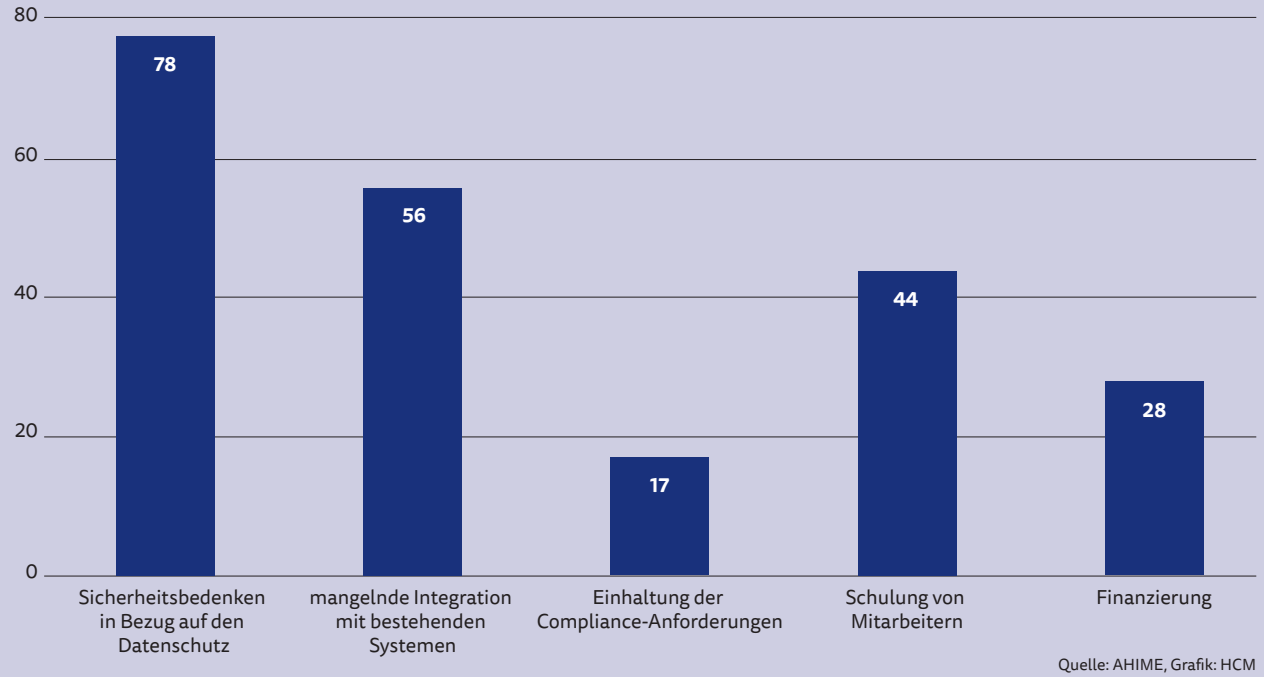
WhatsApp-Nutzung und fehlende Secure-Messaging-Strategien

Besorgniserregend ist, dass 28 % der Befragten in ihren Institutionen WhatsApp als Messenger nutzen, obwohl es nicht den Anforderungen des Datenschutzes und der Vertraulichkeit im Gesundheitswesen entspricht. Dies unterstreicht die Notwendigkeit einer klar definierten Secure-Messaging-Strategie, die sich auf Patienten, Mitarbeiter und Partner sowie Datenschutz und GDPR konzentriert. Die Umfrage zeigt, dass 50 % der Befragten angeben, dass ihre Institution noch keine solche Strategie implementiert hat. Dies weist auf ein großes Verbesserungspotenzial hin, um die Kommunikation im Gesundheitswesen sicherer und effizienter zu gestalten. Nur ein Drittel der befragten Mitarbeiter gab an, dass ihre Institution eine offizielle Plattform für mobiles Messaging und Zusammenarbeit eingerichtet oder aktiviert hat. Dies zeigt, dass in vielen Krankenhäusern und Gesundheitseinrichtungen noch Handlungsbedarf besteht, um den sicheren und effektiven Informationsaustausch über mobile Geräte zu gewährleisten.

Hoffnung auf TI-Messenger-Standards der gematik

Krankenhäuser setzen große Hoffnungen in die TI-Messenger-Standards der gematik, da sie eine sichere und effiziente Kommunikation im Gesundheitswesen versprechen. Durch die Implementierung dieser Standards können Zusammenarbeit und Patientenversorgung verbessert werden, während gleichzeitig Daten-

Welches sind die größten Herausforderungen, mit denen Sie im Zusammenhang mit Mobile Messaging und Zusammenarbeit im Gesundheitswesen konfrontiert sind, und wie haben Sie diese bewältigt?



Quelle: AHIME, Grafik: HCM

schutz und Vertraulichkeit gewährleistet bleiben. Die gematik-Standards stellen somit einen wichtigen Schritt zur Optimierung von Arbeitsabläufen in Krankenhäusern und Gesundheitseinrichtungen dar.

Interoperabilität als Schlüssel zur effektiven Kommunikation im Gesundheitswesen

Die Implementierung des TI-Messenger-Standards der gematik hat sich in der deutschen Gesundheitsversorgung als äußerst nützlich erwiesen, um die Secure-Messaging-Kommunikation zwischen den verschiedenen Akteuren zu verbessern. Laut Umfragen gaben eine große Mehrheit der Befragten an, dass der Einsatz dieser Standards sehr nützlich oder eher nützlich ist, während nur eine geringe Minderheit von 5 % angab, dass sie eher nicht nützlich seien.

Besonders wichtig ist dabei die Interoperabilität des TI-Messenger, da sie eine nahtlose Kommunikation zwischen verschiedenen Institutionen und Akteuren im Gesundheitswesen ermöglicht. Durch die Kompatibilität der verschiedenen Secure-Messenger-Dienste mit dem TI-Messenger-Standard der gematik können die Kommunikationswege effektiv gestaltet werden, was wiederum zu einer verbesserten Zusammenarbeit und Patientenversorgung führt.

Die Rolle von Secure-Messenger-Diensten in der Zukunft der digitalen Gesundheitsversorgung

Zusammenfassend lässt sich sagen, dass Secure-Messenger-Dienste eine wichtige Rolle in der Kommunikation im Gesundheitswesen spielen. Allerdings haben beliebte Messenger-Dienste wie WhatsApp gezeigt, dass sie nicht mit den Datenschutzrichtlinien des Gesundheitssektors vereinbar sind und daher als unsichere Kommunikationskanäle angesehen werden müssen.

Der TI-Messenger-Standard der gematik bietet eine vielversprechende Lösung für die sichere und effektive Kommunikation im Gesundheitswesen. Die Implementierung dieser Standards hat sich als äußerst nützlich erwiesen, um die Secure-Messaging-Kommunikation zwischen den verschiedenen Akteuren zu verbessern. Besonders wichtig ist dabei die Interoperabilität des TI-Messenger, da sie eine nahtlose Kommunikation zwischen verschiedenen Institutionen und Akteuren im Gesundheitswesen ermöglicht.

In Zukunft wird die Entwicklung und Implementierung von Secure-Messenger-Diensten eine immer wichtigere Rolle im Gesundheitswesen spielen, da sie eine schnelle und effiziente Kommunikation ermöglichen und gleichzeitig den Datenschutz gewährleisten. Krankenhäuser und Gesundheitseinrichtungen müssen sicherstellen, dass sie sichere und vertrauliche Kommunikationskanäle für ihre Mitarbeiter, Patienten und Partner haben, um eine optimale Patientenversorgung und Datenschutz zu gewährleisten.

AHIME Studie

Sicherer Datenaustausch im Gesundheitswesen

Handlungsrichtlinien für den Einsatz von Secure-Messaging-Diensten

Die vorliegende Studie untersucht die Auswirkungen der Nutzung von mobilen Messaging- und Kollaborationsplattformen auf die Risiken im Gesundheitswesen, insbesondere in Bezug auf Datenschutz, Datenverletzungen, Cyberangriffe und Nichteinhaltung von Vorschriften. Basierend auf einer Umfrage unter einer breiten Palette von Gesundheitsdienstleistern wurden verschiedene Aspekte der Nutzung von mobilen Messaging- und Kollaborationsplattformen untersucht, darunter die Einführung von Plattformen, Schulungen der Mitarbeiter, Sicherheitsrichtlinien und -verfahren, Compliance-Unterstützung, Ende-zu-Ende-Verschlüsselung und mobile Funktionen. Die Ergebnisse der Studie bieten einen Einblick in die Praktiken und Bedenken im Zusammenhang mit der Nutzung von mobilen Messaging- und Kollaborationsplattformen im Gesundheitswesen und liefern wichtige Informationen für die Verbesserung von Datenschutz und Compliance.

Datensicherheit bei der Nutzung von privaten Endgeräten im Krankenhaus

Datensicherheit stellt eine der größten Herausforderungen für die Nutzung von mobilen Messaging- und Kollaborationsplattformen im Gesundheitswesen dar. Eine wichtige Frage, die sich in diesem Zusammenhang stellt, ist, auf welchen Endgeräten eine solche Plattform betrieben werden kann. Krankenhäuser müssen sicherstellen, dass ihre Plattform auf Servern oder in der Cloud betrieben wird, die den höchsten Sicherheitsstandards entsprechen. Bring-your-own-device(BYOD)-Richtlinien für private Geräte sind kaum möglich, da es schwer ist, eine effektive Kontrolle über die Datensicherheit dieser Geräte zu gewährleisten. Es besteht das Risiko, dass private Geräte gehackt oder gejailbreakt werden und dadurch die Datensicherheit gefährdet wird. Es gibt nur wenige Vorschriften für private Geräte im Gesundheitswesen, die umgesetzt werden können, um die Sicherheit von Patientendaten zu gewährleisten. Die Einhaltung von Datensicherheitsstandards muss für Organisationen im Gesundheitswesen oberste Priorität haben, um das Vertrauen der Patienten zu erhalten.

Herausforderungen bei der Etablierung mobiler Geräte im Gesundheitswesen: Fähigkeit, Akzeptanz und Kompetenz

Die Akzeptanz von neuen Technologien in der Arbeitswelt ist ein wichtiger Faktor für den Erfolg einer Implementierung. In unserer Studie haben wir festgestellt, dass nicht alle Mitarbeiter in der Gesundheitsbranche mit Smartphones ausgestattet sind. Insbesondere ältere Mitarbeiter nutzen häufig noch traditionelle Kommunikationswege wie Festnetztelefone oder Faxgeräte. Ein Generationenwechsel innerhalb der Belegschaft führt jedoch dazu, dass immer mehr Mitarbeiter mit Smartphones arbeiten.

Es ist jedoch nicht nur wichtig, dass Mitarbeiter mit den entsprechenden Geräten ausgestattet sind, sondern auch, dass sie in der Lage und bereit sind, damit zu arbeiten. Eine hohe Akzeptanz und Kompetenz bei der Nutzung von mobilen Messaging- und Kollaborationsplattformen ist entscheidend für die erfolgreiche Umsetzung einer solchen Strategie. Es ist daher notwendig, Schulungsprogramme und Trainingsmaßnahmen für die Mitarbeiter zu entwickeln, um sicherzustellen, dass sie die notwendigen Fähigkeiten besitzen, um effektiv mit den Geräten und Plattformen zu arbeiten.

Risiken der Nutzung persönlicher Geräte in der Gesundheitsbranche

Die Nutzung persönlicher Endgeräte in der Gesundheitsbranche zur Übertragung und Speicherung von personenbezogenen Daten ist ein wichtiger und gleichzeitig kontrovers diskutierter Aspekt. Die Ergebnisse unserer Studie zeigen, dass eine beträchtliche Anzahl von Mitarbeitern ihre eigenen Geräte für geschäftliche Zwecke nutzt. Dies kann zu einem Risiko für den Datenschutz und die Vertraulichkeit der Patientendaten führen. Insbesondere wenn es um die Übertragung von sensiblen Daten geht, wie zum Beispiel medizinischen Diagnosen oder Behandlungsplänen, müssen alle beteiligten Parteien besondere Vorsicht walten lassen.

In Anbetracht der potenziellen Risiken für den Datenschutz, die mit der Nutzung persönlicher Endgeräte in der Gesundheitsbranche verbunden sind, ist es unerlässlich, dass Institutionen und Organisationen entsprechende Richtlinien und Verfahren implementieren, um sicherzustellen, dass Patientendaten sicher und geschützt bleiben. Die Sensibilisierung der Mitarbeiter für Datenschutz und DSGVO-Vorschriften ist ebenfalls von entscheidender Bedeutung, um ein hohes Maß an Sicherheit und Vertraulichkeit zu gewährleisten.

Die Rolle von Secure-Messenger-Diensten im Strukturwandel des Krankenhauses

Secure-Messenger-Dienste unterstützen den Übergang von einem Strukturkrankenhaus zu einem Prozesskrankenhaus, indem sie eine schnelle, effektive und sichere Kommunikation zwischen den Mitarbeitern ermöglichen. Die Nutzung von Secure-Messenger-Diensten fördert die flexible Zusammenarbeit und ermöglicht einen effizienteren Workflow im Krankenhaus. Darüber hinaus gewährleistet die End-to-End-Verschlüsselung, dass sensitive Informationen sicher ausgetauscht werden können, ohne den Datenschutz zu verletzen.

Ein weiterer Vorteil von Secure-Messenger-Diensten ist ihre Mobilität. Da viele Mitarbeiter heutzutage mobil arbeiten, können Secure-Messenger-Dienste auch auf mobilen Geräten genutzt werden. Dies ermöglicht den Mitarbeitern, auch außerhalb des Krankenhauses schnell und sicher miteinander zu kommunizieren und Informationen auszutauschen.

TIM als gemeinsame Plattform für Messenger-Dienste und IT-Systeme im Gesundheitswesen

Bei der Betrachtung von internen Messenger-Diensten im Krankenhaus ist festzustellen, dass diese oft schon Teil der internen Kommunikationsstrategie sind. Mitarbeiter nutzen diese Dienste, um schnell und einfach miteinander zu kommunizieren und Informationen auszutauschen. Allerdings ist es wichtig zu prüfen, ob diese internen Messenger-Dienste auch mit der TI kompatibel sind und die Anforderungen an die Sicherheit und Vertraulichkeit von Patientendaten erfüllen. Hierbei sollten die Anforderungen der technischen Richtlinie für die Interoperabilität und den Datenaustausch im Gesundheitswesen berücksichtigt werden. Im Hinblick auf externe Messenger-Dienste, die krankenhausübergreifend genutzt werden können, gibt es einige Anbieter, die sich auf die speziellen Anforderungen im Gesundheitswesen konzentrieren. Diese Anbieter stellen sicher, dass die Dienste den Datenschutzbestimmungen entsprechen und die Übertragung von Patientendaten sicher ist. Eine Herausforderung hierbei ist jedoch, dass alle beteiligten Parteien (Krankenhäuser, Praxen, Krankenversicherungen) eine einheitliche Lösung nutzen müssen, um eine reibungslose Kommunikation und einen sicheren Datenaustausch zu gewährleisten. Hierbei kann die TIM (Telematikinfrastruktur für die Medizin) als gemeinsame Plattform dienen, auf der verschiedene Anbieter von Messenger-Diensten und andere IT-Systeme integriert werden können.

Unterstützung der Ambulantisierung: Secure Messaging als Schlüssel zur effektiveren ambulanten Versorgung

Die Ambulantisierung der Gesundheitswirtschaft wird oft als notwendiger Schritt angesehen, um die wachsende Nachfrage nach medizinischer Versorgung zu bewältigen. In diesem Zusammenhang werden auch neue Geschäftsmodelle im Gesundheitswesen diskutiert, die sich auf die ambulante Versorgung konzentrieren. Secure Messaging kann dabei helfen, diesen Wandel zu unterstützen und die ambulante Versorgung effektiver zu gestalten.

Secure Messaging kann eine wichtige Rolle bei der Zusammenarbeit zwischen medizinischen Fachkräften spielen, indem es eine schnel-

le und sichere Kommunikation ermöglicht. Insbesondere bei der ambulanten Versorgung, bei der die Zusammenarbeit zwischen verschiedenen Akteuren wie Ärzten, Krankenschwestern und Pflegediensten häufig erforderlich ist, können Secure Messaging-Dienste den Informationsaustausch erheblich vereinfachen.

Darüber hinaus können Secure Messaging-Dienste auch dazu beitragen, den Patienten in den Mittelpunkt der Versorgung zu stellen. Durch die Möglichkeit, schnell und effektiv mit medizinischen Fachkräften in Kontakt zu treten, können sich Patienten besser betreut fühlen und ihre Fragen und Bedürfnisse schnell und unkompliziert klären.

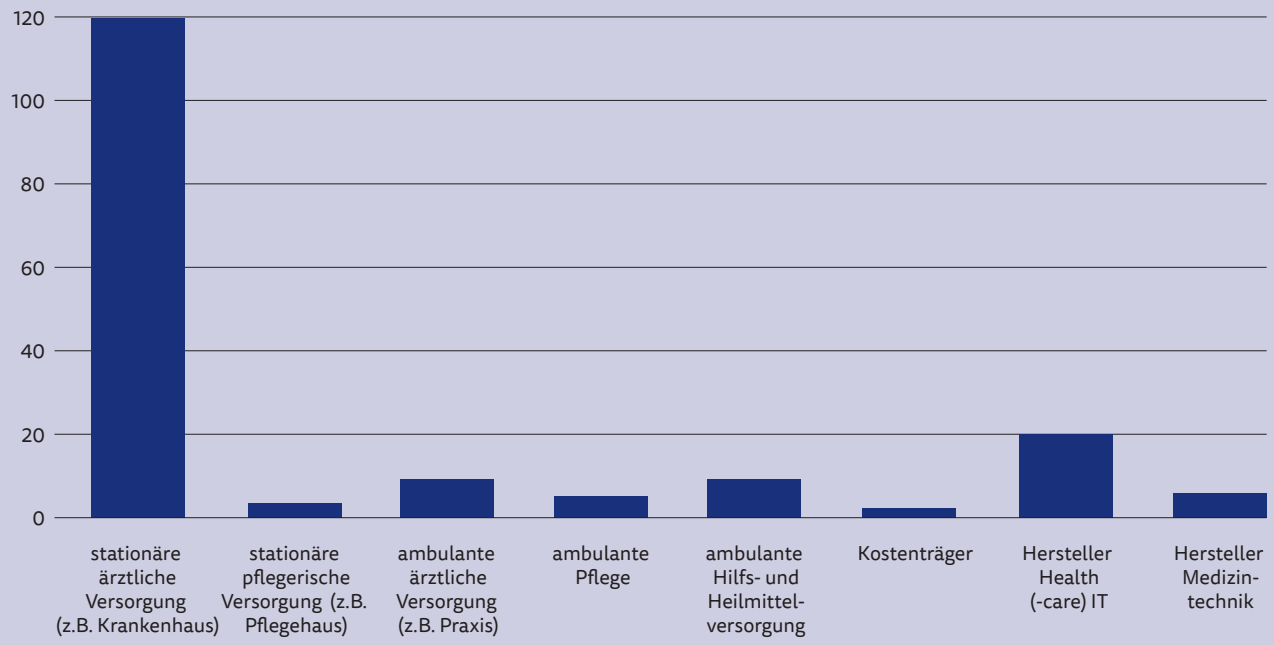
Schaffung einer einheitlichen und interoperablen Infrastruktur durch klare gesetzliche Rahmenbedingungen

Unsere Studie hat gezeigt, dass Secure Messaging-Dienste eine wichtige Rolle in der Gesundheitsbranche spielen. Basierend auf unseren Ergebnissen ziehen wir folgende Forderungen und Konsequenzen für die Gesundheitsbranche:

- Es ist unerlässlich, dass Institutionen und Organisationen klare Richtlinien und Verfahren implementieren, um sicherzustellen, dass Patientendaten sicher und geschützt bleiben, insbesondere wenn es um die Übertragung von sensiblen Daten geht.
- Die Sensibilisierung der Mitarbeiter für Datenschutz und DSGVO-Vorschriften ist ebenfalls von entscheidender Bedeutung, um ein hohes Maß an Sicherheit und Vertraulichkeit zu gewährleisten.
- Krankenhäuser und externe Leistungsbringer sollten sich auf eine einheitliche Lösung für externe Secure Messaging-Dienste einigen, um eine reibungslose Kommunikation und einen sicheren Datenaustausch zu gewährleisten.
- Secure Messaging-Dienste können auch dazu beitragen, den Patienten in den Mittelpunkt der Versorgung zu stellen, indem sie schnell und effektiv mit medizinischen Fachkräften in Kontakt treten können. Institutionen und Organisationen sollten daher sicherstellen, dass Secure Messaging-Dienste in die allgemeine Versorgungsstrategie integriert werden.
- Es ist auch wichtig, dass Krankenhäuser und Praxen sicherstellen, dass interne Messenger-Dienste mit der TI kompatibel sind und die Anforderungen an die Sicherheit und Vertraulichkeit von Patientendaten erfüllen, um einen reibungslosen Informationsaustausch innerhalb der Einrichtung zu gewährleisten.

Es ist dringend erforderlich, dass klare gesetzliche Rahmenbedingungen geschaffen werden, um sicherzustellen, dass die Übertragung und Speicherung von Patientendaten durch Secure Messaging-Dienste den Datenschutz- und Sicherheitsbestimmungen entspricht. Die Schaffung einheitlicher Standards und Richtlinien auf nationaler und internationaler Ebene kann dazu beitragen, dass Institutionen und Organisationen besser in der Lage sind, geeignete Secure Messaging-Lösungen auszuwählen und zu implementieren, die den Anforderungen an die Datensicherheit und Vertraulichkeit von Patientendaten entsprechen. Zudem kann dies dazu beitragen, eine einheitliche und interoperable Infrastruktur zu schaffen, die eine effektive Zusammenarbeit zwischen verschiedenen Akteuren im Gesundheitswesen ermöglicht.

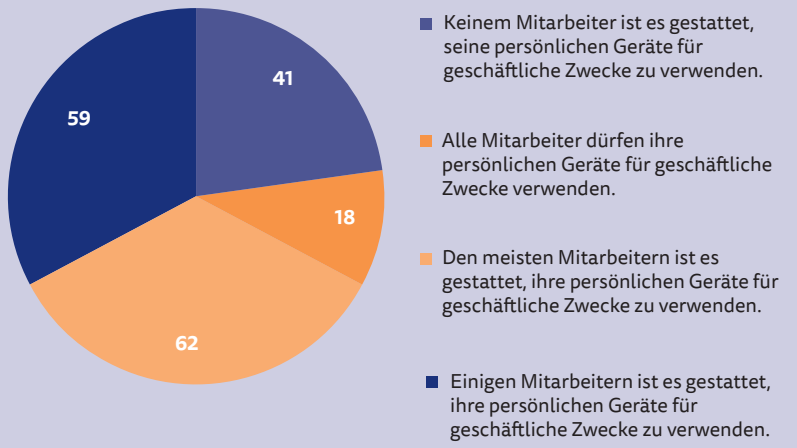
1. In welcher Branche sind Sie tätig?



Quelle: AHIME, Grafik: HCM

Die Mehrheit der Befragten, nämlich 120, ist in der stationären ärztlichen Versorgung tätig, gefolgt von 20 Personen, die bei Herstellern von Health(-care) IT arbeiten. Es gibt auch eine kleine Anzahl von Personen in der stationären pflegerischen Versorgung, ambulanten ärztlichen Versorgung, ambulanten Pflege, ambulanten Hilfs- und Heilmittelversorgung, Kostenträgern und Herstellern von Medizintechnik. Die unterschiedlichen Branchen in der Gesundheitsbranche zeigen die Vielfalt und Komplexität des Sektors und die Notwendigkeit von Technologien wie mobilen Messaging- und Kollaborationsplattformen, um effektive und effiziente Kommunikation und Zusammenarbeit zu ermöglichen.

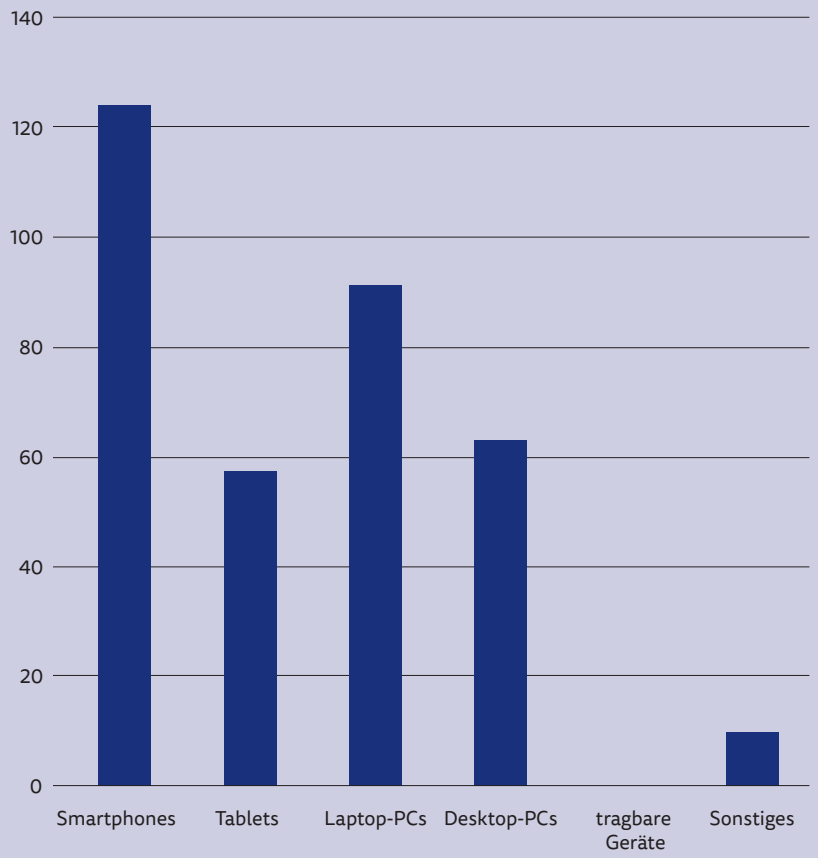
2. Welche der folgenden Optionen beschreibt am besten die Richtlinie Ihrer Organisation für die Nutzung persönlicher Geräte von Mitarbeitern für geschäftliche Zwecke?



Quelle: AHIME, Grafik: HCM

Basierend auf den Umfrageergebnissen scheint es, dass die meisten Organisationen ihren Mitarbeitern erlauben, ihre persönlichen Geräte für geschäftliche Zwecke zu nutzen, obwohl es auch eine bedeutende Anzahl von Organisationen gibt, die diese Praxis nicht erlauben. Es ist wichtig zu beachten, dass die Nutzung persönlicher Geräte für geschäftliche Zwecke bestimmte Risiken mit sich bringen kann, insbesondere in Bezug auf Datenschutz und Datensicherheit. Organisationen sollten klare Richtlinien und Verfahren haben, um sicherzustellen, dass die Verwendung persönlicher Geräte für geschäftliche Zwecke sicher und verantwortungsbewusst erfolgt und die Einhaltung der Datenschutzbestimmungen gewährleistet ist.

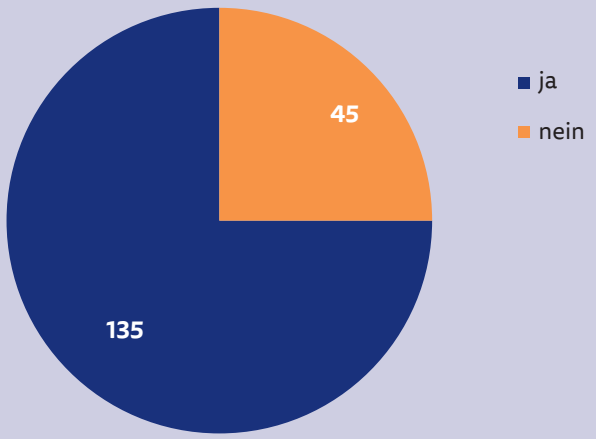
3. Welche ihrer privaten Geräte dürfen die Mitarbeiter Ihres Unternehmens für geschäftliche Zwecke nutzen?



Quelle: AHIME, Grafik: HCM

In der Gesundheitsbranche ist der Schutz von Patientendaten von höchster Priorität. Die Nutzung von privaten Geräten für geschäftliche Zwecke kann jedoch zu erheblichen Sicherheitsrisiken führen, da die Geräte möglicherweise nicht über die erforderlichen Sicherheitsvorkehrungen verfügen oder von unbefugten Personen zugänglich gemacht werden können. Aus diesem Grund ist es wichtig, dass Organisationen in der Gesundheitsbranche klare Richtlinien und Vorschriften für die Nutzung von privaten Geräten für geschäftliche Zwecke festlegen und sicherstellen, dass alle Mitarbeiter diese einhalten. Dies kann durch Schulungen, Überwachung und gezielte Maßnahmen zur Sicherung der Geräte erreicht werden. Es ist auch wichtig, dass die Organisation die Möglichkeit bietet, den Mitarbeitern geeignete geschäftliche Geräte zur Verfügung zu stellen, um die Sicherheit und den Datenschutz der Patientendaten zu gewährleisten.

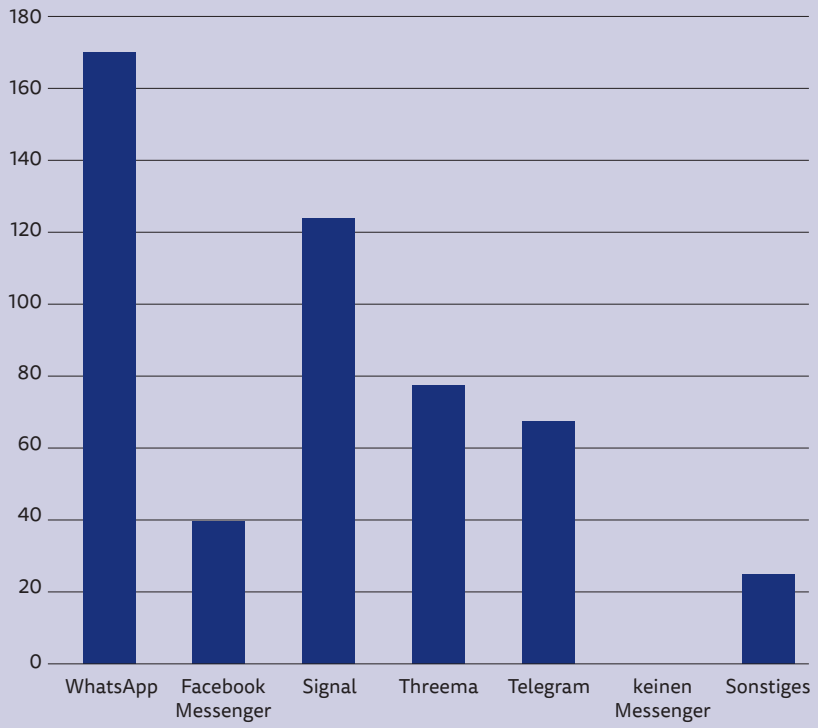
4. Verwenden die Mitarbeiter Ihrer Organisation mobile Nachrichten (SMS oder Textnachrichten über WhatsApp, iMessage, Andriod-Nachrichten usw.), um miteinander oder extern für geschäftliche Zwecke zu kommunizieren?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass eine große Anzahl von Organisationen mobile Nachrichten zur geschäftlichen Kommunikation einsetzt. Obwohl diese Art der Kommunikation oft schnell und praktisch ist, birgt sie auch Risiken für die Sicherheit und den Datenschutz von sensiblen Unternehmensinformationen. Es ist wichtig, dass Organisationen klare Richtlinien und Schulungen zur sicheren Nutzung von mobilen Messaging-Plattformen bereitstellen, um das Risiko von Datenschutzverletzungen zu minimieren und die Sicherheit ihrer Geschäftsdaten zu gewährleisten.

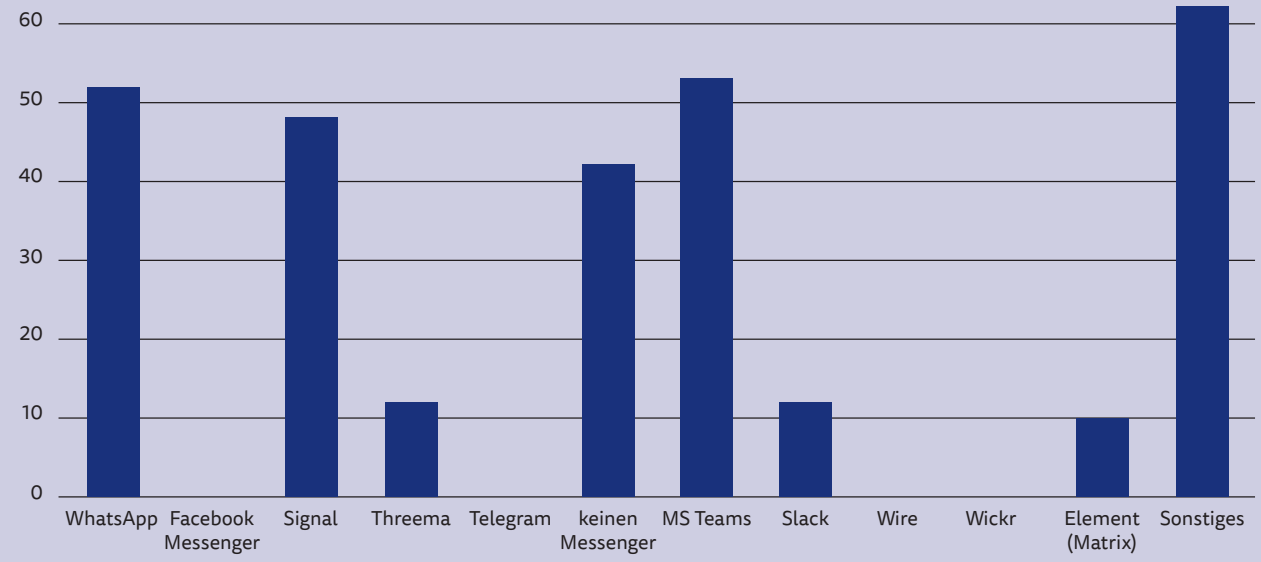
5. Welche der folgenden Messenger-Apps nutzen Sie auf Ihrem privaten Smartphone?



Quelle: AHIME, Grafik: HCM

Basierend auf den Umfrageergebnissen nutzen die meisten der Befragten WhatsApp auf ihrem privaten Smartphone, gefolgt von Signal und Threema. Es ist interessant zu sehen, dass trotz Bedenken hinsichtlich der Datenschutzpraktiken von WhatsApp immer noch viele Nutzer diese App bevorzugen. Allerdings gibt es auch eine beträchtliche Anzahl von Nutzern, die auf Alternativen wie Signal und Threema umgestiegen sind, um ihre Privatsphäre und Sicherheit zu schützen. Es ist zu beachten, dass eine beträchtliche Anzahl von Befragten keine Messenger-Apps auf ihrem privaten Smartphone nutzen. Möglicherweise haben sie Bedenken hinsichtlich der Sicherheit oder bevorzugen es, persönliche Gespräche von geschäftlichen Angelegenheiten zu trennen.

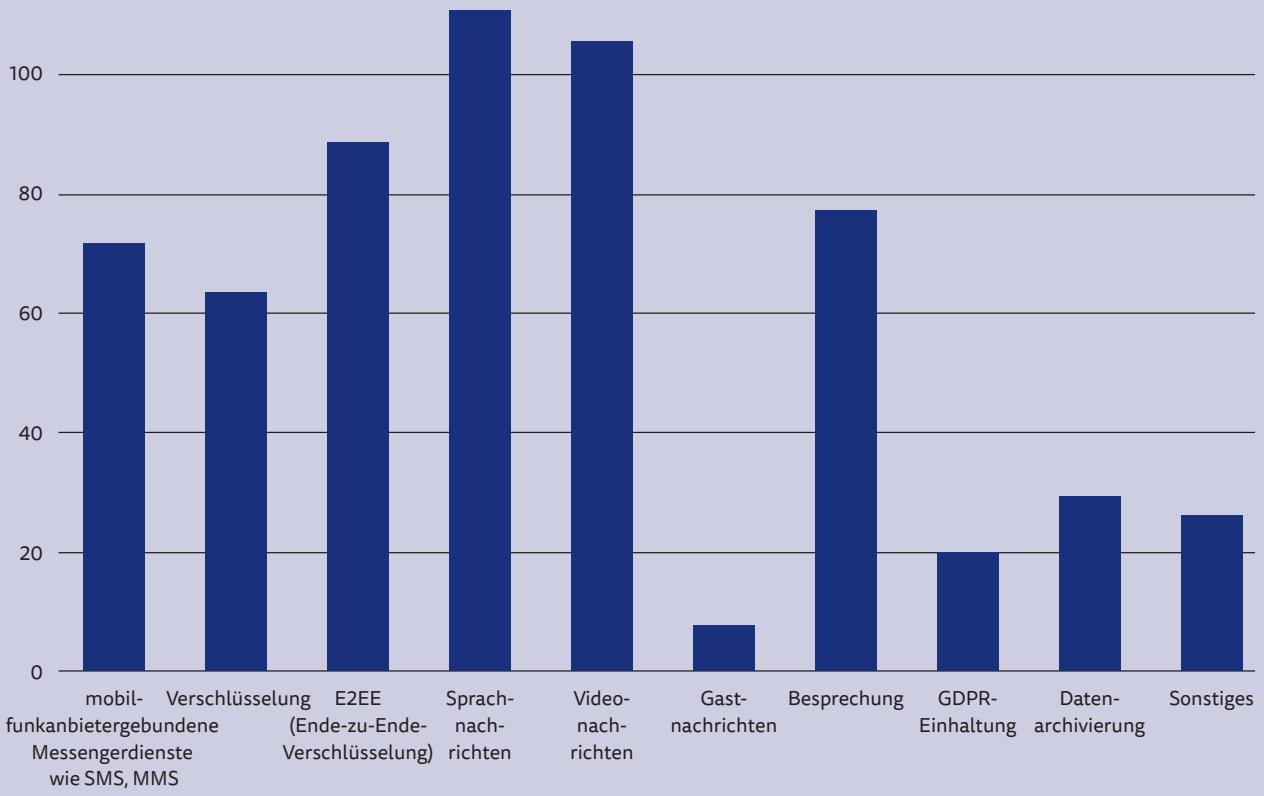
6. Welche Messaging-Anbieter setzen Sie derzeit für Ihre Institution ein?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass die Nutzung von Messaging-Anbietern in Institutionen weit verbreitet ist. Insbesondere WhatsApp und Microsoft Teams werden von vielen Befragten genutzt. Allerdings gibt es auch eine beträchtliche Anzahl von Institutionen, die keinen Messenger einsetzen. Es ist interessant zu sehen, dass Anbieter wie Signal, Threema und Element ebenfalls von einigen Institutionen genutzt werden, die möglicherweise einen höheren Wert auf Datenschutz und Verschlüsselung legen. Die Tatsache, dass viele Befragte „Sonstiges" angegeben haben, deutet darauf hin, dass es eine Vielzahl von Messaging-Anbietern gibt, die von Institutionen genutzt werden und dass es kein „one-size-fits-all"-Tool gibt, das für alle passt. Es ist wichtig, dass Institutionen bei der Auswahl eines Messaging-Anbieters ihre individuellen Bedürfnisse und Anforderungen berücksichtigen, einschließlich Datenschutz, Sicherheit und Interoperabilität mit anderen Systemen.

7. Welche der folgenden Funktionen bietet ihr derzeitiges Tool für Messaging/Teamzusammenarbeit?



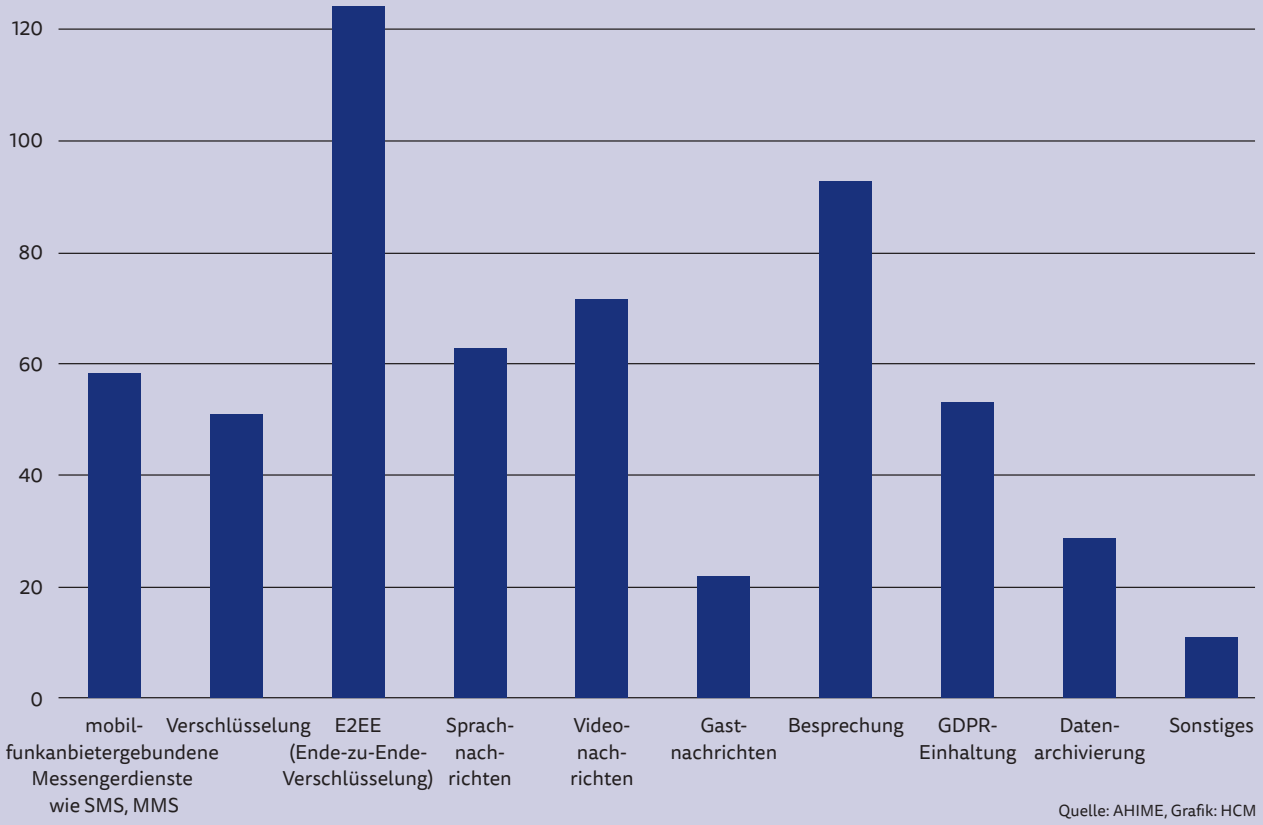
Quelle: AHIME, Grafik: HCM

Basierend auf den Umfrageergebnissen verwenden die meisten Organisationen mobile Messaging- und Kollaborationsplattformen, um die interne Kommunikation und Zusammenarbeit zu verbessern und die Produktivität zu steigern. Eine klare Schulung und Richtlinien für die sichere Nutzung von mobilen Messaging- und Kollaborationsplattformen sind von entscheidender Bedeutung, um Sicherheitsbedenken hinsichtlich des Datenschutzes und der Vertraulichkeit von Patientendaten zu minimieren. Die Einführung von Datenschutz- und Sicherheitsrichtlinien, die Schulung der Mitarbeiter und die Nutzung von Plattformen mit integrierten Sicherheits- und Compliance-Funktionen sind die am häufigsten genannten Schritte zur Minimierung der mit der Nutzung von mobilen Messaging- und Kollaborationsplattformen verbundenen Risiken.

Die Umfrageergebnisse zeigen auch, dass Ende-zu-Ende-Verschlüsselung für viele Organisationen von großer Bedeutung ist, um vertrauliche Unternehmensdaten, geistiges Eigentum und die Privatsphäre zu schützen. Die Einhaltung von Vorschriften und Compliance-Anforderungen bei der Verwendung von mobilen Messaging- und Kollaborationsplattformen wird durch die Implementierung von Sicherheitsrichtlinien und -verfahren, Schulungen und Sensibilisierung der Mitarbeiter sowie durch die Nutzung von Plattformen mit integrierter Compliance-Unterstützung gewährleistet.

Die Umfrageergebnisse zeigen auch, dass eine klare Mobile-Messaging-Strategie von großer Bedeutung ist, um Patienten, Mitarbeiter und Partner effektiv zu erreichen und die Produktivität zu steigern. Die Einrichtung einer offiziellen Plattform für mobiles Messaging und Zusammenarbeit sowie die Umsetzung einer umfassenden Mobile-Messaging-Strategie können dazu beitragen, Risiken im Zusammenhang mit Datenschutz, Datenverletzungen, Cyberangriffen und Nichteinhaltung von Vorschriften zu minimieren.

8. Welche der folgenden Funktionen bietet ihr derzeitiges Tool für Messaging/Teamzusammenarbeit?

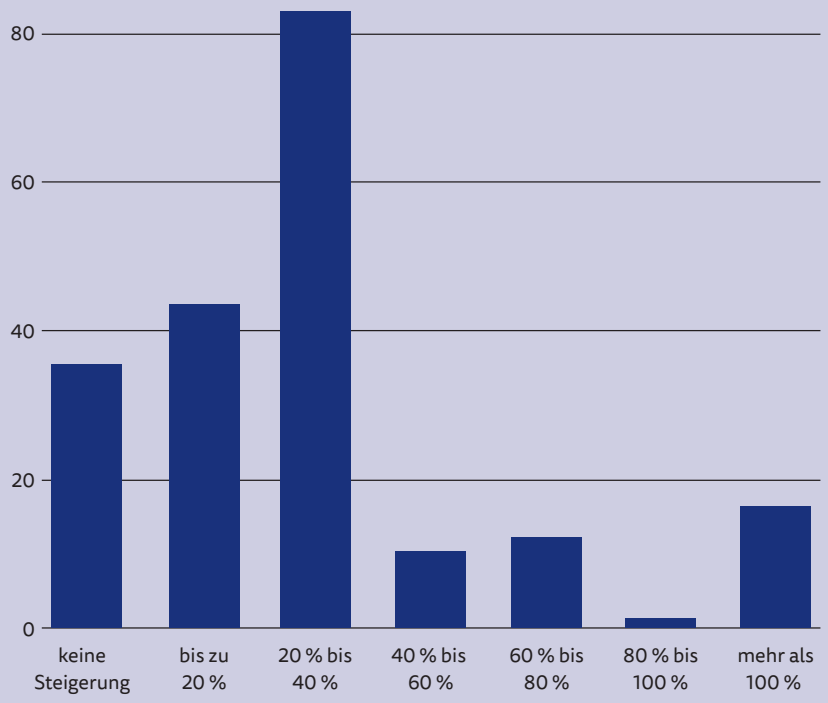


Quelle: AHIME, Grafik: HCM

Mobile Messaging ist heutzutage ein unverzichtbares Instrument für die Zusammenarbeit und die Interaktion zwischen Mitarbeitern und Institutionen. Die Ergebnisse der Umfrage zeigen, dass die meisten Befragten eine offizielle Plattform für mobiles Messaging und Zusammenarbeit eingerichtet haben oder in naher Zukunft planen, dies zu tun. Die Befragten haben verschiedene Maßnahmen ergriffen, um die Risiken im Zusammenhang mit der Nutzung von mobilen Messaging- und Kollaborationsplattformen zu minimieren. Die meisten Befragten gaben an, dass sie ihre Mitarbeiter regelmäßig in Bezug auf die sichere Nutzung von mobilen Messaging- und Kollaborationsplattformen schulen und Sicherheitsrichtlinien implementieren, um sicherzustellen, dass die Plattformen den Datenschutz- und Compliance-Anforderungen entsprechen.

Darüber hinaus zeigte die Umfrage, dass die Befragten eine Ende-zu-Ende-Verschlüsselung als wichtigen Faktor für den Schutz von vertraulichen Unternehmensdaten, geistigem Eigentum und der Privatsphäre ihrer Kunden betrachten. Eine klare mobile Messaging- und Kollaborationsrichtlinie sowie Schulungen für Mitarbeiter sind für eine angemessene Nutzung dieser Technologie entscheidend. Die Befragten schätzten die Produktivitätssteigerung durch die Nutzung von Messaging-Tools als signifikant ein. Die Umfrage ergab auch, dass die Einführung von Mobile-Messaging-Strategien in vielen Organisationen noch ausbaufähig ist und Verbesserungen benötigt werden. In Bezug auf mobile Funktionen zeigte die Umfrage, dass Ende-zu-Ende-Verschlüsselung, Videonachrichten und Besprechung als besonders wichtig erachtet werden. Die Ergebnisse zeigen, dass die meisten Befragten die Bedeutung von Datenschutz und GDPR-Einhaltung bei der Umsetzung von Mobile-Messaging-Strategien berücksichtigen und verschiedene Maßnahmen ergreifen, um Risiken im Zusammenhang mit der Nutzung von mobilen Messaging- und Kollaborationsplattformen zu minimieren.

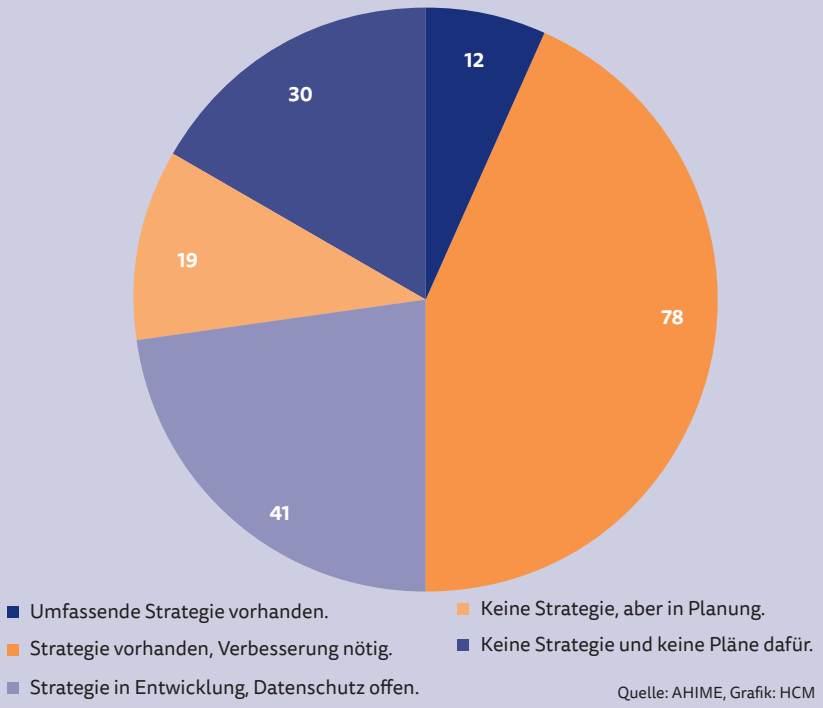
9. Wie hoch schätzen Sie die Produktivitätssteigerung ein, die Ihre Instuítution durch die Nutzung Ihres Messaging-Tools erfährt?



Quelle: AHIME, Grafik: HCM

Mobile Messaging-Tools sind in vielen Organisationen mittlerweile unverzichtbar geworden und können erheblich zur Steigerung der Produktivität beitragen. Unsere Umfrage hat gezeigt, dass die meisten Organisationen, die Messaging-Tools nutzen, eine Steigerung der Produktivität um 20 % bis 60 % verzeichnen. Eine kleine Minderheit (13 %) berichtet sogar von einer Steigerung um mehr als 60 %. Während es einige gibt, die keine signifikante Steigerung der Produktivität durch die Nutzung von Messaging-Tools feststellen, sind diese Fälle eher selten. Die Ergebnisse zeigen, dass Messaging-Tools ein wichtiger Faktor bei der Verbesserung der Arbeitsabläufe und der Produktivität in vielen Organisationen sind.

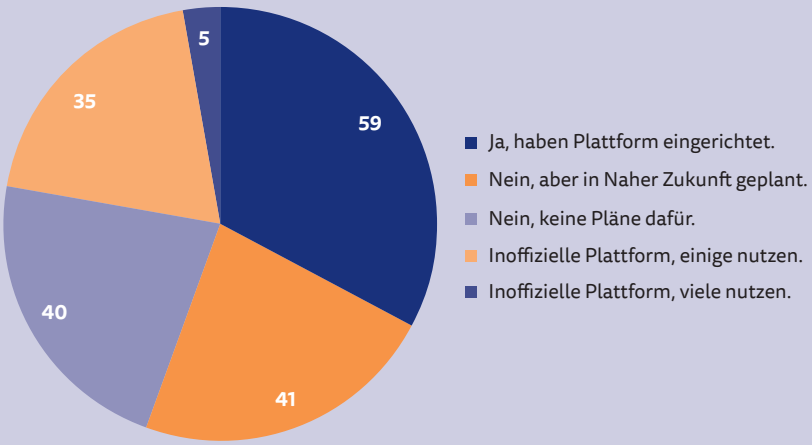
10. Wie steht Ihre Organisation bei der Umsetzung einer Mobile-Messaging-Strategie in Bezug auf Patienten, Mitarbeiter und Partner sowie Datenschutz und GDPR?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass viele Organisationen im Gesundheitswesen eine Mobile-Messaging-Strategie haben oder zumindest in der Planung sind. Es ist jedoch auch klar, dass es noch Verbesserungspotential gibt. Fast die Hälfte der Befragten gaben an, dass ihre Strategie in Entwicklung sei und der Datenschutz noch offen sei. Es ist wichtig zu betonen, dass eine umfassende Mobile-Messaging-Strategie nicht nur die Bedürfnisse von Patienten, Mitarbeitern und Partnern berücksichtigen muss, sondern auch den Datenschutz und die Einhaltung der GDPR. Organisationen sollten sicherstellen, dass ihre Strategie klar definiert ist und regelmäßig überprüft wird, um sicherzustellen, dass sie den sich schnell entwickelnden Bedrohungen im Bereich der Cybersicherheit gerecht wird.

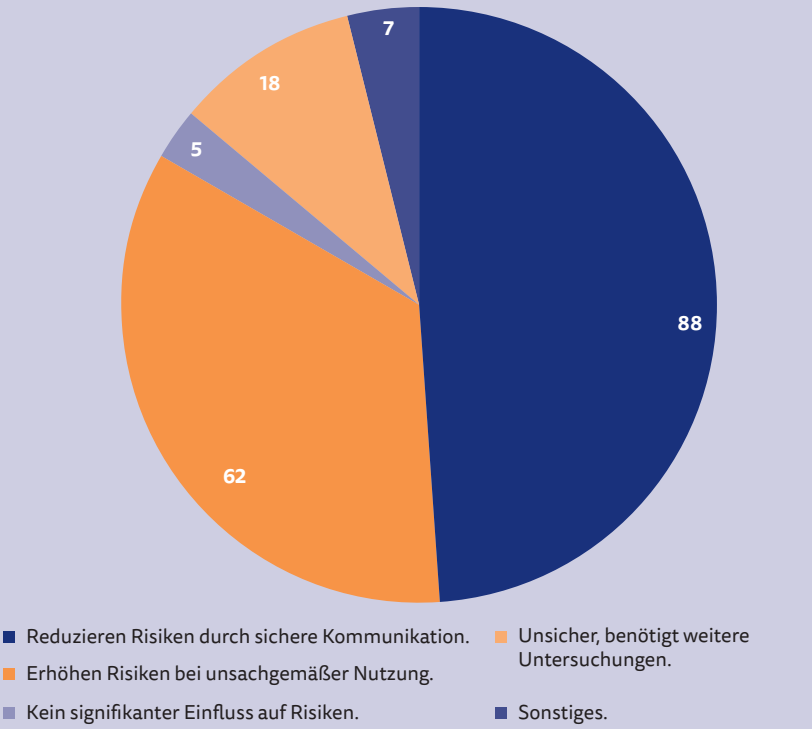
11. Haben Sie für Ihre Mitarbeiter eine offizielle Plattform für mobiles Messaging und Zusammenarbeit eingerichtet/aktiviert?



Quelle: AHIME, Grafik: HCM

Die Einrichtung einer offiziellen Plattform für mobiles Messaging und Zusammenarbeit kann die Arbeitsprozesse im Unternehmen verbessern und den Informationsfluss erleichtern. Unsere Umfrage hat gezeigt, dass knapp die Hälfte der Befragten eine solche Plattform bereits eingerichtet hat. Ein weiterer Teil plant dies in naher Zukunft zu tun, während andere keine Pläne dafür haben oder bereits eine inoffizielle Plattform nutzen. Eine inoffizielle Nutzung kann jedoch zu erhöhten Risiken bezüglich Datenschutz und -sicherheit führen. Es ist daher ratsam, eine offizielle Plattform einzurichten, um den Mitarbeitern eine sichere und geschützte Arbeitsumgebung zu bieten. Zudem sollten Schulungen und Sensibilisierungsmaßnahmen für eine korrekte Nutzung der Plattform sorgen.

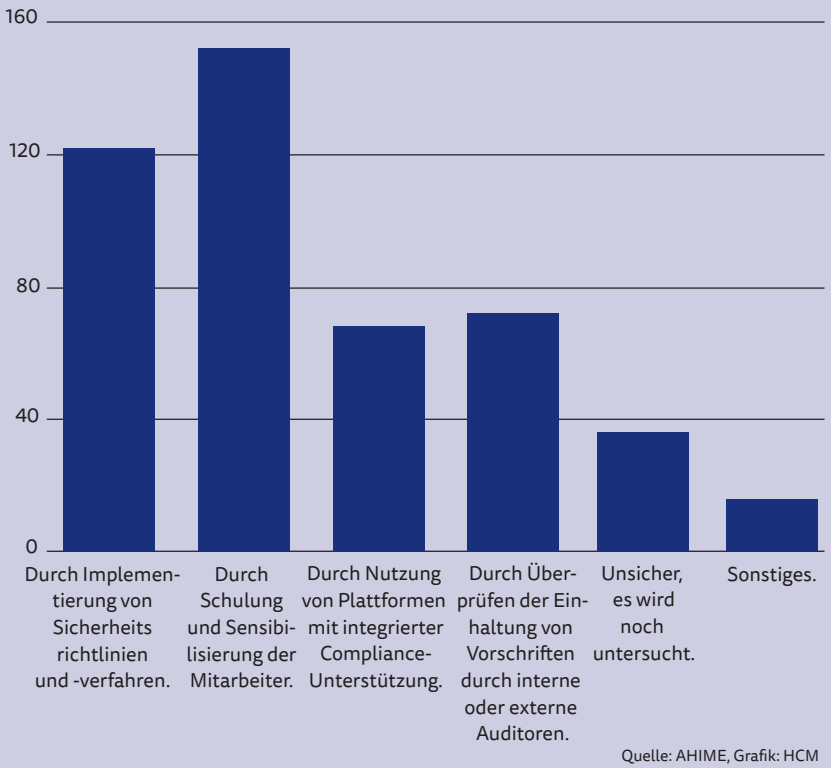
12. Wie beeinflussen mobile Messaging- und Kollaborationsplattformen die Risiken der digitalen Transformation im Gesundheitswesen, einschließlich Datenschutz, Datenverletzungen, Cyberangriffen und Nichteinhaltung von Vorschriften?



Quelle: AHIME, Grafik: HCM

Die Einführung mobiler Messaging- und Kollaborationsplattformen im Gesundheitswesen bringt viele Vorteile mit sich, wie beispielsweise die Möglichkeit einer effektiveren Kommunikation und Zusammenarbeit zwischen den medizinischen Fachkräften. Allerdings können diese Technologien auch mit Risiken verbunden sein, insbesondere im Hinblick auf Datenschutz, Datenverletzungen, Cyberangriffe und Nichteinhaltung von Vorschriften. Unsere Umfrage hat gezeigt, dass 88 Befragte glauben, dass mobile Messaging- und Kollaborationsplattformen Risiken reduzieren können, wenn sie sicher und angemessen genutzt werden. Auf der anderen Seite glauben 62 Befragte, dass eine unsachgemäße Nutzung zu einem erhöhten Risiko führen kann. Es ist wichtig zu beachten, dass mobile Messaging- und Kollaborationsplattformen allein nicht ausreichen, um Risiken zu minimieren, und dass eine klare Kommunikations- und Sicherheitsrichtlinie erforderlich ist, um sicherzustellen, dass Mitarbeiter geschult sind und die Technologie sicher und verantwortungsvoll nutzen. Es ist auch wichtig, dass Organisationen die geltenden Vorschriften und Bestimmungen einhalten und gegebenenfalls mit Experten zusammenarbeiten, um sicherzustellen, dass ihre Systeme sicher und geschützt sind.

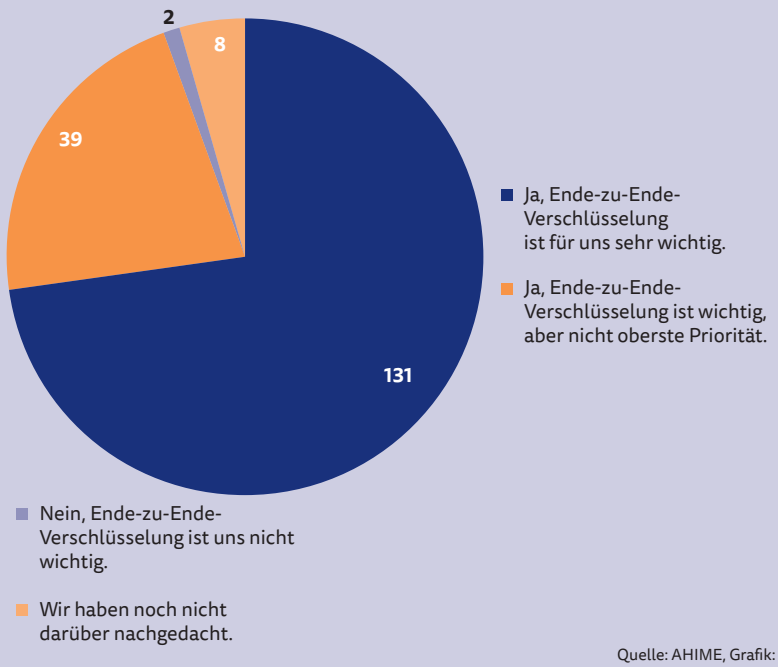
13. Wie wird die Einhaltung von Vorschriften bei der Verwendung von mobilen Messaging- und Kollaborationsplattformen sichergestellt?



Quelle: AHIME, Grafik: HCM

Anhand der Umfrageergebnisse wird deutlich, dass die Einhaltung von Vorschriften bei der Verwendung von mobilen Messaging- und Kollaborationsplattformen für viele Organisationen eine wichtige Rolle spielt. Die meisten Befragten gaben an, dass sie durch die Implementierung von Sicherheitsrichtlinien und -verfahren (122) sowie durch Schulungen und Sensibilisierung der Mitarbeiter (151) sicherstellen, dass die Compliance-Vorschriften eingehalten werden. Ebenfalls von Bedeutung ist die Nutzung von Plattformen mit integrierter Compliance-Unterstützung (68) sowie die Überprüfung der Einhaltung von Vorschriften durch interne oder externe Auditoren (70). Es ist jedoch auch wichtig anzumerken, dass einige Befragte unsicher sind und noch weitere Untersuchungen durchführen müssen, um sicherzustellen, dass sie die Compliance-Vorschriften einhalten (36). Insgesamt zeigen diese Ergebnisse, dass Organisationen verschiedene Methoden anwenden, um sicherzustellen, dass sie im Rahmen der Nutzung von mobilen Messaging- und Kollaborationsplattformen den Compliance-Vorschriften entsprechen.

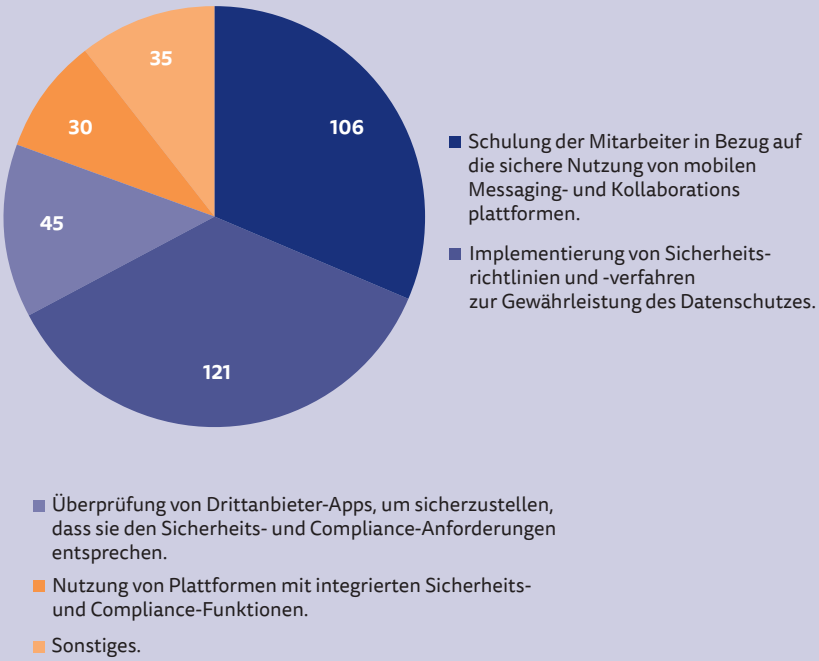
14. Ist eine Ende-zu-Ende-Verschlüsselung (E2EE) für Ihre Organisation wichtig, um vertrauliche Unternehmensdaten, geistiges Eigentum und die Privatsphäre zu schützen?



Quelle: AHIME, Grafik: HCM

Basierend auf den Ergebnissen der Umfrage scheint eine Ende-zu-Ende-Verschlüsselung für die Mehrheit der Organisationen von großer Bedeutung zu sein, um vertrauliche Unternehmensdaten, geistiges Eigentum und die Privatsphäre zu schützen. Eine große Anzahl von Befragten, nämlich 131, gab an, dass E2EE für sie sehr wichtig ist, während nur 2 sagten, dass es für sie nicht wichtig sei. 39 Befragte gaben an, dass E2EE wichtig sei, aber nicht oberste Priorität habe. Es ist zu beachten, dass einige Befragte (8) angaben, dass sie noch nicht darüber nachgedacht haben. Dies zeigt jedoch, dass die Sicherheit und der Schutz sensibler Informationen für viele Organisationen von großer Bedeutung sind. Unternehmen sollten daher darauf achten, dass ihre Kommunikationsplattformen eine starke E2EE-Verschlüsselung bieten und diese regelmäßig aktualisieren, um ihre Sicherheit zu gewährleisten.

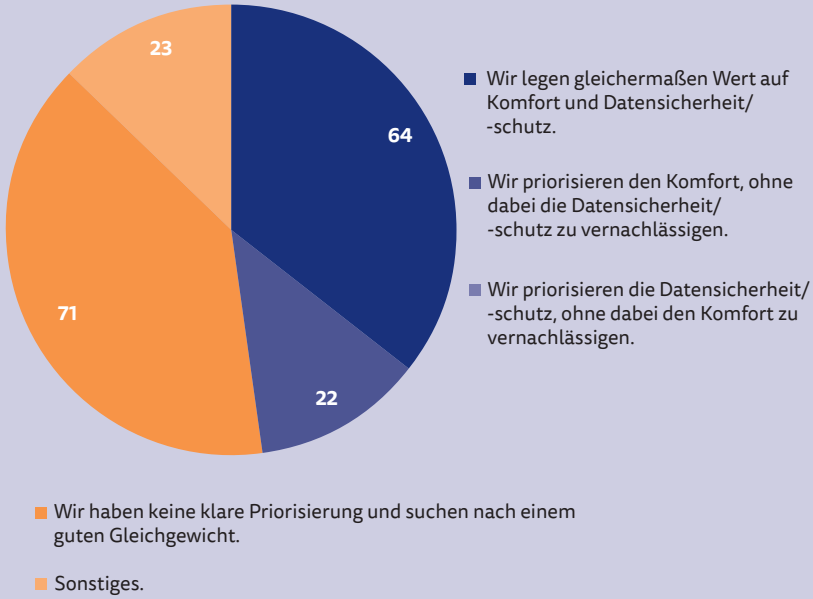
15. Welche Schritte wurden unternommen, um die mit der Nutzung dieser mobilen Messaging- und Kollaborationsplattformen verbundenen Risiken zu mindern?



Quelle: AHIME, Grafik: HCM

In Anbetracht der Risiken, die mit der Nutzung von mobilen Messaging- und Kollaborationsplattformen im Zusammenhang mit der Datensicherheit und dem Datenschutz verbunden sind, haben Unternehmen verschiedene Schritte unternommen, um diese Risiken zu mindern. Dazu gehören Schulungen für Mitarbeiter, um sicherzustellen, dass sie sichere Praktiken bei der Nutzung dieser Plattformen anwenden. Unternehmen haben auch Sicherheitsrichtlinien und -verfahren implementiert, um den Datenschutz zu gewährleisten, und Drittanbieter-Apps überprüft, um sicherzustellen, dass sie den erforderlichen Sicherheits- und Compliance-Anforderungen entsprechen. Einige Unternehmen haben Plattformen mit integrierten Sicherheits- und Compliance-Funktionen genutzt, um das Risiko von Datenschutzverletzungen zu minimieren. Es ist wichtig, dass Unternehmen in der heutigen digitalen Welt die erforderlichen Schritte unternehmen, um die Datensicherheit und den Datenschutz zu gewährleisten und gleichzeitig die Vorteile von mobilen Messaging- und Kollaborationsplattformen zu nutzen.

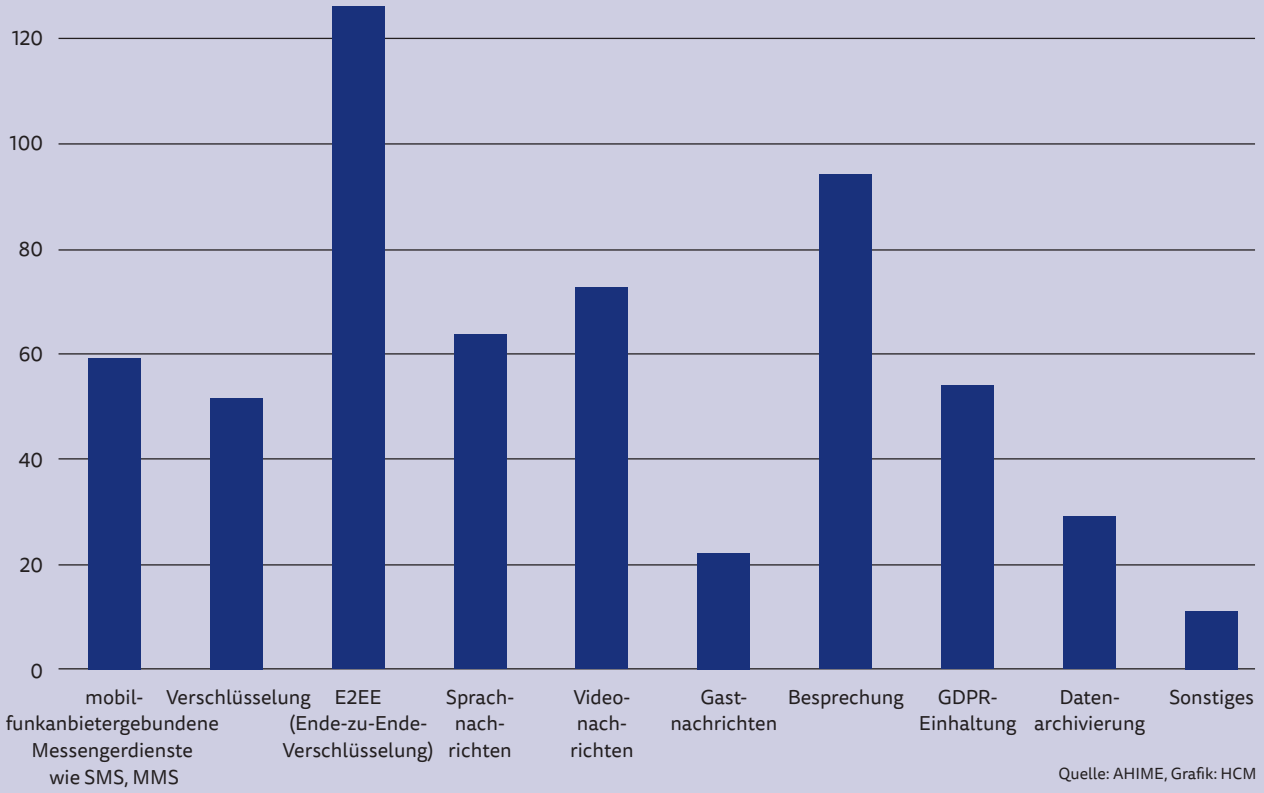
16. Wie wägen Sie den Komfort von Mobile Messaging mit den potenziellen Risiken für die Datensicherheit und den Datenschutz ab?



Quelle: AHIME, Grafik: HCM

Das Abwägen von Komfort und Sicherheit ist eine wichtige Frage, der sich Organisationen bei der Nutzung von Mobile Messaging und Kollaborationsplattformen stellen müssen. Es ist erfreulich zu sehen, dass die Mehrheit der Befragten gleichermaßen Wert auf Komfort und Datensicherheit und -schutz legt, da dies ein Hinweis darauf ist, dass die Organisationen sich der Bedeutung beider Faktoren bewusst sind. Einige Organisationen priorisieren jedoch entweder den Komfort oder die Datensicherheit und -schutz, was darauf hinweist, dass es noch Raum für Verbesserungen gibt. Es ist wichtig, dass Organisationen bei der Nutzung von Mobile Messaging und Kollaborationsplattformen ein ausgewogenes Verhältnis zwischen Komfort und Datensicherheit/ -schutz finden, um ein hohes Maß an Sicherheit und effektive Zusammenarbeit zu gewährleisten.

17. Welches sind die größten Herausforderungen, mit denen Sie im Zusammenhang mit Mobile Messaging und Zusammenarbeit im Gesundheitswesen konfrontiert sind und wie haben Sie diese bewältigt?



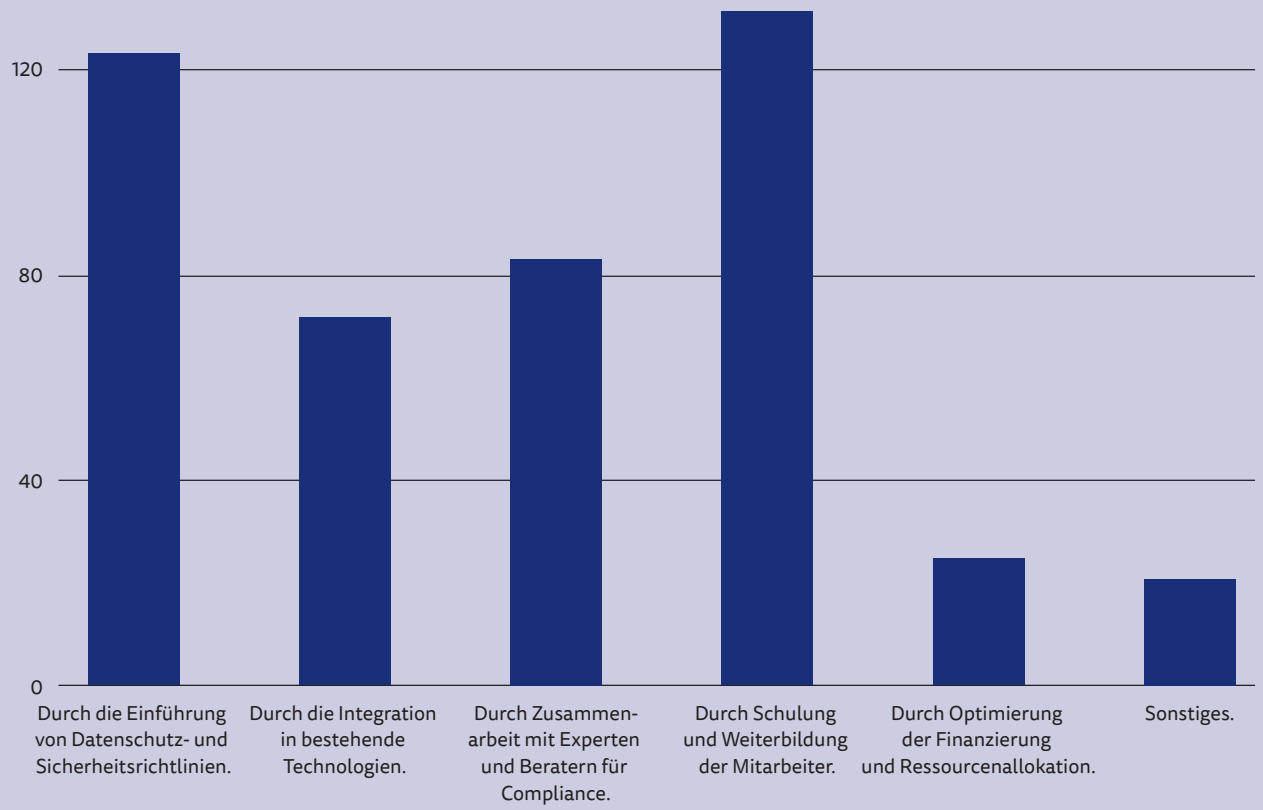
Quelle: AHIME, Grafik: HCM

Mobile Messaging und Zusammenarbeit sind wichtige Werkzeuge im Gesundheitswesen, um die Kommunikation und Koordination zwischen den verschiedenen Akteuren zu verbessern. Allerdings gibt es auch zahlreiche Herausforderungen, die bei der Einführung und Nutzung dieser Technologien auftreten können. Unsere Umfrage zeigt, dass Datenschutz- und Sicherheitsbedenken in Bezug auf Patientendaten eine der größten Herausforderungen darstellen. Es ist entscheidend, dass Organisationen klare Datenschutz- und Sicherheitsrichtlinien haben und sicherstellen, dass ihre Mitarbeiter in der sicheren Nutzung von mobilen Messaging- und Kollaborationsplattformen geschult sind.

Darüber hinaus kann es eine Herausforderung sein, mobile Messaging- und Kollaborationsplattformen in bestehende Systeme und Technologien im Gesundheitswesen zu integrieren. Hier kann eine enge Zusammenarbeit mit Experten und Beratern für Compliance helfen, um sicherzustellen, dass die Plattformen den geltenden Vorschriften und Compliance-Anforderungen entsprechen.

Eine weitere Herausforderung besteht darin, Mitarbeiter in Bezug auf die sichere und effektive Nutzung von mobilen Messaging- und Kollaborationsplattformen zu schulen. Hier können regelmäßige Schulungen und Schulungsprogramme für Mitarbeiter sowie schriftliche Richtlinien und Leitfäden zur Nutzung von Messaging- und Kollaborationsplattformen helfen. Schließlich ist es auch wichtig, eine angemessene Finanzierung und Ressourcenallokation sicherzustellen, um die Einführung und Nutzung von mobilen Messaging- und Kollaborationsplattformen im begrenzten Budget im Gesundheitswesen zu unterstützen.

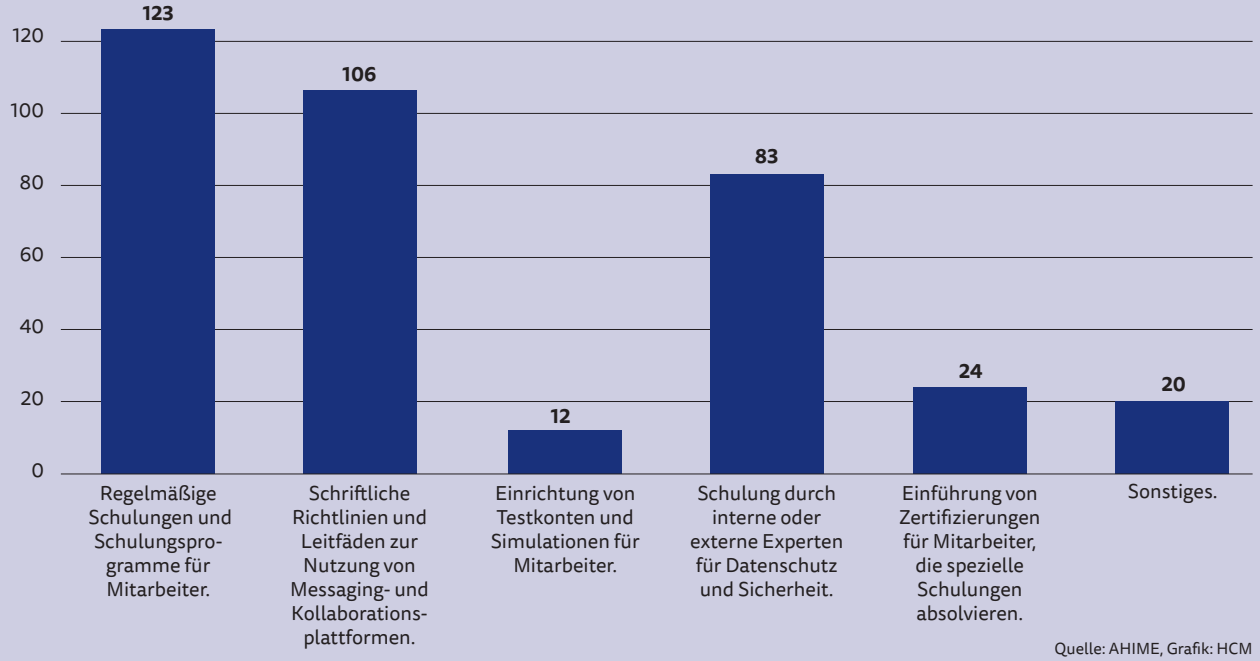
18. Wie haben Sie die oben genannten Herausforderungen bewältigt?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass Unternehmen und Organisationen Herausforderungen im Zusammenhang mit der Einführung von mobilen Messaging- und Kollaborationsplattformen auf unterschiedliche Weise bewältigen. Eine klare Mehrheit hat dabei auf Schulungen und Weiterbildungen der Mitarbeiter gesetzt, um sicherzustellen, dass diese die Plattformen angemessen nutzen können. Ebenfalls beliebt sind die Einführung von Datenschutz- und Sicherheitsrichtlinien sowie die Zusammenarbeit mit Experten und Beratern für Compliance. Es ist offensichtlich, dass es keine „Einheitslösung" für die Herausforderungen im Zusammenhang mit der Einführung von mobilen Messaging- und Kollaborationsplattformen gibt, sondern dass Unternehmen und Organisationen individuelle Strategien entwickeln müssen, die zu ihren spezifischen Bedürfnissen passen.

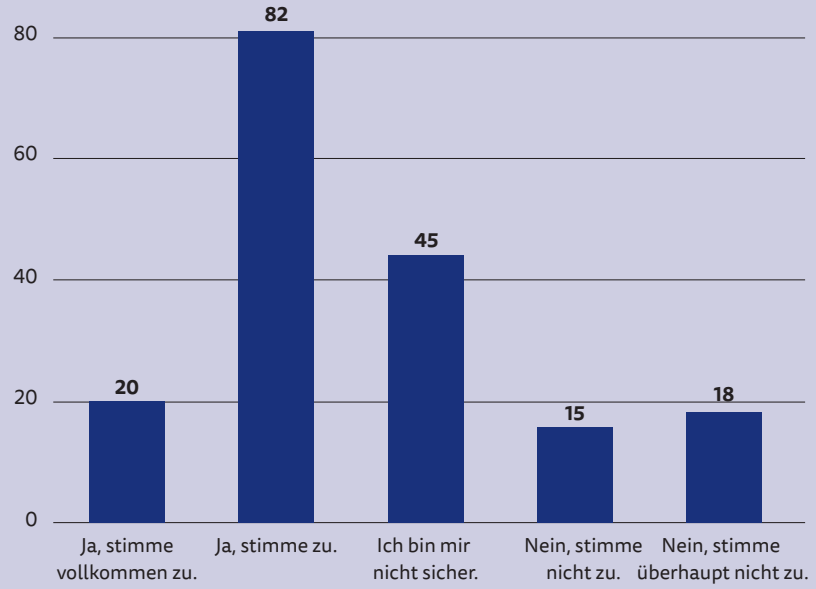
19. Wie stellen Sie sicher, dass Ihre Mitarbeiter in der angemessenen Nutzung von mobilen Messaging- und Kollaborationsplattformen geschult sind?



Quelle: AHIME, Grafik: HCM

Es ist wichtig sicherzustellen, dass Mitarbeiter in der angemessenen Nutzung von mobilen Messaging- und Kollaborationsplattformen geschult sind, um das Risiko von Datenschutzverletzungen und Sicherheitslücken zu minimieren. Die Umfrageergebnisse zeigen, dass regelmäßige Schulungen und Schulungsprogramme für Mitarbeiter sowie schriftliche Richtlinien und Leitfäden zur Nutzung von Messaging- und Kollaborationsplattformen die am häufigsten genutzten Methoden sind. Es ist jedoch auch wichtig, dass Schulungen durch interne oder externe Experten für Datenschutz und Sicherheit sowie die Einführung von Zertifizierungen für Mitarbeiter, die spezielle Schulungen absolvieren, in Betracht gezogen werden. Letztendlich ist es wichtig, dass Organisationen sicherstellen, dass ihre Mitarbeiter gut geschult sind, um ein hohes Maß an Datenschutz und Sicherheit zu gewährleisten.

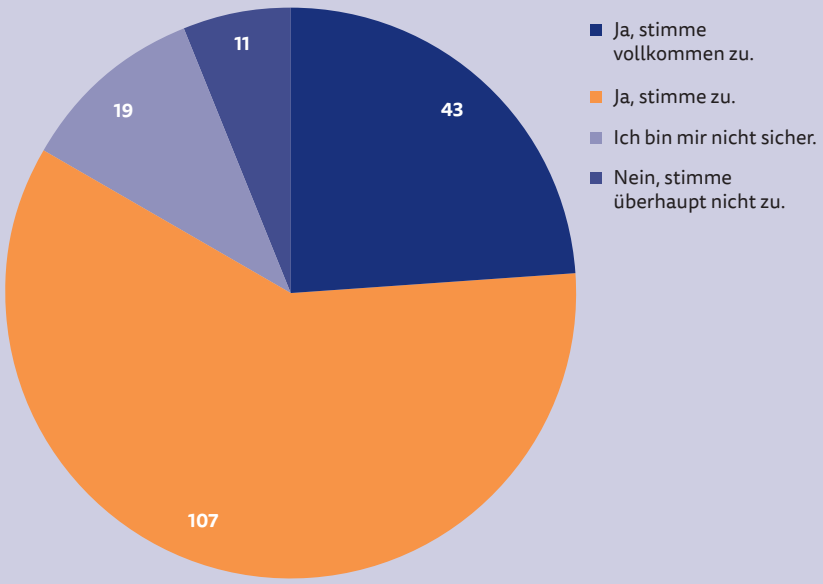
20. Kommunikationsplattformen sind die Grundlage für eine effektive Cybersicherheitsstrategie. Stimmen Sie zu?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass es unter den Befragten keine eindeutige Zustimmung gibt, dass Kommunikationsplattformen die Grundlage für eine effektive Cybersicherheitsstrategie darstellen. Während 20 Befragte (ca. 10 %) vollständig zustimmen und 82 (ca. 4 1%) zustimmen, gibt es auch 15 (ca. 7 %) Befragte, die nicht zustimmen und 18 (ca. 9 %) Befragte, die überhaupt nicht zustimmen. Es gibt jedoch auch 45 (ca. 23 %) Befragte, die sich nicht sicher sind, ob Kommunikationsplattformen die Grundlage für eine effektive Cybersicherheitsstrategie bilden. Dies zeigt, dass es in dieser Frage unterschiedliche Meinungen gibt und dass eine sorgfältige Prüfung der Vor- und Nachteile von Kommunikationsplattformen im Hinblick auf Cybersicherheitsstrategien notwendig ist.

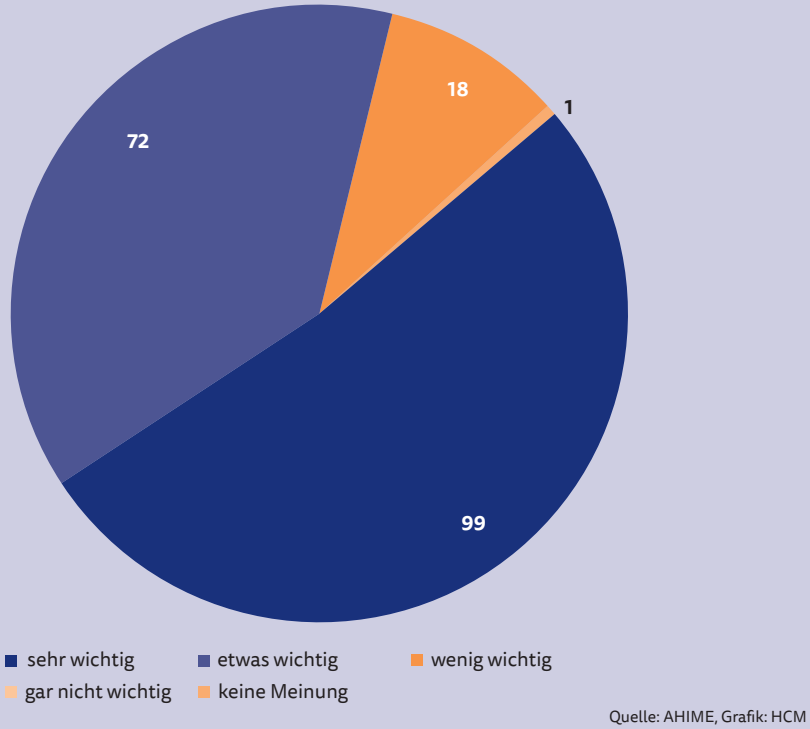
21. Kommunikationsplattformen sind von grundlegender Bedeutung für eine effektive digitale Transformation in einer Organisation. Stimmen Sie zu?



Quelle: AHIME, Grafik: HCM

Eine klare Mehrheit von 150 Befragten stimmte zu oder stimmte vollkommen zu, dass Kommunikationsplattformen von grundlegender Bedeutung für eine effektive digitale Transformation in einer Organisation sind. Dies unterstreicht die wichtige Rolle, die solche Plattformen bei der Verbesserung von Arbeitsabläufen und der Zusammenarbeit zwischen Mitarbeitern spielen können. Die 30 Befragten, die sich nicht sicher waren oder nicht zustimmten, könnten dazu beitragen, die Bedenken und Herausforderungen zu identifizieren, die bei der Implementierung von Kommunikationsplattformen auftreten können. Eine effektive Kommunikationsplattform sollte in der Lage sein, die Bedürfnisse und Anforderungen einer Organisation zu erfüllen und gleichzeitig den Datenschutz und die Sicherheit der Kommunikation zu gewährleisten.

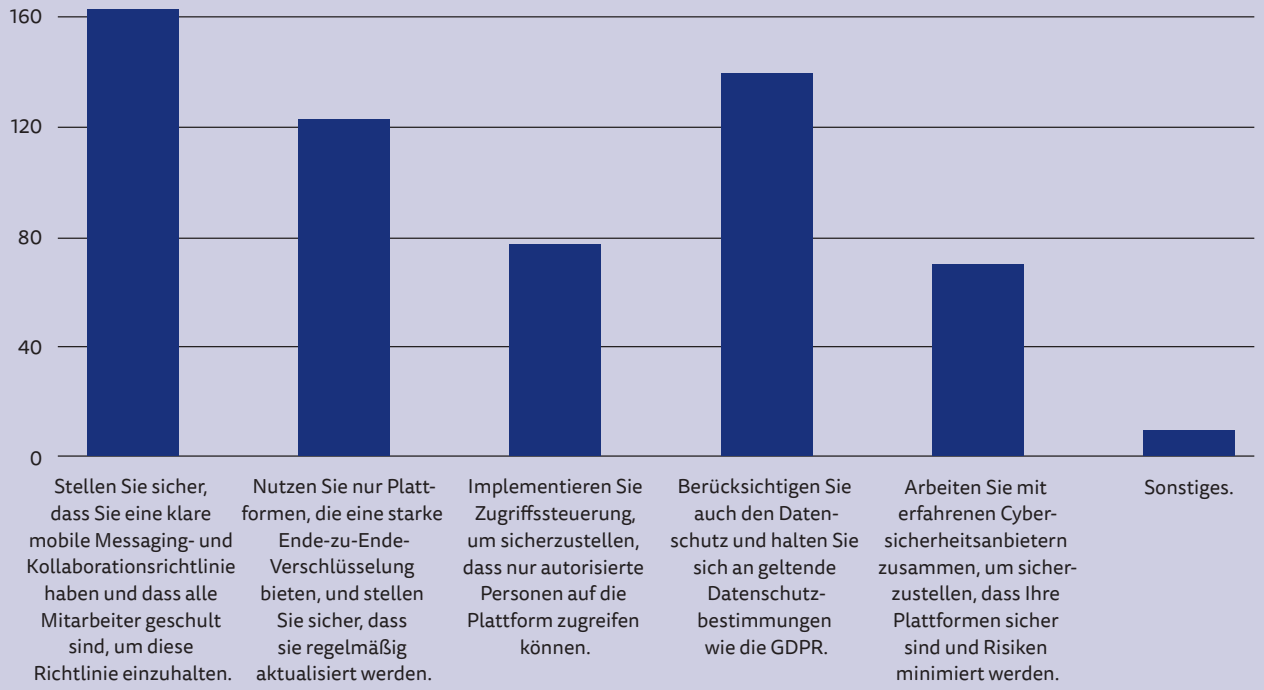
23. Wie wichtig ist es für das Krankenhaus, dass Secure-Messaging-Systeme mit anderen Systemen und Plattformen außerhalb des Krankenhauses interoperabel sind?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen deutlich, dass die Interoperabilität des Secure-Messaging-Systems im Krankenhaus einen hohen Stellenwert hat. Insbesondere die große Anzahl von Befragten (130), die die Interoperabilität des TI-Messenger-Standards als „sehr wichtig" einschätzen, unterstreicht die Bedeutung dieser Funktion für die Verbesserung der Patientenversorgung. Eine nahtlose Kommunikation zwischen verschiedenen Systemen und Plattformen außerhalb des Krankenhauses ist ebenfalls von hoher Relevanz, wie die Ergebnisse zeigen. Während die meisten Befragten die Interoperabilität als „sehr" oder „etwas" wichtig einschätzen, gibt es auch eine beachtliche Anzahl von Teilnehmern (18), die angeben, dass es für sie nur „wenig wichtig" ist. Es ist jedoch wichtig zu betonen, dass eine fehlende Interoperabilität zu Verzögerungen und Informationsverlusten führen kann, was wiederum die Qualität der Patientenversorgung beeinträchtigt. Daher sollte die Interoperabilität von Secure-Messaging-Systemen im Krankenhaus weiterhin ein wichtiges Anliegen sein, um die Effektivität und Effizienz der Gesundheitsversorgung zu verbessern.

22. Welchen Rat würden Sie anderen Organisationen außerhalb des Gesundheitswesens geben (Technologiebranche, Banken, börsennotierte Unternehmen, die vor ähnlichen Herausforderungen stehen), die mobile Messaging- und Kollaborationsplattformen einführen und gleichzeitig die damit verbundenen Risiken minimieren möchten?



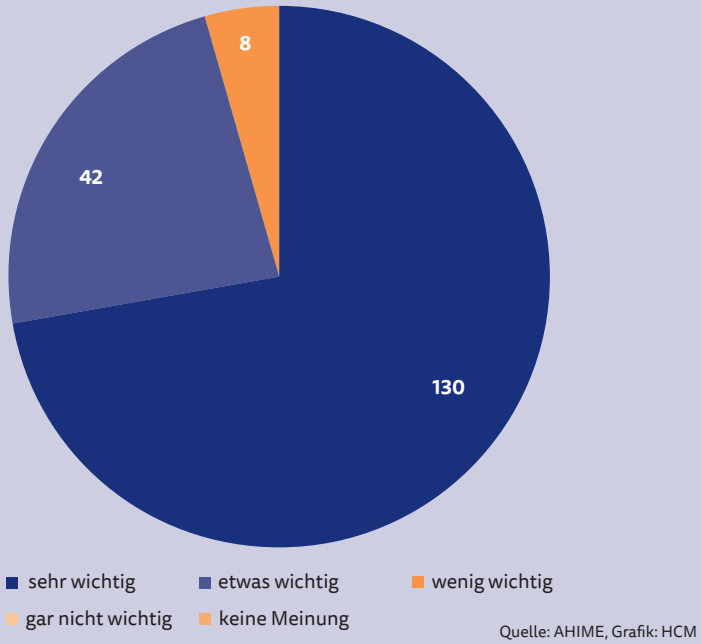
Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass klare mobile Messaging- und Kollaborationsrichtlinien sowie Schulungen für Mitarbeiter zur Einhaltung dieser Richtlinien von großer Bedeutung sind, um Risiken im Zusammenhang mit der Einführung von mobilen Messaging- und Kollaborationsplattformen zu minimieren. Darüber hinaus ist die Nutzung von Plattformen mit starker Ende-zu-Ende-Verschlüsselung und regelmäßigen Aktualisierungen sowie die Implementierung von Zugriffssteuerung zur Sicherstellung, dass nur autorisierte Personen auf die Plattform zugreifen können, wichtig.

Es ist auch entscheidend, dass Organisationen außerhalb des Gesundheitswesens, die mobile Messaging- und Kollaborationsplattformen einführen, den Datenschutz berücksichtigen und sich an geltende Datenschutzbestimmungen wie die GDPR halten. Zusammenarbeit mit erfahrenen Cybersicherheitsanbietern kann auch dazu beitragen, dass die Plattformen sicher sind und Risiken minimiert werden.

Die Ergebnisse der Umfrage zeigen, dass Organisationen außerhalb des Gesundheitswesens, die mobile Messaging- und Kollaborationsplattformen einführen möchten, von den Erfahrungen des Gesundheitswesens lernen können, um sicherzustellen, dass die Plattformen sicher und effektiv genutzt werden können. Eine klare Strategie und Schulungen für Mitarbeiter, die Verwendung von sicheren Plattformen, die Berücksichtigung des Datenschutzes und die Zusammenarbeit mit erfahrenen Cybersicherheitsanbietern sind Schlüsselfaktoren für den Erfolg.

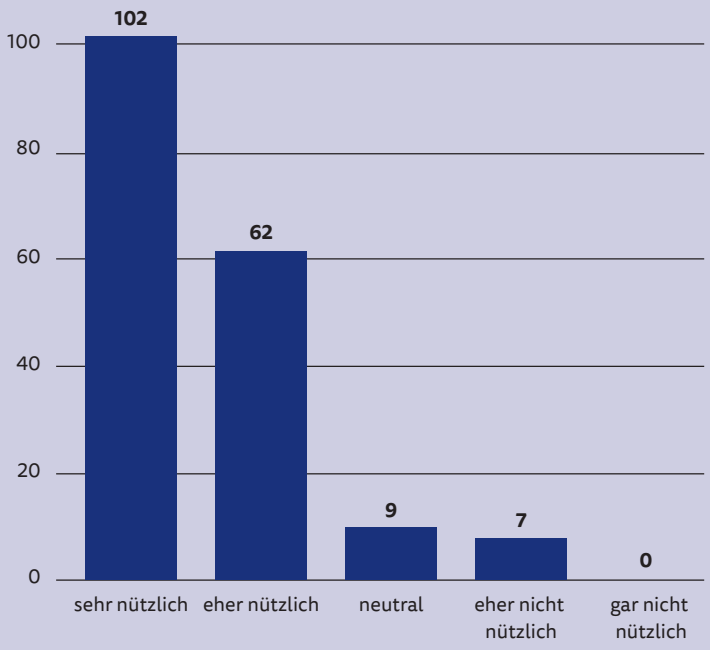
24. Inwiefern ist die Interoperabilität des TI-Messenger-Standards für Secure-Messaging im Krankenhaus für die Verbesserung der Patientenversorgung wichtig?



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen eindeutig, dass die Interoperabilität des TI-Messenger-Standards für Secure-Messaging im Krankenhaus als äußerst wichtig angesehen wird. Mehr als 75 % der Befragten gaben an, dass es für die Verbesserung der Patientenversorgung sehr wichtig oder zumindest etwas wichtig ist. Die Interoperabilität ermöglicht eine reibungslose Kommunikation und einen nahtlosen Datenaustausch zwischen verschiedenen Institutionen und Akteuren im Gesundheitswesen, was zu einer verbesserten Zusammenarbeit und letztendlich zu einer besseren Patientenversorgung führt. Durch die Kompatibilität von verschiedenen Secure-Messenger-Diensten mit dem TI-Messenger-Standard der gematik können Arbeitsabläufe und der Informationsaustausch innerhalb des Krankenhauses sowie zwischen verschiedenen Krankenhäusern und anderen Einrichtungen optimiert werden. Dadurch können beispielsweise Laborergebnisse oder Röntgenbilder schneller und effizienter ausgetauscht werden, was letztendlich die Diagnose und Behandlung von Patienten verbessert.
Es ist daher wichtig, dass Krankenhäuser und Gesundheitseinrichtungen die Implementierung des TI-Messenger-Standards vorantreiben und sicherstellen, dass die Interoperabilität gewährleistet ist. Nur so können sie eine effektive, sichere und vertrauliche Kommunikation zwischen verschiedenen Akteuren im Gesundheitswesen ermöglichen und eine optimale Patientenversorgung gewährleisten.

25. Bitte bewerten Sie den zukünftigen Nutzen des TI-Messenger Standards der gematik in Bezug auf die Verbesserung der Secure-Messaging-Kommunikation in der deutschen Gesundheitsversorgung:



Quelle: AHIME, Grafik: HCM

Die Umfrageergebnisse zeigen, dass der TI-Messenger-Standard der gematik in Bezug auf die Verbesserung der Secure-Messaging-Kommunikation in der deutschen Gesundheitsversorgung als äußerst vielversprechend angesehen wird. Über 80 % der Befragten bewerten den zukünftigen Nutzen des Standards als sehr nützlich oder eher nützlich. Dies deutet darauf hin, dass die Implementierung dieses Standards einen erheblichen Einfluss auf die effektive und sichere Kommunikation im Gesundheitswesen haben wird.
Die Bewertungen unterstreichen die Erwartungen der Krankenhäuser und Gesundheitseinrichtungen, die große Hoffnungen in den TI-Messenger-Standard der gematik setzen. Durch die Implementierung dieser Standards wird eine sichere und effektive Kommunikation zwischen den verschiedenen Akteuren im Gesundheitswesen ermöglicht, was letztendlich zu einer verbesserten Zusammenarbeit und Patientenversorgung führen wird. Die positiven Bewertungen der Befragten zeigen, dass der TI-Messenger-Standard der gematik als Lösung für die Herausforderungen im Bereich der Secure-Messaging-Kommunikation angesehen wird.
Es ist jedoch wichtig zu betonen, dass die Implementierung des TI-Messenger-Standards der gematik nicht ausreicht, um die Sicherheit und Effektivität der Kommunikation im Gesundheitswesen vollständig zu gewährleisten. Krankenhäuser und Gesundheitseinrichtungen müssen auch sicherstellen, dass ihre Mitarbeiter entsprechend geschult werden und dass Sicherheitsmaßnahmen wie Ende-zu-Ende-Verschlüsselung und autorisierter Zugang implementiert werden. Nur so kann eine umfassende und sichere Secure-Messaging-Kommunikation im Gesundheitswesen gewährleistet werden.

Verfügen Sie über eine sichere Messaging-Strategie für die Mitarbeiter und Patienten?

Mit der fortschreitenden Digitalisierung im Gesundheitswesen gewinnen sichere Messaging-Dienste in Krankenhäusern immer mehr an Bedeutung. Diese Dienste ermöglichen eine schnelle und effiziente Kommunikation zwischen Ärzten, Pflegekräften und anderen Fachkräften.

Die Nutzung von Consumer-Chat-Lösungen wie WhatsApp bedeutet mangelnde Kontrolle, ist nicht sicher und birgt erhebliche Risiken, insbesondere vor dem Hintergrund der EU-Datenschutzgrundverordnung (DSGVO).

NetSfere bietet die Lösung.

NetSfere
Führende konforme und sichere mobile Kommunikation & Kollaborationslösung für das Gesundheitswesen

MOBILITY PARTNER
ENTSCHEIDERFABRIK

EU DSGVO

WINNER
FROST & SULLIVAN
2023 BEST PRACTICES AWARD
GLOBAL SECURE MESSAGING SOLUTIONS

Um mehr zu erfahren, kontaktieren Sie uns unter sales@netsfere.com oder besuchen Sie www.netsfere.com/de