TOP VII Tätigkeitsbericht der Bundesärztekammer

Titel: Datensicherheit in Kliniken und Praxen

Beschluss

Auf Antrag von Prof. Dr. Dr. Wulf Dietrich und Dr. Peter Hoffmann (Drucksache VII - 68) beschließt der 117. Deutsche Ärztetag 2014:

Die Beratungsgesellschaft PwC hat kürzlich in einer Studie zu Datenschutz und Datensicherheit in der Medizin, die an 1.717 europäischen, davon 201 deutschen Kliniken durchgeführt wurde, deutliche Schwachstellen bei Datenschutz und Sicherheit in deutschen Kliniken festgestellt. So sei zum Beispiel eine Verschlüsselung der Patientendaten nur in 40 Prozent der beteiligten deutschen Kliniken üblich gewesen. Der Skandal um die NSA-Abhöraktionen hat in den letzten Jahren gezeigt, dass mit entsprechender technischer Ausrüstung und hoher krimineller Energie fast jede digitale Kommunikation ausgehorcht und ausgewertet werden kann. Die Verunsicherung in der Bevölkerung, speziell den Patienten und den Beschäftigten im Gesundheitswesen, ist groß, da unklar ist, wie sicher digitale Daten heute sind. Moderne Medizin ist auf Vernetzung, Datenspeicherung und digitale Kommunikation angewiesen. Angesichts der allgemeinen Verunsicherung wird der Vorstand der Bundesärztekammer (BÄK) aufgefordert, zu untersuchen, wie sicher Datenspeicherung und Kommunikation in der Medizin heute sind. Hierbei soll unter anderem die Sicherheit bzw. Anfälligkeit von Krankenhausinformationssystemen, Praxissoftware, KV-Datenaustausch und zwischenärztlicher Kommunikation beurteilt werden. Dabei geht es nicht um die konkrete Bewertung einzelner Computersoftware, sondern um die generelle Einschätzung der Datensicherheit in der Medizin. Diese Beurteilung könnte den ärztlichen Umgang mit Computertechnik verbessern und das Vertrauen der Patienten in die Sicherheit ihrer persönlichen Daten erhöhen.

Begründung:

Der NSA-Skandal hat gezeigt, dass die Sicherheit gespeicherter Daten auf drei Ebenen gefährdet ist:

1. Staatliche Stellen haben bei Gefahr im Verzug oder zur Abwehr von Gefahren die rechtliche Möglichkeit, auf gespeicherte persönliche Daten zuzugreifen. Dieses Zugriffsrecht ist nicht auf nationale Grenzen beschränkt.

2. Mit entsprechend technischer Ausrüstung und Computerwissen scheint es möglich zu sein, in praktisch jedes Computersystem einzudringen. Selbst staatliche Stellen

und EU-Institutionen sollen vom US-Geheimdienst überwacht und ausgespäht worden sein.

3. Daten sind nicht immer vor dem Zugriff interner Mitarbeiter geschützt. Der Wikileaks-Informant Bradley Manning hatte einen niederen Dienstgrad, Edward Snowdon war nur ein externer Mitarbeiter. Trotzdem war es beiden möglich, an geheimste Daten heranzukommen und diese zu kopieren. Auch die Schweizer Steuer-CDs wurden von internen Mitarbeitern kopiert.

Es stellt sich daher die Frage, wie sicher medizinische Daten bei Krankenhäusern, Praxen, Krankenkassen, privaten Abrechnungsstellen, Kassenärztlichen Vereinigungen (KV) oder bei der elektronischen Gesundheitskarte (eGK) sind. Von besonderem Interesse ist hier der Schutz der Daten vor dem unberechtigtem Zugriff interner Mitarbeiter oder externer Helfer.