Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG

Bundeskanzlei BK
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Erhebung der datenschutzrechtlichen Situation bei den anerkannten sozialen Krankenversicherern

1. Ausgangslage

Im Rahmen ihrer Aufsichtstätigkeiten waren sowohl das Bundesamt für Gesundheit (BAG) wie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB, Hanspeter Thür) mehrfach tätig, damit sich die Krankenversicherer datenschutzkonform verhalten. Ebenso erfolgten in diesem Zusammenhang verschiedene parlamentarische Eingaben. Abklärungen im Auftrag des BAG und des EDÖB bei einzelnen Krankenversicherern haben ergeben, dass teilweise datenschutzrechtliche Mängel bestehen. Der Bundesrat hat deshalb das BAG beauftragt, bei den Versicherern vermehrt die Datensammlungen zu überprüfen und dabei auch gezielt den EDÖB einzubeziehen.

Im Rahmen einer Arbeitsgruppe haben die beiden Aufsichtsorgane im Dezember 2007 allen Krankenversicherern einen ausführlichen Fragebogen mit 70 Fragen zukommen lassen. Diese flächendeckende Erhebung sollte Aufschluss geben über die datenschutzrechtliche Organisation und die Handhabung des Datenschutzes im Krankenversicherungsbereich. Sie stützt sich auf die aufsichtsrechtlichen Bestimmungen von Artikel 27 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG)[1] sowie von Artikel 21 des Bundesgesetzes über die Krankenversicherung (KVG)[2]. Aufgrund qualitativer wie quantitativer Fragen hatten die Krankenversicherer unter Fristsetzung Fragen zur Organisation und zum internen Datenschutz zu beantworten und die notwendigen Unterlagen und Belege beizusteuern.

In einem ersten Schritt haben sich die Aufsichtsorgane ein umfassendes Bild über die datenschutzrechtliche Situation bei den Krankenversicherern machen können. Es besteht nun in einem zweiten Schritt die Absicht, den Krankenversicherern bei der Verbesserung ihrer datenschutzkonformen Organisationsstruktur behilflich zu sein. Nicht zuletzt sollen aufgrund der Erhebung Anregungen zum freiwilligen Datenschutzaudit sowie zur freiwilligen Datenschutzzertifizierung der Krankenversicherer nach revidiertem DSG geschaffen werden. Um den Datenschutz und die Datensicherheit zu verbessern, können die Krankenversicherer auf freiwilliger Basis ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen, sie sind aber von Gesetzes wegen nicht dazu verpflichtet.

Die Auswertung und Analyse der ausführlichen Antworten und detaillierten Belege war aufwändig. Den 93 Krankenversicherer (Stand Ende 2007) darf mehrheitlich attestiert werden, dass sie fristgerecht gute und vollständige Antworten und Belege abgeliefert haben. Für diese Mitarbeit bedanken sich das BAG und der EDÖB bei allen Krankenversicherern. Diese Kooperation der Krankenversicherer ist zu begrüssen und zeigt, dass sie sich der Datenschutzproblematik bewusst sind. Die Auswertung liegt in Form eines ca. 50seitigen Berichtes vor und stellt - mit den allgemeinen Aufsichtsdaten des BAG - eine gute Grundlage für die Optimierung des Datenschutzes bei den Krankenversicherern dar. Dabei ist mit allem Nachdruck festzuhalten, dass die Krankenversicherer die alleinige Verantwortung tragen, dass ihre hochsensiblen Daten datenschutzkonform bearbeitet werden und keine Sicherheitsprobleme entstehen. Die beiden Aufsichtsbehörden sind bereit, die Krankenversicherer dabei zu unterstützen.

[1] SR 235.1
[2] SR 832.10

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

2. Fragestellungen

Der Fragebogen bezog sich auf folgende Tätigkeitsbereiche der Krankenversicherer:

- Versicherungstätigkeiten ausserhalb des KVG (Durchführung und Vermittlung der Zusatzversicherungen nach VVG[3], der Unfallversicherung nach UVG[4], Versicherungskonzerne: Unterschiede in der Produktenpalette)
- Wirtschaftlichkeitskontrolle (Rechnungskontrolle vor und während der Leistungserfassung sowie bei der Nachkontrolle, Menge Rechnungen und Rechnungskontrolle pro Jahr, Prüfungsrichtlinien und Prüfstellen).
- Vertrauensärztlicher Dienst (Zusammensetzung, organisatorische Eingliederung, sowie personelle und fachliche Unterstellung von Vertrauensärzten und Hilfspersonal, Infrastruktur des vertrauensärztlichen Dienstes, Dossierablage und Zugriffsrechte)
- Case Management (Namen, Stellenprozente, organisatorische Eingliederung und fachliche Unterstellung, Tätigkeit für welche Versicherungssparten oder weitere Krankenversicherer oder Unternehmen, Prozessablauf, Zusammenarbeit mit vertrauensärztlichem Dienst und Leistungserbringern, Einwilligungserklärung, Dossierablage und Zugriffsrechte, Erfolgsboni)
- Ausgelagerte Tätigkeits- und Geschäftsbereiche (welche Arbeiten werden von Dritten ausgeführt, welche Synergien mit anderen Unternehmen oder Versicherungen genutzt, Personendatenfluss zu welchem Zweck, Information über das Outsourcing, Informationskonzept, Gewährleistung des Datenschutzes)
- Datenschutzmanagement bzw. Datenschutzorganisation (Organigramm, Bereichszuständigkeiten, Organisation, Konzept, Bearbeitungsreglemente, Datenfluss, Ausbildung, Datenschutzmanagement als UVG-Versicherer, Angaben zum Datenschutzbeauftragten, Umgang mit Datensammlungen, Einstellung zu Datenschutzaudits und Datenschutzzertifizierung)

3. Wichtigste Aspekte der Analyse

Vorausschickend muss erwähnt werden, dass heute die meisten Krankenversicherer innerhalb einer gleichen Versicherungsgruppe oder eines Krankenkassenverbandes zusammenarbeiten. Diese „Gruppenbildung“ galt es bei den Auswertungsergebnissen zu berücksichtigen. **Sie haben eindeutig ergeben, dass die Krankenversicherer zum jetzigen Zeitpunkt über keine einheitlichen Konzepte und Instrumente für die Einhaltung des Datenschutzes verfügen.**

Insbesondere die Analyse des „Herzstücks“ der Untersuchung - die nähere Betrachtung des Datenschutzmanagements und der Datenschutzorganisation der Krankenversicherer - hat folgende Resultate ergeben:

- **Datenschutzkonzept:** Bei 59 % der Krankenversicherer, welche 90 % der Versicherten versichern, ist ein Datenschutzkonzept vorhanden. Ein Datenschutzkonzept gibt Auskunft über die mittel- und langfristige Strategie, wie der Datenschutz im Betrieb wahrgenommen bzw. die Umsetzung sichergestellt wird. Es beschreibt die Organisation des Datenschutzes und daraus leiten sich die konkreten Aufgaben des Datenschutzbeauftragten und der für die Datensammlungen zuständigen Personen ab. Es ist auch zu erwähnen, dass ein Datenschutzkonzept nicht gesetzlich vorgeschrieben ist.

[3] Bundesgesetz über den Versicherungsvertrag SR 221.229.1

[4] Bundesgesetz über die Unfallversicherung SR 832.20

- **Bearbeitungsreglemente**: Nur 26 % der Krankenversicherer, welche aber 62 % der Versicherten versichern, verfügen über Bearbeitungsreglemente zu ihren schützenswerten Datensammlungen. D.h. bei mindestens 38 % der Versicherten existieren keine Vorgaben, wie mit ihren schützenswerten Daten umgegangen werden muss. Weder Datenschutz noch Datensicherheit können hier gewährleistet werden. Gemäss Gesetzgebung muss für jede meldepflichtige Datensammlung ein Bearbeitungsreglement erstellt und aktuell gehalten werden. Das Sicherstellen der Vollständigkeit und der Aktualität der Bearbeitungsreglemente ist eine Hauptaufgabe des Datenschutzbeauftragten des Krankenversicherers und eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung mit schützenswerten Personendaten.

- **Ausbildung der Datenschutzzuständigen** und Besetzung der **Rolle des Datenschutzverantwortlichen**: Die Datenschutzverantwortlichen von 62 % der Krankenversicherer, die 91 % der Versicherten versichern, verfügen über eine befriedigende Ausbildung. Eine genügende Ausbildung leitet sich aus den Pflichten des Datenschutzverantwortlichen ab. In den anderen Fällen ist der Rolleninhaber nicht autonom und steht in einem Interessenkonflikt. Bei 40 Krankenversicherern verfügt der Datenschutzverantwortliche nicht über ein schriftliches Pflichtenheft über seine Rolle.

- 80 % der Krankenversicherer mit 91 % der Versicherten verfügen über einen Datenschutzverantwortlichen. Dieses Resultat ist zu begrüssen. Betriebe ohne Datenschutzverantwortlichen sind verpflichtet, alle ihre Datensammlungen dem EDÖB anzumelden und aktuelle Bearbeitungsreglemente zu unterhalten.

Bezüglich aller Ergebnisse ist festzuhalten, dass die Qualität des Abschneidens der einzelnen Krankenversicherer nicht von deren Grösse oder einer Gruppenbildung abhängt. Im Gegenteil, gerade kleine Kassen haben z.B. gute bis sehr gute Bearbeitungsreglemente vorgelegt.

Trotz der aufgezeigten Mängel ist festzuhalten, dass die Krankenversicherer für die ganze Datenschutzproblematik sensibilisiert sind und auch mehrfach die Bereitschaft bekundet haben, sich in diesem Bereich verbessern zu wollen. So hat sich denn auch eine klare Mehrheit bereit erklärt, sich einem regelmässigen freiwilligen Datenschutzaudit zu unterziehen. Im Weiteren haben bereits heute einzelne Krankenversicherer in Kenntnis des zu erwartenden Grossaufwands angegeben, sich zu gegebener Zeit einer freiwilligen Datenschutzzertifizierung unterziehen zu wollen. Eine Datenschutzzertifizierung stösst aber dennoch auf weniger Akzeptanz als ein Datenschutzaudit. Auch diese Bereitschaft zu Datenschutzaudit bzw. -zertifizierung ist übrigens nicht von der Grösse der Kasse abhängig.

Die aufgezeigten Probleme bezüglich Datenschutzmanagement und Datenschutzorganisation der Krankenversicherer widerspiegeln sich auch in den anderen untersuchten Bereichen:

- Wirtschaftlichkeitskontrolle
- Vertrauensärztlicher Dienst
- Case Management
- Outsourcing in einem engen Zusammenhang

Nachfolgend wird auf diese Sachverhalte kurz eingegangen:

Wirtschaftlichkeitskontrolle

Im Rahmen der Erhebung fand eine erste zusammenfassende Analyse über die Rechnungskontrolle vor, während und nach der Leistungserfassung statt. Gemäss den Angaben der Krankenversicherer wurden im Jahre 2006 ca. 62 Mio. Rechnungen bearbeitet. Davon ist die Verarbeitung von ca. 50 % der Rechnungen automatisiert. Es handelt sich vor allem um TARMED-Rechnungen, die entweder noch durch die Mitarbeitenden vor der Freigabe geprüft werden oder ganz automatisch bis zur Zahlung ohne manuelle Intervention laufen. Bei nicht automatisierter Rechnungsbearbeitung werden entweder alle Rechnungen oder nur ein Teil auf die Wirtschaftlichkeit geprüft, z.B. alle Rechnungen über CHF 1'000.00.

Festgestellt wurde, dass eine Vielfalt von EDV-Systemen vorhanden ist. Die gebräuchlichen Standardprogramme können von den Benutzern, bzw. den Krankenversicherern, den Bedürfnissen entsprechend angepasst werden. Ebenso können die Prüfprogramme von den Krankenversicherern individuell angepasst und mit einzelnen definierten Prüfkriterien „gespeist" werden. Die Mehrheit der Krankenversicherer (vor allem grosse und Versicherungsgruppen) verfügen über kassenspezifische Leistungshandbücher oder interne Richtlinien. Die Kompetenzen der Mitarbeitenden sind grösstenteils definiert.

Aufgrund der erhaltenen Informationen ist nicht ersichtlich, ob die verantwortlichen Mitarbeitenden zusätzlich zu den Leistungs-, bzw. Rechnungsdaten auch zu den besonders schützenswerten Daten der versicherten Person zugreifen können. In Bezug auf die Gewährleistung des Datenschutzes erweist sich eine mehrfach gegebene Antwort, wonach allgemein alle medizinisch und administrativ notwendigen Daten aufgenommen werden (unabhängig davon, ob die Rechnungsstellung elektronisch oder auf Papier erfolgt) als problematisch.

Im Bereich der Wirtschaftlichkeitskontrolle ist deshalb darauf zu achten, dass die Krankenversicherer bei der Datenaufnahme, bzw. -beschaffung das Verhältnismässigkeitsprinzip jederzeit beachten. Von den Krankenversicherern ist zu erwarten, dass sie die Prozesse betreffend Personendaten, insbesondere besonders schützenswerte Daten, mittels eines Bearbeitungsreglementes schriftlich festhalten. Sinnvoll wären auch regelmässige interne Prüfungen über die Einhaltung der datenschutzrechtlichen Vorschriften.

Vertrauensärztlicher Dienst

Die Unabhängigkeit des Vertrauensarztes sowie des vertrauensärztlichen Dienstes (VAD, bei grossen Krankenversicherern und Versicherungsgruppen) ist heute allgemein anerkannter Standard. Nicht überall jedoch wird unter Unabhängigkeit das Gleiche verstanden. So gibt es immer noch Vertrauensärzte, die ihre Mitarbeitenden nicht selbst auswählen dürfen und auch arbeiten vereinzelte Vertrauensärzte nach wie vor im Zusatzversicherungsbereich. Was bei den einzelnen Krankenversicherern in Bezug auf Datenschutzmanagement und Datenschutzorganisation im Grossen fehlt, ist auch im Bereich der Vertrauensärzte mangelhaft. Die Unabhängigkeit auf der strukturellen Ebene bedingt hier auch eigene Bearbeitungsreglemente, die klar umreissen, welche Kompetenzen und Aufgaben den einzelnen Vertrauensärzten und ihren Assistenten zukommen.

Besondere Fragestellungen ergeben sich bei den Vertrauensärzten, die im Mandatsverhältnis arbeiten. Wie werden die Patientendossiers dort datenschutzkonform aufbewahrt, wo der Vertrauensarzt für verschiedene Krankenversicherer gleichzeitig tätig ist? Ist die Auslagerung des VAD durch kleinere Versicherungsgruppen an einen ausgelagerten firmenfremden VAD gesetzeskonform und wie werden daselbst die Patientendossiers der einzelnen kleinen Krankenversicherer getrennt aufbewahrt?

Die ganze Datenschutzproblematik im Bereich der Vertrauensärzte wird im Zusammenhang mit E-Health und dem elektronischen Patientendossier neue Dimensionen annehmen, die es bereits heute vorausschauend in die richtigen Bahnen zu lenken gilt.

Case Management

Einleitend muss festgehalten werden, dass das Case Management im KVG nicht explizit geregelt ist. Mit der Einführung des Case Managements als Massnahme zur Optimierung der Leistungen, zur Kostenkontrolle und zur Kostenminimierung sind die Krankenversicherer bemüht, die Vorgaben für eine Kostenübernahme aufgrund der Kriterien von Artikel 32 KVG, wonach die Leistung wirksam, zweckmässig und wirtschaftlich sein muss, umfassend zu erfüllen. Dieses kostenbewusste Vorgehen namentlich bezüglich der Zweckmässigkeit einer Behandlung steht in einem Spannungsverhältnis zu den einschlägigen Datenschutzbestimmungen, welche auch in diesem Bereich anwendbar sind.

Unter Case Management wird nicht überall das Gleiche verstanden. Die Case Manager sind bei den Krankenversicherern mehrheitlich unter das Leistungsmanagement eingegliedert, was einer Beeinflussungsmöglichkeit von dieser Seite förderlich ist. Die verschiedenen Arten von Case Management haben meist eigene Ablagen, die nicht im vertrauensärztlichen Dienst untergebracht ist. Bei fast allen Krankenversicherern arbeiten die Case Manager zudem noch für andere Versicherungszweige. Die meisten Krankenversicherer bekundeten Mühe, den Prozessablauf eines Case Management detailliert darzustellen bzw. die notwendige Zusammenarbeit mit dem Vertrauensarzt und dem Leistungserbringer zu beschreiben. Die Einwilligungserklärungen der Versicherten sind sehr verschieden, zum Teil unverständlich und sind als „Vollmacht“ für den Austausch der Gesundheitsdaten nicht genügend. Ausserdem fehlt in der Einwilligungsklausel häufig die Ausstiegsklausel. Eine korrekt erteilte Zustimmung der Versicherten ist aber unabdingbar, damit die Case Manager Einblick in die Gesundheitsdaten und allenfalls weitere Angaben und Unterlagen erhalten können.

Für den Case Management Bereich sollen deshalb datenschutzrechtlich optimierte Leistungs-Kontrollprozesse erarbeitet werden. Auf der strukturellen Ebene ist dessen fachliche und organisatorische Unterstellung zu überprüfen und allenfalls zu korrigieren.

Outsourcing

Vor allem bei den grossen Gruppen der Versicherer decken die im Auftrag von Dritten durchgeführten Aufgaben die ganze Bandbreite von anfallenden Tätigkeiten. Ein Hauptteil der an externe Firmen ausgelagerten Arbeiten betrifft die elektronische Datenverarbeitung, die Digitalisierung und die entsprechende Aufbereitung aller Datenbereiche. Mit der Digitalisierung der Patientendossiers inklusive des ganzen Rechnungswesens hat sich eine neue hochkomplexe Organisation aufgedrängt. Diese hat selbstredend Auswirkungen auf den Datenschutz. Die internen Zugriffsrechte bedürfen einer eingehenden Regelung, die den kasseninternen Strukturen vollauf Rechnung trägt. Im Zentrum stehen Sicherheitsfragen, die nach Vorfällen (Datenklau, Verlust von Daten, Weiterleitung an Unberechtigte usw.) in den umliegenden Ländern (Deutschland, GB, Norwegen) umso ernster zu nehmen sind. Es ist mit aller Klarheit darauf hinzuweisen, dass die Krankenversicherer als Inhaber der Datensammlung die volle Verantwortung für die Sicherheit dieser hochsensiblen Daten tragen.

Bei den kleineren Krankenversicherern bleibt der Datenschutz einigermassen überschaubar. Das Outsourcing von spezifischen Aufgaben ist hier weitaus geringer. Der Zusammenschluss der kleineren Krankenversicherer wie der Einsatz im Verbund eines Partnerpools führt jedoch letztendlich zu ähnlichen Problemen.

Im Zusammenhang mit dem Outsourcing interessierte auch, ob die Versicherten darüber hinreichend informiert werden. In den wenigsten Fällen geben die Versicherer einen umfassenden Einblick in die Liste ihrer Outsourcing-Partner. Mehrheitlich wird mittels Infoschreiben, Zeitschriften, Broschüren und Jahresberichte informiert.

Geprüft wurde letztlich, ob die Versicherer beim Outsourcing an Dritte die Anforderungen des Datenschutzes erfüllen. Die Qualität der Verträge, welche den Umfang des Outsourcings, die Datenschutzanforderungen, die Konsequenzen bei Nichteinhaltung und das Kontrollverfahren beinhalten, ist unterschiedlich. Vielfach verfügen die Versicherer über kein geeignetes Kontrollverfahren, mit dem sie die Einhaltung der Datenschutzanforderungen überprüfen können.

4. Weiteres Vorgehen

Das BAG und der EDÖB werden in den nächsten Monaten die diversen offenen Fragen weiter bearbeiten. An die Adresse der Krankenversicherer werden folgende Empfehlungen abgegeben:

- Jeder Krankenversicherer sollte ein Datenschutzkonzept (Strategie) erarbeiten.
- Es muss bei jedem Krankenversicherer ein Verzeichnis der Datensammlungen unterhalten werden. Für jede Datensammlung mit besonders schützenswerten Personendaten wird ein Bearbeitungsreglement unterhalten (Beschreibung der Prozesse inkl. Verantwortlichkeiten, Berechtigungen, Datenfluss sowie der technischen Massnahmen zur Datensicherheit).
- Es sollte bei jedem Krankenversicherer ein Verantwortlicher für den Datenschutz und für jede Datensammlung ein Inhaber bezeichnet werden. Die Aufgaben dieser Rollen werden in einem Pflichtenheft beschrieben.
- Datenschutzverantwortliche müssen über die erforderlichen Fachkenntnisse verfügen.
- Es sollen regelmässig verwaltungsexterne Datenschutzaudits durchgeführt und die Resultate den Aufsichtsbehörden unterbreitet werden.