

Zusammenwachsen der Technologien als Herausforderung für Datenschutz und Datensicherheit

Vernetzung und die Integration von Technologien sind aktuelle Themen dieser Zeit. Ob dieses Ziel unter dem Oberbegriff der „Mobility“, „Cloud“ oder anderen Schlagworten behandelt wird, ist dabei unerheblich für die Herausforderungen im Bereich der Sicherheit und des Datenschutzes.

Die Verschmelzung der Kommunikationstechnik, Medizintechnik und Versorgungstechnik in Richtung „IP-Plattformen“ der Informationstechnik und der Ausbau der Telemedizin fordern die Kliniken in Deutschland in besonderem Maße heraus. Neben dem traditionell hohen Anspruch an den Schutz personenbezogener Daten, der intensiv und verantwortungsbewusst im Rahmen der eingesetzten Anwendungsverfahren gehandhabt wird, ergeben sich zusätzliche Herausforderungen durch Vernetzung und Integration einer Vielzahl weiterer technischer Systeme und der Bereitstellung dort erhobener Daten im Interesse der Versorgungs- und Behandlungsqualität des Patienten.



Gleichzeitig werden die gesammelten Daten im Interesse der reibungslosen Prozessgestaltung mobilisiert und treffen damit – theoretisch – auf eine fast unüberschaubare Anzahl weiterer potentieller Strukturen und Endgeräte.

Dabei sind nicht alle „Betriebsmodelle“ mit den Anforderungen an die Sicherheit und den Datenschutz kompatibel. Begriffe wie „Cloud“, „Mobility“, „BYOD“ und andere werden schnell überreizt (hype) und halten den notwendigen Anforderungen an professionelle und sichere Strukturen nicht ohne Weiteres stand. Verschiedene, mit der Informationstechnologie verschmelzende Technologien, primär die Medizintechnik, zeichnen sich durch erheblichen Nachholbedarf bei der Sicherheit und Aktualität der eingesetzten Verfahren aus. Vormals „Insellösungen“ mit niedrigem bis keinem Gefährdungsgrad werden zunehmend in „vernetzte“ Strukturen integriert und bei ungenügender Härting gegen Angriffe zum Sicherheitsrisiko. Darüber hinaus muss stets der Faktor Mensch durch Sensibilisierung, Schulung und Ausbildung auf Chancen und Risiken der Technologien hingewiesen werden.

Für Kliniken in Deutschland dominiert daher immer der Schutzgrad der verwalteten Daten vor der maximalen technologischen Verfügbarkeit. Die Sicherheit der den Krankenhäusern anvertrauten Daten hat die oberste Priorität und erfordert manchmal auch Verzicht aus Verantwortung.

Michael Thoss,
Vorstandsmitglied, Bundesverband der Krankenhaus-IT-Leiterinnen/Leiter e.V.

Mitherausgeber

