

Die elektronischen Prozesse sind jetzt sicher

Beim UKE in Hamburg werden alle Prozesse elektronisch abgewickelt. Als eine der ersten Kliniken setzt es deshalb auf eine Sicherheits-Zertifizierung nach ISO 27001.

Martin Ortgies, Königsplutter

Das Universitätsklinikum Hamburg-Eppendorf (UKE) gilt nicht nur wegen seines Neubaus als das modernste Klinikum Europas: Hier läuft alles elektronisch, von der Patientenaufnahme über die elektronische Patientenakte bis zur Übergabe der Entlassungsdokumente beim Ausscheiden. Die Einführung der elektronischen Patientenakte ist am UKE sehr weit fortgeschritten: Innerhalb eines fünfstufigen Prozesses durchläuft das UKE bereits die Phase vier und wickelt alle Prozesse elektronisch ab. Das hat viele Vorteile insbesondere für die Qualität der medizinischen Prozesse. Die Kehrseite ist die Abhängigkeit des Klinikums von der Verfügbarkeit der IT-Systeme. Dass sie einer Zertifizierung standhalten können muss, war bereits Maßgabe in der Ausschreibung für die elektronischen Patientenakte.

Offizielle Zertifizierung der Informationssicherheit

„Wir müssen die verlässliche Verfügbarkeit und Stabilität der IT-Systeme jederzeit gewährleisten. So haben wir uns für die Sicherheits-Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz entschieden“, berichtet

Dr. Peter Gocke, Geschäftsbereichsleiter Informationstechnologie des UKE. Das Informations-Sicherheits-Management-System (ISMS) stellt die dauerhafte Einhaltung normierter Sicherheitsabläufe sicher. Das angestrebte ISO-Zertifikat fungiert als offizieller Nachweis dafür, dass das Klinikum für die Informationssicherheit alles Notwendige unternommen hat. Aus Sicht des IT-Chefs gibt es zu diesem Weg keine Alternative. „Wir wollten keinen externen Gutachter, der kluge Empfehlungen abgibt und dann wieder geht. Eine solche Zertifizierung ist ein bleibender Prozess, der mit laufenden Audits verbunden ist“, unterstreicht Dr. Gocke die Entscheidung.

„Für die Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) muss das Klinikum nachweisen, alle erforderlichen Maßnahmen unternommen zu haben, um die Verfügbarkeit, Vertraulichkeit und Integrität des betrachteten Informationsverbunds angemessen sicherzustellen. Welche Maßnahmen hier notwendig und angemessen sind, wird innerhalb des Prozesses zur genannten Sicherheits-Zertifizierung auf Basis von IT-Grundschutz ermittelt“, berichtet Maik Opitz, ISO 27001 Auditor und Security-Berater von DS Data Systems. Er hat die Zertifizierungsvorbereitungen des Klinikums begleitet und notwendige Maßnahmen initiiert.

Informationsverbund elektronische Patientenakte

Herzstück des Informationsverbunds elektronische Patientenakte ist das Klinische Arbeitsplatzsystem (KAS) von Siemens (Soarian Clinicals und Soarian Health Archive). Dieses Workflow-orientierte Kran-

kenhausinformationssystem übernimmt die Steuerung der gesamten Arbeitsabläufe von der Aufnahme des Patienten bis zu seiner Entlassung. Das SAP-Modul IS-H für die administrative Verwaltung der Patienten-Stammdaten gehört ebenfalls zum Informationsverbund sowie weitere Fachapplikationen wie das Medikations-System ATC-Host. Auch die technische Infrastruktur mit 100 Servern, den Netzwerkelementen und mehreren Tausend Clients zählt zu diesem Informationsverbund.

Für die zusätzlichen Aufgaben zur Vorbereitung der Zertifizierung hatte sich der IT-Bereich durch externes Personal verstärkt, weil die internen Ressourcen nicht ausgereicht hätten und auch das spezielle Know-how für die Sicherheits-Zertifizierung fehlte. Das UKE hatte sich hier durch DS Data Systems aus Braunschweig unterstützen lassen, da das Unternehmen bereits über umfangreiche Erfahrungen mit ISO 27001-Zertifizierungen verfügte, die Gesundheitsbranche kannte und qualifizierte Spezialisten vorweisen konnte.

Große Ziele und gute Ergebnisse

Das Hauptziel ist die Absicherung einer hohen Verfügbarkeit der IT-Systeme. Hier hat das UKE die Messlatte auf 99,3% gelegt. Erreicht werden muss dabei die technische Verfügbarkeit inklusive regelmäßiger Wartungszeiten einschließlich der tatsächlichen Verfügbarkeit aus Sicht der Anwender.

Als wesentliche Voraussetzungen für ein funktionierendes Informations-Sicherheits-Management-System sieht Gocke fünf Elemente: eine zentrale IT-Organisation, qualitätsgesicherte Softwaresysteme, Verzicht auf Eigenentwicklungen, standardisierte

Prozesse und die Akzeptanz durch die Mitarbeiter.

Die Bewertung des IT-Leiters über die Erfahrungen mit der Einführung eines ISMS sind kurz und bündig: „Wir profitieren nachhaltig davon.“ Anwender wie Pflegekräfte erwarten ein funktionierendes KAS und stellen fest, dass es auch verfügbar und performant ist. Für die IT ist es eine wichtige Absicherung, weil durch die Zertifizierung bestätigt wird, dass die umgesetzten Sicherungsmaßnahmen State of the Art sind. „Als CIO tue mich jetzt leichter, die Kosten der IT zu rechtfertigen. Kosten und Nutzen sind transparenter, und die Maßnahmen sind nachweisbar für die Geschäftsprozesse notwendig. Wir können jetzt die Risiken sicher managen, agieren nicht von Maßnahme zu Maßnahme, sondern haben alles Notwendige im System verankert. Damit kann ich auch ruhiger schlafen.“

Für das UKE ist das Management der Informationssicherheit ein permanenter Prozess geworden. Die IT betreut 26 IT-Systeme, die sich ständig verändern und weiterentwickelt werden. Das gesamte Klinikum profitiert neben einer dauerhaft hohen Verfügbarkeit der IT-Systeme, der Wahrung von Vertraulichkeit und Integrität der Informationen auch davon, dass durch standardisierte Abläufe die Zusammenarbeit zwischen den Bereichen besser läuft. Sicherheitsfunktionen wie die durchgängige Anwendung digitaler Signaturen oder die Verfügbarkeit aller Informationen in einem zentralen Zugriffsarchiv sind etabliert. Schnittstellen sind klar definiert, und wenn etwas schwarz auf weiß steht, kontrolliert, aktiv umgesetzt und laufend verbessert wird, ergeben sich auch verlässlichere Prozesse.

| www.uke.de |