Patientenportale im Verbund sicher betreiben

WIE EIN VIER-FAKTOREN-MODELL DIE SICHERHEIT IN MULTI-TENANT-CLOUDS GEWÄHRLEISTET

Online-Termine buchen, Befunde und Medikationspläne abrufen, sicher mit Ärzten kommunizieren. Was für Patienten selbstverständlich erscheint, basiert auf komplexen Krankenhausportalen. Diese Plattformen sind heute unverzichtbar für Patienten, Ärzte, Mitarbeitende und Partner. Sie bieten Funktionen wie Terminmanagement, Datenaustausch, Dokumentenverwaltung und die Anbindung an die Telematikinfrastruktur. Doch sie bergen auch Risiken und können Einfallstore für Cyberangriffe sein.

Dies gilt insbesondere für Verbundportale, über die 50, 100 oder mehr Kliniken eine gemeinsame Plattform nutzen. Ihre Architektur unterscheidet sich grundlegend von Einzelhaus-Lösungen: Multi-Tenant-Clouds verarbeiten Daten unterschiedlicher Träger von kommunalen Kliniken bis zu Universitätskrankenhäusern. Die zugrunde liegende Interoperabilitätsplattform ermöglicht den Datenaustausch zwischen verschiedenen Systemen und Standorten. Dafür führt sie Daten aus unterschiedlichen Quellen zusammen und sorgt für ein nahtloses Zusammenspiel über Organisationsgrenzen hinweg.

ENTSCHEIDEND BLEIBT DIE KONTINUIERLICHE ÜBERPRÜFUNG IN DER PRAXIS – DENN SICHERHEIT IST EIN FORTLAUFENDER PROZESS.

Andreas G. Henkel, Chief Product Officer, the i-engineers GmbH/AG, www.tie.ch/

Lokale Gateways verbinden die Plattform mit Krankenhausinformationssystemen, PACS und spezialisierten Lösungen wie Laborinformationssystemen. Es entsteht ein komplexes Geflecht von Verantwortlichkeiten, das klare Governance erfordert. Zugleich wächst der regulatorische Druck: Seit Juli 2025 ist das BSI-C5-Testat für Cloud-Dienste im Gesundheitswesen verpflichtend, seit Dezember 2025 gelten für rund 29.500 Einrichtungen verschärfte Meldepflichten nach NIS2. IT-Verantwortliche brauchen daher neue Ansätze, um diese Komplexität sicher zu beherrschen.

Das Vier-Faktoren-Modell der Portalsicherheit

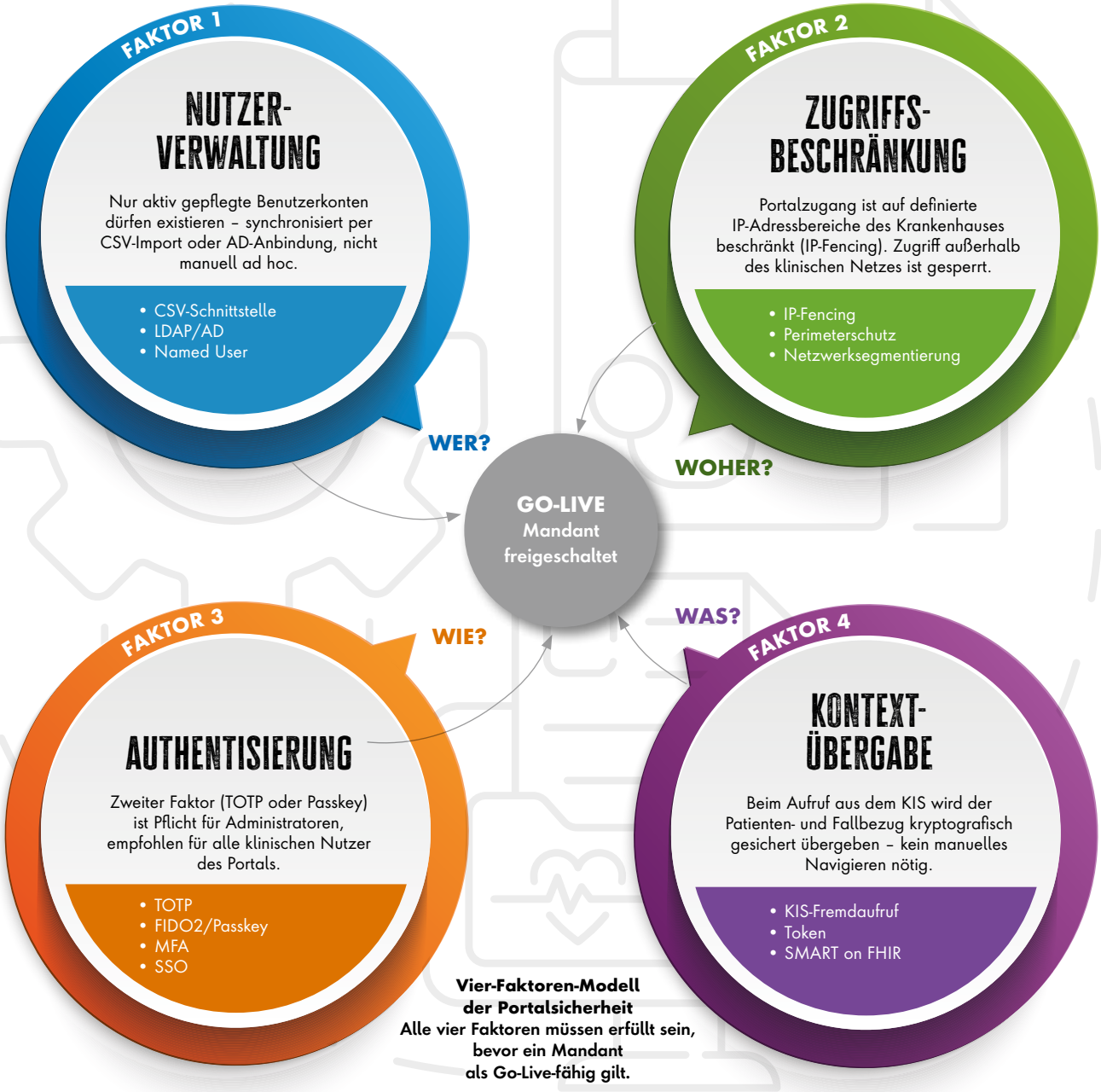
Die Sicherheit beginnt beim Nutzerzugang. Zugang zu Patientendaten wird nur gewährt, wenn vier Bedingungen erfüllt sind: Die Nutzerverwaltung stellt sicher, dass ausschließlich aktive Benutzerkonten existieren, synchronisiert etwa über CSV-Schnittstellen oder Active Directory. Zugriffsbeschränkungen begrenzen den Zugang auf definierte IP-Bereiche und blockieren externe Zugriffe. Die Authentifizierung erfordert neben dem Passwort einen zweiten Faktor, etwa einen Passkey wie Fingerabdruck, mindestens für Admin-Konten. Schließlich stellt die Kontextübergabe sicher, dass Patienten- und Fallbezug kryptografisch gesichert aus dem Krankenhausinformationssystem übermittelt werden.

Das Gateway als Sicherheitsbrücke

Krankenhäuser schützen ihre Kernsysteme mit segmentierten Netzwerken, DMZ-Architekturen, Firewalls und Intrusion-Detection-Systemen. Verbundportale mit eingehenden externen Verbindungen würden diese Schutzschichten unterlaufen. Ein lokales Gateway löst dieses Problem: Es wird in der DMZ betrieben und baut ausschließlich ausgehende, mTLS-gesicherte Verbindungen zur zentralen Plattform auf. Eingehende Ports bleiben geschlossen, öffentliche IP-Adressen entfallen. Das Gateway prüft jede Nachricht auf Einwilligungen und validiert die Mandantenzuordnung, bevor Daten das Krankenhaus verlassen. So bleibt die Sicherheitsarchitektur intakt.

Verantwortlichkeiten klar regeln

In konsortialen Projekten arbeiten Softwarehersteller und Infrastrukturbetreiber oft ohne direkten Vertrag zusam-



men. Das erschwert belastbare Sicherheitsnachweise. Beide Seiten benötigen daher ein Typ-2-BSI-C5-Testat, das die Wirksamkeit der Kontrollen über zwölf Monate belegt. Eine RACI-Matrix, strukturiert nach den BSI-C5-Kontrollbereichen, schafft Klarheit über Zuständigkeiten: Wer setzt um (Responsible), wer trägt Verantwortung (Accountable), wer berät (Consulted), wer wird informiert (Informed)? Bereiche wie physische Sicherheit, Mandantentrennung, Netzwerkmanagement, Backup, Verschlüsselung, Incident Response und Patch-Management erfordern eindeutige Zuordnungen. Quartalsweise Reviews halten die Matrix aktuell.

COMPLIANCE-AMPEL

- Alle 4 Faktoren erfüllt → Go-Live
- 1–3 Faktoren erfüllt → Nachbesserung
- 0 Faktoren → Kein Go-Live

Regulatorische Anforderungen: BSI C5, NIS2, KRITIS

Das BSI-C5-Testat umfasst 17 Anforderungsbereiche, von physischer Sicherheit bis Portabilität. Der Typ-2-Nachweis belegt die Wirksamkeit der Kontrollen

im Prüfzeitraum. Krankenhäuser mit mehr als 30.000 stationären Fällen jährlich gelten als KRITIS-Betreiber und müssen zusätzlich den branchenspezifischen Sicherheitsstandard B3S erfüllen, der auch Anforderungen an das Business Continuity Management stellt. NIS2 verkürzt die Meldefristen deutlich: 24 Stunden für die Erstmeldung, 72 Stunden für einen Bericht und 30 Tage für den Abschlussbericht. Verstöße können die Geschäftsführung persönlich haftbar machen. Für Verbundportale bedeutet das: Eskalationsprozesse müssen klar definieren, welcher Partner welche Meldung in welchem Zeitfenster absetzt. Auch in der Schweiz und Österreich steigen die Anforderungen.

Architektur als Sicherheitskonzept

Gateways im Krankenhaus kommunizieren ausschließlich über Mutual TLS mit Perfect Forward Secrecy. Zugelassen ist nur TLS 1.3 mit AEAD-Algorithmen. Im Backend stellt eine OID-basierte Mandantentrennung sicher, dass kein Krankenhaus auf fremde Daten zugreifen kann, und zwar weder über APIs noch auf Datenbankebene. Georedundante Rechenzentren sichern die Verfügbarkeit, N+1-Konfigurationen minimieren Ausfallrisiken. Ruhende Daten werden mittels AES-256 und Transparent Data Encryption geschützt. Das Verfahren hält auch Quantencomputern stand. Für asymmetrische Verfahren im TLS-Handshake empfiehlt das BSI eine schrittweise Umstellung auf Post-Quantum-Kryptografie. Ein vollständiges Krypto-Inventar ist dabei unerlässlich.

Datensouveränität der Patienten

Im Verbundportal verwalten Patienten ihre Daten selbst. Die DSGVO-Vorgaben zu Auskunft, Löschung und Datenübertragbarkeit müssen systemübergreifend umgesetzt werden. Löschkonzepte unterscheiden zwischen nicht-medizinischen Daten, die vollständig entfernt werden, und medizinischer Dokumentation, die zunächst ein Soft-Delete erhält. Ein Master-Patient-Index unterstützt Änderungen, die der Patient initiiert. Die Authentifizierung erfolgt gestuft: von der Registrierung über Zwei-Faktor-Verfahren bis zur Identitätsverifikation via eID oder VideoIdent, künftig ersetzt durch EUID-Wallets. Die Consent-Verwaltung ist mehrstufig organisiert und berücksichtigt Krankenhaus, Dokumentenkategorie und Zugriffsgruppe. Das Standard-Datenschutzmodell SDM 3.1 bietet mit seinen sieben Gewährleistungszielen einen strukturierten Bewertungsrahmen.

Von der Theorie zur Praxis

RACI-Matrizen dürfen nicht ungenutzt bleiben; regelmäßige Überprüfungen und Anpassungen an neue Bedrohungen sind unerlässlich. Penetrationstests, SIEM-Auswertungen und BCM-Übungen müssen mandantenspezifisch auswertbar sein, damit jedes Krankenhaus seinen Compliance-Status kennt. Die Support-Kette vom First-Level bis zum Herstellerteam muss den BSI-C5-Personalkontrollen genügen, insbesondere wenn Support-Mitarbeiter Zugriff auf Patientendaten haben. Tabletop-Übungen simulieren Szenarien wie Ransomware-Angriffe oder Rechenzentrumsausfälle und testen die Eskalationswege.

Fazit

Der sichere Betrieb von Patientenportalen im Verbund erfordert das Zusammenspiel aus klarer Governance, durchdachter Architektur, geregelten Verantwortlichkeiten und der konsequenten Umsetzung regulatorischer Anforderungen. Dank intersektoraler Operabilität ist dies über alle Bereiche hinweg möglich. Modelle wie der Vier-Faktoren-Ansatz und Gateway-Architekturen helfen, die Komplexität zu beherrschen. Entscheidend bleibt die kontinuierliche Überprüfung in der Praxis – denn Sicherheit ist ein fortlaufender Prozess.

Andreas G. Henkel