Einführung

Überblick über die wichtigsten Themen rund um garrioCOM

- Voraussetzungen und Bestellung
- Allgemein häufig gestellte Fragen
- Häufig gestellte Fragen für Praxisnutzer
- Informationen für Datenschutzbeauftragte
- Videosprechstunde
- Sicherheit
- Hinweise zu lokalen Firewalls

Voraussetzungen und Bestellung

garrioCOM als Praxis bestellen

garrioCOM kann über unser Bestellformular bestellt werden.

Voraussetzungen für die Nutzung von garrioCOM

Um garrioCOM in der Praxis zu nutzen wird lediglich ein aktueller Browser (bspw. Google Chrome oder Mozilla Firefox) sowie eine Internetverbindung benötigt. Die mobile Version von garrioCOM (Download hier) kann auf aktuellen Smartphones betrieben werden und ist in den jeweiligen Stores (Apple App Store und Google Play Store) verfügbar.

Unterstützung von Tablet-Geräten

Die garrioCOM-App (Download hier) kann auch auf Tablets verwendet werden. Hingegen ist die Browser-Version nicht für die Nutzung mit den Tablet-Browsern optimiert und somit nicht möglich.

Computer oder Smartphone - für den jeweiligen Einsatzzweck optimiert

Auf Seiten der **Praxis** wird ein Computer mit einem modernen Browser benötigt, um garrioCOM zu nutzen. Ergänzend dazu ist die Nutzung eines modernen Smartphones für die Praxis optional möglich. Dies ersetzt jedoch nicht die Browser-basierte Applikation.

Für die **Patienten** gibt es lediglich die Möglichkeit der Smartphone-App. Für Patienten ist die nutzung von garrioCOM somit nur mit einem Handy möglich. Dies bietet deutlich bessere Handhabbarkeit für den Schutz der sensiblen Patientendaten.

Dateiversand und Dateiformate

Dateien mit folgenden Formaten können mit garrioCOM zwischen Gesundheitspartner und Patient sowie Gesundheitspartnern untereinander versendet werden: Dokumente als PDF sowie Bilder als JPEG und PNG.

Sichere Kommunikation für sensible Gesundheitsdaten

Aufgrund der durchgängigen Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmern können jegliche medizinischen oder persönlichen Dokumente und Daten sicher und verschlüsselt ausgetauscht werden. Die Limitierung gilt lediglich für das Dateiformat (s.o. PDF, JPEG, PNG). Welche Inhalte versendet werden obliegt den Nutzern.

Schnittstelle zu Arztinformationssystemen (AIS) / Praxisverwaltungssystemen (PVS)

In der aktuellen Version ist ein Austausch mittels automatischer technischer Schnittstelle zwischen AIS/PVS und garrioCOM nicht möglich. Wir entwickeln zur Zeit jedoch zweierlei Schnittstellen, mit denen Sie in Zukunft sowohl aus Ihrem bestehenden PVS Dokumente per garrioCOM übermitteln können als auch Daten aus garrioCOM in Ihr bestehenden PVS laden können. Damit der Weg von garrioCOM in Richtung PVS funktioniert muss jedoch Ihr PVS diese Schnittstelle allerdings ansprechen können.

Kalendersynchronisierung mit Arztinformationssystemen (AIS) / Praxisverwaltungssystemen (PVS)

In der aktuellen Version ist ein Austausch mittels automatischer technischer Schnittstelle zwischen AIS/PVS und garrioCOM nicht möglich. Aufgrund der vielen verschiedenen, proprietären bestehenden AIS/PVS arbeiten wir an einer standardisierten Schnittstelle, welche von den AIS/PVS angesprochen werden kann.

Keine Limitierung der Benutzerzahl

Mit garrioCOM können Sie beliebig viele Benutzer (Ärzte, MFA) anlegen.

Keine Limitierung der Geräte

Mit garrioCOM können Sie beliebig viele Geräte verbinden und nutzen.

Kosten

garrioCOM ist derzeit (Stand: 15.11.2024) kostenfrei über unser Bestellformular für Teilnehmer der AOK-Haus- und Facharztverträge sowie Mitglieder des Hausärzteverbandes und des MEDIVERBUNDs erhältlich.

Die Videosprechstunde kann optional für 25€ zzgl. MwSt. pro Monat und Arzt hinzugebucht werden. (Stand: 15.11.2024, siehe Bestellformular).

Über die garrio GmbH

Die garrio GmbH ist eine Tochterfirma der MEDIVERBUND AG.

Mindestlaufzeit & Kündigungsfrist

Laufzeit & Kündigung:

Die Mindestlaufzeit für den **garrioCOM** Messenger Dienst beträgt 12 Monate. Der Vertrag kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden.

Widerrufsrecht:

Der Kunde ist berechtigt, den Vertrag innerhalb von 14 Tagen ab dem Tag des Vertragsschlusses ohne Angabe von Gründen in Textform zu widerrufen.

(siehe Link : Nutzungsbedingungen Gesundheitspartner – garrio.de)

Firewall und Antivirus

Bezüglich Firewall und Antivirus-Software bestehen aktuell keine besonderen Voraussetzungen, da garrioCOM als reine Browser-Software betrieben wird. Falls Sie dennoch eine restriktive Firewall-Regel haben, gilt dies zu beachten: Hinweise zu lokalen Firewalls.

Schutz vor externen Angriffen

Wir halten uns bei der Entwicklung und dem Betrieb von garrioCOM an die Vorgaben und Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/). Zudem wird garrioCOM regelmäßig durch sog. Penetrationstest von unabhängigen Sicherheitsexperten überprüft, um die Einhaltung der vorgenannten Vorgaben und Empfehlungen zu bestätigen.

Allgemein häufig gestellte Fragen

Browser- Sicherheit und Browser- Einstellungen

Hintergrund: Sicherheitsfaktor

Damit garrioCOM nach der Ersteinrichtung weiterhin wie vorgesehen funktioniert und aufgerufen werden kann ist die korrekte Konfiguration des verwendeten Browsers entscheidend.

Bei der Ersteinrichtung wird zunächst die Administrations-Anwendung von garrioCOM (https://admin.garrio.de) mit einem PC der Praxis verbunden. Die so hergestellte Verbindung zwischen Praxis und den garrio-Systemen im garrio-Rechenzentrum wird mittels auf dem Praxis-PC gespeicherten Daten verifiziert. Gleiches gilt für die Verbindung der Praxis-Anwendung von garrioCOM (https://praxis.garrio.de) mit den Arbeitsplätzen der Praxis.

Damit diese Verifizierung und Absicherung auch bei späteren Verwendungen der Applikationen einwandfrei funktionieren und garrioCOM von der Praxis genutzt werden kann, muss die Speicherung dieser Daten vom Browser zugelassen werden und – entscheidend – vom Browser dauerhaft behalten werden. **Eine automatische Löschung dieser Daten führt dazu, dass garrioCOM nicht genutzt werden kann.**

Inkognito-/Privater-Modus

Da es im Inkognito-/Privat-Modus keine Möglichkeit gibt die Daten zur Verifizierung der Arbeitsplätze zu erhalten (in diesem Modus wird nach Sitzungsende immer gelöscht), ist dieser Modus für die sinnvolle Nutzung von garrioCOM nicht geeignet und nicht empfohlen.

Selbstverständlich funktioniert garrioCOM weiterhin in diesem Modus, die Verifizierung der Arbeitsplätze muss dann jedes Mal durch die Wiederherstellung der Verbindung neu erfolgen.

Updated on 10. Januar 2024

Ende-zu-Ende-Verschlüsselung von Nachrichten

E2EE = end-to-end-encryption

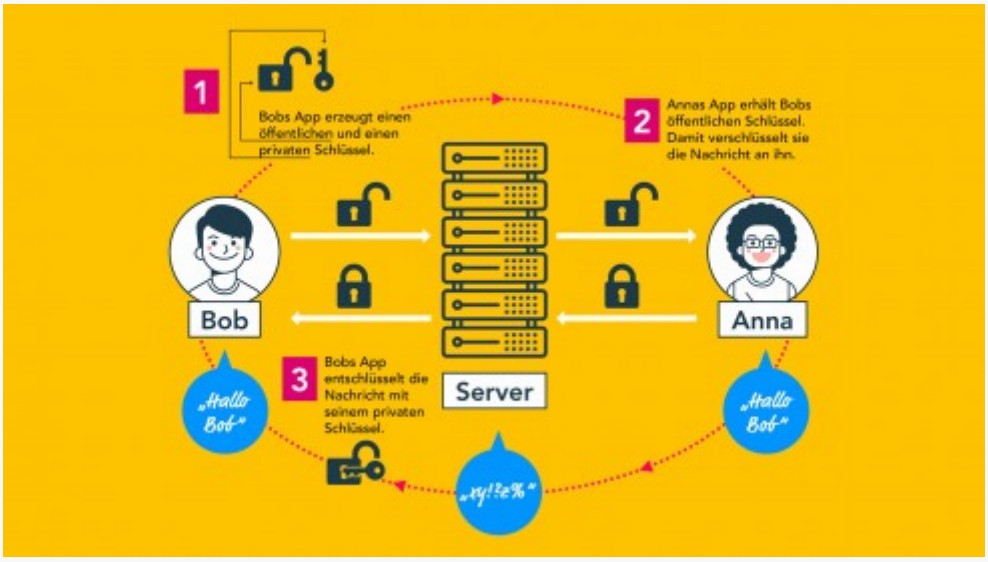


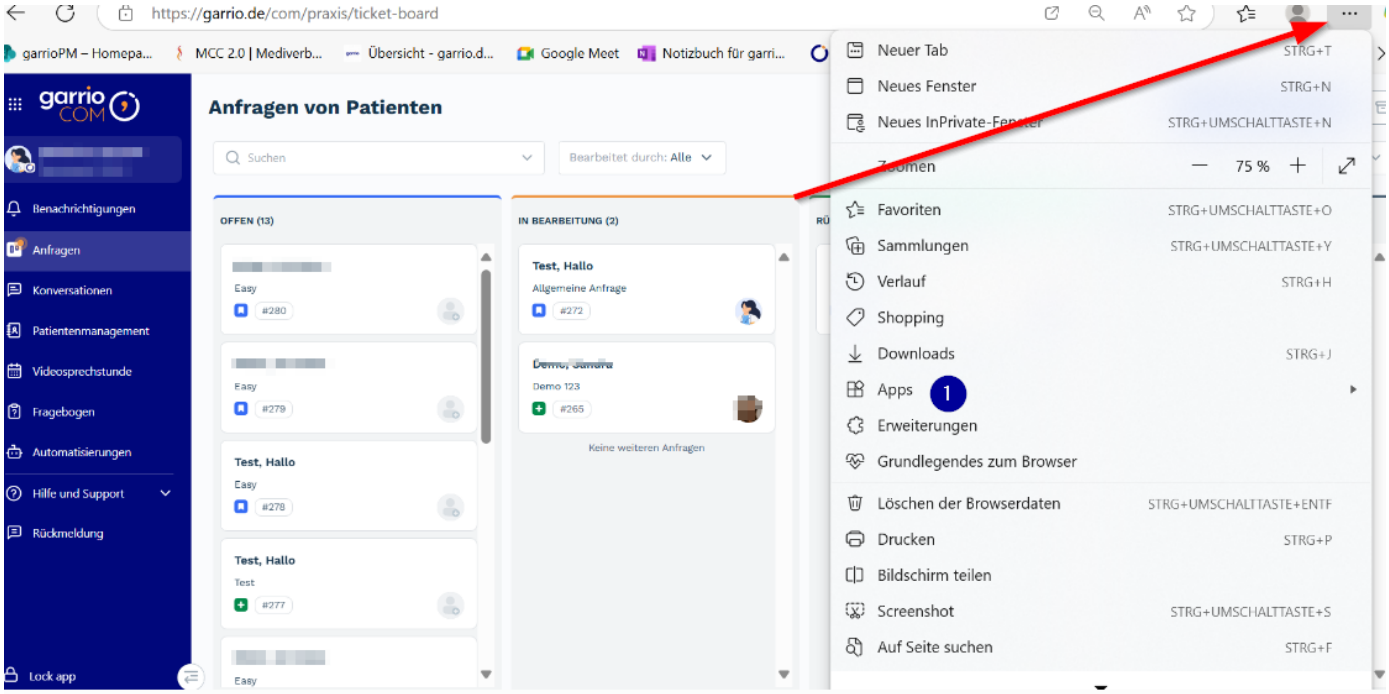
Bild von : [Ende-zu-Ende-Verschlüsselung einfach erklärt – iRights.info – iRights.info]

Updated on 15. November 2023

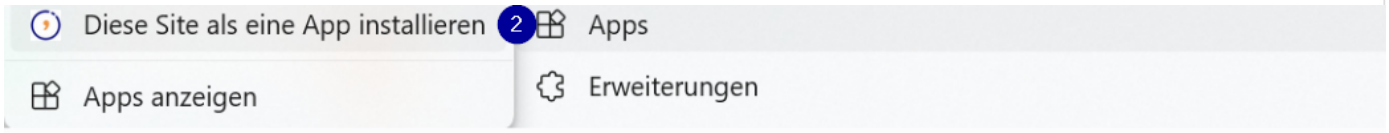
garrioCOM Messenger-Dienst zur Taskleiste hinzufügen (Beispiel Edge Browser)

Möchten Sie den garrioCOM Messenger zur Taskleiste hinzufügen, geht man wie folgt vor:

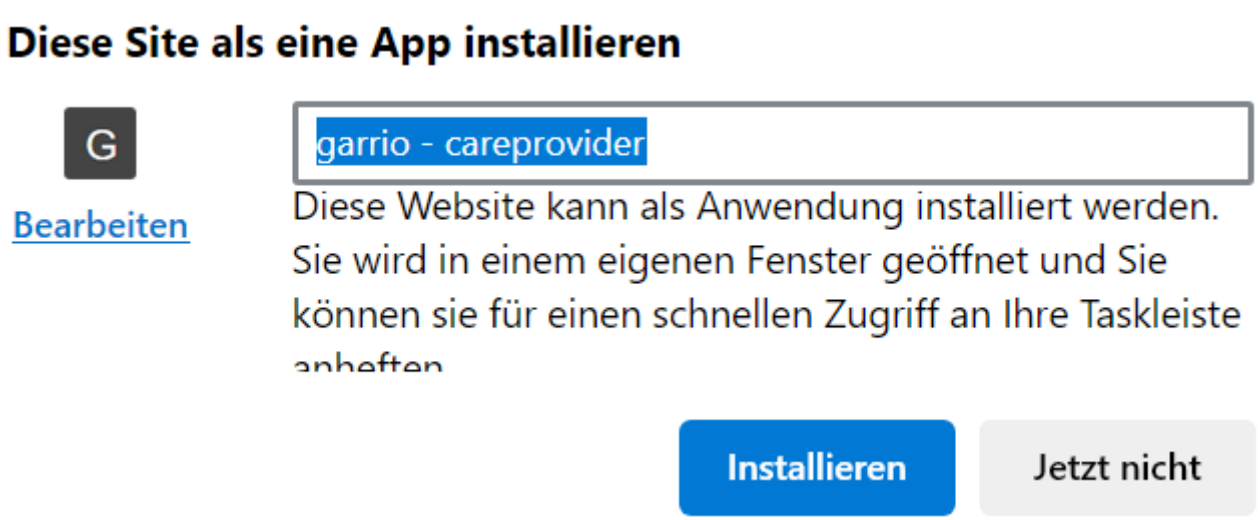
1. Öffnen Sie den garrioCOM Messenger über den Edge-Browser.
2. Klicken Sie auf die drei Punkte im rechten oberen Bereich des Fensters (siehe Pfeil im Bild).



3. Nun klicken Sie auf **(1) „Apps“** und anschließend auf **(2) „Diese Seite als eine App installieren“**.



4. Es erscheint ein weiteres Fenster, in dem Sie erneut auf **„Installieren“** klicken.



5. Im letzten Fenster wählen Sie den Bereich aus, an den die garrioCOM App angeheftet werden soll.

Updated on 10. April 2024

Zu beachten bei der Nutzung von Huawei-Smartphones und Android-Versionen unter 11 sowie Shift Smartphones (kleines Unternehmen aus NRW)

Bitte beachten Sie dass die Nutzung von garrioCOM auf Smartphones der Marke HUAWEI, derzeit nicht möglich ist, da der Hersteller des Nutzung von Google Play-Stores nicht unterstützt. Huawei verfügt jedoch über einen eigenen Play-Store. Hier prüfen wir aktuell ab wir diesen in Zukunft auch bedienen werde.

Für Android- Versionen: es werden Android-Versionen 11, 12,13, und 14 unterstützt. Für alle älteren Versionen gilt, Android- Smartphones bis Version 10 und älter gelten als unsicher und werden daher nicht unterstützt.

Shift Smartphones: Nutzung der garrioCOM App auf diesen Smartphones nicht möglich.

Updated on 23.06.2026

Häufig gestellte Fragen für Praxisnutzer

Wie/ wo kann ich als Praxis/ Pflegeeinrichtung garrioCOM bestellen?

Praxen können garrioCOM ganz unkompliziert über das **Bestellformular** auf der garrioCOM Website bestellen.

Link zum Bestellformular: https://garrio.de/bestellung/

Wie stelle ich den garrioCOM Praxis Messenger-Dienst wieder her, nachdem der Browserverlauf gelöscht wurde?

Wenn Sie den Browserverlauf gelöscht haben, werden auch die Zugangsdaten für den garrioCOM Messenger, die auf diesem Gerät gespeichert waren, gelöscht. Um den Zugang wiederherzustellen, melden Sie sich auf der garrioCOM Adminwebseite an. Navigieren Sie anschließend zum Reiter **„Vertrauenswürdige Geräte“**, erstellen Sie dort einen neuen **"Magischen Verknüpfungslink"**, und kopieren Sie diesen. Öffnen Sie danach ein neues Browserfenster und fügen Sie den zuvor erstellten und kopierten Magischen Link in die Adressleiste des neu geöffneten Browserfensters ein.

Updated on 5. August 2024

Wie verbinde ich ein Smartphone mit dem garrioCOM Messenger (Praxisversion)

Um vom Smartphone auf den garrioCOM Messenger-Dienst zugreifen zu können und sich mit Ihrer eigenen Praxis zu verbinden, gehen Sie wie folgt vor:

1. Öffnen Sie die **garrioCOM Messenger App** auf Ihrem Smartphone.
2. Klicken Sie auf **„Profil des Gesundheitspartners“** und stimmen Sie dem Zugriff auf die Smartphone-Kamera zu.

3. Öffnen Sie den garrioCOM Messenger auf einem Praxis-PC und klicken Sie auf den **Account-Avatar** (rechts oben, siehe Bild).

- Es erscheint ein Fenster, in dem Sie auf **„Anmeldung bei der mobilen App“** klicken und anschließend den angezeigten QR-Code mit Ihrem Smartphone scannen (siehe Bild).



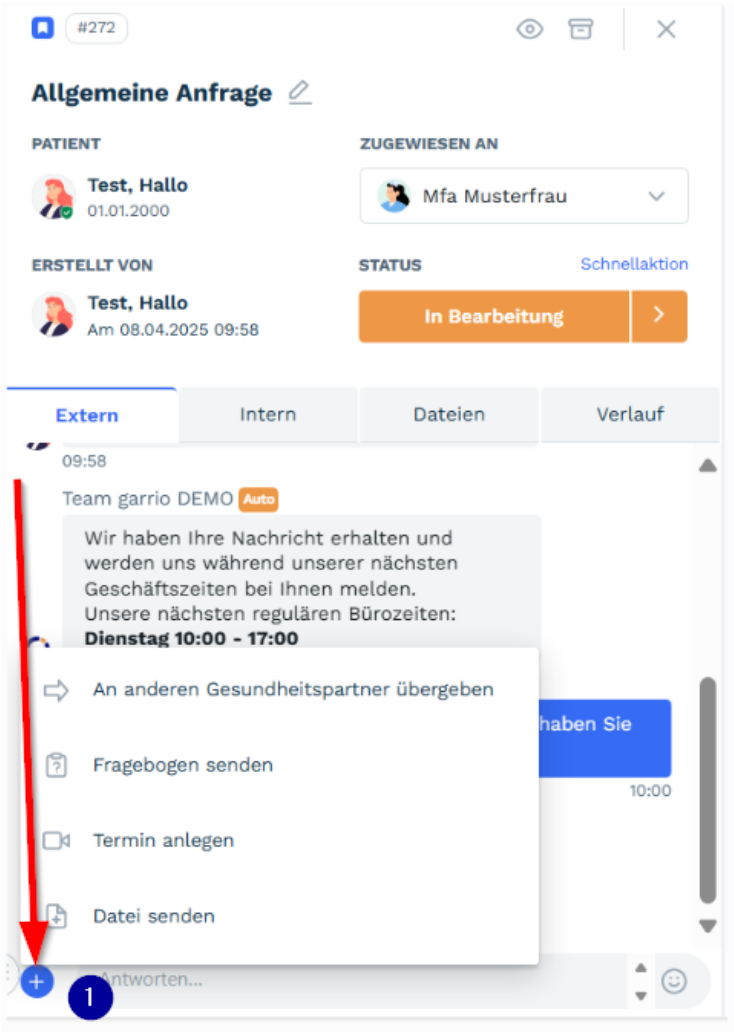
Updated on 18. März 2024

Wie versendet ich Dateien/ Befunde/ Arztbriefe an Patienten/ Praxen

Dateien wie Arztbriefe, Befundmitteilungen und Ähnliches können problemlos wie folgt an Patienten oder Praxen versendet werden:

1. Öffnen Sie über die **Anfragenpinnwand** oder über **Konversationen** auf der garrioCOM Praxiswebseite den gewünschten Chat oder erstellen Sie einen neuen Chat.

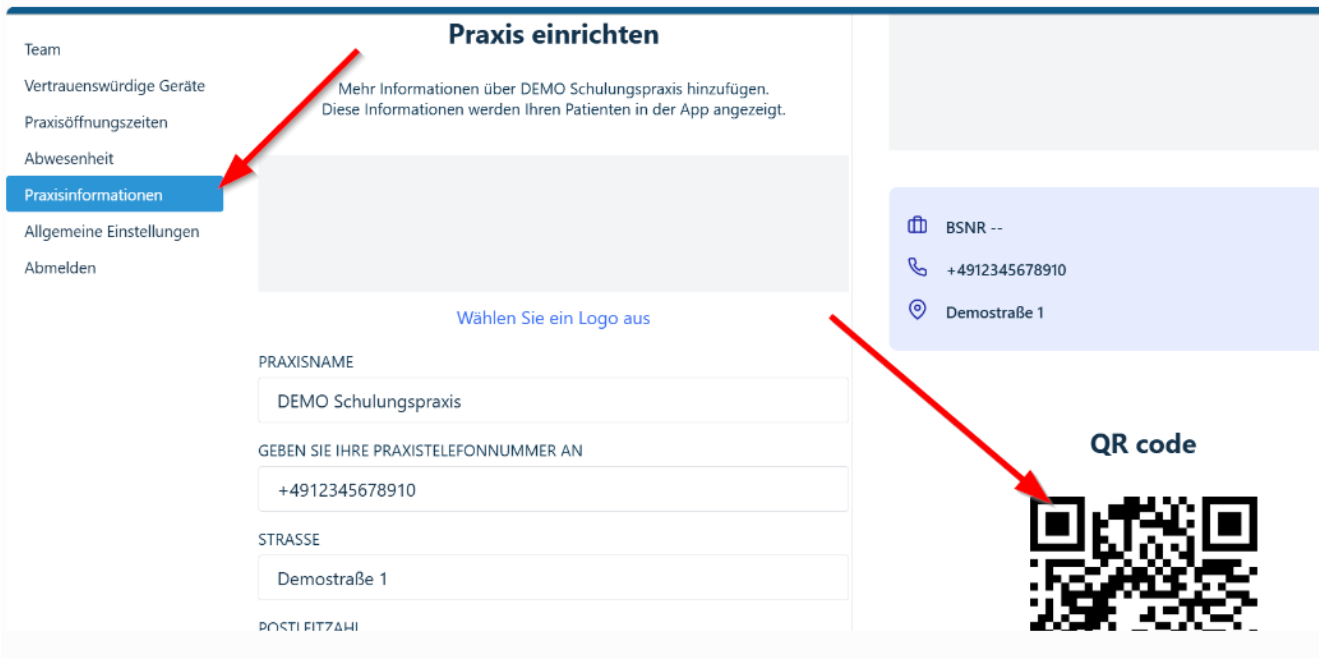
- Anschließend klicken Sie auf das (+) Symbol, das sich im unteren Bereich des geöffneten Chatfensters, links neben der Tippleiste befindet. (siehe Bild1)
- Nun können Sie die gewünschte Kategorie (z.B.: "Datei oder Fragebogen") auswählen und über den Enterbutton absenden.



Updated on 25. März 2024

Wo finde ich den QR-Code über den sich Patienten mit meiner Praxis verbinden können?

- Öffnen Sie die **garrioCOM Adminwebsite** und loggen Sie sich ein.
- Navigieren Sie zu den **Praxisinformationen** (siehe Bild).
- Ihr **Praxis QR-Code** befindet sich auf der rechten Seite des Bildschirms, diesen können Sie nun ausdrucken und in der Praxis/ Wartezimmer aufhängen und/ oder über den Downloadbutton herunterladen und auf Ihrer Praxiswebseite einpflegen. (siehe Bild)



Updated on 12. März 2024

Zurücksetzen des Sicherheitsschlüssels

Wenn Sie den Sicherheitsschlüssel zu Ihrem Nutzerprofil verloren haben, können Sie ihn während des **Anmeldeprozesses** zurücksetzen.

1. Klicken Sie auf den Button **„Sicherheitsschlüssel zurücksetzen“**.
2. Bestätigen Sie den Vorgang im nächsten Schritt.

⚠ **Bitte beachten Sie, dass dabei alle alten Nachrichten verloren gehen.** ⚠

Updated on 5. August 2024

Videosprechstunde

Was ist erforderlich für die Teilnahme an einer Videosprechstunde?

Für die Teilnahme an einer Videosprechstunde benötigen Sie eine eigene Webcam, ein Mikrofon und einen modernen Browser. Unterstützt werden Google Chrome oder Mozilla Firefox.

Welche Sicherheitsmaßnahmen sind erforderlich?

Achten Sie darauf, dass während der Videosprechstunde keine unbefugte Person mithört und dass Ihr Gerät abgesichert ist (mit Virenschutz, Firewall usw.). Bitte beachten Sie, dass trotz aller technischen Maßnahmen Sicherheitsrisiken niemals vollständig ausgeschlossen werden können.

Werden meine Daten an Dritte weitergegeben?

Es werden keinerlei Informationen an Dritte weitergegeben. Während der Sprechstunde wird eine direkte Peer-to-Peer-Verbindung aufgebaut, bei der der Datenaustausch ausschließlich zwischen den beiden Sprechstundenteilnehmern stattfindet. Der Klarname des Patienten wird ebenfalls nur über diese Peer-to-Peer-Verbindung ausgetauscht und kann somit ausschließlich vom Arzt und keinem anderen Dritten eingesehen werden.

Was ist eine Peer-to-Peer Verbindung?

Im Kontext dieser Anwendung bezieht sich eine Peer-to-Peer-Verbindung auf eine direkte Verbindung zwischen den Teilnehmern der Videosprechstunde (Arzt und Patient). Um eine stabile Verbindung herzustellen, müssen die Adressen der beteiligten Nutzer ausgetauscht werden. Hierfür wird ein STUN-Server verwendet. Wenn es dem Server nicht möglich ist, den Adressaustausch durchzuführen (z. B. aufgrund einer zu restriktiv eingestellten Firewall), wird der Verbindungsaufbau abgebrochen. In solchen Fällen kann keine Videosprechstunde durchgeführt werden.

Wird die Internet-Kommunikation verschlüsselt?

Ja, Ihre Kommunikation wird durch verschiedene Protokolle abgesichert. Die Kommunikation mit dem Signal-Server erfolgt über TLS-Verschlüsselung. Eine eventuelle Dateiübertragung zum anderen Sprechstundenteilnehmer wird separat durch das DTLS-Protokoll verschlüsselt. Die verschlüsselte Übertragung von Medienströmen wie Video und Audio wird schließlich durch das SRTP-Protokoll gewährleistet.

Warum fordert mich mein Browser auf, bestimmte Rechte zu erteilen?

Ihr Browser fordert Sie auf, bestimmte Rechte zu erteilen, um bestimmte Funktionen und Zugriffe während der Videosprechstunde zu ermöglichen. Dies ist eine browser-spezifische Sicherheitsmaßnahme, die den Missbrauch von Kamera oder Mikrofon durch nicht vertrauenswürdige Seiten verhindert. Dies kann beispielsweise den Zugriff auf Ihre Kamera, Ihr Mikrofon oder andere Geräte betreffen, die für die reibungslose Durchführung der Videosprechstunde benötigt werden. Die Bereitstellung dieser Rechte ermöglicht eine optimale Nutzung der Funktionalitäten innerhalb der Videosprechstunde. Bitte gewähren Sie diese Rechte, um eine Videoverbindung starten zu können.

Klein- und Großgruppenvideosprechstunde

Die Möglichkeit zur Durchführung von Klein- und Großgruppenvideosprechstunden ist möglich.

Ist die Videosprechstunde KBV-zertifiziert?

Für unsere Videosprechstunde nutzen wir die zertifizierte Lösung doccura+ (doccuraplus, Bayerische TelemedAllianz GmbH, https://www.kbv.de/media/sp/liste_zertifizierte-Videodienstanbieter.pdf, Stand 18.01.2024).

Informationen für Datenschutzbeauftragte

garrioCOM Messenger

garrioCOM ist ein Messenger, der zwischen **Gesundheitspartnern (i. d. R. Arztpraxen)** und **Patienten** einsetzbar und als Software-as-a-Service und als App verfügbar ist.

Aufbau, personenbezogene Daten und datenschutzrechtliche Verantwortung

Konto des Gesundheitspartners

Es gibt ein Konto für die Arztpraxis (Anwendung innerhalb einer Software, cloudbasiert – auch innerhalb der App möglich).

Zur Erstellung des Kontos der Arztpraxis sind Praxisdaten und Daten der Nutzer (Ärzte/MFA) notwendig. Eine Identifizierung des Kunden ist in Bezug auf das Konto der Arztpraxis für die garrio GmbH notwendig (kostenpflichtig).

- Für diese Daten des Nutzerkontos ist die garrio GmbH datenschutzrechtlich verantwortlich im Sinne der DSGVO.

Konto des Patienten

Es gibt ein Konto für den Patienten (Anwendung innerhalb der App).

1. Zur Erstellung dieses Kontos sind lediglich ein Benutzername und ein Passwort festzulegen. Beides vergibt sich der Patient selbst. Optional hat der Patient zukünftig die Möglichkeit seine E-Mail-Adresse anzugeben, um im Falle eines Verlustes des Passworts, dieses über die E-Mail- Adresse zurücksetzen zu lassen.
2. Dabei muss der Benutzername nicht der richtige Name sein, es ist jedes Pseudonym möglich, soweit es noch nicht genutzt wird. Das Passwort wird verschlüsselt hinterlegt. Eine Identifizierung des Patienten ist nicht erforderlich und seitens der garrio GmbH auch nicht gewünscht.
   - Für diese Daten (Benutzername und ein Passwort) ist die garrio GmbH datenschutzrechtlich verantwortlich im Sinne der DSGVO.
3. Darüber hinaus hat der Patient Daten wie Klarname, Adressdaten, Kontaktdaten, Versichertendaten in seinem Konto anzugeben (garrioCOM-Kontodaten für die Arztpraxis),

damit die Arztpraxis ihn identifizieren kann. Im Rahmen des Arzt-Patienten-Verhältnisses ist die Identifizierung und Transparenz essenziell. Diese Daten sind komplett Ende- zu Ende verschlüsselt.

- Die datenschutzrechtliche Verantwortung liegt für diese Daten **nicht** bei der garrio GmbH. Sie ist auch nicht Auftragsverarbeiter, da die Daten aufgrund der Verschlüsselungskonstruktion für die garrio GmbH anonymisiert sind und damit keine personenbezogenen Daten verarbeitet werden. Die garrio GmbH hat keine Möglichkeit auf Daten innerhalb der Konten zuzugreifen, diese einzusehen, zu ändern oder zu löschen, d. h. sie hat auch keine Möglichkeit Betroffenenrechten gemäß der DSGVO umzusetzen.
- Die datenschutzrechtliche Verantwortung liegt **beim Patienten** und - soweit Daten an die Arztpraxis übermittelt werden und dadurch in den Einflussbereich der Arztpraxis gelangen - **bei der Arztpraxis**.

Dies gilt sowohl für die „garrioCOM-Kontodaten für die Arztpraxis“ als auch für die Nachrichten (Gesundheitsdaten und -informationen, Befunde, Röntgenbilder, Arztbriefe, etc.), die der Patient dem Arzt schickt.

Die garrioCOM-Kontodaten für die Arztpraxis werden durch die Kopplung mit der Praxis für diese freigeschalten. Darüber hinaus bestimmt der Patient zu jeder Zeit selbst darüber, ob und welche Daten er an welche Praxis übermittelt. Auf das Konto des Patienten mit all seinen Inhalten hat einzig und allein der Patient Zugriff und Verfügungsgewalt.

garrioCOM: Nutzen und Verhältnis Arzt-Patient

garrio GmbH stellt den Arztpraxen und Patienten garrioCOM zur Verfügung, um sich im Rahmen des zwischen ihnen bestehenden oder sich anbahnenden Behandlungsvertrages (Art. 9 Abs. 2 lit. h, Abs. 3; Art. 6 Abs. 1 lit. b DSGVO) auszutauschen.

Der Patient muss sich mit den Praxen, die garrioCOM verwenden und mit denen er über diese Plattform kommunizieren möchte, koppeln. So kann die Praxis den Patienten eindeutig identifizieren.

Die Koppelung folgendermaßen möglich:

1. In der Praxis über einen QR Code, der vor Ort erstellt und anschließend vom Patienten über die App eingescannt wird (sichere Identifizierung).
2. Über einen allgemeinen QR-Code der Praxis, der über ein Schreiben der Praxis an die Patienten oder über Handzettel verteilt werden und vom Patienten über die App eingescannt wird (unsichere Identifizierung, wir empfehlen Arztpraxen vor der Versendung persönlicher Informationen über garrioCOM, einmal eine persönliche Verifizierung des Patienten in der Praxis vorzunehmen).

Ein Patient kann sich mit mehreren Praxen koppeln und sich mit den Praxen unabhängig voneinander austauschen.

Sicherheit, Funktionen

Die Plattform ist Ende zu Ende verschlüsselt. Die Schlüssel und Sicherheitsschlüssel, um die Inhalte im eigenen Konto zu entschlüsseln oder einen Kontozugang wiederherzustellen liegen ausschließlich bei den Nutzern (Die Schlüssel für die Nutzer einer Arztpraxis liegen bei den Nutzern der Arztpraxis, die Schlüssel für den Patienten liegen beim Patienten). Ohne diese Schlüssel kann ein verlorenes Passwort und damit ein verlorener Zugang zum eigenen Konto nicht wiederhergestellt werden. Die Nutzer werden deutlich darauf hingewiesen. [Freiwillige Möglichkeiten: Patient kann zusätzlich zu seinem Nutzernamen eine E-Mail-Adresse angeben, über die das Passwort zurückgesetzt werden kann. Außerdem kann auf expliziten Wunsch der Schlüssel bei garrio hinterlegt werden, was einzig dem Komfort dient; der Schlüssel wir ausschließlich zur Anmeldung verwendet. Schlüsselzuordnung erfolgt über sein Konto.

Ein Patient kann

- Nachrichten an die gekoppelte Arztpraxis senden und Nachrichten von der Arztpraxis empfangen,
- Dokumente (Arztbriefe, Diagnosen, Röntgenbilder, etc) über die App in sein Konto laden und an die Arztpraxis senden und entsprechende Dokumente empfangen.
- Der Patient kann sich mit mehreren Praxen koppeln.

Eine Arztpraxis kann

- Nachrichten an die mit der Praxis gekoppelten Patienten senden und Nachrichten von den Patienten empfangen,
- Dokumente (Arztbriefe, Diagnosen, Röntgenbilder, Rundschreiben etc) an die Patienten senden und entsprechende Dokumente empfangen.
- Vom Patienten über garrioCOM erhaltene Nachrichten und Dokumente werden im Konto der Arztpraxis sichtbar und gespeichert. Unterlagen können aus garrioCOM in die Patientenakte übernommen werden.

Zugriff durch Hersteller und Betreiber garrio GmbH

Betreiber/Hersteller von garrioCOM ist die garrio GmbH. Diese und ihre Mitarbeiter haben keinerlei Zugriffsmöglichkeiten auf die Daten, die zwischen Arztpraxis und Patienten ausgetauscht werden. Dies ist auch explizit so gewünscht, um einen geschützten Raum und vertraulichen Austausch zwischen Arztpraxis und Patienten zu gewährleisten.

Diese Situation ermöglicht keine Zuordnung der verschlüsselten Inhalte zu einem Benutzerkonto. Diese Situation ändert sich, wenn die Möglichkeit der Schlüsselhinterlegung bei garrio wahrgenommen wird, denn dadurch entsteht grundsätzlich die Möglichkeit der Entschlüsselung. Der Schlüssel wird jedoch ausschließlich für den Log-in und die Nutzung der App durch den Nutzer verwendet. Garrio greift **nicht** auf die Inhalte zu. Dieser Schutz wird durch technische und organisatorische Maßnahmen, z. B. Auditierung der Zugriffe, gewährleistet.

Videosprechstunde

Was ist erforderlich für die Teilnahme an einer Videosprechstunde?

Für die Teilnahme an einer Videosprechstunde benötigen Sie eine eigene Webcam, ein Mikrofon und einen modernen Browser. Unterstützt werden Google Chrome oder Mozilla Firefox.

Welche Sicherheitsmaßnahmen sind erforderlich?

Achten Sie darauf, dass während der Videosprechstunde keine unbefugte Person mithört und dass Ihr Gerät abgesichert ist (mit Virenschutz, Firewall usw.). Bitte beachten Sie, dass trotz aller technischen Maßnahmen Sicherheitsrisiken niemals vollständig ausgeschlossen werden können.

Werden meine Daten an Dritte weitergegeben?

Es werden keinerlei Informationen an Dritte weitergegeben. Während der Sprechstunde wird eine direkte Peer-to-Peer-Verbindung aufgebaut, bei der der Datenaustausch ausschließlich zwischen den beiden Sprechstundenteilnehmern stattfindet. Der Klarname des Patienten wird ebenfalls nur über diese Peer-to-Peer-Verbindung ausgetauscht und kann somit ausschließlich vom Arzt und keinem anderen Dritten eingesehen werden.

Was ist eine Peer-to-Peer Verbindung?

Im Kontext dieser Anwendung bezieht sich eine Peer-to-Peer-Verbindung auf eine direkte Verbindung zwischen den Teilnehmern der Videosprechstunde (Arzt und Patient). Um eine stabile Verbindung herzustellen, müssen die Adressen der beteiligten Nutzer ausgetauscht werden. Hierfür wird ein STUN-Server verwendet. Wenn es dem Server nicht möglich ist, den Adressaustausch durchzuführen (z. B. aufgrund einer zu restriktiv eingestellten Firewall), wird der Verbindungsaufbau abgebrochen. In solchen Fällen kann keine Videosprechstunde durchgeführt werden.

Wird die Internet-Kommunikation verschlüsselt?

Ja, Ihre Kommunikation wird durch verschiedene Protokolle abgesichert. Die Kommunikation mit dem Signal-Server erfolgt über TLS-Verschlüsselung. Eine eventuelle Dateiübertragung zum anderen Sprechstundenteilnehmer wird separat durch das DTLS-Protokoll verschlüsselt. Die verschlüsselte Übertragung von Medienströmen wie Video und Audio wird schließlich durch das SRTP-Protokoll gewährleistet.

Warum fordert mich mein Browser auf, bestimmte Rechte zu erteilen?

Ihr Browser fordert Sie auf, bestimmte Rechte zu erteilen, um bestimmte Funktionen und Zugriffe während der Videosprechstunde zu ermöglichen. Dies ist eine browser-spezifische Sicherheitsmaßnahme, die den Missbrauch von Kamera oder Mikrofon durch nicht vertrauenswürdige Seiten verhindert. Dies kann beispielsweise den Zugriff auf Ihre Kamera, Ihr Mikrofon oder andere Geräte betreffen, die für die reibungslose Durchführung der Videosprechstunde benötigt werden. Die Bereitstellung dieser Rechte ermöglicht eine optimale Nutzung der Funktionalitäten innerhalb der Videosprechstunde. Bitte gewähren Sie diese Rechte, um eine Videoverbindung starten zu können.

Klein- und Großgruppenvideosprechstunde

Die Videofunktion steht sowohl für Einzel- und Kleingruppen als auch für Großgruppen zur Verfügung.

Buchung, Abrechnung und Kündigungsfrist

Die Videosprechstundenfunktion wird per Lastschrifteinzug abgerechnet. Bitte beachten Sie, dass diese Zusatzfunktion mit einer Frist von drei Monaten zum Ende des Quartals gekündigt werden kann. Sollten Sie sich entscheiden, die Funktion zu kündigen, können Sie dies entsprechend der Frist tun. Es ist auch möglich, die Funktion nachträglich zu buchen oder die Anzahl der Ärztinnen/Ärzte zu erhöhen.

Ist die Videosprechstunde KBV-zertifiziert?

Für unsere Videosprechstunde nutzen wir die zertifizierte Lösung doccura+ (doccuraplus, Bayerische TelemedAllianz GmbH, https://www.kbv.de/media/sp/liste_zertifizierte-Videodienstanbieter.pdf, Stand 14.11.2024).

Sicherheit

Benutzerkonto

Für die Nutzung von garrioCOM werden diverse Benutzerkonten benötigt.

- Als Patient oder Patientin: dieses Konto kann während der Registrierung in der garrioCOM Smartphone-App für den Bereich "Patienten" selbst angelegt werden.
- Als Professional, also als Praxismitarbeiter oder Praxismitarbeiterin (Arzt oder Ärztin, MFA): dieses Konto wird von einem Praxis-Administrator im garrio-Administrations-Tool angelegt.
- Als Praxis-Administrator: die initialen Zugangsdaten für Ihr garrio-Administrations-Tool werden nach Eingang und Verarbeitung der Bestellung versendet.

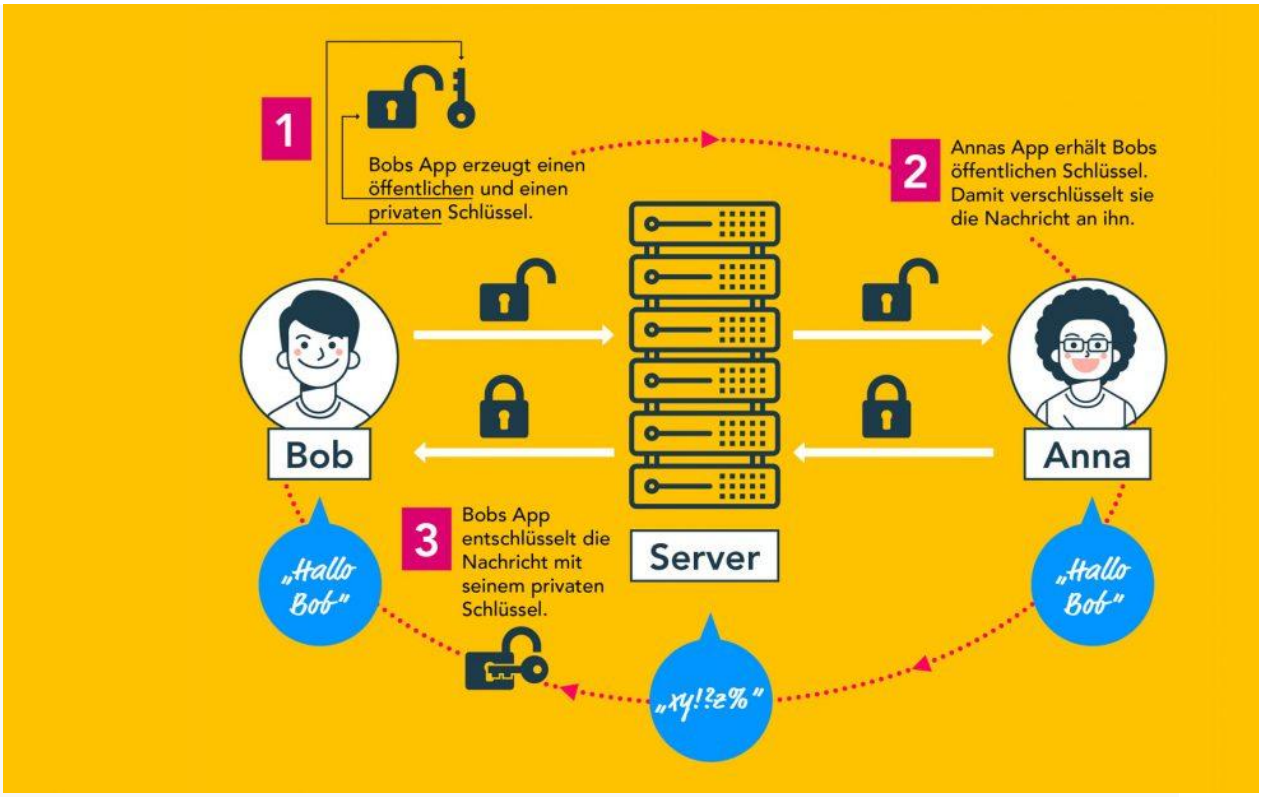
Zum Schutz des Kontos wird jeweils ein Passwort verwendet, welches die gängigen Sicherheitsmerkmale (geheim, Mindestlänge, verwendete Zeichen) aufweisen muss.

Ende-zu-Ende Verschlüsselung

Die mit garrioCOM gesendeten Nachrichten sind Ende-zu-Ende verschlüsselt. Dies bedeutet, dass nur die legitimen Teilnehmer eines Nachrichtenaustauschs Zugriff auf diese Nachrichten haben.

Dazu benötigen alle Teilnehmer einen sog. Sicherheitsschlüssel.

Hier ein einfacher Überblick zum Thema Ende-zu-Ende Verschlüsselung, häufig auch als End-to-End-Encryption (E2EE) bezeichnet.



Quelle: [mobilsicher.de]

Sicherheitsschlüssel

Der Sicherheitsschlüssel dient (einfach gesprochen) der Verschlüsselung und Entschlüsselung der Nachrichten. Jedes Benutzerkonto hat einen eigenen Sicherheitsschlüssel. Der Sicherheitsschlüssel kann bspw. nach Verlust neu erzeugt werden, der Zugriff auf ältere Nachrichten ist dann allerdings nicht mehr möglich.

Lokale Speicherung auf dem eigenen Gerät

Was bedeutet das?

Wenn Sie Ihren Sicherheitsschlüssel lokal speichern, bedeutet das, dass er ausschließlich auf Ihrem eigenen Gerät (z.B. Smartphone, Computer) gespeichert wird. Nur Sie haben Zugriff auf diesen Schlüssel. Achten Sie darauf, dass Sie den Schlüssel an einem wieder auffindbaren Ort ablegen (bspw. "Eigene Dokumente") und nicht in "Downloads" belassen, da dieser Ordner möglicherweise automatisch geleert wird und der Sicherheitsschlüssel dann verloren ist.

Hinweis: viele Geräte speichern Dokumente standardmäßig in der Cloud, also auf Systemen des Anbieters (bspw. iCloud bei Apple).

Vorteile:

- **Höchste Sicherheit:** Da der Schlüssel nur auf Ihrem Gerät gespeichert ist, ist er vor unbefugtem Zugriff durch Dritte am besten geschützt.
- **Volle Kontrolle:** Sie haben jederzeit die vollständige Kontrolle über Ihren Schlüssel und können ihn nach Belieben verwalten.
- **Keine Abhängigkeit:** Sie sind nicht von externen Diensten abhängig, um auf Ihre Nachrichten zugreifen zu können.

Nachteile:

- **Verlustrisiko:** Wenn Sie Ihr Gerät verlieren oder es beschädigt wird, kann Ihr Schlüssel unwiederbringlich verloren gehen.
- **Verwaltungsaufwand:** Sie müssen selbst für die sichere Aufbewahrung und Verwaltung Ihres Schlüssels sorgen.
- **Komplexität:** Für technisch weniger versierte Nutzer kann die Verwaltung eines privaten Schlüssels komplex sein.

Zentrale Speicherung im garrioCOM-System

Was bedeutet das?

Bei der zentralen Speicherung wird Ihr Sicherheitsschlüssel auf einem sicheren Server gespeichert, der von unserem Dienst betrieben wird. Sie haben weiterhin Zugriff auf Ihren Schlüssel, aber die Verwaltung erfolgt durch uns.

Vorteile:

- **Komfort:** Sie müssen sich nicht um die Verwaltung Ihres Schlüssels kümmern.
- **Zugriff von überall:** Sie können von jedem Gerät auf Ihre Nachrichten zugreifen, solange Sie Ihre Zugangsdaten haben.
- **Wiederherstellung:** Sollte Ihr Gerät verloren gehen, können Sie Ihren Schlüssel in der Regel wiederherstellen.

Nachteile:

- **Vertrauensfrage:** Sie müssen unserem Dienst vertrauen, dass Ihre Daten sicher gespeichert werden.
- **Potenzielles Risiko:** Obwohl wir höchste Sicherheitsstandards anwenden, besteht immer ein theoretisches Risiko, dass unbefugte Dritte Zugriff auf Ihren Schlüssel erhalten könnten.

Bewertung

Die Wahl zwischen lokaler und zentraler Speicherung hängt von Ihren individuellen Bedürfnissen und Ihrer Risikobewertung ab. Wenn Ihnen höchste Sicherheit und vollständige Kontrolle am wichtigsten sind, ist die lokale Speicherung die bessere Wahl. Wenn Sie Wert auf Komfort und einfache Handhabung legen, ist die zentrale Speicherung eine attraktive Option.

Hinweise zu lokalen Firewalls

Einleitung

Grundsätzlich sollte garrioCOM in Ihrer jeweiligen Praxis-Umgebung problemlos auf den unterstützten Browsern funktionieren. In manchen Fällen sind jedoch Firewalls o. ä. Schutzmaßnahmen aktiv, auf welche wir keinen Einfluss haben und welche entsprechende Regeln einstellen müssen. Diese finden Sie hier.

Notwendige Regeln

- Domains: *.garrio.de
- IP-Adresse: 94.186.181.222
- Ports: 443
- Sonstiges: es werden WebSockets (verschlüsselt) verwendet
- Es muss sichergestellt werden, dass diverse JavaScript Dateien von diesen Quellen geladen werden können. Beispielsweise blockieren manche Systeme den Zugriff auf nötige Skript-Dateien, die genannten Fehlermeldungen können dann so aussehen: "Laden fehlgeschlagen für das <script> mit der Quelle 'https://garrio.de/com/admin/_next/static/chunks/7521- f2bd62cc6fade827.js'."