PRESSEMITTEILUNG

9. März 2012

Ausgestaltung der Notfallzugriffe auf Patientendaten im UKE formell beanstandet

Der Notfallzugriff ermöglicht jedem Arzt des Universitätsklinikums Hamburg-Eppendorf (UKE) unabhängig davon, ob er eine Behandlung durchführt, auf alle elektronischen Daten der Patienten zuzugreifen. Dies kann in außergewöhnlichen, sehr zeitkritischen Situationen medizinisch geboten sein. Bislang fehlen jedoch die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz vor einem Missbrauch dieses Instruments.

Der Arzt, der den Notfallzugriff nutzt, bekommt lediglich einen Warnhinweis. Anschließend wird er aufgefordert, einen Grund für den Zugriff außerhalb seines normalen Berechtigungsprofils anzugeben. Eine Kontrolle dieser Gründe oder eine stichprobenartige Prüfung der Protokolldateien auf Unregelmäßigkeiten und Auffälligkeiten findet jedoch nicht statt. Wer missbräuchlich auf Patientendaten von beispielsweise Prominenten, Kollegen oder Bekannten zugreift, muss daher kaum fürchten, entdeckt zu werden. Dabei ist das Missbrauchspotential hoch: Über den Zugriff erfährt der Nutzer von allen jemals zu dem Patienten im UKE sowie den Tochterunternehmen erfassten Daten. Das kann von der Behandlung eines Unfalls bis zur HIV-Infektion reichen.

Auf Nachfragen des Datenschutzbeauftragten räumte das UKE ein, dass allein im Oktober 2010 insgesamt 6.400 Abfragen über diesen Notfallzugriff erfolgten. Täglich bis zu 290mal. Aktuellere Daten hat der Datenschutzbeauftragte trotz Anforderung bisher nicht erhalten. Die hohen Zugriffszahlen lägen zumeist an „Prozessablaufschwierigkeiten“. Das seien Probleme der Schnittstellen und Systemintegration, die die Ärztinnen und Ärzte über den Notfallzugriff lösen. Allerdings konnten durchschnittlich 45 Notfallzugriffe pro Tag damit nicht erklärt werden, ihre Rechtmäßigkeit blieb offen.

Auf die formelle Beanstandung hin hat das UKE nun drei Wochen Zeit zur schriftlichen Stellungnahme. Für die Umsetzung geeigneter Kontrollmaßnahmen wurde eine dreimonatige Frist gesetzt. Gefordert wird ein regelmäßiger Bericht über Anzahl und Gründe der Notfallzugriffe. Außerdem muss ein Konzept zur Auswertung der Zugriffsprotokolle erstellt und umgesetzt werden. Weiter muss auch eine Lösung für die technischen Prozessablaufprobleme gefunden werden. Ziel muss es insgesamt sein, den Notzugriff in seinen Ausmaßen deutlich einzudämmen und auf seine eigentliche Bestimmung zu begrenzen.

„Die Problematik des Notfallzugriffs ist dem UKE seit mehr als zwei Jahren bekannt. Trotz intensiver Gespräche und datenschutzrechtlicher Begleitung unsererseits ist es nicht gelungen, das UKE zu einem datenschutzgerechten Verfahren zu bewegen. Unsere Geduld ist nunmehr erschöpft. Angesichts der Sensibilität der Daten und der Vielzahl von

Berechtigten und Betroffenen muss das UKE nun unverzüglich in die Umsetzung der technischen und organisatorischen Maßnahmen zur Sicherung der Patientendaten eintreten“, so Johannes Caspar, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.

Pressekontakt:

Arne Gerhards, Tel.: 040/42854-4153