Der richtige Umgang mit elektronischen Patientendaten

von Gerold Lauper, Leiter Informationssicherheitsmanagement bei Keyon

ISO 27799 regelt messbar und strukturiert den Umgang mit Patientendaten und medizinischer Informatik.

Elektronische Patientenakten sind heute aus Gesundheitsorganisationen nicht mehr wegzudenken. Gespeichert auf einer Health Card haben berechtigte Personen zukünftig unabhängig vom Ort rund um die Uhr Zugriff darauf. Geht es nach dem Bundesrat, dann ist das elektronische Patientendossier bis 2015 eingeführt – aber ist die Sicherheit und der Zugriff auf die Patientendaten gewährleistet? Der neue ISO 27799-Standard bietet Hand.

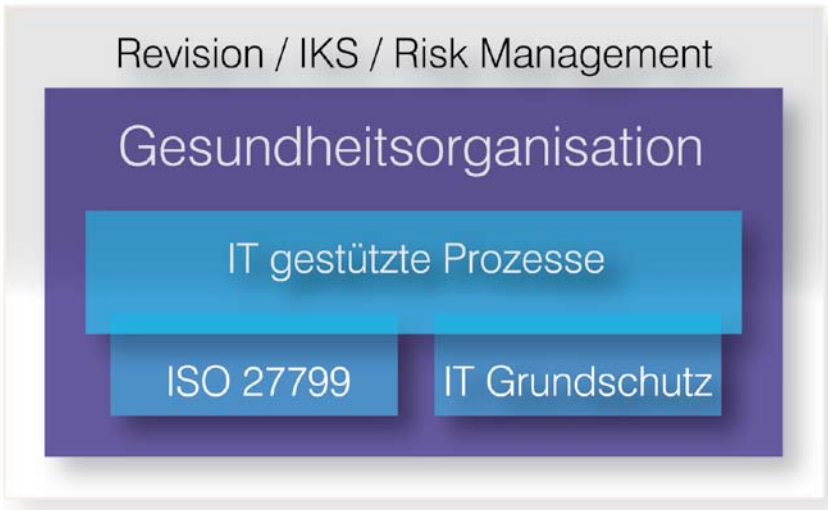
Der IT-Sicherheitsstandard fürs Gesundheitswesen

ISO/IEC 27799:2008 ist der Standard für Informationssicherheit im Gesundheitswesen unter Verwendung des etablierten ISO/IEC 27002. Er liefert detaillierte Anleitungen und Vorgehensweisen für den sicheren Umgang mit Gesundheitsinformationen und orientiert sich an Best-Practice-Ansätzen. Mit einer pragmatischen Implementierung dieser Norm können Gesundheitsorganisationen effizient und messbar bestehende organisatorische und technische Prozesse optimieren und erhalten so ein Cockpit für das vom Gesetzgeber verlangte Interne Kontrollsystem (IKS).

Ziele für die IT-Sicherheit im Gesundheitswesen

Das Gesundheitswesen, die betroffenen Patienten, sowie der Datenschutz stellen hohe Anforderungen an die Vertraulichkeit, Verfügbarkeit und Integrität von Patientendaten. Neben allgemeingültigen Vorgaben zur Informationssicherheit fokussiert sich der Standard auf die folgenden, für das Gesundheitswesen wichtigen Punkte:

- Aufrechterhaltung der Privatsphäre von Patienten
- Sichere Behandlung von Patienten auf Basis von integren Patienteninformationen
- Schnelle Verfügbarkeit von Patientendaten für zeitkritische Behandlungen
- Verfügbarkeit, Wartung und Betrieb von medizinischen Systemen



Moderne ISMS basieren auf etablierten Standards und bieten eine toolbasierte Unterstützung für die effiziente Umsetzung und Revision.

Standards weisen den sicheren Weg

ISO 27799 legt Umfang, Ziele und Messgrössen fest, zu denen die Konformität (Compliance) des Systems nachgewiesen werden kann. Konkrete Anforderungskataloge geben Orientierungshilfen beim Aufbau eines Managementsystems für Informationssicherheit (ISMS).

ISO 27799 spezifiziert, welche Elemente ein ISMS enthalten muss und welche Anforderungen an das Management der IT-Sicherheit zu stellen sind. Der Standard formuliert Prozesse und Massnahmenziele, überlässt es jedoch dem Anwender, detaillierte Prozesse und Einzelmassnahmen auszuwählen.

Der IT-Grundschutz-Standard des Bundesamts für Sicherheit in der Informationstechnik (BSI) schliesst hier die Lücke und liefert konkrete Massnahmen und Vorgehensweisen, um die Zielsetzungen von ISO 27799 erfüllen zu können.

Pragmatische Einführung – Rascher Erfolg

Alle notwendigen Elemente für die effiziente und rasche Einführung und Durchsetzung von ISO 27799 sind bekannt und auf dem Markt verfügbar. Spezifische Tools bieten vorgefertigte Module an, die es erlauben, sich sofort auf die praktische

Umsetzung des Standards zu konzentrieren. Das Zuschneiden an die individuellen Bedürfnisse und Verhältnisse des Unternehmens wird über die Parametrisierung erreicht. Zu den wichtigsten Bestandteilen gehören:

- Modellieren von Prozessen, Komponenten und Organisationsstrukturen
- Festlegen von Sicherheitszielen und Massnahmen
- Planung der Einführung und Durchsetzung
- Unterstützung für Umsetzung und Betrieb
- Unterstützung für die laufende Kontrolle und Verbesserung
- Mechanismen für Kommunikation, Ausbildung und Sensibilisierung
- Geeignete Dokumentation für Betrieb und Revision

Mit einer pragmatischen Vorgehensweise werden systematisch nach und nach Prozesse, Abteilungen, Organisationen, Systeme etc. in das Informationssicherheitsmanagement eingebunden. Die einzelnen Elemente werden den Massnahmen des IT-Grundschutz-Standards gegenübergestellt, um so die Zielvorgaben gemäss ISO 27799 zu bewerten. Dieses Vorgehen stellt sicher, dass Prozesse definiert, messbar und nachvollziehbar umgesetzt, durchgesetzt und weiterentwickelt werden können.

Fazit

Ein ISMS ist das wesentliche Instrument für das Verständnis, den Betrieb, die Weiterentwicklung und Beurteilung von IT-gestützten Prozessen und Systemen. Die Einführung der Health Professional Card resp. des elektronischen Patientendossiers stellt das Gesundheitswesen vor neue Herausforderungen, die mit Unterstützung eines ISMS besser verstanden, geplant und umgesetzt werden können. Etablierte Standards und auf dem Markt verfügbare Komponenten erlauben es, sich direkt auf die entsprechende Informationssicherheit von Patientendaten und Systemen zu konzentrieren.

Mit ISO 27799 gut gerüstet für die Herausforderungen elektronischer Patientendossiers und HPC.

Gerold Lauper
Dipl. Ing. ETH,
Betriebswissenschafter ETH
Leiter Informationssicherheitsmanagement bei Keyon.
Lauper@keyon.ch