

# UKE: Zertifizierte Informationssicherheit

Elektronische Patientenakte mit Soarian Clinicals und Soarian Health Archive erhält BSI-Gütesiegel

**Das Universitätsklinikum Hamburg-Eppendorf (UKE) zählt mit seinen 1.500 Betten zu den größten Krankenhäusern Deutschlands. Rund 8.900 Mitarbeiter kümmern sich hier jährlich um circa 330.000 Patienten. Seit Jahren ist das UKE konsequent auf Erfolgs- und Wachstumskurs – nicht zuletzt dank seiner hochmodernen IT-Landschaft.**

Gegenüber 2005 wurden die Patientenzahlen im letzten Jahr um über 50 % gesteigert, die Case-Mix-Punkte stiegen sogar um fast 60 % auf rund 108.000. 2010 erzielte das UKE mit einem Überschuss von 2 Millionen Euro auch erst-

mals ein positives Jahresergebnis. Diese Erfolge sind die Früchte einer konsequenten Umstrukturierung: Seit 2004 hat das UKE seine administrativen, technischen und klinischen Prozesse komplett neu geordnet, einen neuen Klinikbau in Betrieb genommen und gezielt in eine moderne Infrastruktur investiert. In diesem Zusammenhang wurde 2008 ein webbasiertes Klinisches Arbeitsplatzsystem (KAS) mit Soarian® Clinicals und Soarian® Health Archive eingeführt (wir berichteten in Ausgabe 12 (April 2010) ab S. 48). Die flächendeckend verfügbare elektronische Patientenakte (ePA) erlaubt es dem UKE, papierlos zu arbeiten. Dies stellt allerdings auch völlig neue Anfor-

derungen an die Sicherheit der Systeme. Um eine Papierakte zu lesen, benötigt man keine Technik – im papierlosen Krankenhaus aber sind funktionierende IT-Systeme schlicht unersetzlich. „Die elektronische Patientenakte trägt maßgeblich zur Effizienz unserer Prozesse bei“, sagt Dr. Peter Gocke, Leiter des Geschäftsbereichs Informationstechnologie des UKE. „Aber IT-Systeme können auch ausfallen. Je mehr von der Technik abhängt, desto wichtiger ist es, sich Gedanken über ihre Sicherheit zu machen.“

## IT-Verfügbarkeit 99,97 Prozent

Daher betreibt das UKE einen hohen technischen Aufwand, um die Verfügbarkeit des Systems sicherzustellen. Denn ein „Papier-Back-up“ war für das UKE von Anfang an keine Option. So ist bereits das Netzwerk auf hohe Verfügbarkeit und Ausfallsicherheit angelegt. Die Netzwerkanbindung einzelner Räume ist prinzipiell auf zwei Wege verteilt, sodass bei einem Ausfall nur maximal die Hälfte der Anschlüsse eines Raums betroffen ist. Das Klinische Arbeitsplatzsystem und das Archiv laufen auf redundanten Servern mit gespiegeltem Datenbestand, die sich für den Fall eines Brandes oder anderer Zwischenfälle in unterschiedlichen Gebäuden befinden. Etwaige Konfigurationsänderungen werden grundsätzlich erst an einem Testsystem durchgeführt und nur, wenn

## Kurz zusammengefasst

Das Universitätsklinikum Hamburg-Eppendorf (UKE) hat für seine elektronische Patientenakte mit Soarian® Clinicals und Soarian® Health Archive das Gütesiegel für Informationssicherheit erhalten, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) an Unternehmen vergeben wird: das „ISO 27001-Zertifikat auf der Basis von IT-Grundschutz“.

Das UKE ist das erste deutsche Krankenhaus, bei dem der gesamte Informationsverbund der elektronischen Patientenakte (ePA) – vom Archivserver über die Netzwerkkomponenten bis hin zu den Endgeräten der Anwender – vom BSI überprüft und nach der internationalen Norm ISO 27001 zertifiziert wurde.



Das Neue Klinikum des UKE – hier die großzügige Eingangshalle – vereint 16 Kliniken unter einem Dach.

alles komplikationslos verläuft, auf das Produktivsystem übertragen. Eine dritte Datenbank enthält noch einmal eine sekundengenaue Kopie der elektronischen Patientenakte, die bei einem gleichzeitigen Ausfall beider Standorte als Read-only-System zur Verfügung gestellt werden kann.

Die Verfügbarkeit der elektronischen Patientenakte liegt heute inklusive der Wartungsfenster bei 99,97 Prozent. Im Vergleich dazu befand sich die Papierakte nur in etwa 60 Prozent der Fälle gerade dort, wo sie gebraucht wurde. Trotzdem, so Dr. Peter Gocke, hatte mancher angesichts der Abhängigkeit seiner täglichen Arbeit von der Technik noch „ein ungutes Gefühl“. Dem sollte die

ISO-27001-Zertifizierung begegnen – denn „mehr geht nicht im Umfeld von IT-Sicherheit“. Die „ISO-27001-Zertifizierung auf Basis von IT-Grundschutz“ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) betrifft beim UKE nicht nur sämtliche an der elektronischen Patientenakte beteiligten IT-Systeme, die Netzwerkinfrastruktur, die circa 100 Server und mehrere Tausend Clients, sondern bezieht auch organisatorische Aspekte und die Anwender selbst ein. Das UKE ist damit das erste Krankenhaus in Deutschland, bei dem der gesamte Informationsverbund der elektronischen Patientenakte vom BSI überprüft und nach ISO 27001 zertifiziert wurde.

**„Der Datenzugriff durch Personen, die an der Behandlung eines Patienten zu beteiligen sind, ist in Soarian sehr elegant geregelt.“**

**Dr. Peter Gocke,**  
Leiter des Geschäftsbereichs  
Informationstechnologie  
am Universitätsklinikum  
Hamburg-Eppendorf

# „Die elektronische Patientenakte trägt maßgeblich zur Effizienz unserer Prozesse bei.“

Dr. Peter Gocke,  
Leiter des Geschäftsbereichs Informationstechnologie  
am Universitätsklinikum Hamburg-Eppendorf



„IT-Grundschatz“ bezeichnet eine vom BSI entwickelte Methode für erforderliche Sicherheitsmaßnahmen bei der IT-Infrastruktur. Das Zertifikat bestätigt die erfolgreiche Umsetzung dieser Maßnahmen sowie die Einhaltung der Anforderungen der internationalen Norm ISO 27001 an ein Informationssicherheits-Managementsystem (ISMS). Zur Unterstützung stellt das BSI spezielle Werkzeuge zur Verfügung. Dazu zählen Standards und Hilfestellungen zum Informationssicherheitsmanagement sowie die sogenannten IT-Grundschatz-Kataloge, die auf über 4.000 Seiten mögliche Gefährdungen und geeignete Standardsicherheitsmaßnahmen für zahlreiche IT-Konfigurationen beschreiben.

## Optimierungen nach Best Practices

„Das Thema Informationssicherheit hat für uns grundlegende Bedeutung. Deshalb hatten wir bereits in die Ausschrei-

bung für das klinische Arbeitsplatzsystem die Forderung nach Zertifizierungsfähigkeit aufgenommen“, berichtet Dr. Gocke. Im April 2010 war die Digitalisierung so weit vorangeschritten, dass die ersten Aktivitäten dafür starten konnten: Struktur- und Sicherheitsanalysen, Schutzbedarfsbewertung, die Definition der erforderlichen Maßnahmen und schließlich deren Umsetzung. Nach der Abarbeitung des BSI-Katalogs von Best-Practice-Maßnahmen wurde die damit erreichte Sicherheit im Hinblick auf mögliche Schadensszenarien überprüft.

Ein wichtiger Bestandteil der Vorbereitung war die „Härtung der Systeme“, wie Dr. Gocke es nennt. Die Kernkomponenten der elektronischen Patientenakte, Soarian Clinicals und Soarian Health Archive, boten in puncto Sicherheit bereits beste Voraussetzungen. An anderen Stellen aber bestand durchaus noch Optimierungspotenzial: So werden jetzt alle Server gegeneinander abgeschottet, sehr viel

mehr Ports als früher sind standardmäßig gesperrt, und die interne Netzwerkkommunikation wurde auf das sichere Protokoll HTTPS umgestellt. „Soarian spricht ja von Haus aus HTTPS, da gab es keine Probleme. Aber ein Server eines anderen Herstellers bekam Probleme bei parallelen Zugriffen über HTTP und HTTPS, da mussten wir nachbessern“, berichtet Dr. Gocke.

„Die Herausforderung bestand weniger in den notwendigen technischen Maßnahmen als vielmehr in ihrer ausführlichen Dokumentation“, ergänzt Maik Fleischer, einer der Siemens-Berater, die das UKE bei der Zertifizierungsvorbereitung unterstützt haben. Das Siemens-Team kümmerte sich um die technologischen Aspekte des Prozesses, führte Analysen und Tests durch, begleitete notwendige Nachrüstungen und Umstellungen und übernahm auch die Abstimmung mit anderen Herstellern. Außerdem hatte das UKE noch Spezialisten von

„Viele Anwender sagen zum Beispiel, dass sie USB-Sticks jetzt sogar zu Hause mit mehr Achtsamkeit verwenden.“ Bestandteil des Informationssicherheitsmanagements am UKE ist auch das sogenannte IT-Board, auf dem alle gemeldeten sicherheitsrelevanten Vorfälle diskutiert werden. Außerdem wurde eine „IT-Visite“ eingeführt, bei denen IT-Mitarbeiter im direkten Kontakt mit den Anwendern vor Ort über die Nutzung der Systeme sprechen.

Gefragt, welchen Stellenwert das Thema Datenschutz bei der Informationssicherheit einnimmt, fasst sich Dr. Peter Gocke kurz: „Datenschutz ist die Pflicht, Informationssicherheit ist die Kür.“ Mit Soarian Clinicals und Soarian Health Archive kann er notwendige Datenschutzvorgaben problemlos umsetzen. „Zum Beispiel ist der Datenzugriff durch andere Personen, die an der Behandlung eines Patienten zu beteiligen sind, in Soarian sehr elegant über Konsile und Leistungsstellen geregelt“, erklärt Dr. Gocke. „Und im Notfall kann jeder Arzt auch im System nach Patientendaten suchen – will er aber darauf zugreifen, muss er sein Passwort und eine Begründung eingeben, und sein Zugriff wird protokolliert.“

Im Oktober 2010 waren endlich alle Maßnahmen umgesetzt und die notwendigen Referenzdokumente erstellt. Über den Jahreswechsel 2010/2011 durchleuchteten dann Sicherheitsexperten des BSI im Rahmen eines Vor-Ort-Audits vierzehn Tage lang die sicherheitsrelevanten Systeme und Prozesse des UKE auf Herz und Nieren. Das Ergebnis: ein 160 Seiten starker Prüfbericht, der nun seinerseits noch in der Zertifizierungsstelle des BSI überprüft werden musste. Im April war es dann endlich soweit: Auf der conhIT 2011 in Berlin übergab das BSI dem Universitätsklinikum Hamburg-Eppendorf das ISO-27001-Zertifikat auf der Basis von IT-Grundschutz für den Informationsverbund seiner elektronischen Patientenakte. „Die Mühe hat sich gelohnt“, zeigt sich IT-Leiter Dr. Gocke zufrieden. „Wir haben von den Best Practices des IT-Grundschutzes eine Menge gelernt. Vor allem aber haben wir es jetzt schwarz auf weiß: Wir haben alles Notwendige dafür getan, dass unser Informations-

verbund sicher ist. Die Zertifizierung vermittelt uns Sicherheit, den Anwendern, meinen Mitarbeitern in der IT – und mir. Sie ist gelebtes Risikomanagement.“

„Wir von Siemens sind natürlich stolz, dass Soarian Clinicals als bisher einziges Klinikinformationssystem in Deutschland diese strenge und umfassende BSI-Sicherheitszertifizierung bestanden hat“, fügt Maik Fleischer hinzu. „Außerdem konnten wir in diesem Prozess wertvolles Wissen darüber sammeln, wie wir von Anfang an eine optimale Konfiguration ausliefern können. Davon werden unsere Kunden profitieren.“

Die BSI-Zertifizierung muss regelmäßig erneuert werden. Am Jahresende steht bereits das erste Überwachungsaudit an – das UKE und Siemens sind bereit.

## Auf einen Blick

**Universitätsklinikum  
Hamburg-Eppendorf**

**Gründung:** 1889

**Träger:** Öffentlich-rechtliche  
Körperschaft,  
eigenständig wirtschaftend

**Geschäftsführung:**  
*Ärztlicher Direktor (komm.):*

Prof. Dr. Guido Sauter

*Kaufmännischer Direktor:*

Dr. Alexander Kirstein

*Direktor für Patienten- und*

*Pflegemanagement:*

Joachim Pröbß

*Dekan:* Prof. Dr. Dr. Uwe Koch-Gromus

**Eingesetztes KIS:** Soarian Clinicals

**Archiv- und Dokumenten-  
managementsystem:**

Soarian Health Archive

**Mitarbeiter:** circa 8.900

**Betten:** 1.500

**Patienten pro Jahr (stationär):**  
circa 76.000

**Patienten pro Jahr (ambulant):**  
257.000

Data Systems aus Braunschweig ins Boot geholt, die beim Thema Informationssicherheitsmanagement beratend zur Seite standen.

### Gelebtes Risikomanagement

Denn Informationssicherheit bedeutet mehr als IT-Sicherheit. Zusätzlich zum Schutz der IT-Systeme und der regelmäßigen Suche nach möglichen Schwachstellen muss ein zuverlässiges System für das sichere Risikomanagement etabliert werden. Auch die Arbeitsabläufe, in denen die Systeme verwendet werden, sind dabei von Bedeutung. Deshalb werden bei der BSI-Zertifizierung auch die sicherheitsrelevanten Prozesse, etwa beim Informationszugriff oder bei der Passwortvergabe, sowie das Wissen der Mitarbeiter überprüft. Im UKE absolvieren jetzt die Anwender einmal im Jahr eine Schulung zum Thema Informationssicherheit. „Die Resonanz auf die Schulung ist sehr erfreulich“, lächelt Dr. Gocke.

### Info/Kontakt:

[www.siemens.de/soarian](http://www.siemens.de/soarian)  
[ulf.fischer@siemens.com](mailto:ulf.fischer@siemens.com)