„Patientendaten gehören nicht in den Müll oder in die Online-Versteigerung, sondern müssen ordnungsgemäß gelöscht werden“

Von Professor Dr. Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit

Immer wieder ist von Datenskandalen die Rede, wenn Patientendokumentationen im Müll oder im Altpapiercontainer landen und nicht ordnungsgemäß vernichtet wurden. Dies kann nicht nur datenschutzrechtliche, sondern im Hinblick auf die Verschwiegenheitspflicht auch strafrechtliche Folgen nach sich ziehen.

Während jedem Arzt der verantwortungsbewusste Umgang mit Unterlagen in Papier hinlänglich bekannt sein dürfte, darf nicht vergessen werden, dass die Speicherung von Informationen zunehmend elektronisch im PC erfolgt. Der Datenschutz und die Verschwiegenheitspflicht müssen bei der Ausgestaltung der Technik konsequent Berücksichtigung finden; dies betrifft auch den Fall, wenn der PC samt Festplatte ausgetauscht, verkauft, verschenkt oder sonst vom Arzt aus der Hand gegeben wird. Dann muss darauf geachtet werden, dass die personenbezogenen Patientendaten nicht zu unberechtigten Dritten gelangen bzw. die Patientengeheimnisse offenbart werden. Wie Papierunterlagen sind auch elektronische Daten sicher zu löschen. Hierzu reichen bloße Löschbefehle hingegen nicht; diese führen grundsätzlich nur dazu, dass der Speicherplatz, auf dem die Daten abgelegt sind, zum Überschreiben freigegeben wird. Wann dies jedoch geschieht, ist offen, so dass die Daten und Informationen wieder rekonstruiert werden können. Das Bundesamt für Sicherheit in der Informationstechnik gibt z.B. Hinweise, wie ein sicheres Löschen oder auch Vernichten erfolgen kann. Soweit man auf spezialisierte Anbieter zur Löschung der Daten oder Vernichtung der Datenträger zurückgreifen möchte, müssen jedoch auch hierbei der Datenschutz und die Verschwiegenheitspflicht gewahrt sein. Neben einem schriftlichen Auftragsvertrag und der Kontrolle durch den Arzt sollte hierbei darauf geachtet werden, dass die Datenträger an sich sicher verschlüsselt sind, damit dem Auftragnehmer keine Geheimnisse offenbart werden. Trotz Einschaltung eines Auftragnehmers verbleibt aber letztlich die datenschutzrechtliche Verantwortung dennoch beim Arzt selber. Die Kosten im Fall der Inanspruchnahme eines spezialisierten Anbieters sind auch nicht besonders hoch. Von dem Fall der Auftragsvergabe unabhängig stellt die sichere Verschlüsselung des Datenträgers an sich ohnehin auch eine geeignete Maßnahme dar, dass im Falle eines Diebstahls die Daten nicht von Unbefugten zur Kenntnis genommen werden können.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit steht für Rückfragen sehr gern zur Verfügung (Klosterwall 6. 20095 Hamburg, Telefon: 040/42854-4040, E-Mail: mailbox@datenschutz.hamburg.de).