swisscom

Sicherheit und Prozess-automatisierung im Gesundheitswesen

Enable, drive and protect your business.

Die Prozessautomatisierung im Gesundheitswesen bietet grosse Chancen bei der Entlastung des Pflegepersonals von administrativen Aufgaben. Swisscom entwickelt massgeschneiderte Lösungen, die die Schweizer Gesundheitsinstitutionen dabei unterstützen, diese Ziele zu erreichen. Sie macht dies in enger Zusammenarbeit mit ausgewiesenen Technologie- und Branchenpartner*innen. Dabei steht die Sicherheit der Gesundheitsdaten an oberster Stelle.

Anhand von umgesetzten Automatisierungsprojekten in den Bereichen Leistungscontrolling und MQI-Kennzahlen mit unserer Partnerin Oase Health Solutions AG aus der ambulanten und stationären Langzeitpflege beleuchten wir erstens die konkreten Anforderungen an die Verarbeitung von Personendaten und zweitens die Massnahmen, welche Swisscom zur Gewährleistung zum Schutz sensibler Daten umsetzt.

Datenschutzanforderungen für den Umgang mit sensiblen Personendaten

Im Rahmen dieser Automatisierungsprojekte wurden besonders schützenswerte Personendaten im Sinne des schweizerischen Datenschutzgesetzes (DSG) sowie der europäischen Datenschutz-Grundverordnung (DSGVO) verarbeitet. Es handelt sich um Gesundheitsdaten, die einer erhöhten Schutzbedürftigkeit unterliegen.

Um den höchsten Standard im Bereich Datenschutz und Datensicherheit zu gewährleisten, gelten folgende Anforderungen:

1. **Datenstandort Schweiz**
   Sämtliche Personendaten müssen ausschliesslich in Rechenzentren innerhalb der Schweiz gespeichert und verarbeitet werden. Eine Datenverarbeitung oder -speicherung im Ausland – auch temporär – ist ausgeschlossen.

2. **Sichere Datenverbindung**
   Der Datenaustausch mit Pflegeinstitutionen, Spitex-Organisationen und weiteren autorisierten Partner*innen muss über verschlüsselte, gesicherte Verbindungen erfolgen.

3. **Technische und organisatorische Massnahmen (TOM)** Es sind umfassende technische und organisatorische Massnahmen umzusetzen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen.

4. **Einhaltung gesetzlicher Vorgaben**
   Die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen ist zwingend. Dies umfasst insbesondere:

   - das revidierte Schweizer Datenschutzgesetz (DSG) und die Datenschutzverordnung (DSV)
   - die europäische Datenschutz-Grundverordnung (DSGVO)

5. **Transparenz und Nachvollziehbarkeit**
   Die Verarbeitung von Daten muss jederzeit nachvollziehbar und dokumentiert sein. Zugriff, Änderung oder Weitergabe von Daten sind zu protokollieren. Betroffene Personen haben ein Recht auf Auskunft, Berichtigung und Löschung ihrer Daten im Rahmen der gesetzlichen Vorgaben.

6. **Vertraulichkeitsverpflichtung und Schulung**
   Alle Mitarbeitenden und involvierten Personen, die Zugang zu den sensiblen Daten haben, sind zur Vertraulichkeit zu verpflichten und regelmässig im Umgang mit Datenschutz und Informationssicherheit zu schulen.

Diese Anforderungen bilden die Grundlage für die sichere und datenschutzkonforme Verarbeitung sensibler Gesundheitsdaten im Projektkontext. Nur durch die konsequente Umsetzung dieser Massnahmen kann das Vertrauen von Patientinnen und Patienten sowie den beteiligten Organisationen gewährleistet werden.

«Die hohen Datenschutzanforderungen im Umgang mit sensiblen Personendaten im Gesundheitswesen haben Oase Health Solutions dazu veranlasst, eine Partnerschaft mit Swisscom einzugehen. Die private Cloud von Swisscom erfüllt alle notwendigen Anforderungen an Sicherheit und Datenschutz. In Gesprächen mit potenziellen Kunden stellt Oase Health Solutions immer wieder fest, dass das Vertrauen in Swisscom sehr gross ist – ein wichtiger Faktor für die Akzeptanz und den Erfolg der gemeinsamen Lösungen. Zudem bringt Swisscom ihre langjährige technologische Erfahrung im Bereich Automatisierung ein, was die Entwicklung und den Support effizienter und zukunftssicherer Systeme zusätzlich unterstützt.»

Statement von Elisabeth Villiger
CEO
Oase Health Solutions AG

oase
health solutions

Massnahmen zur Sicherstellung der datenschutzkonformen Verarbeitung von Gesundheitsdaten

Swisscom setzt gezielt auf eine Vielzahl von Sicherheitsmassnahmen, um den bestmöglichen Schutz der sensiblen Patientendaten zu gewährleisten. Die Plattformen, welche Prozessautomatisierungslösungen unterstützen, sind auf dem höchsten Sicherheitsniveau ausgelegt und bieten Datensicherheit auf Tier-4-Niveau.

Zugangskontrollen werden nach dem Prinzip des «Need-to-Know» und «Least-Privilege» umgesetzt. Kunden haben die Möglichkeit, durch einen von ihnen bestimmten Auditor, Audits durchführen zu lassen.

Das Personal von Swisscom durchläuft strenge Sicherheitsprüfungen. Das schliesst Überprüfungen von Strafregister und Betreibungsregister sowie regelmässige Leumundsüberprüfungen ein. Zudem wird umfassend geschult und es gelten strikte Best Practices, um sicherzustellen, dass alle Mitarbeitenden in Sicherheitsfragen hochkompetent sind. Zutrittskontrollen und segregierte Aufgaben sorgen dafür, dass sensible Informationen nur von autorisierten Personen eingesehen werden können.

Swisscom profitiert von ihrer langjährigen Erfahrung im Banking-Sektor und den strikten FINMA-Regulatorien, die besonders hohe Datenschutzauflagen und Datenverschlüsselungstechniken wie AES-256 und Transparent Data Encryption einschliessen.

Dieser Erfahrungsschatz wird nun gewinnbringend für die Schweizer Gesundheitsinstitutionen eingesetzt.

Spezifische Security-Dimensionen

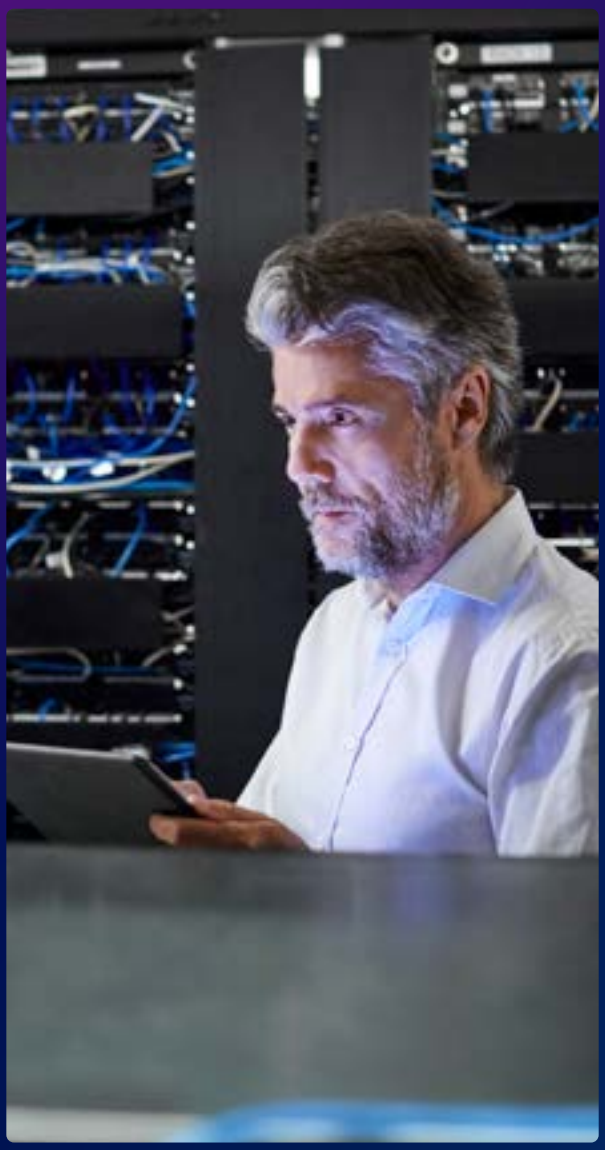
Bei der Umsetzung und dem Betrieb von Lösungen im Bereich Prozessautomatisierung sind die folgenden fünf Security-Dimensionen von zentraler Bedeutung:

1. Datenschutz und Vertraulichkeit
2. Zugriffskontrolle
3. Integrität
4. Betriebssicherheit
5. Compliance

Mit folgenden Massnahmen stellt Swisscom diese Dimensionen sicher und gewährleistet dadurch die Sicherheit für ihre Partner*innen sowie Kundinnen und Kunden umfassend:

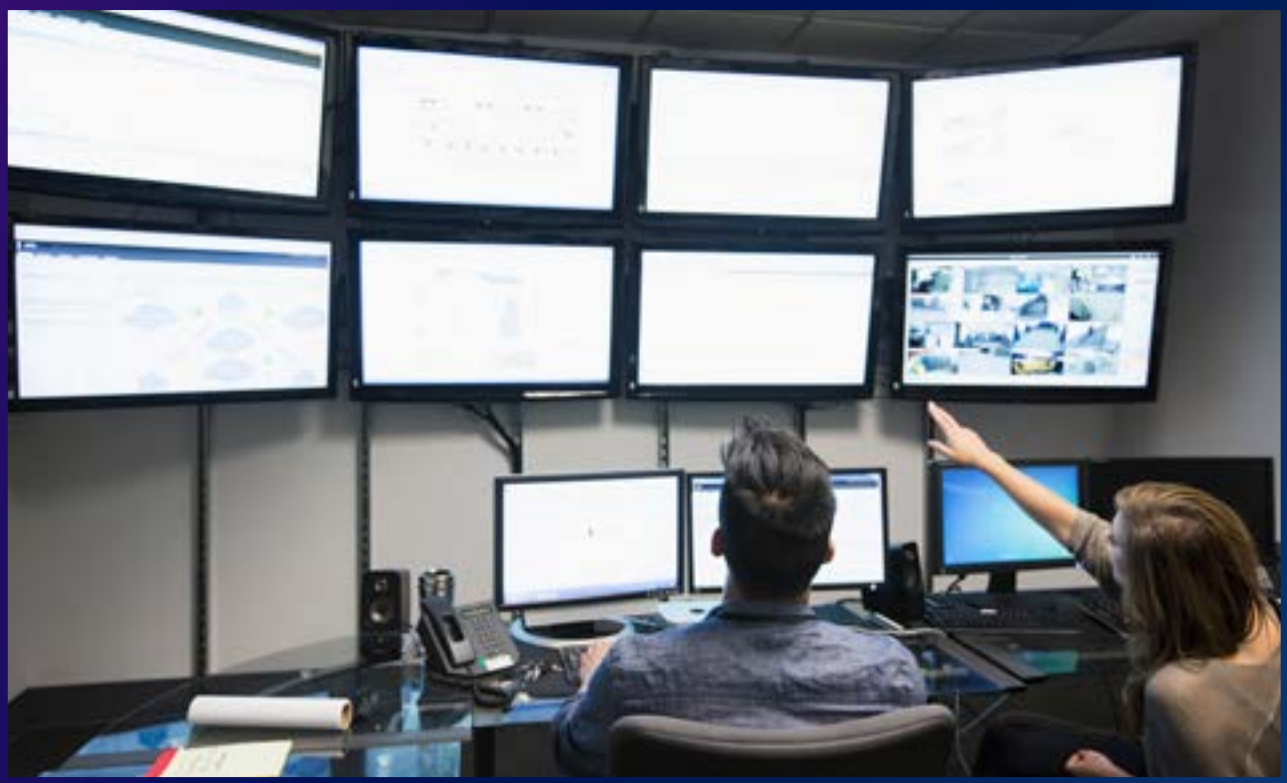
Datenschutz und Vertraulichkeit
Der Schutz von Patientendaten ist von zentraler Bedeutung. Swisscom stellt sicher, dass sensible Daten während des gesamten automatisierten Prozesses nicht gefährdet oder unbefugt weitergegeben werden. Workshops und Schulungen, beispielsweise in Zusammenarbeit mit der Fachhochschule OST, gewährleisten den Wissenstransfer und die Sensibilisierung für Datenschutzthemen.

Zusätzlich wird durch strikte Daten-Segregation garantiert, dass Kundendaten sauber getrennt und geschützt sind.



Zugriffskontrolle
Die Zugriffskontrolle bildet eine weitere Säule der Datensicherheit. Nur autorisierte Personen erhalten Zugang zu den RPA-Systemen und den dazugehörigen Daten. Dies wird durch regelmässige Berechtigungs-Audits unterstützt, bei denen alle sechs Monate das Identity and Access Management (IAM) kontrolliert und durch Mitarbeitende bestätigt wird.
Strikte Zugriffsrechte und die restriktive Vergabe von Berechtigungen stellen sicher, dass sensible Informationen geschützt bleiben.

Integrität
Um die Integrität der Daten und der automatisierten Prozesse zu bewahren, setzt Swisscom auf Validierungs- und Überprüfungsmechanismen. Das Vier-Augen-Prinzip, sowohl intern als auch mit Kunden, Code-Reviews und umfangreiches Testing mit Endkunden sind nur einige der Massnahmen. Fehlerfeststellungen und Qualitätskontrollen über mehrere Layer und eine sichere Deployment-Pipeline tragen massgeblich zur sicheren Implementierung bei. Audit-Logs und Audit-Trails bieten zusätzliche Sicherheit und nachvollziehbare Kontrolle über den Zugang zu den Systemen.

Betriebssicherheit
Swisscom garantiert die Betriebssicherheit der Systeme und Infrastruktur durch fortlaufende Sicherheitsmassnahmen wie Firewalls, Detection- und Präventionssysteme sowie regelmässige System-Updates. Die Spezifikationen für das Tier-4-Rechenzentrum bieten höchstes Sicherheitsniveau. Darüber hinaus sorgen detaillierte Kundenberatungen zu Security-Themen sowie Netzwerk-Monitoring durch das Swisscom SOC/CSIRT für eine überwachte und geschützte Plattform.

Compliance
Swisscom unterstützt Gesundheitsinstitutionen dabei, die gesetzlichen Vorschriften und branchenspezifischen Bestimmungen einzuhalten. Dazu gehören das Datenschutzgesetz (DSG), EDÖB, DSGVO und lebenswichtige Informationssicherheitsrichtlinien. Kunden können ihre eigenen Auditoren bestimmen, welche die Plattformen kontrollieren. Regelmässige Schulungen und E-Learnings stellen sicher, dass Mitarbeitende von Swisscom betreffend Datenschutzfragen stets auf dem neuesten Stand sind.