Berufsverband der
Deutschen Radiologen

BDR-Stellungnahme
zu den Presseberichten
über Datenlecks von Patientendaten

Patientendaten gehören zu den intimsten Daten, die über einen Menschen gespeichert werden können. Sie unterliegen deshalb der ärztlichen Schweigepflicht. Jede unbefugte Weitergabe an Dritte ist dem Arzt verboten und sogar strafrechtlich sanktioniert.

Es gehört deshalb zur den wichtigsten ärztlichen Pflichten, Patientendaten so zu verwalten und zu speichern, dass diese wirksam vor dem Zugriff Dritter geschützt sind. Der Arzt hat für die Einhaltung der Schweigepflicht und des Datenschutzes auch dann zu sorgen, wenn Praxismitarbeiter oder EDV-Betreuer Zugriff auf Patientendaten haben sollen oder müssen. Dasselbe gilt, wenn er seine Daten auf externe Serverspeicher auslagert.

Damit ist es natürlich nicht vereinbar, wenn radiologische Bilddaten offen zugänglich im Internet abrufbar sind, jeder einzelne Datensatz und jedes einzelne Bild, das Rückschlüsse auf den Patienten zulässt ist eines zu viel. Den Rechercheuren ist zu verdanken, dass dieser Umstand bekannt geworden und so umgehend behoben werden konnte.

Die Art, wie das Thema jedoch in die Öffentlichkeit kommuniziert und journalistisch ausgeschlachtet wurde, ist typisch für den inzwischen leider allgegenwärtigen Sensationsjournalismus und hat mit seriöser Berichterstattung wenig gemein. Nicht jeder skandalöse Vorgang erreicht auch gleich die Dimension eines Skandals, sondern wird es oft erst durch die mediale Bearbeitung. Ohne in den einschlägigen Berichten explizit genannt zu werden, werden die „Datenlecks“ ohne weiteres den Radiologen zugeordnet und in Fernsehberichten ausschließlich radiologische Geräte und Praxen gezeigt – naheliegend ging es doch um radiologische Bilddaten und trotzdem falsch, denn Verursacher waren Arztpraxen zuweisender Fachgruppen, die die Bilddaten ihrer Patienten in die

eigene Praxis-EDV eingespielt haben und diese nicht ausreichend abgesichert hatten. Inzwischen ist bestätigt, dass es sich bei der Datenpanne in Ingolstadt nicht um den oder die Server der in Ingolstadt tätigen Radiologen handelt, sondern um eine einzige Praxis anderer Fachrichtung, die die radiologischen Daten ihrer Patienten in den eigenen Server einliest und dort speichert. Nach den Zahlen ist das auch für Kempen in NRW anzunehmen. Nachgewiesen bei den sicher gründlichen und akribischen Recherchen wurden demnach zunächst ZWEI offen zugängliche Praxisserver in Deutschland mit insgesamt über 13.000 Datensätzen (die in den Berichten schnell zu 13.000 Betroffenen werden). Zählt man dabei jede MRT-Aufnahme oder jedes Röntgenbild als einzelnen Datensatz, dann dürfte die Zahl der betroffenen Patienten zum Glück überschaubar sein. Das BSI wurde über 17 ungeschützte Server informiert.

Ungeschützte Server sind zwar tatsächlich über das Internet ohne Weiteres einsehbar und offenbar war für einen Datenzugriff in den dargestellten Fällen auch kein Passwort erforderlich, das heißt aber noch nicht, dass die Server auch ohne Weiteres auffindbar, also gleichsam öffentlich zugänglich waren. Vielmehr musste der Server bzw. dessen „Internetadresse“ – die sogenannte IP (eine Zahl im Format XXX.XXX.XXX.XXX) bekannt sein, um tatsächlich Zugriff zu erhalten. Diese Ziffern – speziell für medizinische Datenserver – herauszufinden, ist alles andere als einfach und nur mit spezieller Software möglich. Es konnte deshalb bisher auch nicht bestätigt werden, dass tatsächlich unbefugte Zugriffe erfolgt sind. Hoffentlich bleibt es dabei.

Angesichts der Zahl von über 72.000 Arztpraxen und ca. 2.100 Krankenhäusern mit über 392.400 Ärzten in Deutschland sind 17 ungeschützte Datenserver die unglückliche, aber extreme Ausnahme in Einzelfällen. Richtig ist deshalb der Umkehrschluss:

Patientendaten sind in Deutschland sicher!!

Viel Rauch um Nichts also? Nicht ganz, aber aus einer Mücke, die in der Tat gar nicht existieren dürfte, wurde mal wieder ein veritabler medialer Elefant.
Die Berichte sollten aber jeden Arzt dazu veranlassen, seine Datenschutzkonzepte zu überprüfen.