Entschließung der 81. Konferenz
der Datenschutzbeauftragten des Bundes und der Länder
am 16./17. März 2011 in Würzburg

Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dabei insbesondere folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.
4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.
5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.
6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.
7. Grundstandards – wie beispielsweise die Revisionssicherheit – sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass

entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)
- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KV-SafeNet eingehalten werden.