

Doctolib



Krisenresilienz in Kliniken und Praxen

Wo das deutsche Gesundheitswesen bei sicherer
Kommunikation und Notfallplänen steht.

Inhaltsübersicht

1. Zentrale Ergebnisse zur Krisenresilienz zusammengefasst
2. Was bedeutet Krisenresilienz im Gesundheitswesen?
3. Studiendesign und Methodik
4. Ergebnisse
5. Von den Studienergebnissen zu konkreten Handlungsfeldern

Arztpraxen und Kliniken müssen täglich unter hohem Zeitdruck handeln: Sie koordinieren Teams, treffen zeitkritische Entscheidungen und versorgen Menschen in besonderen Belastungssituationen.

Gerade in der Notaufnahme kann eine Verzögerung von wenigen Minuten den Behandlungserfolg beeinflussen. Doch auch in Praxen müssen medizinische Entscheidungen schnell und zuverlässig

abgestimmt werden. Eine sichere Kommunikation über mobile Endgeräte ist deshalb zentral: Nachrichten müssen unmittelbar, datenschutzkonform und an die richtigen Personen gelangen.

Wie gut das deutsche Gesundheitswesen auf solche Situationen vorbereitet ist, hat Doctolib in einer YouGov-Umfrage untersucht.



1. Zentrale Ergebnisse zur Krisenresilienz zusammengefasst

Das Gesundheitswesen verfügt über eine hohe Bereitschaft zu sicherer digitaler Kommunikation, aber vielerorts fehlen noch die strukturellen Voraussetzungen und die praktische Vorbereitung auf einen Ernstfall oder Notfall.

- 43 % der Klinikärzt:innen haben schon allgemeine Messenger wie WhatsApp für den beruflichen Austausch genutzt, 41 % der Praxisärzt:innen tun dies aktuell auch.
- 66 % der Klinikärzt:innen und 65 % der Praxisärzt:innen würden auf allgemeine Messenger verzichten, wenn es eine ebenso einfach nutzbare, zuverlässige, sichere Alternative auf dem eigenen Gerät gäbe.
- Übungen zum Ausfall digitaler Systeme finden bislang nur bei 35 % der Klinikärzt:innen und 21 % der Praxisärzt:innen statt.
- 84 % der Bevölkerung erwarten ausschließlich sichere und datenschutzkonforme Kommunikationslösungen.

2. Was bedeutet Krisenresilienz im Gesundheitswesen?

Krisenresilienz bedeutet, auch unter außergewöhnlichen Bedingungen (Notfällen, Stromausfall, Naturkatastrophen) handlungsfähig zu bleiben, sicher zu kommunizieren und die Versorgung der Patient:innen aufrechtzuerhalten.

Ein **Notfall** ist eine akut eintretende Situation, in der Menschen unmittelbar (medizinische) Hilfe benötigen. Von einer Krise spricht man, wenn eine schwierige Lage oder Situation besteht. Der **Ernstfall** bezeichnet das Eintreten eines für möglich gehaltenen [gefährlichen] Ereignisses. Das können außergewöhnliche Ereignisse sein, die die regulären Abläufe und die Versorgung insgesamt beeinträchtigen, etwa auch ein mehrstündiger Stromausfall oder eine Naturkatastrophe.

Bei der Beurteilung der Krisenresilienz spielen folgende Dimensionen eine Rolle:

1. Sichere DSGVO-konforme Kommunikation in Praxen und Kliniken
2. Technische und organisatorische Voraussetzungen
 - Verfügbare Dienstgeräte oder eine Verfügbarkeit und sichere Nutzung auf privaten Endgeräten
 - Stabile und geschützte Kommunikationssysteme
 - Funktionierende Kommunikation auch in Notfällen, wenn auf die zentrale IT oder das Kliniknetzwerk nicht zugegriffen werden kann oder keine Zeit ist
 - Klare Vorgaben, welche Kommunikationskanäle erlaubt sind, festgelegte Verantwortlichkeiten im Notfall
3. Notfallpläne und Übungen
 - Dokumentierte Notfall- und Kommunikationspläne
 - Schulungen für Mitarbeiter:innen
 - Regelmäßige Übungen und Simulationen
4. Vertrauen und transparente Aufklärung der Bevölkerung
 - Wie gut, denkt die Bevölkerung, ist das Gesundheitswesen auf einen Ernstfall oder Notfälle vorbereitet
 - Besorgnis über geopolitische Entwicklungen
 - Informationsstand über die Speicherung ihrer Patientendaten

3. Studiendesign und Methodik

Um diese Fragen zu beantworten, hat Doctolib eine umfassende Umfrage durchgeführt.

YouGov-Umfrage im Auftrag von Doctolib

 **Methodik:**
Online-Umfrage im YouGov-Panel

 **Feldzeit Ärzt:innen:**
9.–21. Juli 2026

 **Feldzeit Bevölkerung:**
9.–21. Juli 2026

Befragt wurden:

 **220** approbierte Klinikärzt:innen

 **208** approbierte Ärzt:innen aus Praxen

 **1.053** Personen ab 18 Jahren aus der Bevölkerung in Deutschland

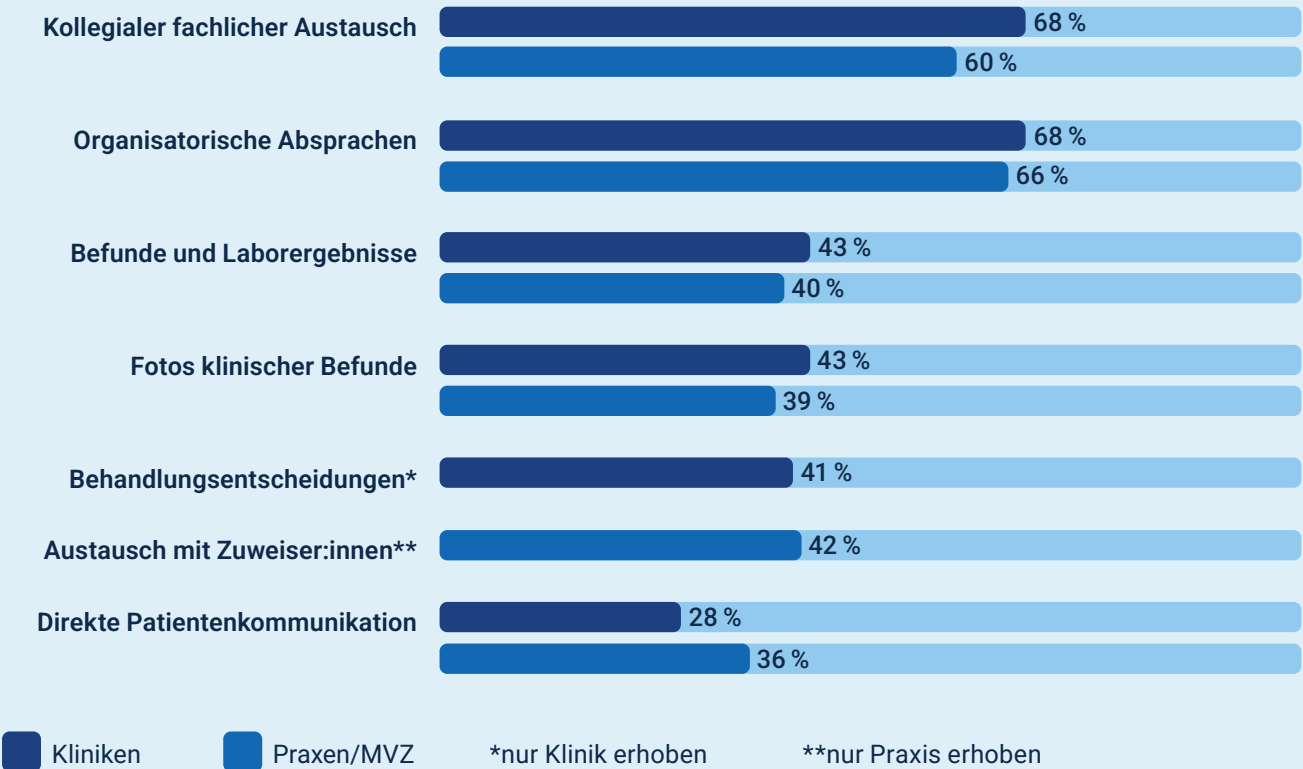
Die Bevölkerungsstichprobe ist repräsentativ nach Alter, Geschlecht und Region.

4. Ergebnisse

Die Ergebnisse zeigen: Im deutschen Gesundheitswesen besteht noch eine Lücke zwischen der Kommunikationsrealität im Alltag und den Anforderungen an Krisenresilienz und Datenschutz. Allgemeine Messenger sind in Kliniken und Praxen noch weitverbreitet, und es fehlt vielerorts an verbindlichen Notfallplänen, regelmäßigen Übungen und zertifizierten Kommunikationslösungen für den schnellen Austausch – auch wenn Gesundheitsfachkräfte dies als sinnvoll erachten würden. Die Bevölkerung hat klare Erwartungen an Einrichtungen, die Gesundheitsdaten verwalten und im Ernstfall handlungsfähig bleiben müssen. Denn Krisenresilienz im Gesundheitswesen hängt auch davon ab, wie sicher, schnell und zuverlässig Informationen ausgetauscht und Notfallsituationen vorbereitet werden.

Für welche Inhalte werden allgemeine Messenger im beruflichen Kontext eingesetzt?

68 % der Klinikärzt:innen und 60 % der Praxisärzt:innen haben allgemeine, nicht zertifizierte Kanäle schon für den fachlichen Austausch genutzt. Unter denjenigen, die allgemeine Messenger beruflich einsetzen, haben 43 % der Klinikärzt:innen und 40 % der Praxisärzt:innen darüber auch patientenbezogene Inhalte wie Befunde und Laborergebnisse verschickt.



4.1 Kommunikation im Krisenfall: zwischen Vertrautem und Sicherem

Im Arbeitsalltag dominieren weiterhin vertraute Kommunikationswege, darunter auch allgemeine Messenger, weil sie schnell, bequem und unmittelbar verfügbar sind.

Welche Kommunikationsmittel werden für den fachlichen Austausch genutzt?

- Gespräch vor Ort (Klinik 73 %, Praxis 58 %)
- Diensttelefon (Klinik 61 %, Praxis 56 %)
- Institutionelle E-Mail (Klinik 58 %, Praxis 28 %)
- Allgemeine Messenger wie WhatsApp (Klinik 43 %, Praxis 41 %)
- Apezialisierte Kommunikationslösungen wie Doctolib Connect (Klinik 19 %, Praxis 22 %)



Was sind die Gründe für die Nutzung von allgemeinen Messengern für berufliche Zwecke?

- Kolleg:innen und Vorgesetzte nutzen sie ebenfalls (Klinik 64 %)
- Schneller und bequemer als offizielle Systeme (Klinik 45 %, Praxis 50 %)
- Privatgerät ist einfacher und schneller nutzbar (Praxis 43 %)
- Im Umfeld gängige Praxis (Praxis 34 %)
- In zeitkritischen Lagen bleibt keine Zeit für andere Wege (Klinik 42 %, Praxis 28 %)
- Patient:innen oder Zuweiser:innen kommunizieren darüber (Klinik 30 %, Praxis 27 %)
- Kein Diensttelefon vorhanden (Klinik 9 %, Praxis 17 %)

Wie häufig nutzen Ärzt:innen allgemeine Messenger für berufliche Zwecke?

- Täglich (Klinik 43 %, Praxis 38 %)
- Mehrmals pro Woche (Klinik 40 %, Praxis 48 %)
- Einmal pro Woche (Klinik 8 %, Praxis 6 %)
- Seltener als einmal pro Woche (Klinik 7 %, Praxis 7 %)
- Sie wissen es nicht/keine Angabe (Klinik 2 %, Praxis 1 %)

Warum nutzen Ärzt:innen zertifizierte/ für das Gesundheitswesen entwickelte Kommunikationslösungen?

- Sie sind datenschutzrechtlich konform (Klinik 61 %, Praxis 68 %)
- Die Einrichtung/Praxis schreibt es vor (Klinik 39 %, Praxis 29 %)
- Sie sind genauso einfach wie allgemeine Messenger (Klinik 24 %, Praxis 20 %)
- Kolleg:innen/Partnereinrichtungen nutzen sie ebenfalls (Klinik 42 %, Praxis 47 %)
- Die Sicherheit der Patientendaten ist ihnen persönlich wichtig (Klinik 51 %, Praxis 49 %)
- Sie sind gesetzlich dazu verpflichtet (Klinik 28 %, Praxis 28 %)
- Sie wissen es nicht/keine Angabe (Klinik 0 %, Praxis 2 %)

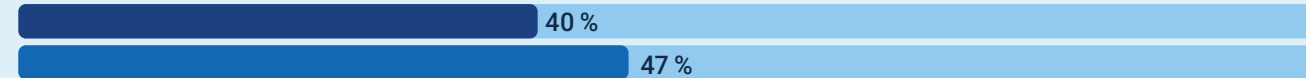
Sicherheit bzgl. Datenschutzkonformität

Wie sicher sind sich die Befragten, dass die für den fachlichen Austausch genutzten Kommunikationsmittel den Datenschutzanforderungen für den Umgang mit Patientendaten entsprechen?

Sehr sicher, sie nutzen ausschließlich zugelassene, zertifizierte oder geprüfte Kommunikationsmittel



Weitgehend sicher, sie gehen davon aus, dass die genutzten Kommunikationsmittel konform sind, haben es aber nicht selbst geprüft



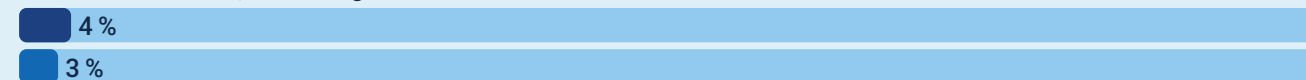
Nicht sicher, sie wissen nicht genau, ob alle genutzten Kommunikationsmittel den Anforderungen entsprechen



Ihnen ist bewusst, dass sie teilweise Kommunikationsmittel nutzen, die nicht vollständig konform sind



Sie wissen es nicht, keine Angabe



Klinik Praxis

Welche der folgenden Risiken sehen Ärzt:innen bei der beruflichen Nutzung allgemeiner Messenger?

- Unbefugte Dritte oder ausländische Behörden könnten Zugriff auf Patientendaten erhalten (Klinik 43 %)
- Die Nutzung für Patientendaten kann gegen die DSGVO verstoßen (Klinik 49 %)
- Im Fall eines Hacks oder Datenlecks könnten Patientendaten in falsche Hände geraten (Klinik 58 %)
- Patientendaten können versehentlich an falsche Personen gesendet oder ohne Wissen des Absenders weitergeleitet werden (Klinik 51 %)
- Bei Geräteverlust oder -diebstahl können Unbefugte Zugriff auf Patientendaten erhalten (Klinik 39 %)
- Sie halten keines dieser Risiken für relevant in ihrem Alltag (Klinik 8 %)
- Ihnen sind diese Risiken nicht bekannt (Klinik 0 %)
- Sie wissen es nicht/keine Angabe (Klinik 3 %)

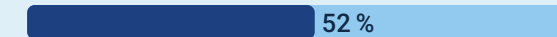


Besorgnis über Kommunikationszuverlässigkeit im Ernstfall

- Besorgt (Klinik 63 %, Praxis 60 %)
- Nicht besorgt (Klinik 17 %, Praxis 16 %)

Was würde die Kommunikation in der Einrichtung im Ernstfall zuverlässiger machen?

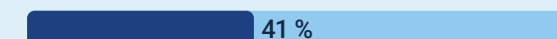
Systeme, die auch bei Ausfall der internen Infrastruktur laufen



Zertifizierte Lösung, so einfach wie allgemeine Messenger



Unabhängig von zentraler IT auf allen Geräten nutzbar



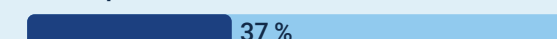
Finanzielle Unterstützung



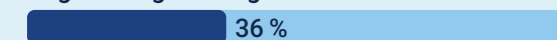
Einheitliche Standards im Sektor



Notfallplan allen bekannt machen



Regelmäßige Übungen



Kliniken Praxen/MVZ

4.2 Die strukturellen Voraussetzungen für sichere Kommunikation

Ärzt:innen sind bereit, auf sichere Kommunikationslösungen umzusteigen, wenn diese genauso einfach, schnell und zuverlässig funktionieren wie die bisher genutzten Kanäle.

66 % der Klinikärzt:innen und 65 % der Ärzt:innen in Praxen würden zu einer zertifizierten Lösung wechseln.

Diese Probleme stehen einer sicheren Kommunikation im Weg

A. Fehlende Dienstgeräte und Infrastruktur

- Kein Dienstgerät vorhanden (Klinik 38 %, Praxis 41 %)
- Dienstgerät vorhanden, aber Privatgerät überwiegend genutzt (Klinik 15 %, Praxis 19 %)

B. Unklare oder fehlende institutionelle Regeln

- Nutzung ist erlaubt/toleriert (Klinik 32 %)
- Es gibt keine klare Regelung (Klinik 42 %)
- Nutzung ist nicht erlaubt, wird aber praktiziert (Klinik 20 %)
- Unklar, ob es Regelung gibt (Klinik 6 %)

C. Bereitschaft, zu wechseln

- Würde zu zertifizierter Lösung wechseln (Klinik 66 %, Praxis 65 %)
- Kennen keine sichere Lösung (Klinik 47 %)

D. Anforderungen an eine solche Lösung

- Zertifizierte Lösungen, so einfach wie allgemeine Messenger, z. B. Doctolib Connect (Praxis 58 %): info.doctolib.de/connect
- Systeme, die auch bei Ausfall der internen Infrastruktur laufen (Klinik 52 %)
- Unabhängig von zentraler IT auf allen Geräten nutzbar (Klinik 41 %)



„In der Notaufnahme entscheidet häufig [...] das Zusammenspiel vieler kleiner Abläufe – und dabei zählt oft jede Minute. Digitale Echtzeitkommunikation [...] beschleunigt Entscheidungen [...] und hilft, Mikrokrise schneller zu lösen. Dabei sind immer Daten von [Patient:innen und Kolleg:innen] im Spiel. Privat genutzte Messenger sind in der Notfallkommunikation ungeeignet – bis hin zu unzulässig. Am Klinikum Solingen haben wir mit Doctolib Connect eine Lösung gefunden, die schnell, datenschutzkonform und auch dann verfügbar ist, wenn es darauf ankommt.“



Dr. med. Patric Tralls,

Chefarzt für Notfall- und Akutmedizin am Städtischen Klinikum Solingen

Sichere Kommunikation sollte nicht nur vorgeschrieben, sondern so eingeführt werden, dass sie im Alltag tatsächlich praktikabel ist.



4.3 Notfallplanung und Übungen: Resilienz muss eingeübt werden

Ein Notfallplan schafft noch keine Resilienz, wenn er nicht bekannt ist, regelmäßig trainiert und unter realistischen Bedingungen erprobt wird.

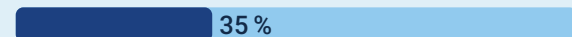
Nur ein Teil der Klinikärzt:innen kennt den Krankenhausalarm- und einsatzplan und wurde dazu geschult. In vielen Praxen gibt es keinen dokumentierten Notfallplan oder der Plan ist nicht dem gesamten Team bekannt.

Kenntnis des Krankenhausalarm- und einsatzplans (KAEP)

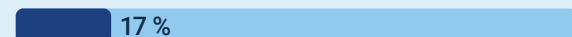
Kenne ihn, wurde informiert oder geschult



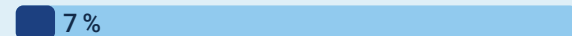
Kenne die Abläufe, nie offiziell geschult



Nie informiert, wüsste nicht, was zu tun ist



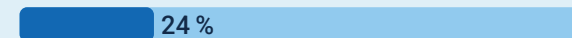
Es gibt keinen solchen Plan



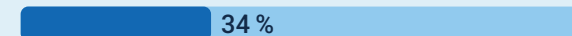
Kliniken

Kenntnis des schriftlichen Notfallplans in Praxen

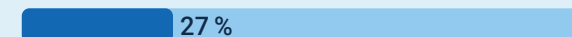
Schriftlicher Plan dem ganzen Team bekannt



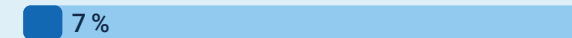
Teilweise oder kein dokumentierter Plan, aber handlungsfähig



Kein Plan, wir würden improvisieren



Wäre derzeit nicht beherrschbar

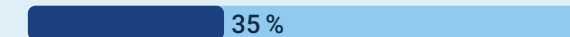
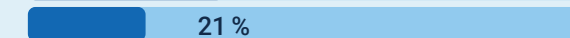


Praxen/MVZ

Simulationen zum Ausfall digitaler Systeme finden relativ selten statt. Gleichzeitig halten 45 % der Klinikärzt:innen und 56 % der Praxisärzt:innen Übungen für sinnvoll.

Übung/Simulation für den Ausfall digitaler Systeme in den letzten 2 Jahren

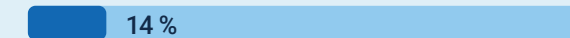
In den letzten 2 Jahren durchgeführt



Nicht durchgeführt, halte ich aber für sinnvoll



Halte ich nicht für nötig



Kliniken Praxen/MVZ

4.4 Die Perspektive der Bevölkerung: Sicherheit, Transparenz und Erwartungshaltung

Für die Bevölkerung ist Krisenresilienz nicht nur eine Frage der Versorgungssicherheit, sondern auch des Vertrauens in den Schutz und die transparente Kommunikation persönlicher Gesundheitsdaten.

84 % erwarten ausschließlich sichere datenschutzkonforme Lösungen.

Was sind die Sorgen der Bevölkerung?

- 56 % sind besorgt, dass geopolitische Entwicklungen die medizinische Versorgung in Deutschland gefährden könnten
- 64 % der Bevölkerung halten das Gesundheitswesen für eher schlecht oder gar nicht auf digitale Ausfälle vorbereitet
- 44 % haben Angst vor Verzögerungen bei Terminen, Diagnosen und Behandlungen, 43 % haben Angst, dass Praxen/Kliniken vorübergehend nicht erreichbar sind, 40 % befürchten Ausfälle geplanter Eingriffe/Behandlungen
- 49 % fühlen sich nicht gut über die Speicherung ihrer persönlichen Gesundheitsdaten informiert

Welche Erwartungen und Forderungen hat die Bevölkerung?

84 % der Befragten erwarten, dass im Gesundheitswesen ausschließlich sichere datenschutzkonforme Kommunikationslösungen genutzt werden.

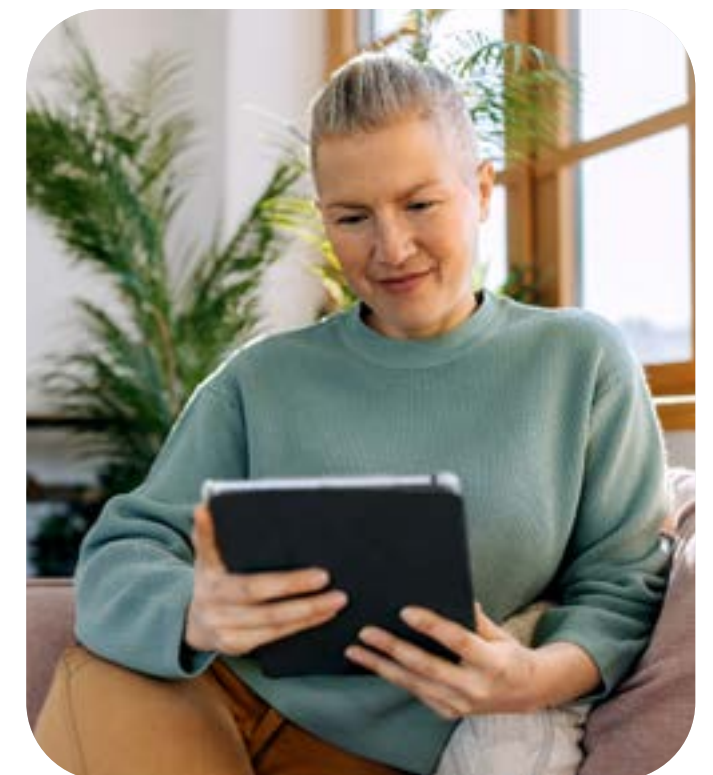
Die Hauptverantwortung dafür, dass das Gesundheitswesen in Krisensituationen handlungsfähig bleibt, sehen 47 % in der Gesetzgebung, 44 % bei Praxen/Kliniken und 29 % bei Technologieunternehmen.

Wenn sie erfahren würden, dass ihre Ärzt:in einen allgemeinen Messenger wie WhatsApp nutzt, würden 26 % den/die Ärzt:in darauf ansprechen, 17 % sich bei einer Datenschutzbehörde beschweren und 13 % die Praxis/Klinik wechseln.

77 % wollen außerdem informiert werden, falls die eigenen Daten von einem IT-Sicherheitsvorfall betroffen sein könnten.

Was das Vertrauen der Bevölkerung stärken würde

- Klare gesetzliche Vorgaben zur Notfallkommunikation (56 %)
- Nachweis, dass nur zertifizierte Lösungen genutzt werden (40 %)
- Transparente Informationen zum Schutz der Gesundheitsdaten (40 %)
- Öffentlich kommunizierte Übungen (32 %)





5. Von den Studienergebnissen zu konkreten Handlungsfeldern

Die Studie zeigt einen klaren Handlungsauftrag: Sichere Kommunikation muss technisch verfügbar, institutionell geregelt, praktisch eingeübt und gegenüber den Patient:innen transparent vermittelt werden.

Aus den Ergebnissen lassen sich für Praxen und Kliniken 4 Handlungsfelder ableiten.

1. Sichere und leicht zugängliche Kommunikationslösungen einführen

Praxen und Kliniken benötigen Kommunikationslösungen, die schnell, intuitiv und datenschutzkonform im gesamten Team funktionieren und auch auf vorhandenen mobilen

Endgeräten genutzt werden können. Die Kommunikation muss auch bei Ausfällen der zentralen IT oder der internen Infrastruktur verfügbar bleiben. Konkrete erste Schritte:

- **Bedarf erfassen:** Prüfen, in welchen Situationen im Praxis- oder Klinikalltag schnell kommuniziert werden muss und welche Informationen dabei ausgetauscht werden müssen.
- **Lösung finden und erproben:** Eine sichere und einfach bedienbare Kommunikationslösung auswählen und zunächst einen Testlauf in einem ausgewählten Team durchführen.
- **Ausfallsicherheit prüfen:** Sicherstellen, dass die Kommunikationslösung auch unabhängig von der zentralen IT funktioniert.
- **Lösung evaluieren:** Nach der Erprobungsphase Erfahrungen und Feedback auswerten und entscheiden, ob die Lösung dauerhaft und flächendeckend eingeführt wird.

2. Klare Regeln für zulässige Kommunikationskanäle schaffen

Einrichtungen sollten eindeutig festlegen, welche Kommunikationskanäle für welche Inhalte und Situationen zugelassen sind. Diese Vorgaben müssen allen Mitarbeiter:innen bekannt sein und regelmäßig überprüft werden. Für die praktische Umsetzung bieten sich folgende Schritte an:

- **Kanäle zuordnen:** Für verschiedene Inhalte und Situationen passende Kommunikationswege definieren.
- **Unzulässige Kommunikationskanäle benennen:** Kommunizieren, welche Kanäle grundsätzlich nicht genutzt werden dürfen, weil sie privat oder nicht fürs Gesundheitswesen zertifiziert sind.
- **Gründe und Regeln vermitteln:** Vorgaben sichtbar machen, regelmäßig schulen und aktuell halten.

3. Notfallpläne teamweit bekannt machen und regelmäßig üben

Notfallpläne sollten nicht nur dokumentiert, sondern im gesamten Team bekannt, verständlich und zugänglich sein. Regelmäßige Schulungen und realitätsnahe Übungen helfen dabei, Zuständigkeiten zu klären und Abläufe im Ernstfall sicher anzuwenden. Damit diese Pläne im Ernstfall wirksam sind, sollten Einrichtungen zunächst:

- **Zuständigkeiten festlegen:** Rollen, Vertretungen und Eskalationswege definieren.
- **Teams schulen:** Notfallpläne sowohl bei der Einarbeitung als auch regelmäßig im Arbeitsalltag vermitteln.
- **Abläufe üben:** Szenarien wie denkbare Notfälle oder Stromausfälle simulieren und die Pläne anschließend anpassen.

4. Patient:innen transparent informieren

Zur Krisenresilienz gehört auch eine verlässliche Kommunikation mit Patient:innen. Einrichtungen sollten erklären, wie sie Gesundheitsdaten schützen, über welche Kanäle sie in einem Krisenfall informieren und wie Betroffene bei einer Beeinträchtigung der Versorgung aktiv benachrichtigt werden. Für eine verlässliche Krisenkommunikation sind insbesondere folgende erste Schritte sinnvoll:

- **Grundsätzlich informieren:** Patient:innen einmalig schriftlich darüber informieren, wie ihre Gesundheitsdaten geschützt werden
- **Verantwortlichkeiten klären:** Festlegen, wer Patient:innen im Krisenfall informiert und welche Kanäle genutzt werden.
- **Vorlagen vorbereiten:** Verständliche Informationen für Terminänderungen und nächste Schritte entwickeln.



Doctolib

Doctolib GmbH, Friedrichstraße 111, 10117 Berlin, Amtsgericht Charlottenburg (Berlin) HRB 175963 B. Geschäftsführer: Nikolay Kolev, Stanislas Niox-Château. Stand: Oktober 2026. Doctolib übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Inhalte und der Verknüpfungen zu Websites Dritter (externe Links).

Doctolib stellt Informationen zu den Funktionalitäten und zur Implementierung der Softwarelösung Doctolib bereit. Auf Basis unserer Erfahrung im Bereich Telemedizin unterstützen wir Sie gern bei der Einschätzung möglicher betriebswirtschaftlicher Effekte, z. B. durch eine individuelle Business-Case-Betrachtung in Ihrem spezifischen Kontext. Bitte beachten Sie, dass wir keine rechtliche oder umfassende Fördermittelberatung leisten und hierzu keine Befugnis haben. Für eine rechtsverbindliche Bewertung oder Förderantragstellung empfehlen wir die Einbindung spezialisierter Beratungsunternehmen oder von Rechtsanwälten:innen.