Vortrag 1: Datenschutz anwenderfreundlich gestalten

Der erste Block behandelte die Vernetzung von Systemen in der Diagnostik, in der Behandlung, in der Pflege und in der Verwaltung der Krankenhäuser und Kliniken.
Zu Beginn ging es um die Frage, ob einem Hersteller eines Krankenhausinformationssystems (KIS) von einer Aufsichtsbehörde ein Bußgeld auferlegt werden kann, wenn dieser nicht zur Gewährleistung des Datenschutzes beiträgt. Es wurde festgestellt, dass die Datenschutzgrundverordnung (DS-GVO) die Verantwortlichen in die Pflicht nimmt, also diejenigen, die Zwecke und Mittel der Verarbeitung festlegen. Dies sind hier die Krankenhäuser bzw. deren Träger. Sie wählen die KIS aus, konfigurieren und betreiben diese. Strafen oder Bußgelder für Hersteller sind nicht vorgesehen. Krankenhäuser und ihre Trägern können die Hersteller jedoch mit Investitionsentscheidungen und vertragsrechtlichen Instrumenten beeinflussen. Die Datenschutzaufsichtsbehörden haben Anforderungen an KIS in der Orientierungshilfe Krankenhausinformationssysteme formuliert. Bei der Erstellung der Orientierungshilfe wurden Hersteller und Verbände gehört.
Ferner wurde diskutiert, wie mit dem in der DS-GVO vorgesehenen Zertifizierungsverfahren der Datenschutz in KIS verbessert werden kann, und nach welchen Kriterien und Verfahren Gesundheits-Apps auf ihre Datenschutzkonformität geprüft werden können. Das Ergebnis war, das solche Verfahren und Kriterienkataloge bisher nicht zur Verfügung stehen. Dies ist auf drei Ursachen zurückzuführen: Erstens sind die Zertifizierungsregeln der DS-GVO nur auf Verarbeitungsvorgänge im Sinne der DS-GVO anwendbar. Das bedeutet, dass Produkte wie KIS oder Gesundheits-Apps nach diesen Regeln nur als Teil einer Verarbeitung bei einem Verantwortlichen oder einem Auftragsverarbeiter (Dienstleister) geprüft werden können. Zweitens sind die Zertifizierungsstellen, also die Stellen, die die Prüfungen übernehmen sollen, noch nicht akkreditiert. Drittens liegen die Kriterien, nach denen die Zertifizierungsstellen prüfen sollen, noch nicht vor. An den beiden letzten Punkten arbeiten die Datenschutzaufsichtsbehörden in Deutschland und Europa.
Ein weiterer Punkt war die Anwendbarkeit von Microsoft Windows 10 im Krankenhausbetrieb. Es wurde festgestellt, dass Windows 10 in seiner derzeitigen Form nicht datenschutzkonform einsetzbar ist. Selbst mit umfangreichen technischen Schutzmaßnahmen lassen sich datenschutzrechtliche Risiken nicht vollständig vermeiden.
Zuletzt wurde die Frage aufgeworfen, welche Verfahren zur Zugriffskontrolle in KIS verwendet werden können. Systeme auf der Basis von kontaktbehafteten oder kontaktlosen persönlichen Chipkarten und anderen Hardware-Elementen (so genannten Token) können hierzu geeignet sein. Insbesondere in Kombination mit PINs oder Passwörtern können sie zu einer gleichermaßen sicheren und bequemen Benutzung von KIS beitragen. Systeme auf der Basis von biometrischen Verfahren wie Fingerabdruck oder Gesichtserkennung sind hingegen nur unter sehr engen Voraussetzungen datenschutzrechtlich zulässig, da sie tief in die Rechte der Beschäftigten in den Krankenhäusern eingreifen.