Anlage 10

zur Vereinbarung zwischen dem Zentralinstitut für die kassenärztliche Versorgung in der Bundesrepublik Deutschland und der Kassenärztlichen Vereinigung gemäß § 80 SGB X

Sicherheitsziele für die ZI-Datenstelle

Sicherheitsziele für die ZI-Datenstelle

Das Zentralinstitut übernimmt die Aufgaben des zentralen Erwerbs von vertraglichen Verordnungsdaten gemäß § 300 Absatz 2 SGB V. Darüber hinaus werden vom Zentralinstitut pseudonymisierte Verordnungsdaten mit pseudonymisierten aus vertragsärztlichen Abrechungsdaten stammende Diagnosedaten arzt- und patientenbezogen zusammengeführt, um somit eine Datenbasis zu schaffen, auf deren Grundlage das Zentralinstitut die KVen bei der Erfüllung ihrer gesetzlichen Aufgaben unterstützen soll. Folgende Sicherheitsziele sind für das Zentralinstitut essentiell für die Aufgabenerfüllung die im Zusammenhang mit den o.g. Daten stehen maßgeblich. Die Erreichung der Sicherheitsziele wird durch entsprechende technische und organisatorische Maßnahmen unterstützt, die im Sicherheitskonzept der ZI-Datenstelle, das unter Beteiligung eines BSI-zertifizierten Auditors auf Basis von BSI-Grundschutz 100-1, 100-2 und 100-3 erstellt wurde.

1. Vertraulichkeit

Zum Schutz der Persönlichkeitsrechte liegen sowohl patientenidentifizierende als auch arztidentifizierende Daten in der Datenbank des Zentralinstituts in pseudonymisierter Form vor. Der Zugang zu IT-Diensten und der Zugriff auf Informationen ist ausschließlich auf ein notwendiges Minimum an qualifizierten und namentlich benannten Mitarbeitern des Zentralinstituts reduziert, die mit entsprechenden dedizierten Rechten ausgestattet sind. Die Datenverarbeitung erfolgt ausschließlich zum Zweck der Datenanalysetätigkeiten, auf dessen Grundlage das Zentralinstitut die KVen bei der Erfüllung ihrer gesetzlichen Aufgaben unterstützt. Der gute Ruf des Zentralinstituts ist mit allen Mitteln zu bewahren. Daher werden sehr hohe Anforderungen an die Sicherstellung der Vertraulichkeit aller Informationen gestellt.

2. Datenintegrität und Authentizität

Alle anzunehmenden Datenbestände, die in den IT-Verbund der Datenstelle des Zentralinstituts gespeichert und verarbeitet werden sollen, sind zuvor einer Authentizitätsprüfung zu unterziehen. Erst nach zweifelsfreier Sicherstellung der Authentizität der Daten sind die anzunehmenden Daten zu den Gesamtdatenbeständen hinzuzufügen. In allen Phasen der Datenverarbeitung ist sicherzustellen, dass die Gesamtdatenbestände weder geändert noch gelöscht werden und manipulationsfrei in der Datenbank gelagert werden.

3. Revisionsfähigkeit

Alle Maßnahmen von IT-Diensten und IT-Sicherheitsmaßnahmen sind revisionssicher zu dokumentieren. Jeder Arbeitsschritt und jeder Vorgang muss transparent nachvollziehbar sein. Eine regelmäßige Kontrolle der Funktionalitäten der IT-Dienste und der IT-Sicherheit ist durchzuführen. Sämtliche Verarbeitungsprozesse müssen lückenlos nachvollziehbar sein. Es ist zu jedem Zeitpunkt zu dokumentieren, welche berechtigten Mitarbeiter wann und auf welche Weise auf den IT-Verbund in der Datenstelle des Zentralinstituts zugegriffen haben.

4. Verfügbarkeit und Zuverlässigkeit

Alle Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Dies impliziert die Verfügbarkeit und Zuverlässigkeit der zur Verarbeitung erforderlich eingesetzten IT-Systeme, Datenbanken und Analysesoftware, die als Komponenten die Basis zur Handlungsfähigkeit und Effizienz bilden. Der sichere Betrieb aller eingesetzten IT-Komponenten ist hierbei unabdingbar. Ein Ausfall der IT-Systeme bzw. einem Datenverlust ist durch entsprechende technische und organisatorische Maßnahmen entgegenzuwirken. Voraussetzung für die Aufrechterhaltung der Verfügbarkeit ist die Sicherstellung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle.

5. Nicht-Abstreitbarkeit

Im Bereich der Nicht-Abstreitbarkeit werden zwei elementare Aspekte unterschieden. Die Nicht-Abstreitbarkeit der Herkunft und die Nicht-Abstreitbarkeit des Erhaltens von Datenlieferungen. Bei der Nicht-Abstreitbarkeit der Herkunft kann das Zentralinstitut nachweisen, welche Institution der Sender der Datenlieferung ist und der Sender kann nicht abstreiten, die Datenlieferung gesendet zu haben. Im Fall der Nicht-Abstreitbarkeit des Erhaltens einer Datenlieferung kann der Sender der Datenlieferung nachweisen, dass die Datenlieferung beim Empfänger (Zentralinstitut) eingegangen ist. Der Dateneingang kann nicht abgestritten werden.