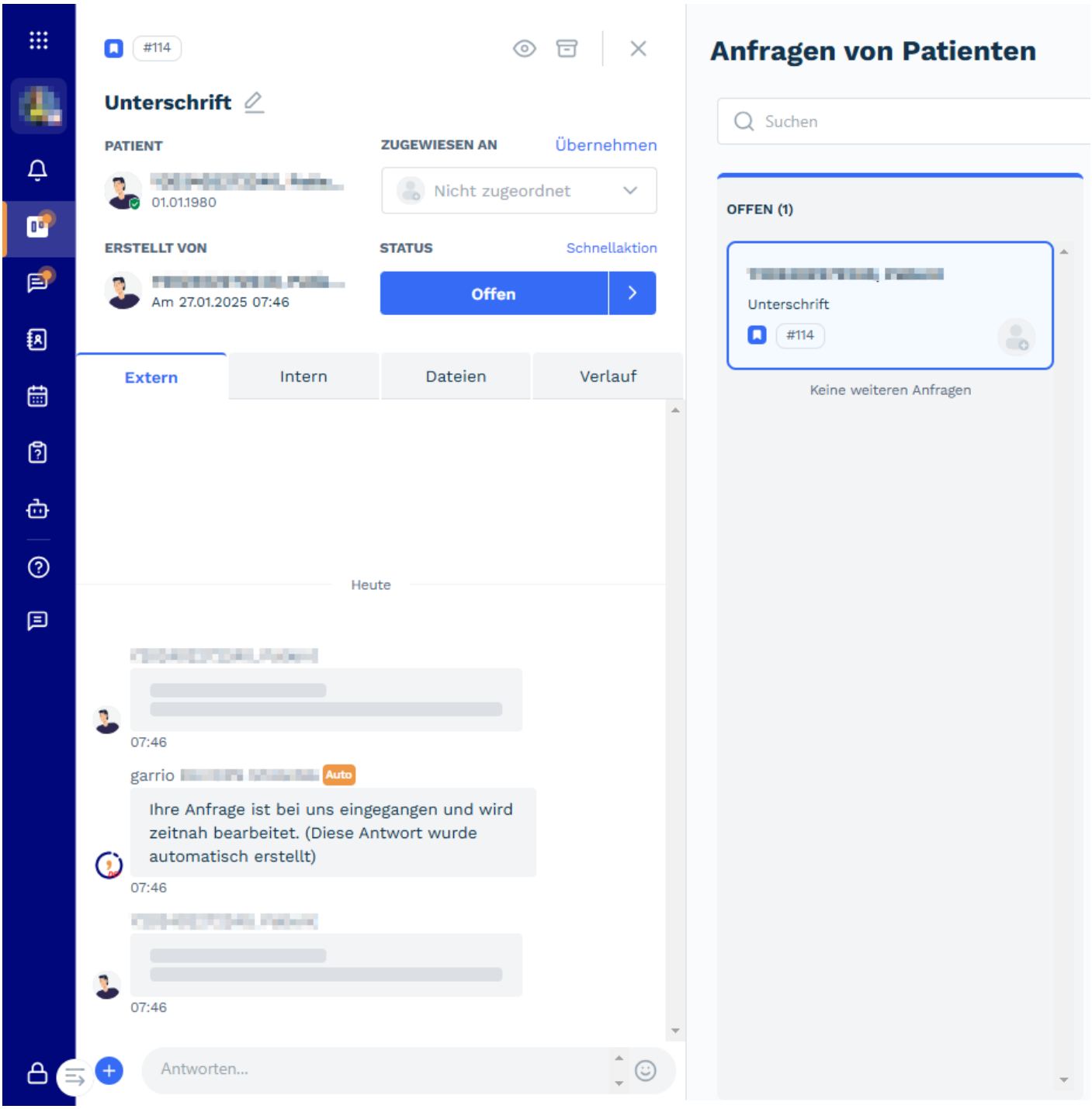
Die Nachrichten der Patienten werden nicht angezeigt

Beschreibung des Problems

In der Anfragepinnwand werden die Nachrichten von Patienten nicht dargestellt, da sie nicht entschlüsselt werden können. Die Nachrichten werden lediglich ausgegraut angezeigt, wie der beigefügte Screenshot veranschaulicht.



Lösung

Das beschriebene Problem ist als eine systemimmanente Sicherheitsfunktion zu betrachten. Der Hauptzweck dieser Sicherheitsfunktionen besteht darin, die Vertraulichkeit und Integrität der Kommunikation zu gewährleisten. Sie dienen dazu, sicherzustellen, dass ausschließlich die intendierten Empfänger die Nachrichten einsehen können und dass eine Manipulation der Nachrichten während der Übertragung unterbunden wird. Wenngleich es mitunter zu Unannehmlichkeiten kommen kann, wenn Nachrichten nicht entschlüsselt werden können, stellt dies einen wesentlichen Kompromiss für eine sichere Kommunikation dar.

Technische Hintergründe

Es existieren mehrere Gründe, warum Nachrichten versandt werden können, die der Empfänger nicht entschlüsseln und lesen kann. Diese Sicherheitsfunktionen dienen im Wesentlichen dem Schutz der Privatsphäre und der Integrität der Kommunikation. Die folgenden Ausführungen geben Aufschluss über die Hauptgründe und den Zweck dieser Funktionen.

Fehlende oder falsche Schlüssel

- **Wie es passiert:** Die Ende-zu-Ende-Verschlüsselung (E2EE) funktioniert durch den Austausch von kryptografischen Schlüsseln zwischen den Kommunikationspartnern. Jeder Teilnehmer besitzt einen privaten Schlüssel, der geheim gehalten wird, und einen öffentlichen Schlüssel, der mit anderen geteilt wird. Nachrichten werden mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und können nur mit dessen privatem Schlüssel entschlüsselt werden. Wenn der Empfänger keinen passenden privaten Schlüssel hat (z.B. weil er ein neues Gerät verwendet oder seinen Schlüssel zurückgesetzt hat), kann er die Nachricht nicht entschlüsseln.
- **Zweck:** Dies verhindert, dass jemand, der die Nachricht abfängt (z.B. ein Hacker oder der Serverbetreiber), den Inhalt lesen kann. Nur der rechtmäßige Empfänger mit dem passenden privaten Schlüssel kann die Nachricht entschlüsseln.

Nicht verifizierte Sitzungen

- **Wie es passiert:** Element (und andere E2EE-Messenger) ermöglichen es, mehrere Geräte gleichzeitig zu verwenden (z.B. Smartphone, Laptop, Tablet). Jedes dieser Geräte wird als "Sitzung" betrachtet. Die Option "Verschlüsselung auf verifizierte Sitzungen beschränken" sorgt dafür, dass Nachrichten nur an Sitzungen gesendet werden, die der Benutzer explizit als vertrauenswürdig verifiziert hat. Wenn diese Option aktiviert ist und der Absender eine Nachricht an ein Gerät sendet, das der Empfänger noch nicht verifiziert hat, kann die Nachricht nicht entschlüsselt werden.
- **Zweck:** Diese Funktion schützt vor sogenannten "Man-in-the-Middle"-Angriffen. Wenn ein Angreifer Zugriff auf ein unautorisiertes Gerät des Empfängers erlangt, könnte er Nachrichten abfangen. Durch die Verifizierung von Sitzungen stellt der Benutzer sicher, dass Nachrichten nur an seine vertrauenswürdigen Geräte gesendet werden.

Nachrichten gesendet, während der Empfänger offline war und keine Schlüssel verfügbar waren

- **Wie es passiert:** In einigen Fällen kann es vorkommen, dass eine Nachricht gesendet wird, während der Empfänger offline ist und sein Gerät keine Verbindung zum Server hat, um die notwendigen Schlüssel auszutauschen. Wenn der Empfänger später online geht, fehlen möglicherweise die notwendigen Informationen, um die Nachricht zu entschlüsseln.
- **Zweck:** Dies ist oft eine Folge der Art und Weise, wie E2EE implementiert ist. Es stellt sicher, dass Nachrichten auch dann nicht entschlüsselt werden können, wenn der Server kompromittiert wird.

Probleme mit der Zeit und Datums-Synchronisierung

- **Wie es passiert:** Kryptographische Prozesse sind oft zeitabhängig. Wenn die Systemzeit auf den Geräten von Sender und Empfänger stark abweicht, kann dies zu Problemen bei der Schlüsselvereinbarung und Entschlüsselung führen.
- **Zweck:** Dies ist eher eine technische Randbedingung, die aber dennoch relevant sein kann.

Version #4
Erstellt: 2025-01-24 15:20:25 CET
Zuletzt aktualisiert: 2026-06-17 11:46:25 CEST