

SBK Pressemeldung

Digitale Identifikation: Datenschutz auf europäischer Grundlage

Europaweit einheitliche Vertrauensniveaus regeln, wie man sich für eine digitale Anwendung identifizieren kann. Die SBK erklärt, welche Auswirkungen das auf die Identifikationsprozesse im Gesundheitswesen hat.

Wissen Sie, was der Unterschied zwischen Identifikation und Authentifizierung ist? Was eIDAS und Vertrauensniveaus sind? Die fortschreitende Digitalisierung, die Einführung von digitalen Identitäten, und der elektronischen Patientenakte (ePA) für alle sowie die verstärkte Nutzung von Daten zu Forschungszwecken wird die Diskussionen um Chancen aber auch Risiken rund um ein digitales Gesundheitswesen in Deutschland anfachen. Im Mittelpunkt die Frage: Wie können wir die gesammelten Gesundheitsdaten soweit schützen, dass ein Missbrauch so weit möglich ausgeschlossen ist? Die folgenden Begriffe werden dabei immer wieder auftauchen.

Am Anfang steht die Identifikation

Wenn von Identifikation die Rede ist, geht es um die erste Anmeldung an einer Anwendung. Um einen Service zu nutzen, muss man sich erstmalig registrieren. Das kennt jeder zum Beispiel vom Online-Einkauf – auch hier wird ein Kundenkonto angelegt, man bekommt einen Nutzernamen und kann sich ein Passwort wählen. Gleiches gilt für das Online-Banking oder eben die Nutzung von Krankenkassen-App und ePA.

Ist dieses Kundenkonto oder der Account erst einmal angelegt, ist es erforderlich, sich bei jedem weiteren Login mit den entsprechenden Zugangsdaten anzumelden. Das wird als Authentifizierung bezeichnet. Bei einer 2-Faktor-Authentifizierung (2FA) muss die Authentifizierung doppelt abgesichert sein, z.B. mit einem Passwort und einem Code, den eine App auf dem Smartphone generiert. Wichtig dabei: Die Absicherungsfaktoren sollten dabei aus unterschiedlichen Kategorien stammen – man spricht dabei von einer Kombination aus Wissen und Besitz. Zur Kategorie „Wissen“ gehört dabei das Passwort oder eine PIN, zur Kategorie „Besitz“ die Chipkarte oder das Smartphone mit dem Code-Generator.

eIDAS-Verordnung: europäische Grundlage für den Schutz der Daten

Die Abkürzung eIDAS steht für „Electronic Identification And Trust Services“. Die so genannte eIDAS-Verordnung enthält verbindliche, europaweit geltende Regelungen in den Bereichen „elektronische Identifizierung“ und „elektronische Vertrauensdienste“.

Ganz vereinfacht gesagt wird darin festgelegt, wie „sicher“ die Identifikation für die unterschiedlichen digitalen Anwendungen gestaltet sein soll. In der Folge gibt diese Festlegung den Ausschlag, wie die Identifikation ausgestaltet werden kann: Reicht eine einfache E-Mail, um sich einen Account anzulegen? Muss man sich einen Passwort-Brief per Post zuschicken lassen oder sich sogar persönlich ausweisen?

Dabei schreibt die Verordnung keine Technologien und Umsetzungen vor. Sie definiert lediglich drei Vertrauensniveaus für Anwendungen: niedrig, substanziell und hoch.

- Ist das Vertrauensniveau „niedrig“, muss der Identitätsnachweis in einer Art und Weise erbracht werden, dass man diesem in geringem Maße vertrauen kann und damit die Gefahr eines Identitätsmissbrauchs verringert wird.
- Ist das Vertrauensniveau „substanziell“, muss der Identitätsnachweis in einer Art und Weise erbracht werden, dass man diesem in gesteigertem Maße vertrauen kann und damit die Gefahr eines Identitätsmissbrauchs maßgeblich verringert wird.
- Ist das Vertrauensniveau „hoch“, muss der Identitätsnachweis in einer Art und Weise erbracht werden, dass man diesem in hohem Maße vertrauen kann und damit die Gefahr eines Identitätsmissbrauchs ausgeschlossen wird.

Gesundheitsdaten haben einen besonders schützenswerten Charakter

Das Vertrauensniveau einer Anwendung definiert sich aus dem Schutzbedarf der Daten, welche innerhalb der Anwendung verarbeitet werden. Gesundheitsdaten wird gemäß EU-DSGVO ein „besonders schützenswerter Charakter“ zugeschrieben. Dementsprechend liegt das Schutzniveau auf der Stufe „hoch“ gemäß eIDAS.

Dieses hohe Niveau erfüllen aktuell zwei Identifikationswege:

1. Identifikation mittels elektronischer Gesundheitskarte (eGK) und dazugehöriger PIN, da der Ausgabe der PIN eine Identifikation auf hohem Vertrauensniveau vorausgeht
2. Identifikation mittels Online-Ausweisfunktion des Personalausweises

Die Festlegung, welche Technologie welchem Niveau entspricht, erfolgt einheitlich in Europa in Form einer sogenannten Notifizierung durch die EU-Kommission.

Trotz europäischer Regelungen herrscht Uneinigkeit

Eine einheitliche Grundlage für Vertrauensniveaus, europaweite Regelungen rund um die Identifikation – da sollte doch eigentlich alles klar sein. Doch Identifikation und Authentifizierung im digitalen Gesundheitswesen sorgen immer wieder für Diskussionen. Denn die Datenschutzbehörden in Deutschland legen die europäische Verordnung besonders streng aus. Stufenpläne zur schrittweisen Einführung eines hohen Schutzniveaus bei der Identifikation oder auch ein freiwilliger Verzicht des Nutzers auf das hohe Schutzniveau bei der Authentifizierung sind in anderen Ländern kein Problem. Hier werden sie von den Datenschutzbehörden abgelehnt.

Über die SBK:

Die SBK Siemens-Betriebskrankenkasse ist die größte Betriebskrankenkasse Deutschlands und gehört zu den 20 größten gesetzlichen Krankenkassen. Als geöffnete, bundesweit tätige Krankenkasse versichert sie mehr als eine Million Menschen und betreut über 100.000 Firmenkunden in Deutschland – mit mehr als 1.800 Mitarbeiterinnen und Mitarbeitern in 86 Geschäftsstellen.

Seit über 100 Jahren setzt sich die SBK persönlich und engagiert für die Interessen der Versicherten ein. Sie positioniert sich als Vorreiter für einen echten Qualitätswettbewerb in der gesetzlichen

Krankenversicherung. Voraussetzung dafür ist aus Sicht der SBK mehr Transparenz für die Versicherten – über relevante Finanzkennzahlen, aber auch über Leistungsbereitschaft, Beratung und Dienstleistungsqualität von Krankenkassen. Im Sinne des Kunden vereint die SBK darüber hinaus das Beste aus persönlicher und digitaler Welt und treibt die Digitalisierung im Gesundheitswesen aktiv voran.

Für Rückfragen:

SBK Siemens-Betriebskrankenkasse

Franziska Herrmann

Stab Unternehmenskommunikation

Heimeranstr. 31

80339 München

Tel.: +49 89 62700-710

Fax: +49 89 62700-60710

E-Mail: franziska.herrmann@sbk.org

Internet: www.sbk.org