Informationsdokument über die Sicherheit der Authenticator-App

Gemäß § 139e Abs. 10 SGB V dürfen wir Ihnen, zusätzlich zur besonders sicheren Anmeldung mit der Gesundheits-ID, auch eine Anmeldung auf niedrigerem Vertrauensniveau per Authenticator-App anbieten. Dabei sind wir verpflichtet, Sie umfassend zu informieren. Dieses Dokument dient dieser Information.

Anmeldeoptionen bei Novego

Für den Zugang zu Ihrem Benutzerkonto in unserer DiGA stehen Ihnen zwei sichere Anmeldemethoden zur Verfügung:

- **Benutzername und Passwort + Authenticator-App**
  Sicherheitsniveau: **„substanziell“** (laut Bundesamt für Sicherheit in der Informationstechnik, BSI)
- **Gesundheits-ID**
  Sicherheitsniveau: **„hoch“** (höchste vom BSI definierte Schutzstufe)

Das BSI unterscheidet drei Stufen:

- **Niedrig** – Basisschutz
- **Substanziell** – starker Schutz
- **Hoch** – sehr starker Schutz, insbesondere für Gesundheitsdaten

Wie funktioniert die Authenticator-App?

Sie laden eine Authenticator-App (Microsoft Authenticator, Google Authenticator, FreeOTP) auf Ihr Smartphone herunter. Bei der erstmaligen Einrichtung wird Ihr Benutzerkonto in der DiGA mit der App verknüpft. Ab diesem Zeitpunkt erzeugt die Authenticator-App bei jedem Login einen zufällig generierten 6-stelligen Zahlencode, der nur für kurze Zeit gültig ist. Diesen Code geben Sie zusätzlich zu Ihrem Benutzernamen und Passwort ein. Dadurch ist Ihr Konto besser geschützt, weil ein Angreifer Ihr Passwort allein nicht mehr nutzen kann. Er müsste zusätzlich Zugriff auf Ihr Smartphone haben.

Schutzwirkung und Restrisiken

Vorteile:

- Schutz vor automatisierten Angriffen wie Brute-Force
- Keine dauerhafte Speicherung von Zahlencodes im Klartext
- Komfortable Nutzung ohne zusätzliche Hardware

Einschränkungen (gegenüber Gesundheits-ID):

- Geringerer Schutz bei Verlust oder Diebstahl des Smartphones
- Kein Schutz auf „hohem“ Niveau gegen staatlich organisierte oder technisch sehr aufwendige Angriffe
- Manipulierte Apps oder kompromittierte Geräte könnten die Sicherheit untergraben

Verantwortung der Nutzer:innen:

- Gerät absichern (PIN, Biometrie, regelmäßige Updates)
- Authenticator-App nur aus offiziellen App-Stores installieren
- Keine Weitergabe des Codes