nevis®

Nevis für gesetzliche und private Kranken-versicherungen

Customer Identity & Access Management
und Strong Customer Authentication
aus einer Hand

Making Security an experience.

Die Herausforderungen für Krankenversicherungen

1

Elektronische Patientenakte

Die elektronische Patientenakte (ePA) wird bereits seit 2021 von den Krankenversicherungen angeboten. Ab 2024 müssen die Krankenkassen den Versicherten ergänzend zur elektronischen Gesundheitskarte – die den Geltungsbereich verschiedener Gesetze wie zum Beispiel das DSGVO und Krankenversicherungsrecht berührt – einen sicheren, digitalen Zugang bereitstellen.

2

Cybersecurity Risiken

Das Gesundheitswesen ist einem breiten Spektrum von Bedrohungen durch Cyberangriffe ausgesetzt. Es besteht ein hohes Risiko von Datenschutzverletzungen, da geschützte Gesundheitsdaten (PHI) für Hacker am wertvollsten sind. Die Bedrohungslandschaft entwickelt sich ständig weiter, was bedeutet, dass die Krankenversicherungen kontinuierlich ihre Abwehrmassnahmen aktualisieren müssen.

3 Einhaltung von Rechtsvorschriften und Datenschutz

Die Gesundheitsbranche muss eine Vielzahl von Rechtsvorschriften einhalten, darunter Vorschriften wie die DSGVO, das Krankenversicherungsrecht und das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG). Diese verlangen von gesetzlichen Krankenkassen und privaten Krankenversicherungen, personenbezogene Kundendaten nachweislich bei der Erhebung, Speicherung und Weiterverarbeitung in allen verwendeten Systemen zu schützen. Diese Anforderungen können sehr komplex und dynamisch sein und erfordern eine kontinuierliche Überwachung und Anpassung.

4 Sektorale Identitätsanbieter

Mit der Einführung des eRezepts setzte die Gematik erstmals auf das Modell eines Identity Provider-Dienstes. Die neuen sektoralen IDPs sollen von den eHealth Anbietern bereitgestellt werden, sodass jeder Anbieter die digitalen Identitäten selbst verwaltet und die Authentifizierung ihrer Kunden durchführt. Es muss sichergestellt werden, dass die notwendige Infrastruktur und das Know-how vorhanden sind, um die Implementierung reibungslos durchzuführen.

Eine sorgfältige Planung und Umsetzung der Lösungen ist erforderlich, um diese Anforderungen zu erfüllen.

5 Verstärkter Wettbewerb

Kunden erwarten zunehmend eine personalisierte und nahtlose Kundenerfahrung, die von den digitalen Technologien, die sie täglich nutzen, geprägt ist. Krankenkassen und Versicherer müssen in der Lage sein, mit den Kundenerwartungen Schritt zu halten und sich schnell an diese Entwicklungen anzupassen, um wettbewerbsfähig zu bleiben. Negative Nutzererfahrungen lassen Versicherte zu anderen Kassen und Versicherungen wechseln.

6 Bedarf an einfachen und sicheren Authentifizierungslösungen

Kundenakzeptanz: Neue Authentifizierungslösungen können für Kunden verwirrend sein, was zu Frustration oder Ablehnung führen kann. eHealth Anbieter müssen sowohl ihre Kunden über die neuen Lösungen informieren und sie bei der Einführung begleiten, als auch sicherstellen, dass ihre Lösungen sicher und robust sind, um Cyberangriffe oder Missbrauch zu verhindern.

7 Anforderungen für DiGA und DiPA

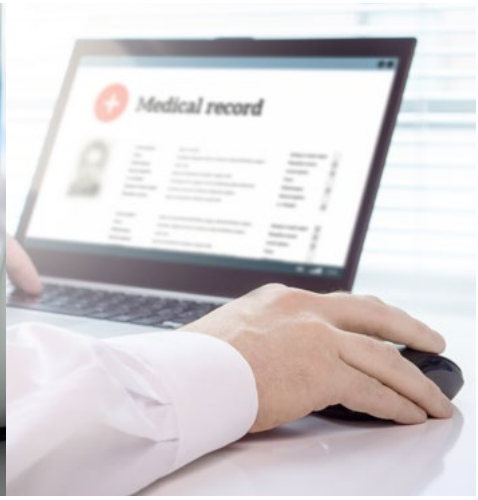
Das BfArM hat neue Prüfkriterien für die Anforderungen an den Datenschutz bei DiGA und DiPA veröffentlicht, welche künftig Grundlage für neue Zertifikate sein werden. Hersteller von Gesundheits- und Pflegeanwendungen müssen nachweisen, dass ihre Anwendungen datenschutzkonform sind und nur berechtigte Personen Zugriff auf Patientendaten haben. Diese umfassen sowohl die Anforderungen der europäischen Datenschutz-Grundverordnung als auch die erweiterten Anforderungen für DiGA und DiPA.

8 Kundenwunsch nach Datensouveränität

Kunden und Patienten erwarten, dass sie ihre Daten sicher und vertraulich behandeln und gleichzeitig den Zugriff auf ihre Daten erleichtern. eHealth-Anbieter müssen daher Wege finden, um Kunden die Kontrolle über ihre Daten zu geben indem sie transparente Datenschutzpraktiken implementieren und die Kunden darüber informieren, wie ihre Daten gesammelt, gespeichert und verwendet werden.

So unterstützt Nevis die Gesundheitsbranche

Vom sicheren Onboarding bis hin zur lebenslangen Kundenbeziehung



Effizientes Identity-Management

Nevis ist das Herzstück der Sicherheits-Infrastruktur von Krankenkassen und Versicherer. Mit Nevis gelingt die Umsetzung der zentralen Identity-Management-Prozesse effizient:

- Account-Aktivierung/Selbstregistrierung
- Bestellung neuer Services und Berechtigungen
- Linken von Identitäten und Credentials
- Delegierte Administration: Berechtigungsverwaltung durch Kunden

Vereinfachter digitaler Zugang

Nevis stellt sicher, dass ein Login-Vorgang, der Zugriff auf eine Applikation oder ein Geschäftsvorgang dem autorisierten Fachkreis zugeordnet werden kann:

- Ärzte, Fachexperten oder Pflegepersonal loggen sich sekundenschnell in das eHealth-Portal ein
- Die Benutzer rufen bequem Patientendaten ab, führen Aktualisierungen oder Transaktionen durch
- Benutzer bestätigen Freigaben mit Fingerabdruck oder Face ID statt mit dem unsicheren Passwort
- Nevis sorgt zudem für verlässliche Verfügbarkeit des eHealth-Portals rund um die Uhr

Beliebte Funktionen

Identity-Management-Lösungen für Dienstleister im Gesundheitswesen decken neben den üblichen IDM-Prozessen weitere beliebte Funktionen ab. Nevis bietet:

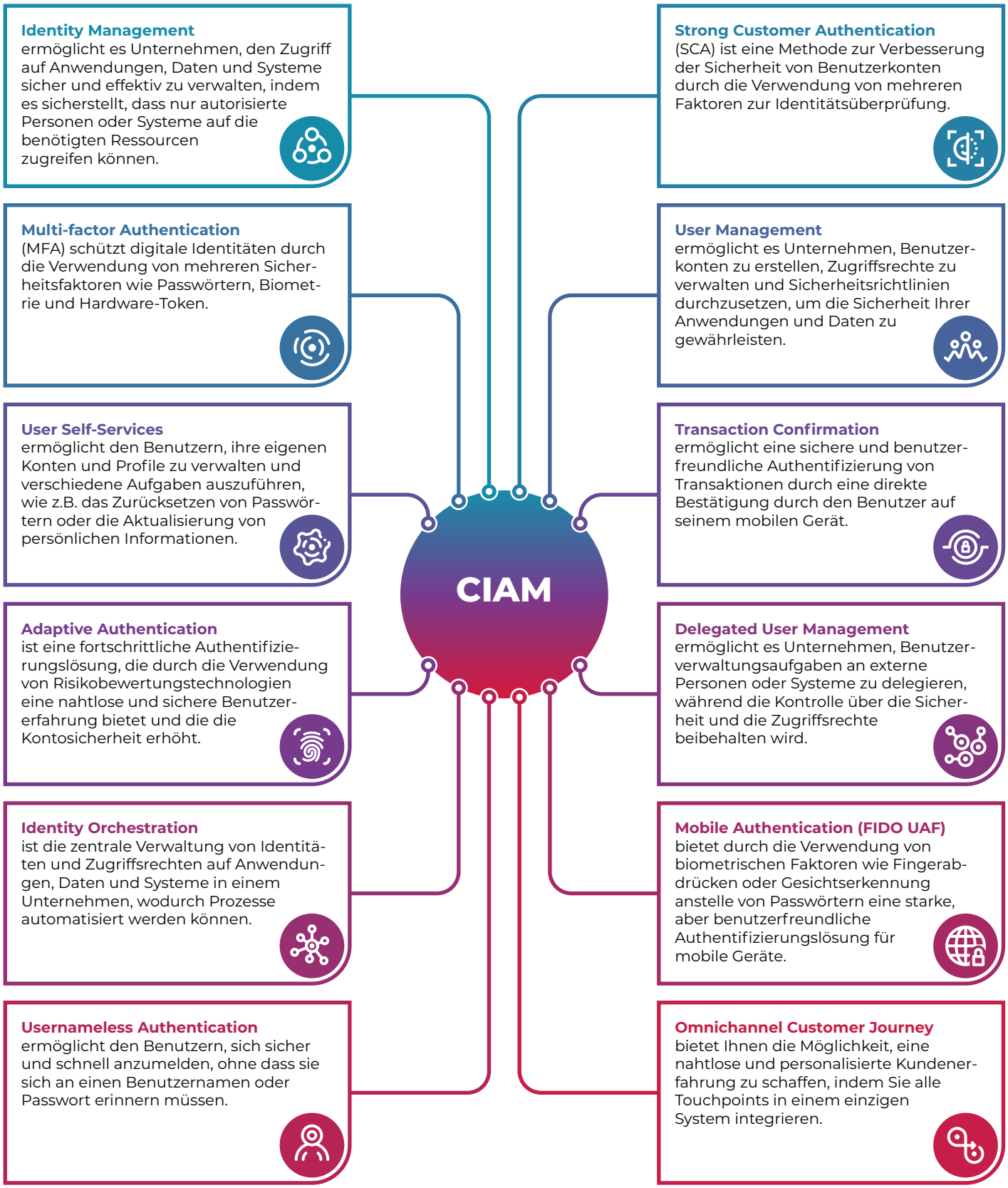
- Austausch von Stammdaten mit dem Kern-System
- Provisionierung der Identity-Daten in verschiedene Umsysteme
- Unterstützung verschiedener Authentisierungsmittel: mTAN, SuisseID, HPC Card, Soft Certs etc.
- Autorisierung auf der Basis von Rollen und Benutzerattributen
- Integration spezieller Client-Software
- Single-Sign-on für Web-Applikationen und weitere Services für den sicheren Datenaustausch

Anbieter von digitalen Leistungen in der Gesundheitsbranche sind sich bewusst, dass sie äusserst sensible Patientendaten schützen müssen. Zudem ist es im Gesundheitswesen wichtig, sehr wirtschaftlich zu arbeiten. Leistungsträger wie Allgemein- und Fachärzte, Kliniken, Röntgeninstitute und Labore, aber auch Krankenversicherungen und Verwaltungen sollten daher über eine effiziente digitalisierte Prozesskette zusammenarbeiten. Da dabei mitunter hochsensible Informationen übertragen werden, ist eine einwandfrei funktionierende Infrastruktur die Voraussetzung für die Partizipation an der integrierten Gesundheitsversorgung.

Die Kundenidentitäts- und Zugriffsverwaltung (Customer Identity and Access Management, CIAM) bietet genau das und trägt gleichzeitig dazu bei, die Kundenbindung zu festigen. Mit CIAM sind eHealth-Anbieter in der Lage, Identitäts- und Profildaten von Kunden zu erfassen und zu organisieren und den Kundenzugriff auf Anwendungen, Dienste, und Online-Profile zu verwalten.

CIAM verbindet Sicherheit, Analytik und Kundenerfahrung zu einer perfekten Lösung für das Daten- und Zugriffsmanagement.

Die wichtigsten CIAM Funktionen für die Gesundheitsbranche



Identity Management
ermöglicht es Unternehmen, den Zugriff auf Anwendungen, Daten und Systeme sicher und effektiv zu verwalten, indem es sicherstellt, dass nur autorisierte Personen oder Systeme auf die benötigten Ressourcen zugreifen können.

Multi-factor Authentication
(MFA) schützt digitale Identitäten durch die Verwendung von mehreren Sicherheitsfaktoren wie Passwörtern, Biometrie und Hardware-Token.

User Self-Services
ermöglicht den Benutzern, ihre eigenen Konten und Profile zu verwalten und verschiedene Aufgaben auszuführen, wie z.B. das Zurücksetzen von Passwörtern oder die Aktualisierung von persönlichen Informationen.

Adaptive Authentication
ist eine fortschrittliche Authentifizierungslösung, die durch die Verwendung von Risikobewertungstechnologien eine nahtlose und sichere Benutzererfahrung bietet und die die Kontosicherheit erhöht.

Identity Orchestration
ist die zentrale Verwaltung von Identitäten und Zugriffsrechten auf Anwendungen, Daten und Systeme in einem Unternehmen, wodurch Prozesse automatisiert werden können.

Usernameless Authentication
ermöglicht den Benutzern, sich sicher und schnell anzumelden, ohne dass sie sich an einen Benutzernamen oder Passwort erinnern müssen.

Strong Customer Authentication
(SCA) ist eine Methode zur Verbesserung der Sicherheit von Benutzerkonten durch die Verwendung von mehreren Faktoren zur Identitätsüberprüfung.

User Management
ermöglicht es Unternehmen, Benutzerkonten zu erstellen, Zugriffsrechte zu verwalten und Sicherheitsrichtlinien durchzusetzen, um die Sicherheit Ihrer Anwendungen und Daten zu gewährleisten.

Transaction Confirmation
ermöglicht eine sichere und benutzerfreundliche Authentifizierung von Transaktionen durch eine direkte Bestätigung durch den Benutzer auf seinem mobilen Gerät.

Delegated User Management
ermöglicht es Unternehmen, Benutzerverwaltungsaufgaben an externe Personen oder Systeme zu delegieren, während die Kontrolle über die Sicherheit und die Zugriffsrechte beibehalten wird.

Mobile Authentication (FIDO UAF)
bietet durch die Verwendung von biometrischen Faktoren wie Fingerabdrücken oder Gesichtserkennung anstelle von Passwörtern eine starke, aber benutzerfreundliche Authentifizierungslösung für mobile Geräte.

Omnichannel Customer Journey
bietet Ihnen die Möglichkeit, eine nahtlose und personalisierte Kundenerfahrung zu schaffen, indem Sie alle Touchpoints in einem einzigen System integrieren.

Geschützt durch Compliance

Die Gesundheitsbranche im Allgemeinen steht laut DSGVO in der Pflicht, personenbezogene Kundendaten nachweislich bei der Erhebung, Speicherung und Weiterverarbeitung in allen verwendeten Systemen zu schützen. Mit Nevis können Gesundheitseinrichtungen sicherstellen, dass ihre IT-Systeme den geltenden Vorschriften und Gesetzen entsprechen. Mit Nevis sind Sie unter anderem automatisch regelkonform nach DSGVO, HIPAA, HITECH, Electronic Prescription of Controlled Substances (EPCS) – und vermeiden unnötige und kostspielige Sanktionen, die Ihrem Unternehmen und dessen Reputation Schaden zufügen.

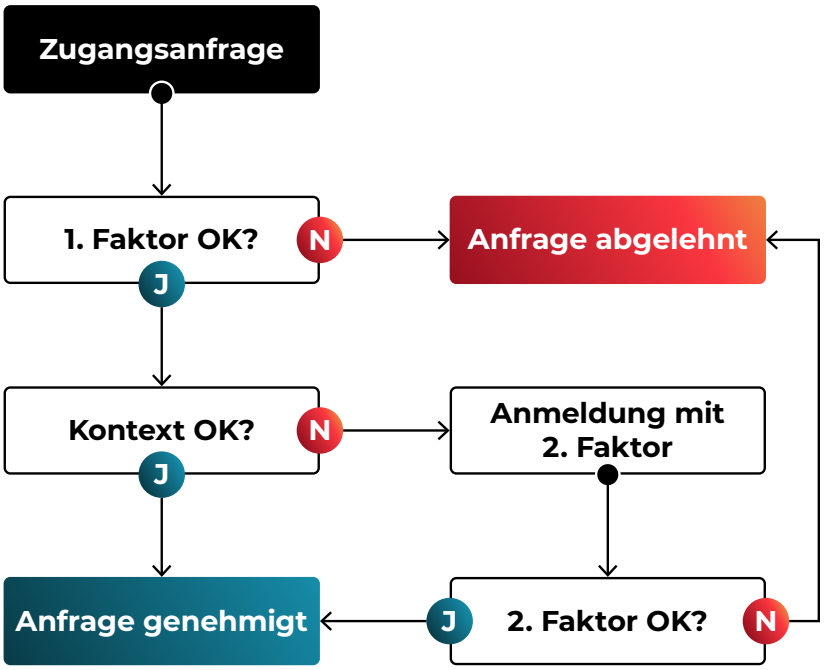
Bequemes Login ohne Sicherheitsverlust

Die heutigen Nutzer von eHealth-Diensten haben nicht nur hohe Erwartungen an die Benutzerfreundlichkeit, sondern legen auch mehr denn je Wert auf einen angemessenen Schutz ihrer persönlichen Daten. Eine Einschränkung der Benutzerfreundlichkeit um der Sicherheit willen oder umgekehrt ist daher keine Option. Das Online-Portal muss daher die Nutzung eines neuen Login-Verfahrens ermöglichen und ausbauen.

Adaptive Authentication

Adaptive Authentication ermöglicht es Gesundheitseinrichtungen, die Authentifizierungsstärke an das jeweilige Risiko anzupassen und so eine sichere Umgebung für Patientendaten gewährleisten.

Wie es funktioniert:



Risikobewertung: Wenn ein Benutzer auf Patientendaten zugreifen möchte, bewertet das System das mit der Anfrage verbundene Risiko anhand von Kriterien wie dem Standort des Benutzers, dem Gerät und dem Zeitpunkt des Zugriffs.

Authentifizierungsstärke: Basierend auf der Risikobewertung entscheidet das System über die erforderliche Authentifizierungsstärke. Sollte die Bewertung als risikoreich ausfallen, werden zusätzliche Authentifizierungsmassnahmen verlangt.

Zugriffskontrolle: Sobald der Benutzer die erforderliche Authentifizierung bereitgestellt hat, gewährt oder verweigert das System anhand der Risikobewertung und der Stärke der Authentifizierung den Zugriff auf die Patientendaten.

Der Gesundheitssektor vertraut auf Nevis

«Der kontinuierliche Ausbau der HIN Plattform erfolgt in enger Abstimmung mit Nevis. Unser gemeinsames Ziel ist und bleibt es, die Digitalisierung des Schweizer Gesundheitswesens und die damit einhergehenden Zugewinne an Nutzerkomfort und Effizienz weiter voranzutreiben.»

Aaron Akeret
Solution Engineer & Enterprise Architect
Health Info Net AG

Erfolgsstories

MediData

MediData – Geschützte Gesundheitsdaten

HIN

HIN – IAM für Gesundheits-Informationsnetzwerk

Kontaktieren Sie uns für ein Beratungsgespräch.

Schweiz (HQ)	+41 43 508 06 81
Deutschland	+49 89 3803 8684
Grossbritannien	+44 20 4579 0404

oder via Kontaktformular:

nevis®

Making security an experience.

Über Nevis

Die Nevis Security AG ist ein Pionier in der digitalen Sicherheit und macht sich weltweit für den Einsatz passwortloser, benutzerfreundlicher Zugangslösungen stark. Als Schweizer Marktführer im Bereich Customer Identity and Access Management (CIAM) stattet Nevis Organisationen aus dem Finanz-, Versicherungs- und iGaming-Sektor mit einem Höchstmass an Datenschutz und nahtlosen Authentifizierungsverfahren aus. Nevis-Technologie sichert mehr als 80 Prozent der Online-Banking-Transaktionen in der Schweiz ab – ein Indiz für Expertise und Engagement für Innovation. Mit Hauptsitz in Zürich/Schweiz und Niederlassungen in ganz Europa baut Nevis seine globale Präsenz durch ein schnell wachsendes Partnernetzwerk permanent aus und unterstreicht damit seine Rolle als wichtiger Akteur im digitalen Ökosystem. Nevis strebt danach, seine Stellung als führende Instanz im Bereich der digitalen Identitätssicherheit weltweit zu stärken und skalierbare, zukunftsweisende Lösungen bereitzustellen, die den wachsenden Anforderungen seiner Kunden gerecht werden.

www.nevis.net