TÄTIGKEITSBERICHT

2011/2012

BAYERISCHES LANDESAMT FÜR
DATENSCHUTZAUFSICHT

14.4 Apothekenrechenzentren

Rezeptdaten dürfen gemäß § 300 Abs. 2 Satz 2 SGB V für andere Zwecke als zur Abrechnung verarbeitet und genutzt werden, wenn sie anonymisiert sind. Ausreichend ist dabei eine faktische Anonymisierung.

Innerhalb des Berichtszeitraums waren wir mit der Frage befasst, in welcher Art und Weise Rezeptdaten von Apothekenrechenzentren an Firmen weitergegeben werden dürfen, die diese Daten insbesondere im Auftrag von Pharmaunternehmen auswerten. Nach § 300 Abs. 2 SGB V dürfen Apotheken zur Erfüllung ihrer Abrechnungsverpflichtungen gegenüber den Krankenkassen Rechenzentren in Anspruch nehmen. Die Rechenzentren dürfen die Daten für im Sozialgesetzbuch bestimmte Zwecke verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind; anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden.

In den bei uns anhängigen Verfahren ging es im Wesentlichen um die Frage, welche konkreten Anforderungen für die Nutzung zu anderen Zwecken an die Anonymisierung der Rezeptdaten zu stellen sind. Prüfungsmaßstab war dabei die gesetzliche Definition in § 3 Abs. 6 BDSG, wonach Anonymisieren das Verändern personenbezogener Daten derart ist, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Das Gesetz geht damit von zwei Möglichkeiten der Anonymisierung aus:

- Bei einer absoluten Anonymisierung werden die Merkmale, die eine Person identifizieren können, aus den Datensätzen entfernt. Dieser Informationsverlust hat zur Folge, dass eine Verknüpfung von Datensätzen über einen bestimmten Zeitraum nicht möglich ist.
- Bei einer faktischen Anonymisierung werden die Merkmale, die eine Person identifizieren können, durch kryptographische Verfahren derart verarbeitet, dass diese mit verhältnismäßigen Mitteln nicht mehr hergestellt werden können. Damit ist ein Rückschluss auf die dahinter stehende natürliche Person ausgeschlossen, eine Verknüpfung der Datensätze über einen gewissen Zeitraum jedoch möglich.

Verfahren zur Gewährleistung einer faktischen Anonymisierung müssen derart ausgestaltet sein, dass die eingesetzten kryptographischen Funktionen bezüglich der Algorithmen und Schlüssellängen sowohl dem aktuellen als auch dem absehbar zukünftigen Stand der Technik entsprechen. Die technischen und organisatorischen Maßnahmen nach § 9 BDSG müssen derart ausgestaltet sein, dass die kryptographischen Schlüssel sicher erzeugt, regelmäßig gewechselt sowie derart sicher verwahrt werden, dass ein Kopieren oder Entwenden der Schlüssel nicht möglich ist. Entsprechendes gilt bei dem Einsatz von asymmetrischen Verschlüsselungsverfahren, wenn sich die Identifikationsmerkmale aus wenigen Ziffern zusammensetzen, um die Möglichkeit einer Brute-Force-Entschlüsselung zu verhindern.

Wenn derart anonymisierte Daten zur zusätzlichen Sicherung über eine unabhängige Stelle (Clearingstelle) laufen, die eine zweite Verschlüsselung der bereits verschlüsselten Identifikationsmerkmale vornimmt, so stufen wir dies als sinnvolle, aber auch notwendige Schutzmaßnahme ein. Auch hier gelten die oben beschriebenen Maßstäbe für die Schlüsselerzeugung, -verwendung und -verwahrung.

Bei den von uns im letzten Jahr geprüften Verfahren sind wir zu dem Ergebnis gekommen, dass die praktizierte Verfahrensweise, abgesehen von geringfügigen Punkten, die bereits behoben wurden, den oben dargestellten Vorgaben entspricht.