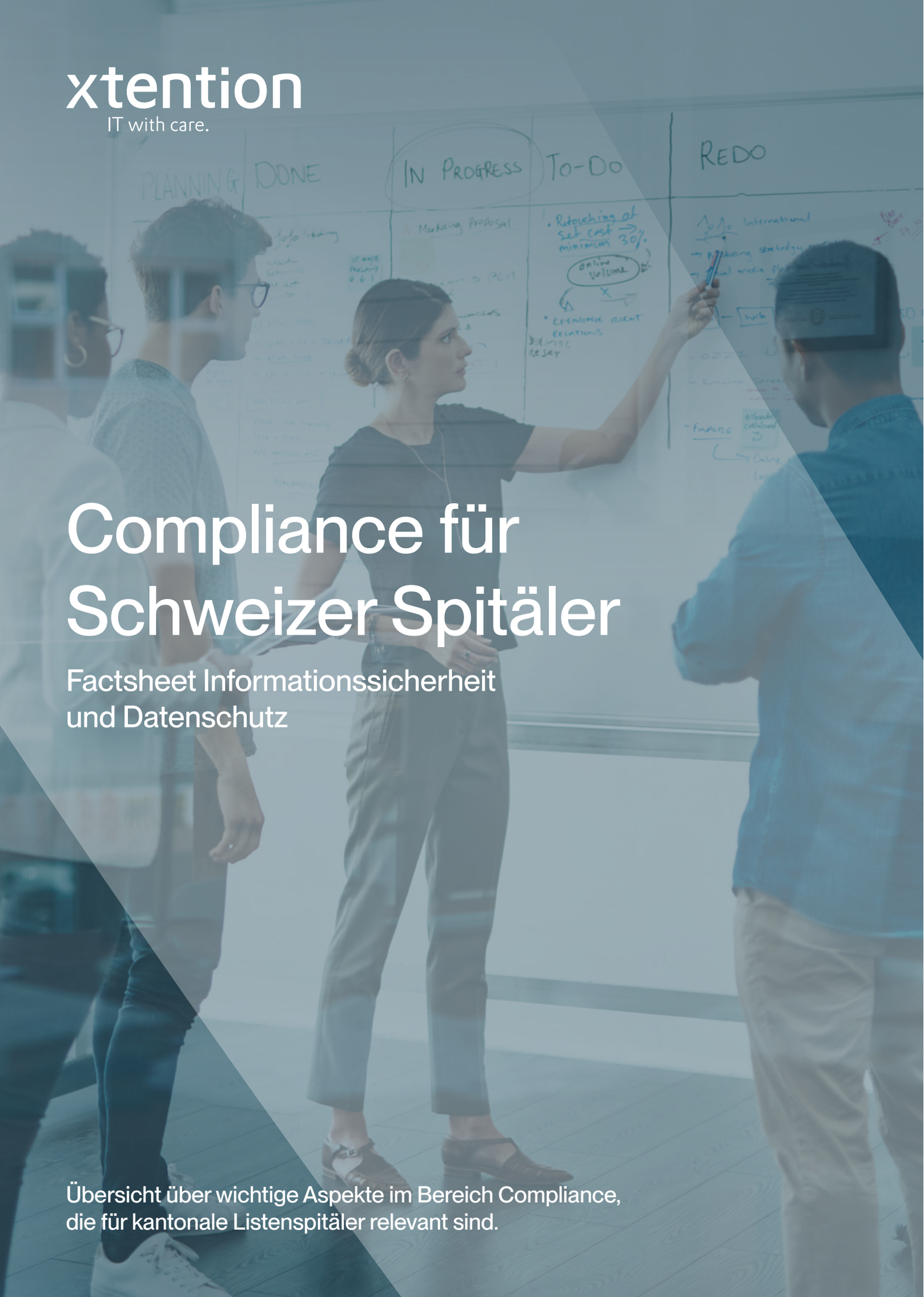
xtention
IT with care.



Compliance für Schweizer Spitäler

Factsheet Informationssicherheit und Datenschutz

Übersicht über wichtige Aspekte im Bereich Compliance, die für kantonale Listenspitäler relevant sind.

1. Informationssicherheit

Die Anforderungen an die Informationssicherheit steigen auch im Gesundheitswesen stark an. **Seit dem 1. April 2025 ist in der Schweiz eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen inkl. Listenspitäler in Kraft.** Der Bundesrat hat am 7. März eine Änderung des Bundesgesetzes über die Informationssicherheit (ISG) beschlossen.

Das Informationssicherheitsgesetz (ISG) ist ein wichtiger Schritt zur Stärkung der Cyberresilienz, auch im Gesundheitswesen.
www.fedlex.admin.ch/eli/cc/2022/232/de

Pflichten

Seit dem 1. April 2025 gilt für Listenspitäler eine gesetzliche Pflicht, Cyberangriffe innerhalb von 24 Stunden ab Entdeckung an das Bundesamt für Cybersicherheit (BACS) zu melden. Es wird erwartet, dass ein Listenspital auch in einer Notfallsituation funktionieren kann.

Ein Cyberangriff ist meldepflichtig, wenn die Funktionsfähigkeit des Spitals gefährdet ist, zu einer Datenmanipulation, einem Abfluss von Informationen geführt hat oder mit Erpressung oder Drohung verbunden ist: **Meldepflicht für Cyberangriffe auf kritische Infrastrukturen gilt ab 1. April 2025**
www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2025/meldepflicht-2025.html

Bei Nichtbeachtung der Meldepflicht sieht das ISG Bussen vor. Die Meldepflicht nach ISG besteht unabhängig von anderen gesetzlichen Verpflichtungen, insbesondere von Datenschutzmeldepflichten nach kantonalem Datenschutzrecht oder der strafrechtlichen Geheimhaltungspflicht nach Art. 321 StGB. Ein Vorfall kann somit mehrere Meldepflichten gleichzeitig auslösen.

Grundlegende Anforderungen an ein Listenspital aus Sicht der Informationssicherheit

Die ISO 27001:2022 definiert ein strukturiertes Managementsystem für die Informationssicherheit (ISMS), das Spitälern ermöglicht, Informationssicherheit ganzheitlich, systematisch und nachvollziehbar zu steuern. **Ein ISMS trägt wesentlich zur Patientensicherheit bei, indem die Verfügbarkeit, Integrität und Vertraulichkeit medizinischer Informationen und kritischer Systeme gestärkt werden.** Gleichzeitig schafft es klare Verantwortlichkeiten und eine verbindliche Governance auf Ebene Spitalleitung und Management. Risiken wie Cyberangriffe, Systemausfälle oder Abhängigkeiten von Drittanbietern werden frühzeitig identifiziert statt nur reaktiv adressiert zu werden. Ein ISMS unterstützt zudem den Nachweis der Einhaltung gesetzlicher und regulatorischer Anforderungen.

Wichtige Anforderungen sind zum Beispiel:

- Betreibung eines Risikomanagements über alle kritischen Geschäftsprozesse und Systeme
- Aufbau und Betrieb einer Sicherheitsorganisation mit klaren Rollen wie z.B. CISO, Incident Management-Prozess oder Steuerungskreis
- Präventiver Schutz vor Malware, Ransomware und Systemausfällen
- Zutritts- und Zugriffsschutzkontrollen
- Regelmässige Überprüfung der Wirksamkeit (Audits, Tests, Übungen, Kennzahlen)
- Schulung und Awarenessbildung zur Informationssicherheit, Datenschutz und Geheimhaltungspflichten
- Kontinuierlicher Verbesserungsprozess (KVP) des ISMS im Spital

Durch definierte Prozesse für Sicherheitsvorfälle, IT-Ausfälle und Notfälle wird die Krisen- und Handlungsfähigkeit eines Spitals deutlich gestärkt. Gleichzeitig werden Lieferanten und IT-Dienstleister kontrolliert und mit klaren Sicherheitsanforderungen eingebunden. Die regelmässige Sensibilisierung der Mitarbeitenden reduziert zudem sicherheitsrelevante Fehler im Alltag.

Für Spitäler bietet ein ISMS folgende Vorteile:

1. **Klare Prozesse und Verantwortlichkeiten:** Governance, Risikoanalyse, Incident Management, Lieferantenmanagement
2. **Nachweisbarkeit:** erfüllt die Dokumentationspflichten gemäss den gesetzlichen Vorgaben und gilt als Best Practice-Ansatz
3. **Integrationsfähigkeit:** lässt sich gut mit den Datenschutzanforderungen und dem Qualitätsmanagement verbinden

Good Governance

Einhaltung von Compliance-Vorgaben ist ein Kernbestandteil einer „Good Governance“: wer Risiken früh adressiert und verantwortungsvoll handelt, schützt das Spital mit seinen sensiblen Informationen und Daten, stärkt das Vertrauen aller Stakeholder und verhindert Probleme, bevor sie entstehen. Die Verantwortung für die Einhaltung der gesetzlichen Vorgaben liegt bei der Spitalleitung bzw. beim obersten Führungsorgan. Die Einführung eines ISMS nach ISO 27001:2022 gilt dabei als internationale etablierte Best Practice, um angemessene Massnahmen zur Risikominderung

2. Datenschutz

Neben der ISG-Meldepflicht gelten weiterhin die bestehenden Meldepflichten bei „Data Breaches“ gemäss den kantonalen Vorgaben für Listenspitäler (Beispiel Kanton ZH): Datenschutzvorfall melden | DSB Kanton Zürich

https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutzvorfall-melden

Praxisbeispiele:

- Versand medizinischer Berichte an falsche Empfänger
- Cyberangriff (z.B. Ransomware), da oft auch Personendaten betroffen sind
- Unerlaubter Datenzugriff durch Dritte (auch intern im Spitalumfeld)
- Während das ISG primär auf die Funktionsfähigkeit des Spitals abstellt, richtet sich die verpflichtende Datenschutzmeldung nach dem Risiko für die betroffenen Personen.

Was ist ein Datenschutzvorfall?

Ein **Datenschutzvorfall** liegt vor, **wenn Personendaten unbeabsichtigt oder unrechtmässig offengelegt, verändert, gelöscht oder unzugänglich gemacht werden.** Die **Meldepflicht** besteht, sobald daraus **ein höheres Risiko für betroffene Personen (Mitarbeitende oder Patienten) entsteht** z.B. etwa durch möglichen Missbrauch der Daten, Identitätsdiebstahl, Stigmatisierung, Reputationsschäden oder Nachteile im beruflichen oder privaten Umfeld.

3. Einsatz von Künstlicher Intelligenz (KI) im Spital

Der Einsatz von KI im Spital eröffnet erhebliche Chancen, erfordert jedoch eine klare rechtliche und sicherheitstechnische Einordnung. Da die Schweiz bisher kein eigenes KI-Regulierungsgesetz wie den EU AI Act kennt, gilt für alle KI-Anwendungen primär das kantonale Datenschutzrecht sowie ergänzend das DSG.

Aus Sicht der Informationssicherheit sind umfassende, technische und organisatorisch Schutzmassnahmen erforderlich, um den Einsatz von KI sicher und beherrschbar einzusetzen. Entscheidend ist der jeweilige Anwendungsfall in der Praxis. Für Spitäler bedeutet dies: z.B. Zweck, Datenkategorien, Speicherorte und Zugriffsrechte müssen vorab definiert werden. Cloud-Anbieter gelten als Auftragsbearbeiter und daher verlangt der Gesetzgeber korrekt ausgestellte Auftragsverarbeitungsverträge (ADV). Aufgrund des erhöhten Risikos wird eine Risikoanalyse in der Form einer Datenschutz-Folgenabschätzung (DSFA) und in manchen Fällen ein ISDS-Konzepts erforderlich. Je nach den kantonalen Vorgaben kann zudem eine Vorabkonsultation der zuständigen kantonalen Datenschutzbehörde notwendig sein.

Einige medizinische KI-Systeme gelten als „High-Risk“, woraus erhöhte Anforderungen an Dokumentation, Monitoring, und Cybersicherheit folgen. Diese Aspekte sollten in einem KI-spezifischen Risikoprozess im Spital berücksichtigt werden. Einige Datenschutzbehörden veröffentlichen auch Merkblätter zum sicheren KI-Einsatz im Spitalalltag.

4. Praxisnahe Unterstützung für Spitäler

x-tention unterstützt Spitäler beim Aufbau, der Weiterentwicklung und dem Betrieb von Informationssicherheits- und Datenschutzmanagementsystemen (ISMS / DSMS), von der Konzeption bis zur nachhaltigen Verankerung in der bestehenden Governance.

Als externe Spezialisten übernehmen wir zudem die Rollen des externen Chief Information Security Officers (CISO) sowie des externen Datenschutzberaters (DSB) und sorgen für eine strukturierte Umsetzung gesetzlicher und regulatorischer Anforderungen.

Ergänzend begleiten wir Spitäler im Bereich der technischen Cyber Security, etwa bei der Früherkennung von Cyberangriffen, beim Security Monitoring oder beim Betrieb eines Security Operations Centers (SOC).

ISG - was heisst das bezogen auf das Schweizer Gesundheitswesen?

Prävention ist besser als Heilen!

Historisch bedingt bedarf es einer Nachrüstung bzw. Implementation eines ISMS in Schweizer Spitälern. Im Jahr 2026 werden viele ein Managementsysteme aufbauen müssen, um sich besser vor Cyberangriffen zu schützen. Spitäler verarbeiten zahlreiche Gesundheitsdaten und sind ein relativ leichtes Ziel für Hacker, da z.B. die IT-Infrastrukturen nicht überall auf dem Stand der Technik sind.

„Ein gestohlenes Patientendossier wird im Darknet für ca. $ 1‘000.00 gehandelt und ist lukrativ für Hacker“.

Ihr Kontakt zu x-tention:

x-tention Informationstechnologie AG

x-tention Informationstechnologie AG
Stelzenstrasse 4,
8152 Glattpark (Opfikon), Schweiz

+41 43222 6022
office@x-tention.ch

x-tention.ch