

# Sichere Patientendaten im Krankenhaus

**Elektronische Patientenakte, elektronische Gesundheitskarte und generell die elektronische Speicherung von Patientendaten machen komplett neue Sicherheitskonzepte für den Einsatz von IT-Systemen notwendig. Die aktuelle Praxis der Krankenhäuser wird dem noch nicht gerecht.**

Eine lückenlose IT-Sicherheit sollte im Umgang mit sensiblen Patientendaten selbstverständlich sein. Trotzdem weisen annähernd zwei von drei Kliniken Mängel in der Informationssicherheit auf. Außerdem räumen nur vier von zehn Krankenhäusern der Einführung eines IT-Risikomanagementsystems die notwendige Priorität ein. Zu diesen Ergebnissen kam bereits 2007 eine Studie von Steria Mumert Consulting.

Henning Kopp, Leiter Information Security bei DS DATA SYSTEMS und Mitglied der gmds-Arbeitsgruppe Archivierung von Krankenunterlagen (AKU), sieht bei Institutionen im Gesundheitswesen die

Verfügbarkeit der Systeme, die Vertraulichkeit und Integrität der Informationen aktuell nicht ausreichend gewährleistet: „Die steigende Abhängigkeit der Geschäftsprozesse von der Informationstechnik und die mangelnde Sensibilisierung der Mitarbeiter im Umgang mit vertraulichen Daten machen die Institutionen anfälliger denn je. Störungen und Ausfälle belegen, dass sich viele Verantwortliche des hohen Risikos nicht ausreichend bewusst sind.“

Sein Fazit: Das Wissen um die organisatorischen und technischen Schwachstellen und um die Anforderungen von internationalen Informations-Sicherheitsstandards sind vielfach noch zu gering.

Krankenhäuser müssen umdenken. Spätestens mit der elektronischen Speicherung von Patientendaten besteht dringender Handlungsbedarf – auch im Interesse der Vorstände und Geschäftsführer, denn sie sind nach aktueller Gesetzeslage persönlich für Versäumnisse und mangelnde Risikovorsorge in der IT verantwortlich.

Ein fahrlässiger Umgang mit Informationstechnik, auch in lokalen Netzwerken, kann diesen Tatbestand unter Umständen bereits erfüllen.

Welcher Art ein angemessenes Sicherheitskonzept sein sollte, muss nicht jedes Krankenhaus neu definieren. Die Einführung eines Informations-Sicherheits-Management-Systems (ISMS) nach der internationalen Norm ISO 27001 hat sich auch im Gesundheitswesen etabliert. Die gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, schreibt für die mit der elektronischen Gesundheitskarte erforderliche Tele-

matikinfrastruktur ebenfalls ein ISMS vor (vgl. „Übergreifendes Sicherheitskonzept der Gesundheitstelematik“).

## Schrittweise zu einem ISMS

Für die Einführung eines ISMS gibt es vielfach bewährte Vorgehensweisen. DS DATA SYSTEMS hatte das Klinikum Braunschweig bei der Einführung eines ISMS beraten und sieht das Vorgehen der Klinik als beispielhaft für andere Institutionen im Gesundheitswesen. Henning Kopp: „Empfehlenswert ist, zunächst kleinere Teilverbände zu bilden.“ Das Städtische Klinikum Braunschweig hatte für den IT-Verbund Elektronische Patientenakte ein ISMS eingeführt und nach ISO 27001 auf der Basis von IT-Grundschutz (ISO27001/GS) zertifizieren lassen und damit bestätigt bekommen, dass zentrale Komponenten seiner IT-Sicherheits-Organisation den strengen Anforderungen der internationalen Zertifizierungsnorm gerecht werden.

Für Krankenhäuser, die sich über das Vorgehen noch nicht sicher sind, empfiehlt Henning Kopp als ersten Schritt, mit einem Workshop zur IT-Sicherheitsanalyse zu beginnen. Wird die Einführung einer Sicherheits-Organisation beschlossen, folgt zunächst die Ermittlung des Ist-Zustands durch erfahrene Security-Experten. Mit einer IT-Risikoanalyse werden die ermittelten Schwachstellen bewertet und Vorschläge für die Planung und Einrichtung geeigneter IT-Sicherheitslösungen gemacht. Mit der Zertifizierung nach „ISO 27001“ oder „ISO 27001 auf der Basis von IT-Grundschutz“ wird schließlich von einem unabhängigen Dritten bestätigt, dass für die IT-Sicherheit alles Notwendige getan und nach dem aktuellen Stand der Technik umgesetzt wird.

DS DATA SYSTEMS ist spezialisiert auf Beratung und Organisation der IT-Sicherheit in Unternehmen und Institutionen. Das Unternehmen besitzt im Gesundheitsbereich langjährige Erfahrung bei den Themen IT-Risiko-Management, technische Security und bei Zertifizierungen nach ISO 27001 und stellt auch den IT-Sicherheitsbeauftragten für Kliniken.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das Städtische Klinikum Braunschweig nach „ISO 27001 auf der Basis von IT-Grundschutz (ISO27001/GS) für den IT-Verbund Elektronische Patientenakte“ zertifiziert.

Foto: Ortgies

[www.datasystems.de](http://www.datasystems.de)

