

Wichtige Information an unsere Patientinnen und Patienten: IT-Sicherheitsvorfall

Genf, 2. Oktober 2026

Das externe Unternehmen, das uns bei der Betreuung unserer Informationssysteme unterstützt, wurde Opfer eines Cyberangriffs. Dieser Vorfall bei unserem Dienstleister hat möglicherweise dazu geführt, dass bestimmte Daten unserer Patientinnen und Patienten eingesehen oder abgerufen werden konnten.

Zum jetzigen Zeitpunkt ist es auf Grundlage der gemeinsam mit unserem Dienstleister durchgeführten Untersuchungen nicht möglich, die betroffenen Patientinnen und Patienten oder das genaue Ausmass des Vorfalls eindeutig zu bestimmen.

Sobald wir von dem Vorfall Kenntnis erhalten haben, haben wir unverzüglich die notwendigen Massnahmen ergriffen, um unsere Systeme zu sichern, die betroffenen Zugänge zu isolieren und gemeinsam mit Cybersicherheitsexperten vertiefte Untersuchungen einzuleiten.

Der Vorfall wurde dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) sowie dem Bundesamt für Cybersicherheit (BACS) gemeldet. Zudem wurde Strafanzeige erstattet.

FAQ & Empfehlungen für Patientinnen und Patienten

1. Um welche Art von Vorfall handelt es sich und welche Daten sind betroffen?

Es handelt sich um einen unbefugten Zugriff auf IT-Systeme über die Infrastruktur unseres externen Dienstleisters.

Personenbezogene und medizinische Daten, die in unserer Datenbank gespeichert sind, könnten möglicherweise eingesehen oder unbefugten Dritten zugänglich gemacht worden sein.

Die bisherigen technischen Untersuchungen haben jedoch nicht eindeutig ergeben, welche Daten tatsächlich eingesehen wurden oder welche Patientinnen und Patienten betroffen sein könnten.

Nach heutigem Kenntnisstand liegen uns keine Hinweise auf eine Veröffentlichung oder missbräuchliche Verwendung der möglicherweise betroffenen Daten vor.

Die technischen Untersuchungen sowie die Überwachung der Situation werden gemeinsam mit unserem Dienstleister intensiv fortgeführt, um den genauen Umfang der betroffenen Daten und Patientinnen und Patienten so präzise wie möglich festzustellen.

2. Welche Risiken bestehen für mich und was sollte ich beachten?

Aufgrund der Art der möglicherweise betroffenen Daten besteht das wichtigste Risiko in einer möglichen missbräuchlichen Verwendung, beispielsweise für Betrugsversuche, Phishing oder Identitätsmissbrauch.

Bis heute sind uns keine missbräuchliche Verwendung oder sonstige konkrete Folgen im Zusammenhang mit diesem Vorfall bekannt.

Vorsorglich empfehlen wir Ihnen dennoch:

- **Bleiben Sie aufmerksam:** Seien Sie vorsichtig bei verdächtigen Nachrichten per E-Mail, SMS, Telefon oder Post, die angeblich von unserer Einrichtung, Ihrer Ärztin oder Ihrem Arzt oder einer offiziellen Stelle stammen.
- **Geben Sie keine Codes oder Passwörter weiter:** Weder Mitarbeitende unseres Teams noch seriöse Institutionen werden Sie telefonisch oder per E-Mail nach Passwörtern, Zugangsdaten oder Bankinformationen fragen.
- **Prüfen Sie Rechnungen sorgfältig:** Kontrollieren Sie bei Mahnungen oder Rechnungen genau den Absender. Bei Zweifeln kontaktieren Sie uns bitte direkt, bevor Sie eine Zahlung vornehmen.

3. Sind meine medizinische Betreuung oder meine Termine betroffen?

Nein. Die Kontinuität Ihrer medizinischen Versorgung und die Sicherheit Ihrer Behandlungen sind vollständig gewährleistet. Ihre Behandlungen und Konsultationen finden wie gewohnt statt.

4. Welche Massnahmen wurden zur Bewältigung der Situation ergriffen?

- Unverzügliche Isolierung der betroffenen Zugänge und verstärkte Absicherung unserer gesamten Serverinfrastruktur.
- Umfassende Sicherheitsüberprüfung unserer Systeme in Zusammenarbeit mit zertifizierten Cybersicherheitsexperten.
- Meldung an die zuständigen Bundesbehörden sowie Einreichung einer Strafanzeige.
- Laufende Überwachung der Situation, um eine mögliche Veröffentlichung oder missbräuchliche Verwendung der betroffenen Daten frühzeitig zu erkennen.
- Strenge Überprüfung der Sicherheitsstandards und -protokolle sämtlicher Unterauftragnehmer und IT-Dienstleister.

5. An wen kann ich mich bei Fragen wenden?

Wir haben eine eigene Anlaufstelle eingerichtet, um Ihre Fragen zu diesem Vorfall zu beantworten:

E-Mail: dpo@ono.world

Online-Informationseite: cliniqueoeil-ono.ch/protection-des-données

Aktuelle Informationen zur Situation werden auf dieser Seite veröffentlicht.

Wir bedauern sehr, dass dieser Vorfall bei unserem Dienstleister bei Ihnen Besorgnis auslösen könnte, und danken Ihnen für Ihr Vertrauen und Ihre Aufmerksamkeit.