Schutz der Patientendaten und Schutz der Versicherten

Bericht des Bundesrates in Erfüllung des Postulates Heim (08.3493)

vom 18. Dezember 2013

Inhalt

1 Ausgangslage

1.1 Postulat Heim (08.3493) "Schutz der Patientendaten und Schutz der Versicherten"

Der Bundesrat wurde durch das überwiesene Postulat Heim (08.3493 – Schutz der Patientendaten und Schutz der Versicherten) beauftragt, in einem Bericht aufzuzeigen, welche Massnahmen gegen die Diskriminierung einzelner Patientengruppen durch neue besondere Versicherungsmodelle und zum Schutz der Patientendaten bei den Krankenversicherern geplant sind. Angesichts der Resultate einer ersten grossen Datenschutzerhebung bei den KVG-Versicherern, welche zwischen dem 4. Dezember 2007 und 16. Juni 2009 stattfand, und der Bedeutung dieses Themas für die involvierten Fachkreise und die Bevölkerung, hat sich der Bundesrat bereit erklärt, über die bereits getroffenen und zusätzlich noch zu treffenden Massnahmen zum Schutze der Patientendaten der Versicherten zu berichten. (vgl. *Beilage 1* : Wortlaut Po 08.3493, Begründung und Stellungnahme Bundesrat).

Der vorliegende Bericht berücksichtigt folgende Vorarbeiten:

- Erste Datenschutzerhebung des Bundesamtes für Gesundheit (BAG) mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bei den KVG-Versicherern (2007-2009).
- Zweite Datenschutzerhebung des BAG (2011-2012) nach Erlass des Kreisschreibens 7.1. am 25. August 2011 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer. Die Ergebnisse dieser Erhebungen stützen sich mehrheitlich auf Angaben der KVG-Versicherer.
- Austausche mit anderen sich mit dem Datenschutz der KVG-Versicherer befassenden Stellen (andere Aufsichtsbehörden [EDÖB, Eidgenössische Finanzmarktaufsicht], Branchenverbände [santésuisse, RVK-Verband der kleinen und mittleren Krankenversicherer, RVK], Datenschutzzertifizierungsstelle [KPMG Schweiz]), Rückfragen beim Ombudsman der Krankenversicherung.
- Laufende Datenschutzkontrollen (Stichproben) vor Ort bei den KVG-Versicherern durch die Sektion Audit des BAG.
- Überprüfung der von den KVG-Versicherern angegebenen Datenschutz- und Datensicherheitsmassnahmen durch den IT-Sicherheitsbeauftragten des BAG).

Weitere seit 2008 eingegangene parlamentarische Vorstösse zum Schutz der Patientendaten sind in der *Beilage 2* aufgeführt.

1.2 Datenschutzvorgaben und Datenbearbeitungsgrundsätze für die KVG-Versicherer

Die KVG-Versicherer müssen zahlreiche Datenschutzbestimmungen hauptsächlich in folgenden Bundeserlassen beachten:

- Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1)
- Verordnung vom 11. September 2002 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSV, SR 830.11)
- Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG, SR 832.10)
- Verordnung vom 27. Juni 1995 über die Krankenversicherung (KVV, SR 832.102)
- Verordnung vom 12. April 1995 über den Risikoausgleich in der Krankenversicherung (VORA, SR 832.112.1)
- Verordnung vom 14. Februar 2007 über die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK; SR 832.105)

- Verordnung des EDI vom 29. September 1995 über Leistungen in der obligatorischen Krankenpflegeversicherung (KLV, SR 832.112.31)
- Verordnung des Eidgenössischen Departements des Innern (EDI) vom 20. März 2008 über die technischen und grafischen Anforderungen an die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK-EDI, SR 832.105.1)
- Verordnung des EDI vom 13. November 2012 über den Datenaustausch für die Prämienverbilligung (VDPV-EDI, SR 832.102.2)
- Verordnung des EDI vom 20. November 2012 über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern (SR 832.102.14)
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1)
- Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11)
- Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (VDSZ, SR 235.13)

Die KVG-Versicherer nehmen als private Unternehmen mit der Durchführung der sozialen Krankenversicherung eine öffentliche Aufgabe des Bundes wahr. Deshalb gelten für sie strengere Regeln als für Unternehmen, die keine solche Aufgabe ausüben:

- KVG-Versicherer sind nur im Rahmen der gesetzlichen Bestimmungen befugt, besonders schützenswerte Personendaten[1] und Persönlichkeitsprofile[2] der Versicherten zu bearbeiten oder bearbeiten zu lassen (z. B. gestützt auf Art. 42 Abs. 3-5, Art. 42*a*, Art. 56, Art. 57 Abs. 4, 6 und 7, Art. 58 Abs. 3, Art. 59, Art. 82- 84, Art. 84*a* und 84*b* KVG). Dabei sind sie an die datenschutzrechtlichen Grundsätze wie das *Legalitätsprinzip*, das *Verhältnismässigkeitsprinzip*, das *Zweckbindungsgebot*, den *Grundsatz von Treu und Glauben*, das *Transparenzprinzip*, die *Datenrichtigkeit* und die *Datensicherheit* gebunden (Art. 4, 5, 7 DSG).

- Das *Legalitätsprinzip*, welchem sie als Unternehmen mit der Aufgabe, die soziale Krankenversicherung durchzuführen, gemäss Artikel 2 Absatz 1 Buchstabe b und Artikel 3 Buchstabe h DSG unterstellt sind, sieht Folgendes vor: Werden Personendaten durch die KVG-Versicherer bearbeitet, ist eine gesetzliche Grundlage nötig. *Besonders schützenswerte Personendaten und Persönlichkeitsprofile* im Sinn von Artikel 3 DSG dürfen nur bearbeitet werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht. Im Einzelfall und nur *ausnahmsweise* können solche Daten auch bearbeitet werden, wenn die betroffene Person *eingewilligt* oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 4 Abs. 1 und Art. 17 Abs. 2 Bst. c DSG). Im KVG bildet insbesondere Artikel 84 die formellgesetzliche Grundlage für die Datenbearbeitung. Demnach dürfen die Versicherer Personendaten nur im Rahmen der ihnen nach dem KVG übertragenen Aufgaben bearbeiten (Art. 84 KVG, wobei die dortige Liste der Durchführungsaufgaben nicht abschliessend ist. Die Bearbeitungszwecke sind aber im KVG abschliessend geregelt).

- Der *Grundsatz der Bearbeitung nach Treu und Glauben* (Art. 4 Abs. 2 DSG) erfordert, dass die Datenbearbeitung für die betroffene Person *transparent* sein muss, d.h. dass eine Datenbeschaffung und jede weitere Datenbearbeitung für die betroffene Person *erkennbar* sein muss, die betroffene Person also aus den Umständen heraus damit rechnen musste oder sie entsprechend informiert bzw. aufgeklärt wird. Die betroffenen Personen sind über die Beschaffung und Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen zu informieren (Art. 14 DSG).

[1] Art. 3 DSG: Besonders schützenswerte Personendaten sind Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen.

[2] Art. 3 DSG: Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

- Das *Verhältnismässigkeitsprinzip* verlangt, dass nur diejenigen Personendaten beschafft und bearbeitet werden, welche *für einen bestimmten Zweck objektiv tatsächlich benötigt und geeignet* sind (Art. 4 Abs. 2 DSG). Daten dürfen nicht über den gesetzlich zugelassenen Umfang und die gesetzlich zulässige Dauer aufbewahrt werden.

- Personendaten dürfen *nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist* (Zweckbindungsgebot; Art. 4 Abs. 3 DSG). Die Personendaten dürfen nicht für andere als die ursprünglichen Zwecke bearbeitet werden.

- Wer Daten bearbeitet, hat sich zu vergewissern, dass diese richtig sind (Wahrheitsgebot; Art. 5 Abs. 1 DSG) und die von der Datenbearbeitung betroffenen Personen haben das *Recht, eine Berichtigung* von unrichtigen Daten zu verlangen (Art. 5 Abs. 2 DSG). Weiter haben diese das Recht, über *alle* diese Daten Auskunft zu verlangen (Art. 8 DSG). Die versicherte Person hat somit das Recht, eine Kopie des gesamten Dossiers des Versicherers – unter Vorbehalt der Dauer der Aufbewahrungspflicht des Versicherers zu erhalten.

- Die Krankenversicherer müssen *ein Verzeichnis sämtlicher Datensammlungen führen* und diese beim EDÖB *zur Registrierung anmelden* (Art. 11*a* DSG, Art. 16 VDSG). Sie sind von dieser Verpflichtung befreit, wenn sie eine für den *betrieblichen Datenschutz verantwortliche Person* bezeichnet haben, die *unabhängig* die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt, oder wenn sie aufgrund eines *Zertifizierungsverfahrens* nach Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben und das Ergebnis der Bewertung dem EDÖB mitgeteilt haben (Art. 11*a* Abs. 2 und 5 Bst. e und f DSG).

- Das Personal der KVG-Versicherer untersteht gemäss Artikel 33 ATSG der *Schweigepflicht*. Ein Verstoss gegen diese Norm stellt ein Vergehen dar und hat strafrechtliche Konsequenzen zur Folge (Art. 92 Bst. c KVG). Zudem ist der Zugriff der berechtigten Angestellten des KVG-Versicherers auf diejenigen Personendaten zu beschränken, welche diese zur Erfüllung ihrer klar umschriebenen Aufgaben benötigen (Art. 9 Abs. 1 Bst. g VDVG). Zusätzlich sind die *Vertrauensärztin oder der Vertrauensarzt und ihr/sein Hilfspersonal* an die Schweigepflicht gemäss Artikel 321 des Strafgesetzbuchs (StGB; SR 311.0) und somit an das *Patientengeheimnis* gebunden.

- Die *Weitergabe von Personendaten* an externe Stellen ist nur in einem *sehr beschränkten Rahmen* zulässig. Zu beachten sind dabei die Artikel 84*a* KVG (Datenbekanntgabe) in Abweichung von Artikel 33 ATSG (Schweigepflicht) und Artikel 82 KVG (besondere Amts- und Verwaltungshilfe) ebenfalls in Abweichung zu Artikel 33 ATSG, Artikel 120 KVV (Informationspflicht der Krankenversicherer über die Datenbekanntgabe und geleistete Amts- und Verwaltungshilfe), Art. 32 Abs. 2 ATSG (Amts- und Verwaltungshilfe) sowie Artikel 47 ATSG (Akteneinsicht). Artikel 84*a* KVG regelt, unter welchen abschliessenden Voraussetzungen die in dieser Bestimmung genannten Organe (und nur diese) in Abweichung von der Schweigepflicht (Art. 33 ATSG) Personendaten genau definierten Dritten offenbaren dürfen. Eine andere Versicherungsgesellschaft, die die Versicherungen nach dem Bundesgesetz vom 2. April 1908 über den Versicherungsvertrag (VVG; SR 221.229.1) anbietet, *ist eine Dritte* im Sinn von Art. 84*a* Abs. 5 KVG. Bietet der KVG-Versicherer selber solche Versicherungen nach VVG an, gelten die ob genannten Grundsätze, so insbesondere die Bearbeitung nach Treu und Glauben und das Zweckbindungsgebot. Dort, wo gleiche (automatisierte) Informationsflüsse für Personendaten aus der obligatorischen Krankenpflegeversicherung und den VVG-Versicherungen ein Datenmissbrauchspotential bergen, müssen *getrennte Bearbeitungswege* gewählt werden. Auch im Rahmen von Artikel 84*a* KVG sind, soweit das KVG keine Ausnahme vorsieht, die obgenannten Regeln des DSG zu beachten.

1.3 Ergebnisse der ersten Datenschutzerhebung (2007-2009)

Die erste flächendeckende Datenschutzerhebung des BAG mit dem EDÖB (4. Dezember 2007 - 16. Juni 2009) hat gezeigt, dass die Krankenversicherer für die Datenschutzproblematik sensibilisiert sind, und dass der Schutz der Daten trotz sehr unterschiedlicher Organisationsstrukturen über weite Strecken sichergestellt ist. Mit der Erhebung wurde aber auch festgestellt, dass in einigen sensiblen Bereichen noch Verbesserungspotential besteht. Mit der Veröffentlichung der Ergebnisse der Datenschutzerhebung am 16. Juni 2009 wurden sinngemäss folgende Empfehlungen abgegeben:

- BAG und EDÖB empfehlen den KVG-Versicherern, ein Datenschutzkonzept zu erarbeiten.
- Die KVG-Versicherer sind verpflichtet, ein Verzeichnis der Datensammlungen zu unterhalten. Für jede Datensammlung mit besonders schützenswerten Personendaten ist ein Bearbeitungsreglement zu unterhalten (insbesondere Beschreibung der Prozesse inkl. Verantwortlichkeiten, Berechtigungen, Datenfluss sowie der technischen Massnahmen zur Datensicherheit).
- BAG und EDÖB empfehlen den KVG-Versicherern, eine verantwortliche Person für den Datenschutz zu bezeichnen. Die Aufgaben dieses Verantwortlichen sind in einem Pflichtenheft zu umschreiben.
- Datenschutzverantwortliche müssen über die erforderlichen Fachkenntnisse verfügen.
- Es sollen von einer dafür spezialisierten Stelle regelmässig externe Datenschutzaudits durchgeführt und die Resultate den Aufsichtsbehörden unterbreitet werden.

Die Ergebnisse der ersten Datenschutzerhebung (Bericht und Zusammenfassung) sind unter folgenden Link veröffentlicht:

http://www.edoeb.admin.ch/themen/00794/01154/01236/01237/index.html?lang=de

2 Massnahmen des Bundesamtes für Gesundheit (BAG) seit der ersten Erhebung von 2007-2009

2.1 Kreisschreiben 7.1 vom 25. August 2011 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer (aktualisiert am 17. Juni 2013)

Obwohl das BAG festgestellt hat, dass die KVG-Versicherer im Anschluss an diese Empfehlungen verschiedene Massnahmen zur Verbesserung der Datenschutzkonformität ihrer Organisation und ihrer Prozesse eingeleitet haben, hat es am 25. August 2011 ein detailliertes Kreisschreiben an diese verschickt, um diese Entwicklung zu verstärken. Das am 1. September 2011 in Kraft getretene Kreisschreiben 7.1 schreibt den KVG-Versicherern nochmals vor, welche verschiedenen Vorkehrungen sie zum Schutz der Personendaten und namentlich der besonders schützenswerten Personendaten (insbesondere Gesundheitsdaten) der Versicherten treffen müssen. Allerdings enthielt damals das Kreisschreiben noch keine detaillierten Vorgaben, wie die KVG-Versicherer den Datenschutz und die Datensicherheit in Zusammenhang mit den Datenlieferungen der Leistungserbringer nach Einführung des Fallpauschalensystems SwissDRG sicherzustellen haben, weil die Regelung für die Übermittlung der abrechnungsrelevanten medizinischen Daten zu jenem Zeitpunkt noch offen war. Inzwischen wurde das Kreisschreiben 7.1 an diese neue Regelung (Art. 42 Abs. 3bis und 4 KVG, Art. 59ff KVV) angepasst und am 17. Juni 2013 den KVG-Versicherern zugestellt (Inkrafttreten am 1. Juli 2013).

Das Kreisschreiben 7.1 empfiehlt den KVG-Versicherern - sofern sie noch keines haben - ein umfassendes ganzheitliches Datenschutz- und Sicherheitskonzept zu erarbeiten, es schreibt ihnen vor, Bearbeitungsreglemente für jede Datensammlung ab dem 1. Januar 2012 dem EDÖB unaufgefordert zur Beurteilung vorzulegen, und wo nötig, die noch fehlenden Datensammlungen oder die für den betrieblichen Datenschutz verantwortlichen Personen ebenfalls beim EDÖB anzumelden. Es erinnert die KVG-Versicherer an die zu beachtenden Regeln bei der Auslagerung von Dienstleistungen und wid-

met ein ganzes Kapitel der Unabhängigkeit des vertrauensärztlichen Dienstes der KVG-Versicherer. In weiteren sieben (neu acht) Anhängen zum Kreisschreiben 7.1 werden technische Fragen zum Datenschutz beantwortet (Rechtsgrundlagen, massgebende Datenschutzbestimmungen, Inhalt des Pflichtenheftes eines/einer Datenschutzverantwortlichen und Hinweise für freiwillige Datenschutzmanagementsysteme und -zertifizierungen, Aufnahme- und Vollmachtsformulare [zur Entbindung von der Schweigepflicht bzw. vom Arztgeheimnis], neu im Anhang 8 Vorgaben zur zertifizierten Datenannahmestelle).

Gleichzeitig kündigte das BAG den KVG-Versichern an, sie einige Monate später gestützt auf das Kreisschreiben zu befragen, welche Vorkehrungen sie getroffen hätten und noch treffen würden. Wo nötig, würden entsprechende Korrekturen angeordnet und deren Umsetzung kontrolliert. Die Vorgaben des Kreisschreibens würden namentlich im Rahmen regelmässiger Kontrollen und Stichproben durch die Sektion Audit des BAG geprüft. Ausserdem wurden die KVG-Versicherer im Kreisschreiben unmissverständlich darauf hingewiesen, dass die Verletzung der Schweigepflicht (Art. 33 ATSG) durch deren Mitarbeitende als Vergehen und strafbares Verhalten geahndet würde (Art. 92 Bst. c KVG) und dass die Missachtung gesetzlicher Datenschutzvorschriften Sanktionen wie die Wiederherstellung des gesetzmässigen Zustandes auf Kosten des Versicherers, eine Verwarnung und Ordnungsbusse, einen Bewilligungsentzug und eine Veröffentlichung dieser Massnahmen nach sich ziehen könne (Art. 21 Abs. 5 und 5bis KVG).

Das Kreisschreiben 7.1 vom 25. August 2011 ist mit Begleitschreiben und den sieben Anhängen in der *Beilage 3* aufgeführt.
Das Kreisschreiben 7.1 vom 17. Juni 2013 ist mit Begleitschreiben und den acht Anhängen in der *Beilage 4* aufgeführt.

2.2 Zweite Datenschutzerhebung von 2011-2012 betreffend die datenschutzkonformen Organisation und Prozesse der KVG-Versicherer

Am 13. Dezember 2011 erhielten alle KVG-Versicherer einen umfangreichen Fragebogen für die Kontrolle der Umsetzung des Kreisschreibens 7.1 zu folgenden Punkten: Stand der Datenschutz- und Datensicherheitskonzepte, Stand der Datenbearbeitungsreglemente, aktuelle Verzeichnisse der Datensammlungen und deren Registrierung beim EDÖB, ausgelagerte Dienstleistungen und datenschutzkonforme Datenbearbeitung durch die Dienstleister, strukturelle Unabhängigkeit des Vertrauensärztlichen Dienstes, verantwortliche Stelle für den betrieblichen Datenschutz und Datenschutzschulungen im Betrieb, Datenschutzmanagementsysteme und -zertifizierungen, Case Management und Inhalt der Vollmachten und Einwilligungserklärungen der Versicherten für die Weitergabe medizinischer Angaben an Dritte. Weitere Fragen mit Bezug zum Postulat Heim 08.3493 betrafen den Datenaustausch zwischen den bei besonderen Versicherungsmodellen involvierten Stellen. Fragen zur Sicherstellung des Datenschutzes und der Datensicherheit in Zusammenhang mit den Datenlieferungen der Leistungserbringer nach Einführung des Fallpauschalensystems SwissDRG wurden von dieser zweiten Erhebung ausgeklammert, weil die Regelung für die Übermittlung der abrechnungsrelevanten medizinischen Daten zu jenem Zeitpunkt noch offen war.

Alle Versicherer, welche die obligatorische Krankenpflegeversicherung durchführen, beantworteten den Fragebogen innert der gesetzten bzw. verlängerten Frist. Auf Antrag wurden einzelne reine Taggeldkassen von dieser Aufgabe befreit. Für die Auswertung der eingegangenen Antworten wurden aber sämtliche KVG-Versicherer (67, wovon sechs Taggeldkassen) berücksichtigt.

Der Fragebogen ist mit dem Begleitschreiben vom 13. Dezember 2011 in der *Beilage 5* aufgeführt.

2.3 Prüfung vor Ort (Audit/Schwerpunkt 2012)

Im Rahmen seiner Aufsichtsfunktion führt das BAG gezielte Kontrollen und Stichproben am Standort der KVG-Versicherer durch. Ziel und Zweck dieser regelmässigen Audits ist die Überwachung des Vollzugs des KVG und dessen Verordnungen sowie der vom BAG erteilten Weisungen. Das Prüfprogramm beinhaltet je nach den beurteilten Risiken die Bereiche Organisation und Unternehmensführung, Versicherungsleistungen und regelmässig den Datenschutz sowie Dienstleistungen und Finanzen. Das Audit erfolgt durch prozess- und ergebnisorientierte Kontrollen.
Das BAG prüft bereits seit 2009 die Einhaltung der Datenschutzbestimmungen bei den Versicherern vor Ort. Seit 2012 stellt die Überprüfung des Datenschutzes eines der Schwerpunkthemen der Audits dar. Die Grundlage der Audit-Prüfung ist das vom BAG erstellte Kreisschreiben 7.1 vom 25. August 2011, in Kraft seit dem 1. September 2011 (aktualisiert am 17. Juni 2013 mit Inkrafttreten am 1. Juli 2013). Dabei wird ermittelt, ob der KVG-Versicherer über eine datenschutzkonforme Organisation verfügt und ob die Abwicklung des Datenschutzes bei der Bearbeitung und Aufbewahrung von Daten und Akten (insbesondere im vertrauensärztlichen Dienst) nach definierten Prozessen und entsprechend den gesetzlichen Bestimmungen nach ATSG, KVG sowie DSG erfolgt. Die Kontrolle vor Ort durch das BAG ersetzt in keiner Weise eine Zertifizierung nach Art. 11 DSG und stellt keine Grundlage zu dieser Zertifizierung dar.

Das BAG hat seit dem 1. Januar 2009 gestützt auf ihre 38 reguläre Audits 24 Weisungen zur datenschutzkonformen Organisation, zu den Datenbearbeitungsreglementen, zur Aufbewahrung (zahn)medizinischer und vertrauensärztlicher Dossiers, zur Aufbewahrung von diagnosebezogenen Daten, welche namentlich von DRG-Rechnungen stammen an kleine, mittlere und grosse Krankenversicherer erteilt. Am Häufigsten erfolgten die Weisungen in den drei zuletzt genannten Bereichen. Überdies erfolgten 25 Empfehlungen an die Krankenversicherer zur Erarbeitung eines Datenschutzkonzeptes und Datenbearbeitungsreglements, zur Anmeldung der Datensammlungen beim EDÖB, zur Meldung eines betrieblichen Datenschutzverantwortlichen an den EDÖB, zur Regelung der Zugriffsrechte auf Personal- und Leistungsdaten der Mitarbeitenden, zur Aufbewahrung vertrauensärztlicher Dossiers, zu kasseninternen Datenschutzkontrollmassnahmen, zur schriftlichen Regelung der Kompetenzen der Hilfspersonen des Vertrauensarztes und zur Einschränkung der Zugriffe im Case Management.
Die Weisungen stützen sich auf eine gesetzliche Grundlage und deren Umsetzung kann vom Versicherer verlangt werden. Dies im Gegensatz zu den Empfehlungen.

2.4 Prüfung der allgemeinen und speziellen Versicherungsbedingungen der KVG-Versicherer

Obwohl die allgemeinen und speziellen Versicherungsbedingungen der KVG-Versicherer der Genehmigung der Aufsichtsbehörde nicht bedürfen, prüft sie das BAG sporadisch. Wenn ein KVG-Versicherer neue Versicherungsbedingungen erlässt, legt er sie dem BAG vor. Eine gezielte Prüfung der allgemeinen und speziellen Versicherungsbedingungen der KVG-Versicherer ergab, dass v.a. die Erlasse für die besonderen Versicherungsformen (HMO- und Hausarztmodelle sowie Versicherungsmodell mit telemedizinischer Beratung) die wesentlichen, jedoch sehr allgemein formulierten Datenschutzgrundsätze und/oder einen Verweis auf die entsprechenden gesetzlichen Bestimmungen enthalten. Speziell geregelt ist z.B. der Zweck der Datenbearbeitung durch den KVG-Versicherer, das mit Einverständnis der versicherten Person mögliche Einsichtsrecht des koordinierenden Arztes bzw. der koordinierenden Ärztin in die für das besondere Versicherungsmodell notwendigen Diagnose-, Behandlungs- und Rechnungsdaten oder bei einem Arztwechsel, und die Weitergabe der notwendigen medizinischen Daten an den neuen koordinierenden Arzt bzw. die neue koordinierende Ärztin.

3. Ergebnisse der zweiten Datenschutzerhebung von 2011-2012

3.1 Datenschutz- und Datensicherheitskonzepte der KVG-Versicherer

Das Datenschutz- und Datensicherheitskonzept ist ein Instrument, mit dem die Versicherer die Grundsätze für die Beschaffung, Bearbeitung, Aufbewahrung, Bewirtschaftung und Bekanntgabe der Daten festlegen. Im Konzept sind unter anderem die Art und der Umfang der Daten definiert, die der Versicherer benötigt, um die ihm vom Gesetz übertragenen Aufgaben wahrzunehmen, der Zweck der Datenbearbeitung sowie die technischen und organisatorischen Massnahmen, die der Versicherer umsetzen muss, um die Einhaltung der Datenschutzvorschriften zu gewährleisten. Das Konzept gibt einen Rahmen vor für die Erarbeitung von Datenbearbeitungsreglementen (Art. 84b KVG; Art. 21 VDSG), Richtlinien zuhanden der Mitarbeitenden und der erforderlichen Massnahmen im Informatikbereich. Es dient als Grundlage, um die Aufgaben der mit dem Datenschutz beauftragten Personen, den Inhalt der Datensammlungen, die Rechte der Personen, deren Daten bearbeitet werden (versicherte Personen), und die Massnahmen zum Schutz unberechtigter Zugriffe auf die Personendaten festzulegen.

Als autonome juristische Einheiten sind die Versicherer für die Erarbeitung ihres Datenschutz- und Datensicherheitskonzepts zuständig. Darin definiert sind die rechtlichen Datenschutzgrundsätze, die der Versicherer einhalten muss. Das Datenschutz- und Datensicherheitskonzept ist zwar gesetzlich nicht vorgeschrieben, aber das BAG empfiehlt, ein solches zu erarbeiten (siehe Kreisschreiben 7.1 vom 25. August 2011, Seite 2, im *Anhang 3*).

Die durchgeführte Datenschutzerhebung (Frage 1.1) hat Folgendes ergeben:

- Mehr als die Hälfte der Versicherer (59%) haben ein Datenschutz- und Datensicherheitskonzept erarbeitet. Das sind gleich viele wie bei der ersten Erhebung 2007 - 2009.

- Es haben mehr grosse als kleine Versicherer ein solches Konzept erarbeitet: 48% der Versicherer mit bis zu 10'000 Versicherten (kleine Versicherer), 67% der Versicherer mit 10'001 bis 150'000 Versicherten (mittlere Versicherer) und 74% der Versicherer mit mehr als 150'000 Versicherten (grosse Versicherer) verfügen über ein Datenschutz- und Datensicherheitskonzept.

Die Mehrheit der Versicherer erarbeiteten dieses Konzept zwischen 2007 und 2011.

Da es sich v.a. um Datenschutz- und Datensicherheitskonzepte handelt, die für besondere Bereiche erstellt wurden (Frage 1.2), betreffen sie vor allem den Informatiksektor und die Tätigkeiten der Vertrauensärztin oder des Vertrauensarztes.

3.2 Datenbearbeitungsreglemente und Konzepte für Zugriffsberechtigungen

Artikel 21 VDSG schreibt den KVG-Versicherern vor, für automatisierte Datensammlungen, die besonders schützenswerte Daten und Persönlichkeitsprofile enthalten, oder mit anderen Datensammlungen verknüpft sind, ein Bearbeitungsreglement zu erstellen. Dieses Reglement beinhaltet Angaben über die interne Organisation des Krankenversicherers, sowie über die Struktur, in welcher die Datensammlung oder das automatisierte Bearbeitungssystem eingebettet ist. Es beschreibt die Datenbearbeitungs- und Kontrollprozeduren und enthält eine Auflistung aller Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung und der eingesetzten Informatikmittel. Es regelt namentlich Art und Umfang der Zugriffsberechtigung auf Personendaten. Das Reglement muss regelmässig angepasst bzw. nachgeführt werden und dem EDÖB in verständlicher Form jederzeit zur Verfügung stehen. Das Sicherstellen der Vollständigkeit und der Aktualität der Bearbeitungsreglemente ist eine Hauptaufgabe der/des Datenschutzbeauftragten des KVG-Versicherers und dient als eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung mit schützenswerten Personendaten.

Artikel 84*b* KVG wiederholt und verdeutlicht diese bereits gemäss VDSG bestehenden Verpflichtungen der KVG-Versicherer, präzisiert jedoch zusätzlich, dass ab dem 1. Januar 2012 die Bearbeitungsreglemente dem EDÖB unaufgefordert zur Beurteilung vorzulegen und zu veröffentlichen sind. Das Bearbeitungsreglement ist aber bereits gültig, wenn der Krankenversicherer es für verbindlich erklärt hat. Ein Bearbeitungsreglement kann für mehrere Datensammlungen gültig sein, wenn das Reglement tatsächlich für die bezeichneten Datensammlungen zur Anwendung gelangt und für jede betreffende Datensammlung die Erfordernisse von Artikel 21 Absatz 2 VDSG erfüllt.

Im Rahmen der zweiten Erhebung geben fast 2/3 der Versicherer (63%) an, für jede automatisierte Datensammlung, die besonders schützenswerte Daten oder Persönlichkeitsprofile enthält oder mit anderen Datensammlungen verknüpft ist, ein Bearbeitungsreglement gemäss Artikel 21 VDSG erstellt zu haben. Mit der Grösse der Versicherer steigt auch die Anzahl derjenigen unter ihnen, welche die geforderten Bearbeitungsreglemente erstellt haben (44% der kleinen Versicherer, 67% der mittleren Versicherer und 95% der grossen Versicherer). Dabei gibt die Mehrheit der Versicherer (66%) an, dies für alle Datensammlungen getan zu haben. Bei den grossen Versicherern sind es fast alle (95%) (Frage 2.1).

Gemäss der ersten Datenschutzerhebung 2007-2009 verfügten hingegen erst 26% der KVG-Versicherer über Bearbeitungsreglemente zu ihren schützenswerten Datensammlungen. Das BAG stellt daher eine positive Entwicklung in diesem Gebiet fest.

Gemäss ihren Angaben haben 73% der KVG-Versicherer ein Konzept für die Zugriffsberechtigungen ihrer Mitarbeitenden erstellt. Auch hier sind die grossen und mittleren Versicherer führend (90% der grossen Versicherer, 83% der mittleren Versicherer und 56% der kleinen Versicherer) (Frage 2.2).

Ein spezifisches Bearbeitungsreglement für die Datenbearbeitung durch den Vertrauensarzt und den vertrauensärztlichen Dienst haben erst 67% der KVG-Versicherer erstellt (28% haben eigene interne Bearbeitungsreglemente formuliert, für 39% der Versicherer gilt ein Bearbeitungsreglement des mit ihnen zusammenarbeitenden Verbandes der kleinen und mittleren Krankenversicherer RVK. Hier schneiden die kleinen und mittleren Versicherer dank ihrer engen Zusammenarbeit mit dem RVK besser ab (Frage 2.3).

Die Mehrheit der KVG-Versicherer (57%) kontrolliert die Bearbeitungsreglemente auf Aktualität und Vollständigkeit jährlich. Die Quote der kleinen (61%) und mittleren Versicherer (67%) ist dabei höher als diejenige der grossen Versicherer (55 %), weil ersteren auch hier die Zusammenarbeit mit dem RVK zugute kommt (Frage 2.4). Der EDÖB überprüft gegenwärtig die ihm zur Beurteilung vorgelegten Bearbeitungsreglemente.

Leider hat nur etwa ein gutes Drittel der KVG-Versicherer (36%) vor, die Bearbeitungsreglemente - wie in Art. 84*b* KVG vorgeschrieben - zu veröffentlichen. Die Versicherer können Geschäftsgeheimnisse von der Veröffentlichung der Unterlagen ausnehmen. Die bei einem knappen Drittel der KVG-Versicherer (28%) vorgesehene Bekanntgabe auf Anfrage entspricht nicht der gesetzlichen Vorgabe (Frage 2.5). Die Veröffentlichung der Bearbeitungsreglemente wird deshalb noch bei einem Grossteil der KVG-Versicherer (64%), auch der grossen Versicherer, gestützt auf Artikel 21 Absätze 2 und 5 KVG mittels Weisungen und allenfalls der Androhung von Sanktionen (Verwarnung und Ordnungsbusse) durchgesetzt werden müssen. Einige diesbezügliche Weisungen wurden bereits erlassen.

3.3 Register der Datensammlungen

Das DSG ermöglicht die Selbstregulierung der Unternehmen im Bereich Datenschutz: Es liegt in der Verantwortung des KVG-Versicherers, dafür zu sorgen, dass die Grundsätze und Vorgaben der Datenschutzgesetzgebung eingehalten werden. Der Krankenversicherer ist als Inhaber der Datensammlung von der Pflicht zur Anmeldung der Datensammlungen befreit, wenn er eine für den betrieblichen Datenschutz verantwortliche Person bezeichnet hat, die unabhängig die betriebsinterne Ein-

haltung der Datenschutzvorschriften überwacht sowie Verzeichnisse der Datensammlungen führt, und wenn der Versicherer diese Person dem EDÖB gemeldet hat (Art. 11a Abs. 5 Bst. e DSG). Dasselbe gilt, wenn er aufgrund eines erfolgreichen Zertifizierungsverfahrens gemäss Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben und das Ergebnis der Bewertung dem EDÖB mitgeteilt hat (Art. 11a Abs. 5 Bst. f DSG).

Erfreulicherweise führt die grosse Mehrheit der KVG-Versicherer (79%) ein Verzeichnis sämtlicher personenbezogenen Datensammlungen gemäss Artikel 11a DSG und Artikel 16 VDSG. Je grösser die Kasse, umso professioneller werden diese gehandhabt (95% der grossen Versicherer, 89% der mittleren Versicherer und 69% der kleinen Versicherer). Bei 6% der Kassen ist ein solches noch in Erarbeitung (Frage 3.1).

Ebenfalls positiv ist, dass mehr als 2/3 der KVG-Versicherer (71%) angeben, dieses Verzeichnis in den letzten drei Jahren zum letzten Mal aktualisiert zu haben (65% der kleinen Versicherer, 89% der mittleren Versicherer und 74% der grossen Versicherer) (Frage 3.2).

Mehr als 1/3 der KVG-Versicherer (36%) gibt an, sämtliche Datensammlungen beim EDÖB angemeldet zu haben. Fast alle (92% derjenigen), die dies nicht getan haben, haben aber einen betrieblichen Datenschutzverantwortlichen bezeichnet. Bei den mittleren und grossen Kassen haben dies alle Krankenversicherer getan, welche die Datensammlungen nicht beim EDÖB angemeldet haben (Frage 3.3).

3.4 Outsourcing

Outsourcing umfasst die Auslagerung von Dienstleistungen, die bisher von den Krankenversicherern selber erbracht wurden, sowie Dienstleistungen, welche die Krankenversicherer bisher selber nicht erbracht haben und die sie neu von einem Dienstleister beziehen.

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die *Daten nur so bearbeitet werden, wie es der Krankenversicherer selber tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht dies verbietet* (Art. 10*a* DSG). Artikel 84 KVG erlaubt den Krankenversicherern, Personendaten einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile durch Dritte bearbeiten zu lassen. Das Kreisschreiben 7.1 enthält zahlreiche Vorgaben an die KVG-Versicherer, welche beim Outsourcing zu beachten sind (vgl. Kreisschreiben 7.1, Ziff. 5 in der *Beilage 3).*

Die Versicherer machen häufig von der Auslagerung von Aufgaben Gebrauch. Nur vier gaben an, keine Aufgaben auszulagern. Mit der Aufgabenübertragung lassen sich die Ressourcen rationalisieren, was sich insbesondere auf die Verwaltungskosten der Krankenkasse positiv auswirkt. Zudem ist es für die kleinen und mittleren Versicherer interessant, den vertrauensärztlichen Dienst des RVK zu beauftragen, statt eigene Vertrauensärzte zu beschäftigen. Die Einsparungen bei den Verwaltungskosten wirken sich letztendlich ebenfalls auf die Prämien aus, was auch im Interesse der Versicherten liegt.

Aus der letzten Erhebung geht hervor, dass die von den Krankenkassen ausgelagerten Aufgaben folgenden Anteilen entsprechen (Frage 4.1):

- 46.3% der Versicherer (31) übertragen Aufgaben aus dem Informatikbereich
- 41.8% der Versicherer (28) übertragen Aufgaben an den RVK
- 28.4% der Versicherer (19) übertragen Aufgaben an santésuisse (SASIS) und an die Gemeinsame Einrichtung KVG
- 35.8% der Versicherer (24) übertragen Aufgaben an den Schadenservice Schweiz, SIZ AG und an Avus AG
- 31.3% der Versicherer (21) übertragen Aufgaben an Medgate
- 16.4% der Versicherer (11) übertragen Aufgaben an Inkassogesellschaften

- 55.2% der Versicherer (37) übertragen Aufgaben an verschiedene Organisationen
- 7.5% der Versicherer (5) übertragen Aufgaben an Dritte im Leistungsbereich

Je nach Grösse der Versicherer variiert der Anteil der an die verschiedenen Beauftragten ausgelagerten Aufgaben:

Beauftragte	Versicherer bis 10'000 Versicherte	Versicherer zwischen 10'001 und 15'000 Versicherten	Versicherer über 150'000 Versicherte
IT (Informatik-Firmen, unter anderem Centris, RR Donnelley, BBT Software, Secon AG, MediData, Bambus, AC Services, IT Surplus...)	30.4% (7 Versicherer)	61.1% (11 Versicherer)	65% (13 Versicherer)
RVK	69.6% (16 Versicherer)	55.6% (10 Versicherer)	10% (2 Versicherer)
santésuisse (SASIS) Gemeinsame Einrichtung	13% (3 Versicherer)	44.4% (8 Versicherer)	35% (7 Versicherer)
Schadenservice Schweiz, SIZ AG, Avus AG	26.1% (6 Versicherer)	44.4% (8 Versicherer)	40% (8 Versicherer)
Inkassogesellschaften	8.7% (2 Versicherer)	16.7% (3 Versicherer)	25% (5 Versicherer)
im Leistungsbereich beauftragte Dritte	4.3% (1 Versicherer)	11.1% (2 Versicherer)	10% (2 Versicherer)
Medgate	13% (3 Versicherer)	38.9% (7 Versicherer)	50% (10 Versicherer)
Verschiedene	30.4% (7 Versicherer)	61.1% (11 Versicherer)	85% (17 Versicherer)

24 Versicherer beauftragen ausländische Dienstleister in Europa, Nordafrika und den USA (Frage 4.2). Diese werden hauptsächlich mit folgenden Aufgaben betraut: Hilfe im Ausland, Abklärungen im Zusammenhang mit im Ausland erbrachten Leistungen, Forderungsinkasso, Versichertenkarte, Telefonumfragen zur Zufriedenheit der Versicherten.

Die Mehrheit der Versicherer überprüft mit folgenden Mitteln, dass die Datenbearbeitung durch beauftragte Dritte der Datenschutzgesetzgebung entspricht (Frage 4.4):

- Audits
- Zertifizierung der beauftragten Organisation
- Kontrolle durch den Datenschutzbeauftragten
- Zusammenarbeitsverträge
- Instruktionen der Mitarbeitenden der beauftragten Organisation
- Kontrolle vor Ort, durch Stichproben.

Aufgrund des Ausmasses der Auslagerungen der Dienstleistungen der Krankenversicherer auf externe und z.T. ausländische Dienstleister kann mittels Stichproben die Einhaltung der spezifischen Vorgaben gemäss Kreisschreiben 7.1, Ziff. 5 überprüft werden.

3.5 Vertrauensarzt und vertrauensärztlicher Dienst

Die Vertrauensärztin oder der Vertrauensarzt gemäss Artikel 57 KVG ist ein besonderes Organ der sozialen Krankenversicherung. Ihre/seine Aufgaben werden in Artikel 57 Absätze 4 und 5 KVG um-

schrieben. Danach berät sie/er den Versicherer in medizinischen Fachfragen sowie in Fragen der Vergütung und der Tarifanwendung. Zudem kommt ihr/ihm eine Überwachungs- und Kontrollfunktion zu. Sie/er überprüft die Voraussetzungen der Leistungspflicht des Versicherers (Art. 57 Abs. 4 KVG). Ihr/ihm obliegt die Kontrolle der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit der Behandlung im Sinn der Artikel 32 und 56 KVG. Ihre/Seine Kompetenz beschränkt sich auf die Beantwortung medizinischer Fachfragen. In fachlicher Hinsicht kann ihr/ihm der Versicherer nichts vorschreiben. In ihrem/seinem Urteil unabhängig, darf sie/er den zuständigen Stellen der Versicherer nur diejenigen Angaben weitergeben, die notwendig sind, um über die Leistungspflicht zu entscheiden, die Vergütung festzusetzen, den Risikoausgleich zu berechnen oder eine Verfügung zu begründen. Dabei wahrt sie/er die Persönlichkeitsrechte der Versicherten (Art. 57 Abs. 7 KVG). Der Leistungserbringer ist in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur der Vertrauensärztin oder dem Vertrauensarzt bekannt zu geben (Art. 42 Abs. 5 KVG).

Die gesetzlich vorgeschriebene Unabhängigkeit der Vertrauensärztin oder des Vertrauensarztes muss sich auch in der Organisation des vertrauensärztlichen Dienstes niederschlagen. Räumlich müssen Lokale des vertrauensärztlichen Dienstes genügend abgetrennt und abschliessbar sein. Die Post darf nur durch Stellen des vertrauensärztlichen Dienstes geöffnet werden und es muss jederzeit sichergestellt sein, dass besonders schützenswerte Personendaten den vertrauensärztlichen Dienst nicht verlassen können. Ein unabhängiges Telefon- und Telefaxnetz ist unabdingbar. Das Informatiksystem muss physisch so organisiert werden, dass die vom vertrauensärztlichen Dienst erstellten Dokumente nur auf eigenen Speichermedien archiviert werden, die wiederum nur den Mitarbeitenden des vertrauensärztlichen Dienstes zugänglich sind. Der Vertrauensärztin oder dem Vertrauensarzt muss zudem die Kompetenz zur Anstellung ihres/seines Hilfspersonals zukommen. Sie/er hat darauf zu achten, dass die Stellen der Hilfspersonen bezüglich ihrer fachlichen und organisatorischen Unterstellung sowie ihres Beschäftigungsgrades für den vertrauensärztlichen Dienst so konzipiert sind, dass sich daraus keine Interessenkonflikte für die Hilfspersonen ergeben. Die Hilfspersonen dürfen nicht mit verschiedenen Aufgaben betraut werden, die miteinander nicht kompatibel sind (z. B. für den vertrauensärztlichen Dienst und die Leistungsabteilung).

Gemäss der zweiten Erhebung verfügen fast die Hälfte der KVG-Versicherer (46%) über externe Vertrauensärzte bzw. einen ausgelagerten vertrauensärztlichen Dienst. In den meisten Fällen nimmt der RVK diese Aufgabe wahr. 77% der kleinen Versicherer und 47% der mittleren Versicherer lagern diese Aufgabe aus. Bei den grossen Versicherern sind es hingegen nur 12%. Die innerhalb der Versichererorganisation tätigen Vertrauensärzte sind unabhängig von der Kassengrösse organisationsmässig hauptsächlich der Direktion unterstellt oder in der Leistungsabteilung angesiedelt (Frage 5.1).

Bei knapp mehr als der Hälfte der Krankenversicherer (53%) arbeiten die Hilfspersonen des Vertrauensarztes nur für ihn. Bei den mittleren und grossen Versicherern ist dies bei 56% bzw. 60% von ihnen der Fall. Bei den anderen Versicherern nehmen die Hilfspersonen des Vertrauensarztes noch andere Aufgaben wahr (Frage 5.2).

Bei 77% der KVG-Versicherer (die ausgelagerten vertrauensärztlichen Dienste eingerechnet) bzw. 82% der kleinen Versicherer, 78% der mittleren Versicherer und 70% der grossen Versicherer, verfügen die Hilfspersonen des Vertrauensarztes über ein schriftliches Pflichtenheft. In 85 % der Fälle (94% der kleinen Versicherer, 72% der mittleren Versicherer, 86% der grossen Versicherer) entsprechen die eingereichten Pflichtenhefte den Erwartungen des BAG (Frage 5.3).

Die an den Vertrauensarzt gerichtete Brief- und elektronische Post gelangt bei praktisch allen Krankenversicherern (bei sämtlichen kleinen und mittleren Versicherern sowie bei 95% der grossen Versicherer) direkt an den Vertrauensarzt (Frage 5.4).

Bei über 90% der KVG-Versicherer aller Versichertenkategorien wird die Briefpost nur durch den Vertrauensarzt und/oder seinen Hilfspersonen geöffnet (Frage 5.5).

Bei 96% der kleinen Versicherer, 100% der mittleren Versicherer und 95% der grossen Versicherer haben nur der Vertrauensarzt und oder seine Hilfspersonen Zugriff auf die elektronische Post des Vertrauensarztes (Frage 5.6). Bei einem der übrigen Versicherer wird die Post vom Geschäftsführer geöffnet. Sechs der übrigen Versicherer haben die Frage nicht beantwortet.

Ausserdem geben 85% der KVG-Versicherer an, die für den Vertrauensarzt bestimmte Post, welche versehentlich von einer anderen kasseninternen Stelle geöffnet wird, unverzüglich dem Vertrauensarzt bzw. dem vertrauensärztlichen Dienst weiterzuleiten. Bei den grossen Versicherern ist dies ausnahmslos der Fall (bei mittleren Versicherern 95%, bei kleinen Versicherern 79%) (Frage 5.7).

Bei 96 % der kleinen Versicherer, 100% der mittleren Versicherer, und 95% der grossen Versicherer sind die Räumlichkeiten des Vertrauensarztes bzw. des vertrauensärztlichen Dienstes in Bezug auf den Datenschutz und die Datensicherheit so ausgestaltet, dass sie den DSG-Vorgaben entsprechen. Der von den kleinen und mittleren Kassen mehrheitlich beim RVK ausgelagerte vertrauensärztliche Dienst ist organisatorisch, räumlich und in Bezug auf die IT-Struktur autonom. Bei den anderen Versicherern hat der vertrauensärztliche Dienst eigene Räumlichkeiten bzw. der Zugang ist gesichert (Frage 5.8).

Die Ablage der besonders schützenswerten Daten beim vertrauensärztlichen Dienst entspricht bei 100% der kleinen und mittleren Versicherer und 95% der grossen Versicherer den DSG-Vorgaben. Die diesbezügliche Organisation fällt je nach Grösse des Krankenversicherers unterschiedlich aus. Die grossen Versicherer, beispielweise, haben einen vertrauensärztlichen Dienst eingerichtet, bei welchem die besonders schützenswerten Daten verwaltet und abgelegt sind (Papier- und/oder eingescannte Dokumente). Über die gleiche Organisation verfügt auch der vom RVK angebotene ausgelagerte vertrauensärztliche Dienst. Bei den Versicherern, welche über einen externen Vertrauensarzt und/oder über keinen vertrauensärztlichen Dienst als solchen verfügen, werden die besonders schützenswerten Daten entsprechend in geschlossenen Schränken aufbewahrt und/oder nach dem Einscannen vernichtet, oder beim externen Vertrauensarzt gelagert. Zugriff zu diesen Daten haben nur die Hilfspersonen des Vertrauensarztes, welche als solche vom Vertrauensarzt bezeichnet wurden (Frage 5.9).

Die Zugriffe zu den besonders schützenswerten Personendaten (Papier- und gescannte Dokumente) des vertrauensärztlichen Dienstes sind verschieden geregelt: Bei 30% der KVG-Versicherer hat nur der Vertrauensarzt Zugriff. Bei 26% der Versicherer sind es der Vertrauensarzt und seine Hilfspersonen, bei 5% der Versicherer sind es der Vertrauensarzt und Personen mit leitenden Funktionen, bei weiteren 5% sind es der Vertrauensarzt, seine Hilfspersonen und Personen mit leitenden Funktionen, bei weiteren 16% der Versicherer sind es der Vertrauensarzt, seine Hilfspersonen und der Rechtsdienst und bei 12% sind es der Vertrauensarzt, seine Hilfspersonen und weitere Personen (Frage 5.10). Die restlichen Versicherer (drei Taggeldkassen und eine sehr kleine Kasse) haben die Frage nicht beantwortet.

91% der kleinen Versicherer, 95% der mittleren Versicherer und 95% der grossen Versicherer geben an, die Umsetzung von Artikel 57 Absatz 7 KVG zu gewährleisten, indem der Vertrauensarzt und der vertrauensärztliche Dienst nur die für einen Entscheid unerlässlichen Angaben an die Kassenverwaltung weiterleiten. Allerdings geben nur 28% von ihnen (19% der kleinen Versicherer, 30% der mittleren Versicherer, 37% der grossen Versicherer) an, dies auch mittels Kontrollmassnahmen sicherzustellen (Frage 5.11).

3.6 Betriebliche/r Datenschutzverantwortliche/r

Wie bereits unter Ziff. 3.3 erwähnt, ist der KVG-Versicherer als Inhaber der Datensammlung von der Pflicht zur Anmeldung der Datensammlungen beim EDÖB befreit, wenn er eine für den betrieblichen Datenschutz verantwortliche Person bezeichnet hat, die unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht, Verzeichnisse der Datensammlungen führt und wenn der Versicherer diese Person dem EDÖB gemeldet hat.

Die für den betrieblichen Datenschutz verantwortliche Person ist entgegen der Bezeichnung nicht verantwortlich für den Datenschutz im Betrieb, sondern hat die Rolle einer Beraterin oder eines Beraters, bzw. einer Aufsichtsstelle (vgl. die französische Version im DSG: conseiller à la protection des données). Die Verantwortung für die Einhaltung der Bestimmungen zum Datenschutz bleibt in jedem Fall beim Inhaber der Datensammlung, also beim Krankenversicherer bzw. bei dessen leitendem Organ (Art. 16 Abs. 1 DSG).

Die oder der Datenschutzverantwortliche muss ihre/seine Funktion organisatorisch und fachlich unabhängig ausüben können, und ein möglicher Interessenkonflikt muss bereits durch ihre/seine organisatorische Stellung vermieden werden. Deshalb sollte ihre/seine Stelle ausserhalb der Linienverantwortlichkeit stehen. Empfohlen wird eine Stabstelle, eine Stelle in der Rechtsabteilung oder in der IT-Abteilung oder eine externe Stelle. Die Rolle und Funktion der für den Datenschutz verantwortlichen Person ist in einem Pflichtenheft zu definieren.

Aus der zweiten Erhebung geht hervor, dass mittlerweile 88% der KVG-Versicherer mindestens eine für den betrieblichen Datenschutz verantwortliche Person gemäss Artikel 11a Absatz 5 Buchstabe e DSG bezeichnet haben. Bei den grossen Versicherern sind es 95% (Frage 6.1). Anlässlich der ersten Erhebung von 2007-2009 verfügten erst 80% der KVG-Versicherer über eine/n Datenschutzverantwortliche/n. Das BAG stellt daher eine positive Entwicklung auf diesem Gebiet fest.

Diese Stelle ist in vielen Fällen der Direktion untergeordnet (40% der Versicherer) und in 19% der Fälle im Rechtsdienst (bei den grossen Versicherern sogar in 42%) untergebracht.

Lediglich 15% der KVG-Versicherer (33% der kleinen Versicherer, 19% der mittleren Versicherer und keine grossen Versicherer) haben eine externe Stelle mit dieser Aufgabe betraut, was gemäss Artikel 12a Absatz 2 VDSG ebenfalls zulässig ist. Die grossen Versicherer haben jedoch nur interne Mitarbeiter dafür bezeichnet (Frage 6.3).

Die kleinen und mittleren Versicherer setzen dafür mehrheitlich (62%) zwischen 0% und 100% Stellenprozente für diese Aufgabe ein, die grossen Versicherer setzen hingegen mehrheitlich (63%) zwischen 50% und mehr als 100% Stellenprozente dafür ein (Frage 6.4).

Dabei üben in 93% der Fälle die für den Datenschutz verantwortlichen Personen noch andere Aufgaben aus. Bei den grossen Versicherern ist dies immer der Fall. Es handelt sich dabei in vielen Fällen um Aufgaben des Direktions- oder IT-Bereichs (Frage 6.5).

69% der KVG-Versicherer (62% der kleinen Versicherer, 81% der mittleren Versicherer und 69% der grossen Versicherer) haben die für den Datenschutz verantwortlichen Personen dem EDÖB gemeldet (Frage 6.6).

In 75% der Fälle (57% der kleinen Versicherer, 88% der mittleren Versicherer, 84% der grossen Versicherer) verfügen die Datenschutzverantwortlichen über ein schriftliches Pflichtenheft. Bei über 90% der Krankenversicherer (100% der kleinen und grossen Versicherer, 79% der mittleren Versicherer) entspricht dessen Inhalt den Erwartungen des BAG. Bei weiteren 8% der Versicherer (19% der kleinen Versicherer, 0% der mittleren Versicherer, 5% der grossen Versicherer) ist ein solches Pflichtenheft noch in Erarbeitung (Frage 6.7).

Bei der ersten Erhebung von 2007-2009 verfügten erst 47% der Datenschutzverantwortlichen über ein schriftliches Pflichtenheft.

Bei 75% der KVG-Versicherer (67% der kleinen Versicherer, 75% der mittleren Versicherer, 79% der grossen Versicherer), welche einen Datenschutzverantwortlichen bezeichnet haben, haben diese Personen eine datenschutzspezifische Ausbildung absolviert (Frage 6.8). Zudem bilden sich bei 95% dieser Versicherer (bei 95% der kleinen Versicherer, 94% der mittleren Versicherer, 100% der grossen Versicherer) die Datenschutzverantwortlichen laufend weiter (Frage 6.9). Die Datenschutzver-

antwortlichen verfügen heute über mehr Qualifikationen als anlässlich der ersten Erhebung von 2007-2009.

Bei 80% der KVG-Versicherer (bei 67% der kleinen Versicherer, 81% der mittleren Versicherer, 90% der grossen Versicherer), welche einen Datenschutzverantwortlichen bezeichnet haben, führen diese Spezialisten Datenschutzschulungen für die Mitarbeitenden durch. Bei 37% der Versicherer (bei 52% der kleinen Versicherer, 33% der mittleren Versicherer, 30% der grossen Versicherer) ist die Teilnahme an den Schulungen für alle Mitarbeitenden des Unternehmens obligatorisch und bei 39% von ihnen (bei 18% der kleinen Versicherer, 45% der mittleren Versicherer, 65% der grossen Versicherer) sind die Schulungen lediglich für neue Mitarbeitende oder einzelne Bereiche z.B. für den Leistungsbereich vorgesehen (Frage 6.10).

3.7 Datenschutzmanagementsystem und Datenschutzzertifizierungen

Die Krankenversicherer können bezüglich der Bearbeitung von Personendaten ihre Datenschutzmanagementsysteme (DSMS) einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen (Art. 11 DSG).

Aus der durchgeführten Erhebung geht hervor, dass lediglich 10% aller KVG-Versicherer ihre Organisation als Ganzes haben zertifizieren lassen, davon die kleinen (9%) und die mittelgrossen (28%) KVG-Versicherer. Allerdings ist hervorzuheben, dass eine Zertifizierung nach Artikel 11 DSG nur bei zwei mittelgrossen KVG-Versicherern durchgeführt wurde. Bei den anderen Versicherern handelt es sich nicht um eine Zertifizierung nach Artikel 11 DSG.

Als Begründung für eine Nicht-Zertifizierung führen 20% aller KVG-Versicherer die Grösse der Kasse (Ressourcen) und/oder die Investitionskosten des Zertifikationsverfahrens (33% der kleinen Versicherer und 34% der mittleren Versicherer) an. Weiter prüfen 44% der KVG-Versicherer (48% der kleinen Versicherer, 33% der mittleren Versicherer und 8% der grossen Versicherer) die Durchführung einer Zertifizierung nach Artikel 11 DSG. Schliesslich teilen 20% der befragten KVG-Versicherer, vorwiegend grosse Versicherer, mit, dass sie sich im Bereich Datenschutz selbst organisiert haben (Frage 7.1).

Von den Versicherern, welche ihre Organisation als Ganzes nicht zertifizieren liessen, haben 11 KVG-Versicherer, davon acht grosse Versicherer, nur einen Teil ihrer Systeme und/oder Verfahren zertifizieren lassen. Gemäss den erhaltenen Angaben sind nur die IT-Abteilungen sowie der vertrauensärztliche Dienst zertifiziert. Die vertrauensärztlichen Dienste verfügen über eine Zertifikation nach Artikel 11 DSG und die IT-Abteilungen über eine IQNet-Zertifikation. Daraus resultiert, dass der vertrauensärztliche Dienst von fünf Versicherern (zwei mittelgrosse Versicherer und drei grosse Versicherer) nach Artikel 11 DSG zertifiziert wurde (Frage 7.2).

Erfreulicherweise kann mit der neuen Erhebung festgestellt werden, dass mehr als 3/4 der KVG-Versicherer (81%) die Einhaltung der Datenschutzbestimmungen innerhalb der Firma kontrollieren (74% der kleinen Versicherer, 94% der mittleren Versicherer und 90% der grossen Versicherer) (Frage 7.3). Sechs von neun Versicherern, welche nicht explizit angeben, die Einhaltung der Datenschutzbestimmungen innerhalb der Firma zu kontrollieren, haben jedoch einen Datenschutzbeauftragten bezeichnet, welcher diese Aufgabe abdecken dürfte.

Bei ca. 2/3 der KVG-Versicherer (63%), welche die Einhaltung der Datenschutzbestimmungen prüfen, werden die Prüfungen durch die interne oder externe Revision und/oder durch den internen Datenschutzverantwortlichen durchgeführt (52% der kleinen Versicherer, 67% der mittleren Versicherer und 85% der grossen Versicherer). Bei 18% der KVG-Versicherer, vorwiegend bei kleinen (22%) oder mittelgrossen (28%) Versicherern, werden diese Prüfungen durch die Direktion oder die Abteilungschefs durchgeführt. Grösstenteils erfolgt die Prüfung der Einhaltung der Datenschutzbestimmungen durch interne Audits. Weiter werden die Prüfungen durch Kontrollprogramme durchgeführt oder sind diese im internen Kontrollsystem (IKS) integriert. In 80% der Fälle finden diese Prüfungen jährlich

statt. Bei 5% der KVG-Versicherer wird diese Prüfung mit einem Intervall von zwei Jahren oder mehr vorgenommen (Frage 7.4).

Auftraggeber für die Prüfung der Einhaltung der Datenschutzbestimmungen ist bei 3/4 der KVG-Versicherer die Geschäftsführung, der Verwaltungsrat, bzw. Vorstand oder das Audit Komitee (70% der kleinen und mittleren Versicherer und 82% der grossen Versicherer). Bei knapp 1/4 der KVG-Versicherer liegt dies in den Kompetenzen des internen Datenschutzverantwortlichen. Grundsätzlich werden die Prüfungsergebnisse dem Auftraggeber schriftlich mitgeteilt (Frage 7.5).

Die bei der ersten Erhebung 2007-2009 festgestellten Ergebnisse, dass die klare Mehrheit der Krankenversicherer bereit waren, sich einem Datenschutz-Audit zu unterziehen oder sich einzelne Krankenversicherer einer Zertifizierung nach goodpriv@cy unterziehen wollen, haben sich somit mit der durchgeführten zweiten Erhebung bestätigt.

3.8 Datenaustausch bei der Durchführung besonderer Versicherungsformen (HMO- und Hausarztmodelle (Ärztenetzwerke/HAM) sowie Versicherungsmodell mit telemedizinischer Beratung)

Die Urheberin des Postulats befürchtet, dass mit den für die Rechnungs- und Wirtschaftlichkeitsprüfung von Spitalrechnungen verlangten ärztlichen Berichten die KVG-Versicherer Risikoprofile der betroffenen Versicherten anfertigen und diese Versicherten von (prämiengünstigen) besonderen Versicherungsmodellen der obligatorischen Krankenpflegeversicherung abhalten könnten. Das KVG sieht jedoch einen diskriminierungsfreien Zugang zu den besonderen Versicherungsformen der obligatorischen Krankenpflegeversicherung vor, und alle in der Schweiz wohnhaften Versicherten können ungeachtet ihres Alters und Gesundheitszustandes auf Beginn eines Kalenderjahres eine besondere Versicherungsform abschliessen, sofern ihr Krankenversicherer diese besondere Versicherungsform in ihrer Wohnregion anbietet. Dennoch wurde den im Postulat geäusserten Bedenken in der zweiten Erhebung des BAG Rechnung getragen.

So wurde bei denjenigen KVG-Versicherern, welche HMO- und Hausarztmodelle sowie Versicherungsmodelle mit telemedizinischer Beratung anbieten, untersucht, welche technischen und organisatorischen datensichernden Massnahmen sie für den Datenaustausch zwischen den involvierten Stellen (Gatekeeper/koordinierende Leistungserbringer, beauftragte Dritte [Dienstleister] und internen Kassenstellen inkl. vertrauensärztlicher Dienst) getroffen haben. Es stellte sich heraus, dass in 91% der Fälle die Informationskanäle mit Verschlüsselungsprotokollen gesichert und mit Passwörtern geschützt sind [Frage 8.1]).

Bestimmte Daten werden zwischen den involvierten Stellen ausgetauscht. Es handelt sich vor allem um administrative Daten, um Verstösse gegen die Bestimmungen in den Modellen der eingeschränkten Wahl der Leistungserbringer zu erkennen. Für die Prüfung der Überweisung des Gatekeepers werden die erfassten Leistungs- und Bestandesdaten, welche im IT-System der Versicherer registriert sind, berücksichtigt (Frage 8.2). Nachstehend wird für zwei Modelle grob aufgeführt, welche Daten zwischen den involvierten Stellen ausgetauscht werden:

Beim *Hausarztmodell* werden Versicherten-Bestände und deren Bruttoleistungskosten monatlich den HAM/HMO geliefert. Die HAM/HMO können die Datenentgegennahme/-Verarbeitung an eine externe Gesellschaft delegieren (z. B. Bluecare AG oder RVK). Jede Betriebsgesellschaft wird individuell beliefert, sodass sie nur die Daten ihrer angeschlossenen Ärztinnen und Ärzte erhält. Der Datenaustausch zwischen den involvierten Stellen findet über gesicherte Kanäle statt (z.B. SFTP-Verbindung [Secure File Transfer Protocol: ein verschlüsselter, Passwort geschützter Datentransfer] oder mit Benutzerzertifikat [bestätigt und sichert mit kryptographischen Verfahren Authentizität und Integrität von Identitäten und Objekten]). Bei den Leistungsdaten handelt es sich um Leistungspositionen, die nach SASIS-Datenpool-Leistungsarten gruppiert wurden. Es sind nur abrechnungsrelevante Angaben vorhanden (keine TARMED-Positionen oder Diagnose-Details). Nebst den Leistungs- und Bestandesda-

ten werden Ärztelisten, Überweisungsmeldungen und Rechnungskopien ausgetauscht. Diese Angaben sind erforderlich, um die Einhaltung der Bestimmungen in den Modellen der eingeschränkten Wahl der Leistungserbringer zu überprüfen.

Beim *Versicherungsmodell mit telemedizinischer Beratung*, wie z.B. Medi 24, erfolgt der Datenaustausch auf gesichertem Weg mittel Secure-E-Mail (entspricht einem Transfer via SFTP). Eine Gesamtstatistik z.B. hinsichtlich das gesamte Anrufvolumen, die Verteilung Männer/Frauen, die totale Nutzungsrate und den erreichten Service Level (keine personifizierten Daten) wird vom Versicherer geliefert. Zudem werden ebenfalls einzelne Anrufdaten (personifizierte Daten), wie z.B. Partner-Nr. der betreffenden Person, Datum, Uhrzeit, Dauer des Gesprächs, Anruf-Typ, wer hat angerufen (betroffene Person oder andere Person), Typ des Anliegens (Triage, Medinfo), Dringlichkeitsstufe der Triage, Call-ID geliefert. In diesem Modell werden keine medizinischen Daten ausgetauscht. Das heisst, die besprochenen medizinischen Anliegen zwischen der Patientin/dem Patienten und dem medizinischen Call Center sind für die Mitarbeitenden des Versicherers nicht ersichtlich. Dem Versicherer wird lediglich mitgeteilt, wer wann angerufen hat.
63% der KVG-Versicherer, welche HMO- und Hausarztmodelle sowie Versicherungsmodelle mit telemedizinischer Beratung anbieten, geben an, keinen Zugriff auf die Patientendossiers zu haben, in den übrigen Fällen sind die Zugriffe mit ganz wenigen Ausnahmen technisch beschränkt. Überdies sind die Zugriffe der Gatekeeper bzw. der koordinierenden Leistungserbringer auf die Patientendossiers in mehr als 3/4 der Fälle ebenfalls technisch beschränkt (Frage 8.3).

Zum Beispiel sind die Zugriffsberechtigungen bei den koordinierenden Leistungserbringern wie folgt beschränkt:

- Authentifizierung mittels FMH-HPC-Karte (hCardManager von H-Net) um sicherzustellen, dass der Hausarzt nur auf die Daten seiner Patienten Zugriff erhält.
- Abwicklung über gesicherte Plattformen, wie AVM-Infonet für den Datenaustausch mit Ärztenetzwerken
- Anbieter für Telemedizin-Beratung werden an das gesicherte HIN-Netzwerk angeschlossen (Health Info Net: stellt allen Partnern im Schweizer Gesundheitswesen eine gesicherte Plattform für den E-Mail-Verkehr und Anwendungen zur Verfügung).
- Gesundheitszentren, wie Santémed, verfügen über ein eigenes Softwareprogramm

Die Versicherer haben keinen Zugriff auf Patientendossiers (medizinische Daten).

An dieser Stelle sei auch folgender Fall erwähnt: Im Jahre 2010 hat das BAG aufgrund einer Anzeige bei der Vertragsauflösung eines grossen Versicherers mit koordinierenden Leistungserbringern kontrolliert, wie die betroffenen Versicherten in die ordentliche Grundversicherung und in ein anderes Hausarztmodell umgeteilt worden sind. Eine Risikoselektion konnte bei der Triage nicht nachgewiesen werden. Vielmehr erfolgten die Einteilungsvorschläge nach dem Zufallsprinzip und die Hochkostenfälle, das Durchschnittsalter und die durchschnittlichen Leistungskosten der Versicherten in beiden Gruppen erlaubten keine Hinweise auf eine Risikoselektion.

3.9 Case Management

Das Case Management ist im KVG nicht explizit geregelt. 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. Das BAG lässt das Case Management bei den KVG-Versicherern zu. Es verlangt jedoch von ihnen, dass sie die Datenschutzgrundsätze der Zweckbindung und Transparenz besonders gewissenhaft beachten.

Aufgrund der zweiten Erhebung ergibt sich, dass 60% der Krankenversicherer ein Case Management betreiben. Bei den grossen Versicherern sind es 75%. Bei den KVG-Versicherern, welche über ein Case Management verfügen, befindet sich dieses bei 55% in der Leistungsabteilung, in 45% der Fälle haben sie es ausgelagert. Bei den grossen Versicherern ist das Case Management immer in der Leistungsabteilung untergebracht (Frage 9.1).

Alle 40 KVG-Versicherer, welche über ein Case Management verfügen, konnten – anders als dies noch anlässlich der ersten Erhebung 2007-2009 der Fall war – den Prozessablauf eines Case Managements verständlich beschreiben. Fast alle haben die dafür nötige Einwilligungserklärung (der versicherten Person) zugestellt. In gut 2/3 der Fälle ist diese Einwilligungserklärung aus Sicht des BAG korrekt, in 20% entspricht sie nur teilweise den Anforderungen, z. B. fehlt die Rückzugsklausel. In 7% der Fälle handelt es sich um eine ungültige Generalvollmacht (Frage 9.2).

Überall wo jetzt ein Case Management besteht, sind die Zugriffe eingeschränkt. In den meisten Fällen haben nur der Case Manager, seine Stellvertretung sowie der Vertrauensarzt bzw. die Vertrauensärztin und seine/ihre Hilfspersonen Zugriff auf das Patientendossier (Frage 9.3).

3.10 Vollmachten und Einwilligungserklärungen

Gemäss Artikel 33 ATSG haben die Versicherer gegenüber Dritten Verschwiegenheit zu bewahren. In Artikel 84a KVG sind die Bedingungen, unter welchen die Versichertendaten bekannt gegeben werden dürfen, abschliessend aufgelistet. Artikel 84a Absatz 5 Buchstabe b KVG sieht insbesondere vor, dass Versichertendaten an Dritte nur bekannt gegeben werden dürfen, sofern die betroffene Person im Einzelfall schriftlich eingewilligt hat. Die Bearbeitung von Daten der versicherten Person ist also nur mit deren freien und aufgeklärten Einwilligung zulässig. Die Einwilligung ist aufgeklärt, wenn die Person zum Zeitpunkt der Einwilligung angemessen informiert worden ist, das heisst, wenn sie in der Lage ist, die Tragweite ihrer Einwilligung abzuschätzen, bzw. wenn sie erkennen kann, welche Daten weitergegeben werden können, welcher Personenkreis diese Informationen weitergeben darf und/oder welchem Personenkreis diese Informationen weitergegeben werden dürfen und was der Zweck der Datenweitergabe ist. Gesundheitsbezogene Daten sind besonders schützenswerte Personendaten im Sinne von Artikel 3 Buchstabe c Ziffer 2 DSG. Ihre Bearbeitung erfordert folglich die ausdrückliche Einwilligung der versicherten Person (Art. 4 Abs. 5 DSG).

Einige Krankenversicherer haben in ihrem Beitrittsformular eine Klausel eingefügt, mit der die zu versichernde Person den KVG-Versicherer ermächtigt, Daten bekannt zu geben und Informationen bei anderen Personen einzuholen. Das BAG überprüft regelmässig die Beitrittsformulare der Versicherer und verlangt von ihnen, dass sie die Fragen und Klauseln, die nicht den gesetzlichen Bestimmungen entsprechen, korrigieren. Die versicherte Person wird manchmal auch aufgefordert, eine Vollmacht zugunsten des Versicherers im Fall von Leistungsfällen zu unterzeichnen. Der Versicherer muss tatsächlich Informationen von Dritten einholen können (z.B. von Leistungserbringern), damit er seine Leistungspflicht überprüfen kann. Gestützt auf Artikel 28 Absatz 3 ATSG muss sich die Vollmacht immer auf einen bestimmten Leistungsfall beziehen. Eine für zukünftige Leistungsfälle ausgestellte Vollmacht ist nicht gültig.

Die durchgeführte Erhebung hat gezeigt, dass die Vollmachtsklauseln in den KVG-Beitrittsformularen und meistens auch jene im Zusammenhang mit Leistungsfällen den Datenschutzbestimmungen entsprechen. Das Gleiche gilt für die Einwilligungsklauseln des RVK für das Case Management.

Die Situation ist komplexer, wenn es um die Einwilligungsklausen auf den Fragebogen für die Zusatzversicherungen geht. Die Versicherer, welche Zusatzversicherungen durchführen, unterstehen dem VVG und damit der Aufsicht der Eidg. Finanzmarktaufsicht (FINMA). Nach Auffassung des BAG fällt die Prüfung dieser Fragebogen somit in den Zuständigkeitsbereich der FINMA. Doch die in einzelnen Fragebogen enthaltene Einwilligungsklausel betrifft auch das KVG, weil sie vorsieht, dass der Versi-

cherungsnehmer/die Versicherungsnehmerin den KVG-Versicherer ermächtigt, dem VVG-Versicherer Informationen über seinen/ihren Gesundheitszustand bekannt zu geben. Teilweise wird in dieser Klausel darauf hingewiesen, dass die Weitergabe der Daten dazu dient, den Versicherungsantrag und die künftigen Leistungsfälle zu beurteilen. Andere Klauseln enthalten keine Angaben zum Zweck der Datenbeschaffung. Wie oben ausgeführt, müssen die Versicherungsnehmer vollständig und transparent informiert werden, bevor sie ihre aufgeklärte Einwilligung geben. Es liegt die Vermutung nahe, dass die Versicherungsnehmer ausgehend vom Text der meisten Einwilligungsklauseln häufig nicht in der Lage sind, die Tragweite ihrer Einwilligung abzuschätzen, bzw. zu erkennen, welche Daten weitergegeben werden können und was der Zweck der Datenweitergabe ist. Eine Pauschalermächtigung für künftige Leistungsfälle verstösst auch gegen Artikel 28 Absatz 3 ATSG.

Da es keine Kompetenzen gegenüber den VVG-Versicherern hat, ist das BAG mit der FINMA zusammengetroffen, um diese Frage zu diskutieren. Die beiden Behörden bemühen sich Lösungen zu finden, die die Regeln sowohl der sozialen Krankenversicherung als auch der Privatversicherungen erfüllen.

4. Datenübermittlung der Spitäler an die KVG-Versicherer im Falle eines Vergütungsmodells vom Typus DRG

Am 23. Dezember 2011 hat das Parlament gestützt auf die parlamentarische Initiative 11.429 Tarmed. Subsidiäre Kompetenz des Bundesrates (BBl 2012 55) einen neuen Artikel 42 Absatz 3bis im KVG verabschiedet. Dieser Absatz sieht vor, dass die Leistungserbringer auf der Rechnung die Diagnosen und Prozeduren nach den aktuellen Klassifikationen kodiert aufführen.

Anschliessend hat der Bundesrat am 4. Juli 2012 die Modalitäten der Datenweitergabe festgelegt (Art. 59a KVV), damit das Verhältnismässigkeitsprinzip gewahrt wird. Spätestens ab 2014 sollen die Spitäler die administrativen und medizinischen Angaben bei der Rechnungsstellung systematisch an eine vom KVG-Versicherer eingerichtete zertifizierte Datenannahmestelle übermitteln. Die Versicherer haben nun bis Ende 2013 Zeit, eine Datenannahmestelle einzurichten und diese gemäss Artikel 11 DSG zertifizieren zu lassen.

Die Zertifizierung wird vom EDÖB überwacht, der die Liste der zertifizierten Datenannahmestellen veröffentlicht. In der Übergangszeit können die medizinischen Angaben einzig zuhanden des Vertrauensarztes systematisch übermittelt werden.

Überdies hat das EDI am 20. November 2012 die gesamtschweizerisch einheitliche Struktur der Datensätze in Form einer Verordnung (Verordnung des EDI über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern) festgelegt. Damit sind die Datensätze mit den administrativen und medizinischen Angaben schweizweit einheitlich definiert. Damit ist auch die Frage der Datenübermittlung – im Rahmen der Rechnungsstellung – zwischen KVG-Versicherern und Spitälern definitiv geregelt.

Die entsprechenden Änderungen des KVG (Art. 42 Abs. 3bis und 4) und der KVV (Art. 59ff) sowie die EDI-Verordnung sind per 1. Januar 2013 in Kraft getreten.

Das BAG und der EDÖB begleiten die Umsetzung dieser Bestimmungen durch die KVG-Versicherer.

5. Fazit

Dieser Bericht stellt eine gute „Auslegeordnung“ dar und informiert umfassend über die aktuelle Situation des Schutzes der Patientendaten bei den Krankenversicherern. Der Bundesrat stellt aufgrund der bisherigen Erhebungen und Kontrollmassnahmen der Aufsichtsbehörden BAG und EDÖB fest, dass die KVG-Versicherer in vielen Bereichen die nötigen Vorkehrungen für eine Sicherstellung des Datenschutzes und der Datensicherheit getroffen haben.

Die Ergebnisse der zweiten Erhebung belegen, dass die KVG-Versicherer frühere Mängel mehrheitlich behoben haben und professioneller mit dem Datenschutz umgehen als noch vor wenigen Jahren. Im Hinblick auf die Durchführung von besonderen Versicherungsmodellen wurden keine konkreten Hinweise für eine zweckfremde Bearbeitung medizinischer Daten gefunden. Zahlreiche Punkte haben sich im Vergleich zur ersten Datenschutzerhebung des BAG/EDÖB (2007-2009) verbessert, andere bleiben aber nach wie vor nicht ganz erfüllt.

Das BAG wird im Rahmen seiner Aufsichtstätigkeit dafür sorgen, dass die noch vorhandenen Mängel korrigiert werden und auch bei seiner künftigen Tätigkeit weiterhin auf eine sorgsame Umsetzung der datenschutzrechtlichen Vorgaben achten. Überdies soll in den nächsten drei bis fünf Jahren ein weiterer Bericht erarbeitet und dem Bundesrat sowie dem Parlament zur Kenntnis gebracht werden.

Aufgrund der verschiedenen Organisationsformen der Versicherer, namentlich der Integrierung des Datenschutzes und der Datensicherheit in den Arbeitsabläufen der Versicherer, können keine allgemeinen Aussagen zu den generierten Kosten des Datenschutzes und der Datensicherheit gemacht werden. Aus den bisherigen Erhebungen geht aber hervor, dass der Datenschutz und die Datensicherheit die Verwaltungskosten nicht in einem hohen Mass beeinflussen.

Die Aufsichtsbehörden BAG und EDÖB verfügen über eine Palette von Instrumenten, um bei Bedarf datenschutzspezifische Korrekturmassnahmen von den KVG-Versicherern zu fordern. Bei Verdacht bzw. Feststellung einer konkreten Datenschutzverletzung in der Praxis oder bei der Entdeckung einer nicht datenschutzkonformen Bestimmung in einem Kassenerlass haben die bisherigen Interventionen des BAG bei KVG-Versicherern zur Folge gehabt, dass der rechtswidrige Zustand behoben wurde.

Gewisse Verbesserungen für den Schutz der Patientendaten müssen auf Gesetzesstufe angegangen werden. Folgende Reformvorlagen des Bundesrates stellen Verbesserungen für den Schutz von Patientendaten in Aussicht:

1. Die bundesrätliche Botschaft zur KVG-Änderung „Risikoausgleich. Trennung von Grund- und Zusatzversicherung“ vom 20. September 2013 (BBl 2013 7953) sieht die institutionelle Trennung von sozialer Krankenversicherung und Zusatzversicherung vor (Art. 12 Abs. 2 E-KVG). Versicherergruppen, die eine Gesellschaft führen, welche die soziale Krankenversicherung betreibt, haben mittels Informationsbarrieren sicherzustellen, dass zwischen den KVG-Versicherern und den übrigen Gesellschaften der Gruppe kein Austausch der Versichertendaten stattfindet (Art. 13 Abs. 2 Bst. g E-KVG). So müssen die Versicherer über getrennte Datenbanken für die Leistungsabrechnungen der Grund- und Zusatzversicherung verfügen. Zudem darf der Vertrauensarzt, der über Leistungen der obligatorischen Krankenpflegeversicherung befindet, nicht derselbe sein wie für die Zusatzversicherungen. Damit soll der Datenschutz verbessert sowie verhindert werden, dass Personendaten des einen Versicherungsbereichs für den anderen verwendet werden, um Risikoselektion zu betreiben (vgl. Botschaft Ziff. 1.2.2 und 5.6).

2. Der Entwurf zum Krankenversicherungsaufsichtsgesetz (E-KVAG; BBl 2012 1941) sieht vor, dass die Krankenkassen ein wirksames internes Kontrollsystem zur Überwachung der Geschäftstätigkeit einrichten, das der Grösse und der Komplexität des Unternehmens angepasst ist (Art. 22 Abs. 1 E-KVAG). Im Bereich des Datenschutzes muss das interne Kontrollorgan die Gesetzeskonformität der Prozesse beurteilen und Berichte erstellen. Mit dem KVAG wird somit innerhalb der Krankenkassen der Datenschutz verstärkt. Insbesondere bei den Versicherungsgruppen ist die Gesetzmässigkeit der

Datenweitergabe fraglich. In diesem Bereich wird der Datenschutz mit dem KVAG wesentlich verbessert, indem die Gesetzesvorlage den Bundesrat ermächtigt, Vorschriften zum internen Kontrollsystem zu erlassen (Art. 44 Abs. 2 E-KVAG).

Der Bundesrat beantragt aufgrund dieser Feststellungen, das Postulat Heim Po 08.3493 "Schutz der Patientendaten und Schutz der Versicherten" abzuschreiben.

6. Beilagenverzeichnis

Beilage 1

Wortlaut Postulat Heim Po 08.3493 Schutz der Patientendaten und Schutz der Versicherten, Begründung und Stellungnahme Bundesrat

Beilage 2

Parlamentarische Vorstösse zum Schutz der Patientendaten (2008-2012)

Beilage 3

Kreisschreiben BAG 7.1 vom 25. August 2011 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer mit Begleitschreiben und sieben Anhängen

Beilage 4

Kreisschreiben BAG 7.1 vom 17. Juni 2013 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer mit Begleitschreiben und acht Anhängen

Beilage 5

Fragen zu datenschutzkonforme Organisation und Prozesse der KVG-Versicherer mit Begleitschreiben vom 13. Dezember 2011

Schutz der Patientendaten und Schutz der Versicherten

Bericht des Bundesrates in Erfüllung des Postulates Heim (08.3493)

vom 18. Dezember 2013

Beilagenverzeichnis

Beilage 1

Wortlaut Postulat Heim Po 08.3493 Schutz der Patientendaten und Schutz der Versicherten, Begründung und Stellungnahme Bundesrat

Beilage 2

Parlamentarische Vorstösse zum Schutz der Patientendaten (2008-2012)

Beilage 3

Kreisschreiben BAG 7.1 vom 25. August 2011 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer mit Begleitschreiben und sieben Anhängen

Beilage 4

Kreisschreiben BAG 7.1 vom 17. Juni 2013 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer mit Begleitschreiben und acht Anhängen

Beilage 5

Fragen zu datenschutzkonforme Organisation und Prozesse der KVG-Versicherer mit Begleitschreiben vom 13. Dezember 2011

Beilage 1

Curia Vista - Geschäftsdatenbank

08.3493 – Postulat

Schutz der Patientendaten und Schutz der Versicherten

Eingereicht von	 Heim Bea
Einreichungsdatum	18.09.2008
Eingereicht im	Nationalrat
Stand der Beratung	Überwiesen

Eingereichter Text

Der Bundesrat wird beauftragt aufzuzeigen, welche Massnahmen gegen die Diskriminierung einzelner Patientengruppen durch die neuen OKP-Versicherungsmodelle und zum Schutz der Patientendaten bei den Versicherern geplant sind.

Begründung

Ein Rechtsgutachten von H+ und eine wissenschaftliche Untersuchung (Master-Arbeit Y. Prieur) bestätigen die Kritik des kantonalzürcherischen Datenschutzbeauftragten: Versicherer verlangten von den Spitälern für die Rechnungsüberprüfung immer öfter vollständige Austritts- und Operationsberichte der Versicherten. Die Versicherer verletzen damit das KVG sowie das Patientengeheimnis. Die Patientenorganisationen DVSP und SPO beurteilen diese Praxis als illegal. Dadurch entsteht ein wachsendes Potenzial für Diskriminierungen - gerade mit Blick auf die neuen Versicherungsmodelle in der OKP: Anhand der so erworbenen Patientendaten können Versicherer Risikoprofile erstellen. Gesundheitlich Beeinträchtigte können gezielt von bestimmten Versicherungsmodellen und von Prämienrabatten ausgeschlossen werden. Dies führt zu einer schleichenden Entsolidarisierung auch in der sozialen Grundversicherung - was dem Volks-Ja zum KVG widerspricht. Die neuen Versicherungsmodelle mit Rabatten können zudem zu Prämienerhöhungen in der Grundversicherung führen. In der Antwort auf die Interpellation 06.3040 wie auch in der Antwort auf die Motion 07.3114 stellt der Bundesrat fest, dass Versicherer den Daten- und Persönlichkeitsschutz unzureichend gewährleisten. Angesichts der Gefährdung des Patientengeheimnisses und des Datenschutzes ist es unverständlich, dass die Aufsichtsbehörden ihre Möglichkeiten für konkrete Massnahmen nicht ausschöpfen.

Der Bundesrat ist gebeten aufzuzeigen, wie er sicherstellt, dass die neuen OKP-Versicherungsmodelle keine einzelnen Patientengruppen diskriminieren.

Das revidierte DSG sieht eine Zertifizierung der Systeme und Verfahren zum Schutz der Patientendaten vor. Es soll geprüft werden, wieweit die Versicherer der freiwilligen Zertifizierung nachgekommen sind. Weiter ist Transparenz zu schaffen über die Weiterverwendung und Aufbewahrungsdauer der Gesundheitsdaten, die im Rahmen der Rechnungsüberprüfung eingefordert werden. Es sei auch die Frage gestellt, wie die Unabhängigkeit von Vertrauensärztinnen und -ärzten, die oft gleichzeitig als Gesellschaftsärzte tätig sind, gewährleistet werden kann.

Stellungnahme des Bundesrates vom 26.11.2008

Der Bundesrat ist in Kenntnis darüber, dass bei einzelnen Krankenversicherern Handlungsbedarf bezüglich der Datenschutzsituation besteht. Daher beauftragte er das Bundesamt für Gesundheit (BAG) als Aufsichtsorgan, diesbezügliche Abklärungen vorzunehmen und entsprechende Massnahmen zu ergreifen. Eine Arbeitsgruppe mit Vertretern des BAG und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

untersuchte mittels einer flächendeckenden Erhebung die gesamten Datenbearbeitungsvorgänge der Versicherer.

Angesichts der Resultate dieser Erhebung und der Bedeutung dieses Themas für breite Fach- und Bevölkerungskreise ist der Bundesrat bereit, innerhalb der nächsten zwei Jahre über die bereits getroffenen und zusätzlich zu treffenden Massnahmen zum Schutze der Patientendaten der Versicherten zu berichten.

Die im Postulat geäusserten Bedenken zur Erstellung von Risikoprofilen, welche den Abschluss von besonderen Versicherungsformen beeinflussen könnten, wird die Arbeitsgruppe bei ihren Arbeiten berücksichtigen. Das Bundesgesetz über die Krankenversicherung sieht aber schon heute einen diskriminierungsfreien Zugang zu den besonderen Versicherungsformen der obligatorischen Krankenpflegeversicherung vor. Alle in der Schweiz wohnhaften Versicherten können nämlich ungeachtet ihres Alters und Gesundheitszustandes auf Beginn eines Kalenderjahres eine besondere Versicherungsform abschliessen, sofern ihr Krankenversicherer diese in ihrer Wohnregion anbietet.

Antrag des Bundesrates vom 26.11.2008
Der Bundesrat beantragt die Annahme des Postulates.

Dokumente

Amtliches Bulletin - die Wortprotokolle

Chronologie / Wortprotokolle

Datum	Rat	
19.12.2008	NR	Annahme.

Erstbehandelnder Rat
Nationalrat

Mitunterzeichnende (28)
Allemann Evi Aubert Josiane Bruderer Wyss Pascale Carobbio Guscetti Marina Daguet André Fehr Hans-Jürg Fehr Jacqueline Graf-Litscher Edith Gross Andreas Jositsch Daniel Kiener Nellen Margret Lumengo Ricardo Marra Ada Nordmann Roger Nussbaumer Eric Pedrina Fabio Rielle Jean-Charles Rossini Stéphane Schenker Silvia Sommaruga Carlo Steiert Jean-François Stöckli Hans Stump Doris Thanei Anita Tschümperlin Andy Voruz Eric Widmer Hans Wyss Ursula

Deskriptoren: Hilfe

Patient/in Krankenkasse Datenschutz Versicherungsaufsicht Personendaten medizinische Diagnose Kampf gegen die Diskriminierung

Ergänzende Erschliessung:
2841

Zuständig

Departement des Innern
(EDI)

Beilage 2

Parlamentarische Vorstösse zum Datenschutz

09.5060 Frage Schenker vom 9. März 2009 "Datentransfer zwischen Spitälern und Krankenkassen"

Die Fragestellerin erkundigt sich, ob auf Bundesebene eine Rechtsgrundlage besteht, die den Austausch der Daten der Versicherten zwischen den Spitälern und den Krankenkassen gestattet.

Antwort des Bundesrates vom 9. März 2009

Der Bundesrat anerkennt, dass in Bezug auf die Datenschutzsituation bei einigen Versicherern Handlungsbedarf besteht. Daher wurden das BAG und der EDÖB beauftragt, mittels einer gesamtschweizerischen Erhebung alle Abläufe im Zusammenhang mit der Datenbearbeitung durch die Versicherer zu untersuchen. In Bezug auf die Schweigepflicht und den Datenschutz unterstehen die von den Krankenversicherern beauftragten Personen den gleichen Regeln wie diese selbst.

09.1025 Frage Heim vom 18. März 2009 "Schutz der Gesundheitsdaten"

Die Fragestellerin erkundigt sich, ob der Datenschutz im Rahmen des Umgangs der Privatversicherungen mit den Gesundheitsdaten ausreichend gewährleistet ist. In ihren allgemeinen Geschäftsbedingungen verlangen die Privatversicherer quasi vollen Zugang zu den Gesundheitsdaten. Mit dem Abschluss des Vertrags gestattet die versicherte Person dem Versicherer, die notwendigen Daten zu bearbeiten und sie zu Bearbeitungszwecken an Mitversicherer oder Dritte zu übermitteln. Zudem kann der Versicherer bei medizinischen Leistungserbringern (Ärzten, Psychologen, Labors, Spitälern), bei Sozial- (AHV, IV, UVG, KVG) sowie Privatversicherern, Amtsstellen, Arbeitgebern und Dritten alle sachdienlichen Informationen einholen. Der Versicherer kann Einblick in die Akten seiner Versicherten nehmen und ist von seiner Geheimhaltungspflicht entbunden.

Antwort des Bundesrates vom 20. Mai 2009

Im Bereich der Privatversicherungen enthalten weder das Versicherungsvertragsgesetz (VVG; SR 221.229.1) noch das Versicherungsaufsichtsgesetz (VAG; SR 961.01) spezifische datenschutzrechtliche Vorschriften. Somit sind die Grundsätze des DSG anwendbar (Verhältnismässigkeit, Zweckmässigkeit und Transparenz). Da es sich bei den Gesundheitsdaten um besonders schützenswerte Personendaten handelt, für deren Bearbeitung eine ausdrückliche Zustimmung der versicherten Person notwendig ist, muss die Aufklärungspflicht des Versicherers hohen Ansprüchen genügen. Die FINMA nimmt keine systematische Prüfung der allgemeinen Geschäftsbedingungen der Privatversicherer vor, führt jedoch auf Anfrage eine Prüfung durch. Stellt sie fest, dass eine Bestimmung gegen die Datenschutzvorschriften verstösst, schreitet sie ein.

09.3515 Interpellation Prelicz-Huber vom 8. Juni 2009 "Fallmanagement. Rechtswidrige Eingriffe in das Patientengeheimnis und Verletzung des Datenschutzes"

Die Interpellantin zeigt sich beunruhigt in Bezug auf den Schutz der Versichertendaten im Rahmen des Case Management (Fallmanagement). Die Fallmanagerinnen und -manager der Krankenversicherer können auf die Gesundheitsdaten in den Spitälern zugreifen. Die Vereinbarungen, die zwischen den Versicherern und den Spitälern abgeschlossen wurden, enthalten unzureichende Bestimmungen hinsichtlich der Wahrung des Arzt- und Patientengeheimnisses. Die Versicherer beschaffen sich Gesundheitsdaten auch ohne Einwilligung der Versicherten.

Antwort des Bundesrates vom 26. August 2009

Die Datenschutzbestimmungen (DSG, VDSG, Art. 33 ATSG, Art. 84–84b KVG, Art. 59 und 120 KVV) sind auf das Fallmanagement anwendbar. Die Versicherten, deren Untersuchungen und Behandlungen von einer Fallmanagerin oder einem Fallmanager begleitet werden, müssen für diese

Begleitung sowie für den Einblick in ihre Gesundheitsdaten ihre freiwillige und ausdrückliche Zustimmung erteilen. Diese Zustimmung ist nur nach vorgängiger Aufklärung gültig, d. h. wenn die versicherte Person zuvor vom Versicherer angemessen informiert wurde. Die Krankenversicherer sind berechtigt, die Daten zu bearbeiten – oder bearbeiten zu lassen –, die sie benötigen, um ihre im Gesetz vorgesehenen Aufgaben zu erfüllen, namentlich um Leistungsansprüche zu beurteilen. Dabei müssen sie das Verhältnismässigkeitsprinzip beachten, d. h. sie dürfen nicht mehr Daten anfordern, als sie für die Erfüllung ihrer Aufgaben benötigen.

11.429 Initiative der SGK-N vom 24. März 2011 "Tarmed. Subsidiäre Kompetenz des Bundesrates"

Im Rahmen dieser Initiative hat das Parlament Artikel 42 Absatz 3bis und 4 KVG verabschiedet.

11.3393 Motion Cassis vom 14. April 2011 "Überprüfung der Swiss-DRG-Abrechnung und Vergütung der Spitäler durch eine gemeinsame neutrale Stelle"

Der Motionär verlangt die Einrichtung einer externen, schuldnerunabhängigen Revisionsstelle, um die Berechnung der Vergütung sowie die Wirtschaftlichkeit der Leistung für die diagnosebezogenen Fallpauschalen (DRG) für akutstationäre Behandlungen zu überprüfen.

Antwort des Bundesrates vom 16. September 2011

Der Leistungserbringer muss dem Schuldner der Vergütung (d. h. im Fall von Behandlungen im Spital dem Versicherer) eine detaillierte und verständliche Rechnung sowie alle notwendigen Angaben zustellen, damit der Letztere die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen kann. Im Rahmen der Umsetzung der neuen Spitalfinanzierung hat der Bundesrat Artikel 59d KVV eingeführt. Nach dessen Absatz 2 muss der Tarifvertrag bei einem leistungsbezogenen Vergütungsmodell, das auf einem Patienten-Klassifikationssystem vom Typ DRG basiert, zusätzlich das Kodierungshandbuch sowie ein Konzept zur Kodierrevision enthalten. Nach Ansicht des Bundesrates steht es den Tarifpartnern frei zu entscheiden, ob sie unabhängige Revisoren mit der Durchführung der Kodierrevision beauftragen möchten oder ob sie diese Aufgabe lieber einer Stelle übertragen möchten, die von den Leistungserbringern und den Versicherern unabhängig ist. Nach dem Scheitern der Vereinbarung zwischen H+ und Santésuisse hat der Bundesrat die Grundsätze der Datenübermittlung auf dem Verordnungsweg geregelt. Dabei hat er sowohl den Datenschutz als auch die Aufgabe der Versicherer im Zusammenhang mit der Rechnungskontrolle berücksichtigt. Die KVV-Revision wurde vom Bundesrat am 4. Juli 2012 verabschiedet (AS 2012 4089).

11.3622 Interpellation Cassis vom 16. Juni 2011 "Daten- und Persönlichkeitsschutz im Fallpauschalen-System Swiss DRG"

Der Interpellant zeigt sich beunruhigt darüber, dass im Rahmen der Einführung der Tarifstruktur Swiss DRG systematisch Diagnosen und durchgeführte Prozeduren in nicht pseudonymisierter Form übermittelt werden.

Antwort des Bundesrates vom 16. September 2011
Der Datenschutz ist dem Bundesrat ein wichtiges Anliegen. Im Rahmen der Verordnungsanpassungen im Zusammenhang mit der Spitalfinanzierung hat er Artikel 59 KVV ergänzt, der den Leistungserbringer verpflichtet, zwei getrennte Rechnungen zu erstellen: eine für die Leistungen zulasten der obligatorischen Krankenpflegeversicherung und eine zweite für die Leistungen zulasten der Zusatzversicherung (Art. 59 Abs. 3 KVV). Ausserdem müssen die diagnosebezogenen Daten in pseudonymisierter Form aufbewahrt werden und diese Pseudonymisierung darf nur durch den Vertrauensarzt des Versicherers aufgehoben werden.

11.3646 Motion der Sozialdemokratischen Fraktion vom 16. Juni 2011 "Patientengerechte, personalverträgliche und qualitätsorientierte Einführung von Fallpauschalen"

Die Motion betrifft die Einführung der Fallpauschalen am 1. Januar 2012. Die Motionärin verlangt unter anderem, dass der Datenschutz gewährleistet wird, dass die systematische Weitergabe von Diagnosen und Prozeduren untersagt wird und dass alle anderen Informationen von unabhängigen Vertrauensärztinnen und -ärzten beurteilt werden.

Antwort des Bundesrates vom 7. September 2011

Wie bei der Interpellation Cassis (11.3622) legt der Bundesrat dar, dass Artikel 59 Absatz 3 KVV vom Leistungserbringer die Erstellung von zwei getrennten Rechnungen verlangt: eine für die Leistungen zulasten der Grundversicherung und eine zweite für die Leistungen zulasten der Zusatzversicherung. Die diagnosebezogenen Daten müssen in pseudonymisierter Form aufbewahrt werden und diese Pseudonymisierung darf nur durch den Vertrauensarzt des Versicherers aufgehoben werden. Für die Bearbeitung der diagnosebezogenen Daten müssen die Versicherer die erforderlichen technischen und organisatorischen Massnahmen treffen. *Diese Motion wurde am 19. September 2011 abgelehnt.*

11.3674 Motion der Grünen Fraktion vom 17. Juni 2011 "Qualitätssicherung mit der Einführung der neuen Spitalfinanzierung"

Im Rahmen der Einführung des Systems Swiss DRG verlangt die Motionärin unter anderem, dass die systematische Übermittlung sensibler Patientendaten an Krankenversicherer oder weitere berechtigte Personen oder Stellen nach den Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten erfolgen muss.

Antwort des Bundesrates vom 16. September 2011

Der Bundesrat weist darauf hin, dass die in der Motion genannte Bedingung bereits generell für die Leistungserbringer und für die Versicherer gilt.

11.3785 Motion Heim vom 14. September 2011 "Zum Schutz des Patienten- und Arztgeheimnisses"

Die Motionärin verlangt, dass zeitgleich mit der Einführung der Swiss DRG sichergestellt wird, dass die Verträge zwischen Leistungserbringern, Kassen und Kantonen Art und Umfang der Datenübermittlung so regeln, dass Arztgeheimnis, Daten- und Persönlichkeitsschutz gewahrt und gesichert sind. Die Kodierrevision ist zu stärken und es ist ein Trust- und Clearingsystem vorzusehen.

Antwort des Bundesrates vom 9. Dezember 2011

Im Zusammenhang mit der Datenübermittlung zwischen den Spitälern und den Versicherern im Zuge der Einführung der Tarifstruktur Swiss DRG misst der Bundesrat dem Datenschutz grosse Bedeutung bei. Verschiedene Massnahmen zur Stärkung der Rechnungskontrolle unter gleichzeitiger Wahrung des Datenschutzes sind in Vorbereitung. Der Bundesrat erinnert daran, dass die beiden gesetzlichen Aufgaben, die Rechnungsprüfung einerseits (Art. 42 KVG) und die Kodierrevision bei einem DRG-Vergütungsmodell andererseits (Art. 59d Abs. 2 KVV), klar voneinander zu unterscheiden sind. Ziel der Kodierrevision ist es, die Qualität der Kodierung in den Spitälern zu prüfen und zu beurteilen. Sie wird im Prinzip nur einmal im Jahr stichprobenweise durchgeführt. Am 6. Juli 2011 hat der Bundesrat im Rahmen der Genehmigung der Tarifstruktur Swiss DRG 1.0 auch das Kodierungshandbuch sowie das Konzept zur Kodierrevision genehmigt, das eine Kontrolle durch unabhängige Revisoren vorsieht.

Nach dem Scheitern der Vereinbarung zwischen H+ und Santésuisse hat der Bundesrat die Grundsätze der Datenübermittlung auf dem Verordnungsweg geregelt. Dabei hat er sowohl den Datenschutz als auch die Aufgabe der Versicherer im Zusammenhang mit der Rechnungskontrolle berücksichtigt. Die KVV-Revision wurde vom Bundesrat am 4. Juli 2012 verabschiedet (AS 2012 4089). Am 20. November 2012 hat das EDI die Verordnung über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern erlassen (SR 832.102.14).

11.5422 Frage Cassis vom 21. September 2011 "Wird der Datenschutz mit einem Kreisschreiben ausgehöhlt?"

Der Fragesteller erkundigt sich, ob das BAG-Kreisschreiben Nr. 7.1 vom 25. August 2011 den Datenschutz und den Entscheid des Parlamentes vom September 2007 verletzt, gemäss dem die Diagnosen und Prozeduren nicht systematisch auf den DRG-Rechnungen aufgeführt werden dürfen.

Antwort des Bundesrates vom 26. September 2011

Im BAG-Kreisschreiben Nr. 7.1 wird festgehalten, was in Artikel 42 KVG vorgesehen ist. Zudem wird auf die gesetzliche Verpflichtung der Leistungserbringer hingewiesen, den Versicherern alle Informationen zu liefern, die diese benötigen. Das Kreisschreiben ordnet keine systematische Übermittlung von Patientendaten an. In einem Grundsatzurteil vom 29. Mai 2009 hat das Bundesverwaltungsgericht festgehalten, dass die geltenden Bestimmungen eine Regelung durch einen Tarifvertrag zulassen, der die systematische Übermittlung bestimmter medizinischer Daten vorsieht, sofern die allgemeinen Grundsätze (insbesondere das Verhältnismässigkeitsprinzip) eingehalten werden. Im Kreisschreiben wird darauf hingewiesen, dass der Versicherer Informationen verlangen darf, die für die Rechnungskontrolle erforderlich sind, und dass er berechtigt ist, die Bezahlung aufzuschieben, bis er diese Informationen erhalten hat.

11.5454 Frage Glauser-Zufferey vom 21. September 2011 "Übermittlung von medizinischen Daten"

Die Fragestellerin erkundigt sich, ob das BAG-Kreisschreiben 7.1 vom 25. August 2011 das Arztgeheimnis missachtet.

Antwort des BAG vom 26. September 2011

Im BAG-Kreisschreiben Nr. 7.1 wird festgehalten, was in Artikel 42 KVG vorgesehen ist. Zudem wird auf die gesetzliche Verpflichtung der Leistungserbringer hingewiesen, den Versicherern alle Informationen zu liefern, die diese benötigen. Das Kreisschreiben ordnet keine systematische Übermittlung von Patientendaten an.

12.5107 Frage Steiert vom 7. März 2012 "Zahlungsverweigerung von Versicherern als Erpressung für die Herausgabe von Patientendaten"

Der Fragesteller erkundigt sich, ob die Praxis der Versicherer zulässig ist, Spitälern die Rechnungsbegleichung zu verweigern, wenn ihnen diese nicht systematisch unverschlüsselte Patientendaten liefern.

Antwort des Bundesrates vom 12. März 2012

Die Versicherer sind gesetzlich verpflichtet, die Rechnungen zu kontrollieren, d. h. die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung zu überprüfen. Nach dem Scheitern der Vereinbarung zwischen den Tarifpartnern (H+ und Santésuisse) hat das Parlament am 23. Dezember 2011 Artikel 42 Absatz 3bis und 4 KVG verabschiedet, gemäss dem die Leistungserbringer auf der Rechnung die Diagnosen und Prozeduren kodiert aufzuführen haben. Mit dieser Gesetzesbestimmung wird dem Bundesrat die Kompetenz übertragen, ausführende Bestimmungen zur Erhebung, Bearbeitung und Weitergabe der Daten zu erlassen. Der Bundesrat hat am 4. Juli 2012 die entsprechenden Verordnungsbestimmungen verabschiedet.

12.5124 Frage Kessler vom 7. März 2012 "Offenlegung von sensiblen Patientendaten. Datenschutz"

Patientenorganisationen haben den Versicherten empfohlen, sensible Daten nur dem Vertrauensarzt zur Verfügung zu stellen. Die Fragestellerin erkundigt sich, wie das BAG garantieren kann, dass die unverschlüsselten Daten beim medizinischen Dienst bleiben.

Antwort des Bundesrates vom 12. März 2012

Mit Hilfe von detaillierten Erhebungen bei den Versicherern überprüft das BAG regelmässig, ob der Vertrauensarzt die gesetzlichen Anforderungen erfüllt. Im Rahmen seiner Audits überprüft das BAG insbesondere, ob sich mit den Räumlichkeiten und Infrastrukturen der Vertrauensärzte deren Unabhängigkeit gegenüber den Versicherern gewährleisten lässt und ob die Patientendaten vertraulich behandelt werden können. Ausserdem kontrolliert das BAG, wie der Zugang zur Korrespondenz geregelt ist und wie die Ablage der persönlichen Daten organisiert ist.

12.5193 Frage Rossini vom 30. Mai 2012 "Krankenkassen und Datenschutz"

Der Fragesteller erkundigt sich, ob die Praxis der Krankenkassen, die Daten zum Gesundheitszustand ihrer Versicherten zu kommerziellen Zwecken zu verwenden, legal ist.

Antwort des Bundesrates vom 4. Juni 2012

Als ausführende Organe im Bereich der sozialen Krankenversicherung unterstehen die Versicherer dem DSG. Gemäss diesem Gesetz dürfen sie die Personendaten der Versicherten nur für den Zweck verwenden, für den diese Daten erhoben wurden. Würde ein Versicherer Daten, von denen er im Rahmen seiner gesetzlichen Pflicht zur Überprüfung der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit einer medizinischen Leistung Kenntnis erlangt hat, zu kommerziellen Zwecken verwenden, würde er gegen die geltenden Datenschutzvorschriften verstossen.

12.441 Parlamentarische Initiative Neirynck vom 13. Juni 2012 "Nationale Datenbank für Daten der medizinischen Bildgebung"

Diese parlamentarische Initiative hat den Zweck, eine nationale elektronische Datenbank zu schaffen, die für jede krankenversicherungspflichtige Person ein Dossier enthält. In diesem Dossier werden sämtliche Bilder der versicherten Person abgelegt, die mit einem Verfahren der medizinischen Bildgebung erstellt wurden. Nur das zugelassene medizinische Personal hat Zugang zu dieser Datenbank, und dies nur nach Einwilligung des Patienten. Diese Initiative verfolgt unter anderem das Ziel, die Einhaltung des Arztgeheimnisses und der Grundsätze des DSG zu gewährleisten.

12.3655 Postulat der SGK-N vom 29. Juni 2012 "Neutrale Clearingstelle für den Datentransfer zwischen Spitälern und Versicherern"

Die Postulantin verlangt vom Bundesrat, einen Bericht über das Potenzial einer neutralen Clearingstelle für den Datenaustausch zwischen Spitälern und Versicherern, über die mit einer solchen Stelle verbundenen Risiken und über die politische Machbarkeit des Projekts zu verfassen. In seinem Bericht soll der Bundesrat unter anderem die Erfahrungen in anderen Ländern mit solchen Clearingstellen, das Kosten-Nutzen-Verhältnis einer solchen Stelle, den Datenschutz und das Arztgeheimnis sowie den Beitrag einer solchen Stelle zum Verfahren für die Prüfung der Wirtschaftlichkeit der Leistungen analysieren. Der Bundesrat soll auch einen Effizienzvergleich zwischen einer neutralen Clearingstelle und einer zertifizierten Datenannahmestelle jedes einzelnen Versicherers vornehmen.

Antwort des Bundesrates vom 29. August 2012

Am 4. Juli 2012 hat der Bundesrat eine Änderung der KVV (AS 2012 4089) verabschiedet, die am 1. Januar 2013 in Kraft getreten ist. Diese Änderung sieht unter anderem vor, dass die Versicherer bis am 31. Dezember 2013 eine Datenannahmestelle einzurichten und zu zertifizieren haben. Mit der Einführung dieser Datenannahmestellen wird die Einhaltung des Datenschutzes gewährleistet. Demzufolge muss abgewartet werden, bis diese Datenannahmestellen während einiger Zeit betrieben wurden, damit die gemachten Erfahrungen mit der Schaffung einer neutralen Clearingstelle verglichen werden können.

Beilage 3

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Kranken- und Unfallversicherung

CH-3003 Bern, BAG

An die KVG-Versicherer

Referenz/Aktenzeichen:
Ihr Zeichen:
Unser Zeichen: Lp
Bern, 25. August 2011

Kreisschreiben 7.1, Datenschutzkonforme Organisation und Prozesse der Krankenversicherer

Sehr geehrte Damen und Herren

In der Beilage lassen wir Ihnen das neue Kreisschreiben 7.1, *Datenschutzkonforme Organisation und Prozesse der Krankenversicherer*, und dessen Anhänge 1 - 7 zukommen. Es ersetzt das bisherige Kreisschreiben 7.1. vom 9. März 2005, *Daten- und Persönlichkeitsschutz und ist* unter folgenden Link auf der BAG-Webseite abrufbar:
http://www.bag.admin.ch/themen/krankenversicherung/02874/02877/06501/index.html?lang=de

Das Kreisschreiben 7.1. listet die für die Krankenversicherer geltenden Datenschutzgrundsätze und -vorgaben auf. Gestützt auf dieses Kreisschreiben werden wir Sie für eine neue Erhebung **im Oktober** befragen, welche Vorkehrungen Sie getroffen haben bzw. noch treffen werden. Wo notwendig, werden entsprechende Korrekturen angeordnet und deren Umsetzung kontrolliert. Grund dafür ist die Annahme des Postulates Heim (P 08.3493, Schutz der Patientendaten.Schutz der Versicherten, Annahme NR 12.12.2008)[1], die Ergebnisse der vom BAG/EDÖB am 16. Juni 2009 veröffentlichten Datenschutzerhebung[2] sowie neue Datenschutzvorschriften namentlich im Hinblick auf die Einführung des verfeinerten Risikoausgleichs sowie der diagnosebezogenen Fallpauschalen im Rahmen der

[1] Das Postulat verlangt vom Bundesrat aufzuzeigen, welche Massnahmen gegen die Diskriminierung einzelner Patientengruppen und zum Schutz der Patientendaten bei den Versicherern geplant sind.
[2] Diese ist unter folgenden Link auf der BAG-Webseite abrufbar:
http://www.bag.admin.ch/themen/krankenversicherung/00295/index.html?lang=de

Bundesamt für Gesundheit
Patricia Leiber
Hessstrasse 27E, CH-3003 Bern
Postadresse: CH-3003 Bern
Tel. +41 31 322 92 23, Fax +41 31 323 00 60
Patricia.Leiber@bag.admin.ch
www.bag.admin.ch

neuen Spitalfinanzierung ab 1. Januar 2012.

Mit freundlichen Grüssen

Abteilung Versicherungsaufsicht
Die Leiterin

Helga Portmann

Beilagen : Kreisschreiben 7.1 mit Anhängen 1 - 7

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Kranken- und Unfallversicherung

CH-3003 Bern, BAG

An die KVG Versicherer

Referenz/Aktenzeichen:
Ihr Zeichen:
Unser Zeichen: Lp/AGM/BEJ/TRE
Bern, 25. August 2011

Kreisschreiben Nr.:	**7.1**
Inkrafttreten:	**1. September 2011**

Datenschutzkonforme Organisation und Prozesse der Krankenversicherer

Dieses Kreisschreiben ersetzt das frühere Kreisschreiben 7.1 vom 9. März 2005, *Daten- und Persönlichkeitsschutz*, und knüpft an die Ergebnisse der vom BAG/Eidg. Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) durchgeführten Datenschutzerhebung vom 4. Dezember 2007 bei den Krankenversicherern an, welche am 16. Juni 2009 veröffentlicht wurden[1]. Es erinnert die Krankenversicherer an die geltenden Datenschutzgrundsätze und -vorgaben. Es soll dazu beitragen, den Datenschutz und die Datensicherheit bei ihren Aktivitäten zu optimieren.

1. Ausgangslage

Die Datenschutzerhebung des BAG/EDÖB vom 4. Dezember 2007 hat gezeigt, dass die Krankenversicherer für die Datenschutzproblematik sensibilisiert sind, und dass der Schutz der Daten trotz sehr unterschiedlicher Organisationsstrukturen über weite Strecken sichergestellt ist. Mit der Erhebung wurde aber auch festgestellt, dass in einigen sensiblen Bereichen noch Verbesserungspotential besteht. Mit der Veröffentlichung der Ergebnisse der Datenschutzerhebung wurden sinngemäss folgende Empfehlungen abgegeben:

[1] http://www.bag.admin.ch/themen/krankenversicherung/00295/index.html?lang=de

Bundesamt für Gesundheit
Hessstrasse 27E, CH-3003 Bern
Postadresse: CH-3003 Bern
Tel. +41 31 323 70 66, Fax +41 31 323 00 60
www.bag.admin.ch

- Das BAG empfiehlt den Krankenversicherern, ein Datenschutzkonzept (eine Strategie) zu erarbeiten.
- Die Krankenversicherer sind verpflichtet, ein Verzeichnis der Datensammlungen zu unterhalten. Für jede Datensammlung mit besonders schützenswerten Personendaten ist ein Bearbeitungsreglement zu unterhalten (Beschreibung der Prozesse inkl. Verantwortlichkeiten, Berechtigungen, Datenfluss sowie der technischen Massnahmen zur Datensicherheit).
- Das BAG empfiehlt den Krankenversicherern, eine verantwortliche Person für den Datenschutz zu bezeichnen. Die Aufgaben dieses Verantwortlichen sind in einem Pflichtenheft zu umschreiben.
- Datenschutzverantwortliche müssen über die erforderlichen Fachkenntnisse verfügen.
- Es sollen von einer dafür spezialisierten Stelle regelmässig externe Datenschutzaudits durchgeführt und die Resultate den Aufsichtsbehörden unterbreitet werden.

Das BAG geht davon aus, dass die Krankenversicherer in der Zwischenzeit weitere Massnahmen zur Verbesserung der Datenschutzkonformität ihrer Organisation und / oder ihrer Prozesse eingeleitet haben bzw. dies noch tun werden. Zur Förderung dieser Entwicklung weist das vorliegenden Kreisschreiben und dessen Anhänge 1 - 7 die Krankenversicherer auf die für sie geltenden Datenschutzbestimmungen hin, welche sich aus den verschiedenen Bundeserlassen[2] ergeben. Neue Datenschutzbestimmungen sind mit fetter Schrift hervorgehoben. Im Hinblick auf die Einführung der diagnosebezogenen Fallpauschalen im Rahmen der neuen Spitalfinanzierung haben diese Datenschutzbestimmungen eine umso grössere Bedeutung.

2. Datenschutz- und Datensicherheitskonzept

KVG Art. **84*b*** (neu, Inkrafttreten am 1.1.2012) / DSG 2, 3, 4, 5, 7/ VDSG 8 -10, 20 + 21

Das BAG empfiehlt allen Krankenversicherern, ein umfassendes ganzheitliches **Datenschutz- und Sicherheitskonzept** zu erarbeiten. Datensicherheit ist ein wesentlicher Bestandteil des Datenschutzes.

Ein Datenschutz- und Sicherheitskonzept gibt Auskunft über die mittel- und langfristige Strategie zur Umsetzung des Datenschutzes und der Datensicherheit im Betrieb. Es beschreibt die Organisation des Datenschutzes. Zudem leiten sich daraus insbesondere die Aufgaben der Personen ab, die innerhalb des Krankenversicherers für den Datenschutz verantwortlich und für die Datensammlungen zuständig sind.

Ein solches Konzept ist zwar gesetzlich nicht vorgeschrieben, es ist aber ein wichtiger Grundstein für den Datenschutz und die Datensicherheit im Betrieb. Gestützt darauf kann der Datenschutz betriebsintern in die Geschäftsabläufe integriert werden. Das Datenschutz- und Sicherheitskonzept bzw. Teile davon kann anschliessend in Richtlinien für die Mitarbeitenden, Sicherheits- und Informationsschutzrichtlinien für die Informatik und andere Bereiche sowie in *Bearbeitungsreglementen* (Art. 11 und 21 VDSG, Art. **84*b*** neu KVG) umgesetzt werden.

Die Umsetzung des Datenschutz- und Sicherheitskonzepts kann auch *technische und organisatorische Massnahmen* erfordern. Die Krankenversicherer müssen hierfür die erforderlichen Mittel bereitstellen (Art. 7 DSG).

[2] Vgl. Anhänge 1 + 2

Ein Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes sowie Angaben, was in einem Bearbeitungsreglement aufgeführt werden muss, ist unter folgenden Link abrufbar:

http://www.edoeb.admin.ch/dokumentation/00445/00472/00935/index.html?lang=de

3. Bearbeitungsreglemente

KVG **84*b*** (neu, Inkrafttreten am 1.1.2012) / VDSG 21

Artikel 21 VDSG schreibt den Krankenversicherern vor, *für automatisierte Datensammlungen*, die *besonders schützenswerte Daten und Persönlichkeitsprofile enthalten*, oder mit anderen Datensammlungen verknüpft sind, ein Bearbeitungsreglement zu erstellen. Dieses Reglement beinhaltet Angaben über die interne Organisation des Krankenversicherers, sowie über die Struktur, in welche die Datensammlung oder das automatisierte Bearbeitungssystem eingebettet ist. Es beschreibt die Datenbearbeitungs- und *Kontrollprozeduren*, und enthält alle Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung und der eingesetzten Informatikmittel. Es regelt namentlich *Art und Umfang der Zugriffsberechtigung auf Personendaten.* Das Reglement muss regelmässig angepasst bzw. nachgeführt werden und dem EDÖB in verständlicher Form jederzeit zur Verfügung stehen.

Das Sicherstellen der *Vollständigkeit* und der *Aktualität* der Bearbeitungsreglemente ist eine Hauptaufgabe der/des *Datenschutzbeauftragten* des Krankenversicherers und dient als eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung mit schützenswerten Personendaten.

Artikel **84*b*** (neu) KVG wiederholt und verdeutlicht diese bereits gemäss VDSG bestehenden Verpflichtungen der Krankenversicherer, präzisiert jedoch zusätzlich, dass die Bearbeitungsreglemente dem EDÖB *zur Beurteilung vorzulegen sind* und *öffentlich zugänglich* sein müssen.

Aufgrund dieser neuen Vorgaben müssen die Krankenversicherer ab dem 1. Januar 2012 ihre Bearbeitungsreglemente dem EDÖB *unaufgefordert zur Beurteilung vorlegen.* Das Bearbeitungsreglement ist aber bereits gültig, wenn der Krankenversicherer es für verbindlich erklärt hat.

Überdies müssen die Krankenversicherer die Bearbeitungsreglemente ab dem 1. Januar 2012 veröffentlichen. Sie haben diese den *interessierten Personen* mittels Publikation auf dem Internet oder in anderer Form zugänglich zu machen. Die Pflicht zur Veröffentlichung besteht dabei unabhängig von einer durch den EDÖB durchgeführten Beurteilung.

Ein Bearbeitungsreglement kann für mehrere Datensammlungen gültig sein, wenn das Reglement tatsächlich für die bezeichneten Datensammlungen zur Anwendung gelangt und für jede betreffende Datensammlung die Erfordernisse von Artikel 21 Absatz 2 VDSG erfüllt.

4. Verzicht auf die Anmeldung der Datensammlungen - Meldung einer für den Datenschutz verantwortlichen Person

DSG 11*a* Abs. 5 Bst. e / VDSG 12*a*

Das DSG ermöglicht die Selbstregulierung der Unternehmen im Bereich Datenschutz: Es liegt in der Verantwortung des Krankenversicherers, dafür zu sorgen, dass die Grundsätze und Vorgaben der Datenschutzgesetzgebung eingehalten werden. Der Krankenversicherer ist als Inhaber der Daten-

sammlung von der Pflicht zur Anmeldung der Datensammlungen befreit, wenn er eine für den **betrieblichen Datenschutz verantwortliche Person** bezeichnet hat, die *unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht, Verzeichnisse der Datensammlungen führt* und diese Person *dem EDÖB gemeldet* hat.

Die für den betrieblichen Datenschutz verantwortliche Person ist entgegen der Bezeichnung nicht verantwortlich für den Datenschutz im Betrieb, sondern hat die *Rolle einer Beraterin oder eines Beraters*, bzw. einer Aufsichtsstelle (vgl. die französische Version im DSG: conseiller à la protection des données). Die Verantwortung für die Einhaltung der Bestimmungen zum Datenschutz bleibt in jedem Fall beim Inhaber der Datensammlung, also beim Krankenversicherer bzw. bei dessen leitenden Organ (Art. 16 Abs. 1 DSG).

Die oder der Datenschutzverantwortliche muss ihre/seine Funktion *organisatorisch und fachlich unabhängig* ausüben können, und ein möglicher Interessenkonflikt muss bereits durch ihre/seine organisatorische Stellung vermieden werden. Deshalb sollte ihre/seine Stelle ausserhalb der Linienverantwortlichkeit stehen. Empfohlen wird eine Stabstelle, eine Stelle in der Rechtsabteilung oder in der IT-Abteilung oder eine externe Stelle. Die Rolle und Funktion der für den Datenschutz verantwortlichen Person ist in einem *Pflichtenheft* zu definieren.

Weiterführende Informationen finden Sie im Anhang 3 und in den Empfehlungen des EDÖB unter folgenden Link:

http://www.edoeb.admin.ch/themen/00794/01609/01611/index.html?lang=de

5. Outsourcing

KVG 84 / DSG 10*a*

Outsourcing umfasst die Auslagerung von Dienstleistungen, die bisher von den Krankenversicherern selber erbracht wurden, sowie Dienstleistungen, welche die Krankenversicherer selber bisher nicht erbracht haben und die sie neu von einem Dienstleister beziehen.

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die *Daten nur so bearbeitet werden, wie es der Krankenversicherer selber tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht dies verbietet* (Art. 10*a* DSG). Artikel 84 KVG erlaubt den Krankenversicherern, Personendaten einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile durch Dritte bearbeiten zu lassen.

Der Krankenversicherer hat den Dienstleister sorgfältig auszuwählen, zu instruieren und zu überwachen. Schnittstellen, Verantwortlichkeiten, Zuständigkeiten und Haftungsfragen sind vertraglich genau zu regeln bzw. abzugrenzen. Die ausgelagerte Funktion ist in das interne Kontrollsystem des Krankenversicherers zu integrieren.

Im Vertrag ist der Bearbeitungszweck für die Daten genau zu umschreiben und der Dienstleister zu verpflichten, die Daten *nur zweck- und weisungsgebunden zu bearbeiten*. Damit ist die Verwendung für eigene oder fremde Zwecke des Dienstleisters ausgeschlossen. Der Dienstleister ist mitsamt den Mitarbeitenden funktionell in die *Schweigepflicht* und das bereichsspezifische Datenschutzrecht des Krankenversicherers einzubinden. Die Mitarbeitenden des Dienstleisters sind vertraglich und nötigenfalls einzelunterschriftlich zur Geheimhaltung zu verpflichten.

Der Krankenversicherer muss sich vergewissern, dass der Dienstleister die *Datensicherheit gewährleistet*. Die Sicherheitsstandards für den Datenaustausch und die Sicherheitsanforderungen, die der

Dienstleister zu erfüllen hat, müssen schriftlich definiert werden. *Personendaten der Versicherten müssen durch angemessene, technische, personelle und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.* Der Dienstleister muss den Datenschutz jederzeit gewährleisten können (vgl. Art. 7 DSG; Art. 8 und 9 VDSG). Der Vertrag muss die Konsequenzen bei Nichteinhaltung der Datenschutzklauseln und bei Auflösung des Vertrags enthalten (Konventionalstrafen, sofortige Sicherstellung von Daten, Auflösung des Vertrags, vollständige Vernichtung der Daten).

Der Dienstleister muss den Krankenversicherer regelmässig über die Datenbearbeitung informieren. Der auslagernde Krankenversicherer, dessen interne und externe Revisionsstelle sowie das BAG müssen den ausgelagerten Geschäftsbereich vollumfänglich, jederzeit und ungehindert einsehen und prüfen können. Der Krankenversicherer muss sich die Einsichts-, Weisungs- und Kontrollrechte vom Dienstleister vertraglich einräumen lassen, damit er ein ordnungsgemässes Controlling gegenüber dem Dienstleister wahrnehmen kann.

Die *Auskunftspflicht des Krankenversicherers* gegenüber den betroffenen Personen bleibt bestehen, da er auch Inhaber der Datenbank bleibt, wenn Personendaten durch einen Dritten bearbeitet werden (Art. 8 Abs. 4 DSG). Der Krankenversicherer muss deshalb jederzeit Zugriff auf die Daten haben, was durch den Dienstleister sicherzustellen ist.

Der Krankenversicherer muss sowohl im Vertrag über den vom Outsourcing betroffenen Bereich als auch im Sicherheitsdispositiv die nötigen Vorkehren treffen, die ihn vor einem plötzlichen und unerwarteten Ausstieg des Dienstleisters schützen und die Weiterführung des ausgelagerten Geschäftsbereichs mit der notwendigen Datensicherheit erlauben.

Aus diesem Grund ist, wenn immer möglich, auf das Outsourcing datensensibler Bereiche ins Ausland zu verzichten. Sollte dies ausnahmsweise der Fall sein, so ist Artikel 6 DSG besonders zu beachten (grenzüberschreitende Datenbekanntgabe nur unter bestimmten Voraussetzungen und unter Einbezug des EDÖB).

Der Krankenversicherer trägt als Inhaber der Datensammlung weiterhin die volle datenschutzrechtliche Verantwortung für den ausgelagerten Geschäftsbereich. Die Krankenversicherer müssen die Versicherten über ihre Outsourcingpraxis hinreichend informieren.

6. Unabhängigkeit der Vertrauensärztin / des Vertrauensarztes und des vertrauensärztlichen Dienstes

STGB 321 / KVG 57, 56, 42 Abs. 5 / KVV 59

Die Vertrauensärztin oder der Vertrauensarzt gemäss Artikel 57 KVG ist ein *besonderes Organ der sozialen Krankenversicherung*. Ihre/seine Aufgaben werden in Artikel 57 Absätze 4 und 5 KVG umschrieben. Danach berät sie/er den Versicherer in medizinischen Fachfragen sowie in Fragen der Vergütung und der Tarifanwendung. Zudem kommt ihr/ihm eine Überwachungs- und Kontrollfunktion zu. Sie/er überprüft die Voraussetzungen der Leistungspflicht des Versicherers (Art. 57 Abs. 4 KVG). Ihr/ihm obliegt die Kontrolle der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit der Behandlung im Sinn von Artikel 32 und Artikel 56 KVG. Ihre/Seine Kompetenz beschränkt sich auf die *Beantwortung medizinischer Fachfragen*. In fachlicher Hinsicht kann ihr/ihm der Versicherer nichts vorschreiben. In ihrem/seinem Urteil *unabhängig*, darf sie/er den zuständigen Stellen der Versicherer nur diejenigen Angaben weitergeben, die *notwendig* sind, um über die Leistungspflicht zu entscheiden, die Vergütung festzusetzen, den Risikoausgleich zu berechnen oder eine Verfügung zu begründen. Dabei wahrt sie/er die Persönlichkeitsrechte der Versicherten (Art. 57 **Abs. 7** KVG, Inkrafttreten am 1.1.2012). Der Leistungserbringer ist in *begründeten Fällen berechtigt* und auf Verlangen der versi-

cherten Person *in jedem Fall verpflichtet,* medizinische Angaben *nur der Vertrauensärztin oder dem Vertrauensarzt* bekannt zu geben (Art. 42 Abs. 5 KVG).

Mit der Einführung der diagnosebezogenen Fallpauschalen per 1. Januar 2012 werden für die Rechnungs- und Wirtschaftlichkeitskontrolle der Krankenversicherer diagnosebezogene Daten nötig werden, damit die neuen Pauschalen nachvollzogen werden können (Haupt- und Nebendiagnosen, Prozeduren). Die Krankenversicherer müssen sicherstellen, dass sie diese besonders schützenswerten Personendaten ausschliesslich für die im Gesetz vorgesehenen Zwecke verwenden. Dazu treffen sie die gemäss Artikel 20 VDSG erforderlichen technischen und organisatorischen Massnahmen (Art. **59 Abs. 1bis** KVV). Überdies müssen sie zur Aufbewahrung der diagnosebezogenen Daten die Personalien der Versicherten pseudonymisieren. *Die Aufhebung der Pseudonymisierung darf nur durch die Vertrauensärztin oder den Vertrauensarzt des Krankenversicherers erfolgen* (Art. **59 Abs. 1ter** KVV).

Die gesetzlich vorgeschriebene Unabhängigkeit der Vertrauensärztin oder des Vertrauensarztes muss sich auch in der *Organisation des vertrauensärztlichen Dienstes (VAD)* niederschlagen. Diese Unabhängigkeit verlangt *eigene Bearbeitungsreglemente*, die klar umreissen, welche Kompetenzen und Aufgaben den einzelnen Vertrauensärztinnen und -ärzten und ihren Hilfspersonen zukommen.

Räumlich müssen Lokale des VAD genügend abgetrennt und abschliessbar sein. Die Post darf nur durch Stellen des VAD geöffnet werden und es muss jederzeit sichergestellt sein, dass besonders schützenswerte Personendaten den VAD nicht verlassen können. Ein unabhängiges Telefon- und Telefaxnetz ist unabdingbar. Das Informatiksystem muss physisch so organisiert werden, dass die vom VAD erstellten Dokumente nur auf eigenen Speichermedien archiviert werden, die wiederum nur den Mitarbeitern des VAD zugänglich sind. Der Vertrauensärztin oder dem Vertrauensarzt muss zudem die Kompetenz zur Anstellung ihres/seines Hilfspersonals zukommen. Sie/er hat darauf zu achten, dass die Stellen der Hilfspersonen bezüglich ihrer *fachlichen und organisatorischen* Unterstellung sowie ihres *Beschäftigungsgrades* für den VAD so konzipiert sind, dass sich daraus *keine Interessenkonflikte* für die Hilfspersonen ergeben. Die Hilfspersonen dürfen nicht mit verschiedenen Aufgaben betraut werden, die miteinander nicht kompatibel sind (z.B. für den VAD und die Leistungsabteilung).

Die Vertrauensärztin oder der Vertrauensarzt und ihre Hilfspersonen machen sich strafbar, wenn sie das Berufsgeheimnis gemäss *Artikel 321 des Strafgesetzbuchs (StGB)* verletzen. Benützt eine Hilfsperson die bei ihrer Tätigkeit für den Vertrauensarzt erhaltenen Personendaten für eine andere Tätigkeit beim selben oder bei einem anderen Versicherer, macht sie sich strafbar.

Vertrauensärzte und Vertrauensärztinnen nach Artikel 57 KVG sollten zur Vermeidung des Vorwurfs einer Risikoselektion keine Risikoprüfung bei neuen Versicherungsverträgen nach VVG vornehmen.

7. Substantiierung bei der Rechnungsstellung

KVG 42 Abs. 3 - 5 / KVG 57 Abs. 4 und 6 / KVV 59

Artikel 42 Absatz 3 KVG hält fest, dass der Leistungserbringer dem Schuldner eine detaillierte und verständliche Rechnung zustellen muss (Satz 1). Er muss ihm alle Angaben machen, die er benötigt, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können (Satz 2). Überdies sieht Artikel 42 Absatz 4 KVG vor, dass der Krankenversicherer eine genaue Diagnose oder zusätzliche Auskünfte medizinischer Natur verlangen kann. Gemäss Artikel 42 Absatz 5 KVG ist der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur der Vertrauensärztin oder dem Vertrauensarzt des Krankenversicherers bekannt zu geben. In diesen Fällen müssen die Leistungserbringer den Vertrauensärztinnen und –ärzten die zur Erfüllung ihrer Aufgaben notwendigen Angaben liefern (Art. 57 Abs. 6 Satz 1 KVG). Diese Aufgaben beinhalten insbesondere die Beratung des Versicherers in Fragen der

Vergütung und Tarifanwendung sowie die Überprüfung der Voraussetzung der Leistungspflicht (Art. 57 Abs. 4 KVG). Gemäss Kommentarliteratur schreiben alle diese Bestimmungen gegenüber den Leistungserbringern eine Offenbarungspflicht sowie eine Offenbarungsermächtigung vor. Der Leistungserbringer wird bei den Tatbeständen von Artikel 42 Absatz 3 Satz 2 und Absatz 4 KVG sowie Artikel 57 Absatz 6 Satz 1 KVG im Verhältnis zum Krankenversicherer von seinem Berufsgeheimnis befreit. Die Offenbarung steht nicht im Belieben des Leistungserbringers, sondern ist gegenüber dem Krankenversicherer gesetzliche Pflicht[3]. Diese Bestimmungen, welche die Leistungserbringer verpflichten, alle leistungsrechtlich relevanten Daten bekannt zu geben, haben bereits jetzt eine grosse Tragweite. Eine umso grössere Bedeutung erhalten sie im Hinblick auf die Rechnungs- und Wirtschaftlichkeitskontrolle für die diagnosebezogenen Fallpauschalen im Rahmen der neuen Spitalfinanzierung. Die Krankenversicherer sind deshalb berechtigt, eine substantiierte Rechnungsstellung im Sinne dieser Ausführungen zu verlangen und bis zu deren Erhalt keine Zahlung zu leisten.

8. Weiteres Vorgehen

Das BAG wird die Einhaltung der Vorgaben zum Datenschutz und zur Datensicherheit gemäss diesem Kreisschreiben weiterhin im Rahmen regelmässiger Kontrollen durch die Sektion Audit prüfen. Im Hinblick auf die Einführung der Spitalfinanzierung sind zusätzliche Sonderaudits mit Stichproben zum Umgang der Krankenversicherer mit den diagnosebezogenen Personendaten ihrer Versicherten geplant.

Im Vorfeld dieser Untersuchungen weisen wir die Krankenversicherer speziell darauf hin, dass die Verletzung der Schweigepflicht (Art. 33 ATSG) durch Personen, die an der Durchführung der sozialen Krankenversicherung beteiligt sind, als strafbares Verhalten (Vergehen) geahndet wird (Art. 92 Bst. c KVG) und dass die Missachtung gesetzlicher Datenschutzvorschriften nach Art und Schwere der Mängel Sanktionen nach Artikel 21 Absätze 5 und 5bis KVG nach sich zieht. Dies beinhaltet auch die Möglichkeit zur Publikation der Massnahmen.

Direktionsbereich Kranken- und Unfallversicherung
Der Leiter

Andreas Faller
Vizedirektor
Mitglied der Geschäftsleitung

Abteilung Versicherungsaufsicht
Die Leiterin

Helga Portmann

Beilagen: Anhänge 1 - 7

[3] Datenschutz im Gesundheitswesen, Herausgeber: B. Hürlimann/R. Jacobs/T. Poledna, Kapitel Datenschutz in der obligatorischen Krankenpflegeversicherung von G. Eugster/R. Luginbühl, S. 98 f, Schulthess 2001

Anhang 1: Gesetzliche Grundlagen mit den massgebenden Datenschutzbestimmungen

- Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1)
- Verordnung vom 11. September 2002 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSV, SR 830.11)
- Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG, SR 832.10)
- Verordnung vom 27. Juni 1995 über die Krankenversicherung (KVV, SR 832.102)
- Verordnung vom 14. Februar 2007 über die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK; SR 832.105)
- Verordnung des EDI vom 20. März 2008 über die technischen und grafischen Anforderungen an die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK-EDI, SR 832.105.1)
- Verordnung des EDI vom 29. September 1995 über Leistungen in der obligatorischen Krankenpflegeversicherung (KLV, SR 832.112.31)
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1)
- Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11)
- Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (VDSZ, SR 235.13)

Anhang 2: Kommentar zu den massgebenden Datenbearbeitungsgrundsätzen und -vorgaben

ATSG 28, 31, 32, 33, 47 / ATSV 8, 9 / KVG 42 Abs. 3-5, 42*a*, **57 Abs.** 6, **7**[4] und 8, 82, **84**[5], **84*a***[6], **84*b***[7], 92 / KVV 6*a*, **28** und **28*a***[8], **59**[9], 76, 120 / DSG 2, 3, 4, 5, 7, 8, **9**[10], 10*a*, 11, 11*a*, 16, 17, **18*a***[11], **18*b***[12], 19, 20, 22, 25, 27, 35 / VDSG 1, 2, 8, 9, 10, 12*a*, 12*b*, 16, 18, 20, 21, 22, 23, **24**[13], 28, 34, 35 / VDSZ

- Krankenversicherer, welche die obligatorische Krankenpflegeversicherung und die freiwillige Taggeldversicherung nach dem KVG durchführen, sind im Rahmen der gesetzlichen Bestimmungen befugt, besonders schützenswerte Personendaten[14] und Persönlichkeitsprofile[15] der Versicherten zu bearbeiten oder bearbeiten zu lassen. So z.B. gestützt auf Artikel 42 Absätze 3-5, Artikel 42*a*, Artikel 56, Artikel 57 Absätze 4, 6 und 7, Artikel 58 Absatz 3, Artikel 59, 82, 83, **84, 84*a*** und **84*b*** KVG. Dabei sind sie an die datenschutzrechtlichen Grundsätze wie das *Legalitätsprinzip*, das *Verhältnismässigkeitsprinzip*, das *Zweckbindungsgebot*, den *Grundsatz von Treu und Glauben*, das *Transparenzprinzip*, die *Datenrichtigkeit* und die *Datensicherheit* gebunden (Art. 4, 5, 7 DSG).

- Als Durchführungsorgane der sozialen Krankenversicherung nehmen die Versicherer eine öffentliche Aufgabe des Bundes im Sinne von Artikel 2 Absatz 1 Buchstabe b und Artikel 3 Buchstabe h DSG wahr und sind als solche dem **Legalitätsprinzip** unterstellt, das Folgendes vorsieht: Werden Personendaten durch die Versicherer bearbeitet, ist eine gesetzliche Grundlage nötig. *Besonders schützenswerte Personendaten und Persönlichkeitsprofile* im Sinn von Artikel 3 DSG dürfen nur bearbeitet werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht. Im Einzelfall und nur *ausnahmsweise* können solche Daten auch bearbeitet werden, wenn die betroffene Person *eingewilligt* hat oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 4 Abs. 1 und Art. 17 Abs. 2 Bst. c DSG). Im KVG bildet insbesondere Artikel **84** die formellgesetzliche Grundlage für die Datenbearbeitung. Demnach dürfen die Versicherer Personendaten nur im Rahmen der ihnen nach dem KVG übertragenen Aufgaben bearbeiten (Art. **84** KVG). Unter den nicht abschliessend aufgeführten Durchführungsaufgaben wird neu auch die Berechnung des verfeinerten Risikoausgleichs (Inkrafttreten per 1.1.2012) aufgeführt (Art. **84 Bst. i** KVG).

- Der **Grundsatz der Bearbeitung nach Treu und Glauben** (Art. 4 Abs. 2 DSG) erfordert, dass die Datenbearbeitung für die betroffene Person *transparent* sein muss, d.h. dass eine Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die betroffene Person *erkennbar* sein muss, die betroffene Person also aus den Umständen heraus damit rechnen

---

[4] Art. 57 Abs. 7 KVG (Ergänzung): Inkrafttreten am 1.1.2012, BBl 2008 19

[5] Art. 84 Einleitungssatz und Bst. i KVG (Ergänzung): Inkrafttreten am 1.1.2012, BBl 2008 19

[6] Art. 84*a* Abs. 1 Einleitungssatz und Bst. f : in Kraft seit 1.1.2009

[7] Art. 84*b* KVG (neu): Inkrafttreten am 1.1.2012, BBl 2008 19

[8] Art. 28 und 28*a* KVV: in Kraft seit 1.1.2009

[9] Art. 59 KVV, verschiedene Absätze in Kraft seit 1.1.2009 bzw. 1.1.2010

[10] Art. 7*a* DSG (aufgehoben) und Art. 9 DSG (Änderung) per 1.12.2010

[11] Art. 18*a* DSG (neu):In Kraft seit 1.12.2010

[12] Art. 18*b* DSG (neu):In Kraft seit 1.12.2010

[13] Art. 24 VDSG (Änderung) per 1.12.2010

[14] Art. 3 DSG: Besonders schützenswerte Personendaten sind Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen.

[15] Art. 3 DSG: Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

musste oder sie entsprechend informiert bzw. aufgeklärt wird. Die betroffenen Personen sind über die Beschaffung und Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen zu informieren (Art. **14** DSG).

- Das **Verhältnismässigkeitsprinzip** verlangt, dass nur diejenigen Personendaten beschafft und bearbeitet werden, welche *für einen bestimmten Zweck objektiv tatsächlich benötigt und geeignet* sind (Art. 4 Abs. 2 DSG). Daten dürfen nicht über den gesetzlich zugelassenen Umfang und die gesetzlich zulässige Dauer aufbewahrt werden.

- Personendaten dürfen *nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist* (**Zweckbindungsgebot**; Art. 4 Abs. 3 DSG). Die Personendaten dürfen nicht für andere als die ursprünglichen Zwecke bearbeitet werden.

- Wer Daten bearbeitet, hat sich zu vergewissern, dass diese richtig sind (**Wahrheitsgebot**; Art. 5 Abs. 1 DSG) und die von der Datenbearbeitung betroffenen Personen haben das *Recht, eine Berichtigung* von unrichtigen Daten zu verlangen (Art. 5 Abs. 2 DSG). Weiter haben diese das Recht, über *alle* diese Daten Auskunft zu verlangen (Art. 8 DSG). Die versicherte Person hat somit - unabhängig von einem Interessennachweis und jederzeit - das Recht, eine Kopie des gesamten Dossiers des Versicherers zu erhalten.

- Die Krankenversicherer müssen *ein Verzeichnis sämtlicher* ***Datenbanken*** *führen* und diese beim EDÖB *zur Registrierung anmelden* (Art. 11*a* DSG, Art. 16 VDSG). Sie sind von dieser Verpflichtung befreit, wenn sie eine für den *betrieblichen Datenschutz verantwortliche Person* bezeichnet haben, die *unabhängig* die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt[16], oder wenn sie aufgrund eines *Zertifizierungsverfahrens* nach Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben haben und das Ergebnis der Bewertung dem EDÖB mitgeteilt haben (Art. 11*a* Abs. 2 und 5 Bst. e und f DSG)[17].

- Das Personal der Krankenversicherer untersteht gemäss Artikel 33 ATSG der **Schweigepflicht**. Ein Verstoss gegen diese Norm hat strafrechtliche Konsequenzen zur Folge (Art. 92 Bst. c KVG). Zudem ist der Zugriff der berechtigten Angestellten des Krankenversicherers auf diejenigen Personendaten zu beschränken, welche diese zur Erfüllung ihrer klar umschriebenen Aufgaben benötigen (Art. 9 Abs. 1 Bst. g VDVG). Zusätzlich sind die *Vertrauensärztin oder der Vertrauensarzt und ihr Hilfspersonal* an die Schweigepflicht gemäss Artikel 321 des Strafgesetzbuchs (StGB; SR 311.0) und somit an das **Patientengeheimnis** gebunden.

- Die **Weitergabe von Personendaten** an externe Stellen ist nur in einem *sehr beschränkten Rahmen* zulässig. Zu beachten sind dabei die Artikel **84*a*** KVG (Datenbekanntgabe) in Abweichung von Artikel 33 ATSG (Schweigepflicht) und Artikel 82 KVG (besondere Amts- und Verwaltungshilfe) ebenfalls in Abweichung zu Artikel 33 ATSG, Artikel 120 KVV (Informationspflicht der Krankenversicherer über die Datenbekanntgabe und geleistete Amts- und Verwaltungshilfe), Art. 32 Abs. 2 ATSG (Amts- und Verwaltungshilfe) sowie Artikel 47 ATSG (Akteneinsicht). Artikel **84*a*** KVG regelt, unter welchen abschliessenden Voraussetzungen die in dieser Bestimmung genannten Organe (und nur diese) in Abweichung von der Schweigepflicht (Art. 33 ATSG) Personendaten genau definierten Dritten offenbaren dürfen. Eine andere Versicherungsgesellschaft, die die Versicherungen nach VVG anbietet, *ist eine Dritte* im Sinn von Art. 84*a* Abs. 5 KVG. Bietet der Krankenversicherer selber solche Versicherungen nach VVG an, gelten die obgenannten Grundsätze, so insbesondere die Bearbeitung nach Treu und Glauben und das Zweckbindungsgebot. Dort, wo gleiche (automatisierte) Informationsflüsse

[16] Vgl. Anhang 3

[17] Vgl. Anhang 4

für Personendaten aus der obligatorischen Krankenpflegeversicherung und den VVG-Versicherungen ein Datenmissbrauchspotential bergen, müssen *getrennte Bearbeitungswege* gewählt werden. Auch im Rahmen von Artikel **84*a*** KVG sind, soweit das KVG keine Ausnahme vorsieht, die obgenannten Regeln des DSG zu beachten.

- Im **Rahmen von Reorganisationen und Fusionen** besteht das Risiko, dass *Unberechtigte Zugriff a*uf personenbezogene Daten erhalten, dass zu viel*e* Daten (zu früh oder den falschen Personen) bekannt gegeben werden, oder dass die Personendaten zweckentfremdet zum Einsatz kommen. Es ist deshalb während Reorganisationen und Fusionen in allen Phasen darauf zu achten, dass übertragene Personendaten weiterhin *nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen war (*Art. **4 A**bs. 2 DSG*)*, und dass *nur berechtigte* Personen einen Zugriff auf die Daten erhalten. Entsprechende Empfehlungen des EDÖB zur Datenweitergabe im Rahmen von Unternehmenszusammenschlüssen finden Sie unter folgenden Link:

  http://www.edoeb.admin.ch/themen/00794/01609/01610/index.html?lang=de

Anhang 3: Checkliste Pflichtenheft der/des Datenschutzverantwortlichen

DSG 11*a* Abs. 5 Bst. e / VDSG 12*a* / DSG 8

1. Ziel der Funktion

- Sicherstellen der Einhaltung der gesetzlichen Bestimmungen zum Datenschutz im Krankenversicherungsunternehmen.
- Ansprechperson gegenüber dem EDÖB/BAG.

2. Kompetenzen und Verantwortung:

- Kontrolle der Bearbeitung von Personendaten.
- Vorschlagen von Massnahmen, falls die Gefahr besteht, dass Vorgaben bzw. Weisungen zum Datenschutz verletzt werden.
- Die/der betriebliche Datenschutzverantwortliche übt ihre/seine Funktion fachlich und organisatorisch unabhängig aus, ohne diesbezüglich Weisungen oder Sanktionen des Inhabers der Datensammlung zu unterliegen.
- Sie/er übt keine Tätigkeiten aus, die mit ihren/seinen Aufgaben als Datenschutzverantwortliche/n unvereinbar sind.
- Sie/er verfügt über die zur Erfüllung der Aufgaben erforderlichen Ressourcen.
- Sie/er hat Zugang zu allen Datensammlungen und Datenbearbeitungen sowie zu allen Informationen, die sie/er zur Erfüllung der Aufgaben benötigt: Umfassendes Einsichtsrecht in Dokumente, Vorführungsrecht im Hinblick auf Datenverarbeitungssysteme, Auskunftsrecht gegenüber sämtlichen für die Datenbearbeitungen verantwortlichen Personen.
- Rapportieren der Situation im Datenschutz gegenüber dem Inhaber der Datensammlung (leitendes Organ).

3. Hauptaufgaben:

- Prüfen aller Verträge und Vorhaben, die eine Bearbeitung von Personendaten beinhalten, auf Einhalten der gesetzlichen und der internen Bestimmungen zum Datenschutz. Durchführung einer Risikoanalyse (Risiko einer unbeabsichtigten oder unberechtigten Datenweitergabe, Datenlöschung oder Datenbearbeitung, eines Datenverlustes oder technischen Fehlers). Empfehlung von Korrekturmassnahmen bei Datenschutzverletzungen.
- Ständige Überprüfung und rechtliche Abgleichung der internen Datenschutzbestimmungen mit der Rechtsentwicklung.
- Schulen und Unterstützen der Mitarbeitenden in allen Fragen im Bereich Datenschutz. Sicherstellen eines schnellen Informationsflusses zwischen der/dem Datenschutzverantwortlichen und der betroffenen Abteilung bei Datenschutzverletzungen.
- Sicherstellen der termingerechten und korrekten Beantwortung von Auskunftsbegehren gemäss Datenschutzgesetzgebung.
- Sicherstellen der regelmässigen Aktualisierung der Bearbeitungsreglemente und der Datensammlungen mit besonders schützenwerten Personendaten.
- Führen des Inventars der Datensammlungen im Betrieb. Es wird empfohlen, mittels standardisierten Formulars sämtliche vorhandenen und geplanten Datensammlungen und Datenbearbeitungen zu erheben und damit Bestand, Mutationen und Löschungen der Datensammlungen zu überwachen. Die/der Datenschutzverantwortliche soll zu jeder Zeit einen Überblick darüber haben, welche Daten in welcher Abteilung bzw. in welchem Bereich bearbeitet werden. Das Inventar der Datensammlungen im Betrieb ist dem EDÖB oder betroffenen Personen, die ein entsprechendes Gesuch gemäss Art. 8 DSG stellen, zur Verfügung zu stellen.

Anhang 4: Datenschutzmanagementsysteme und Datenschutzzertifizierungen

DSG 11 + 11*a* Abs. 5 Bst. f / VDSZ

Um den Datenschutz und die Datensicherheit zu verbessern, können die Krankenversicherer bezüglich der Bearbeitung von Personendaten ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen (Art. 11 DSG). Diese unabhängigen Stellen müssen von der Schweizerischen Akkreditierungsstelle SAS anerkannt sein.

Die Zertifizierung im Sinne der Verordnung über die Datenschutzzertifizierungen (VDSZ) basiert auf den Richtlinien des EDÖB über die Mindestanforderungen an das Datenschutzmanagementsystem (DSMS) (Art. 4 Abs. 3 VDSZ) und dem Leitfaden für das Datenschutzmanagement (Anhang zu den Richtlinien), der unter folgender Adresse zugänglich ist:

http://www.edoeb.admin.ch/org/00828/index.html?lang=de

Die Richtlinien stützen sich auf die internationalen Normen für Managementsysteme, insbesondere ISO/IEC 27001:2005.

Die Zertifizierung im Sinne der VDSZ, das heisst also die Einführung und langfristige Aufrechterhaltung eines zuverlässigen und in die Unternehmensprozesse implementierten Datenschutzmanagementsystems (DSMS), führt in der Regel durch einen systematischen Ansatz bei der Bearbeitung von Personendaten zu einer Kostenreduktion. Ausserdem erhöht sie die Sicherheit bei der Verwendung von Personendaten (z. B. bei der Anwendung der Bestimmungen von Artikel 59 KVV bezüglich der Bearbeitung und Aufbewahrung von diagnosebezogenen Daten) und gewährleistet eine konstante Überwachung der Unternehmensprozesse im Bereich des Datenschutzes im Hinblick auf deren kontinuierliche Verbesserung. Schliesslich kann eine Zertifizierung auch dem Image und dem Vertrauen von Partnern, Versicherten, Behörden und offiziellen Instanzen förderlich sein (Qualitätszeichen).

Zudem müssen die Versicherer ihre Datensammlungen nicht beim EDÖB anmelden, wenn sie aufgrund eines Zertifizierungsverfahrens nach Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben haben und das Ergebnis dem EDÖB mitgeteilt haben (Art. 11*a* Abs. 5 Bst. f DSG). Gerade den kleineren Krankenversicherern, welche nicht über einen betrieblichen Datenschutzverantwortlichen verfügen, ist ein Zertifizierungsverfahren zu empfehlen.

Der Entscheid, eine Zertifizierung des Unternehmens als Ganzes oder bestimmter Verfahren bzw. Bereiche durchzuführen, obliegt dem Versicherer. Die Zertifizierung und die Aufrechterhaltung ihrer Gültigkeit erfordern einen gewissen finanziellen und personellen Aufwand.

Die Höhe der Investition für eine Zertifizierung hängt von deren Umfang (das ganze Unternehmen oder nur bestimmte Verfahren bzw. Bereiche) sowie der Grösse und der Organisation des Versicherers ab (zwischen CHF 35'000.00 und CHF 120'000.00 für das Unternehmen als Ganzes und zwischen CHF 25'000.00 und CHF 35'000.00 für einzelne Bereiche). Hinzu kommen die personellen Ressourcen, die zur Ausarbeitung der Zertifizierungsdokumentation und zur Implementierung des Datenschutzmanagementsystems nötig sind (14 bis 45 Personentage für ein mittleres Unternehmen).

Für die Aufrechterhaltung der Gültigkeit ist mit den Kosten für die jährlichen Zwischenaudits (zwischen CHF 8'000.00 und CHF 25'000.00 je nach Grösse des Unternehmens) und den Personalressourcen für die Durchführung der Zwischenaudits (zwischen 1 ½ und 4 ½ Personentage) sowie den Kosten für die regelmässige Aktualisierung der Dokumentation und die periodische Überwachung der korrekten Verwendung des Datenmanagementsystems (internes Audit, Management Review usw. – 2 bis 5

Personentage pro Jahr) zu rechnen. Für die Ausführung dieser Aufgaben sollte der Krankenversicherer eine/n Datenschutzverantwortliche/n[18] bezeichnen (circa 10 bis 25 % Personentage pro Jahr). Ausserdem dürfen die Kosten für die Rezertifizierung (alle drei Jahre) nicht vergessen werden.

Über den folgenden Link können Sie Zertifizierungsstellen suchen, die von der Schweizerischen Akkreditierungsstelle SAS für die Zertifizierung von Managementsystemen akkreditiert sind:

http://www.seco.admin.ch/sas/index.html?lang=de

[18] Vgl. Anhang 3

Anhang 5: Case Management

Sehr viele Personen sind bei Krankenversicherern versichert, die ein Case Management anbieten.

Im Rahmen eines Case Management werden besonders schützenswerte Personendaten bearbeitet. Da die Case Manager sowohl im Interesse der betroffenen Person als auch des Krankenversicherers handeln und sich dabei Interessenskonflikte ergeben können, müssen die **Grundsätze der Zweckbindung und der Transparenz** besonders gewissenhaft beachtet werden. Speziell dabei ist, dass Case Manager von den Krankenversicherern eingesetzt werden, um die durch einen Unfall oder eine Krankheit entstehenden Kosten möglichst gering zu halten, und um die betroffene Person so zu betreuen, dass sie möglichst rasch wieder gesund wird.

Damit die Case Manager die Datenbearbeitung legal vornehmen können, ist es besonders wichtig, dass sie die betroffene Person über ihre Rolle, ihre Ziele, den Zweck der Datenbearbeitung und ihren Auftraggeber, den Krankenversicherer, informieren. Die Personendaten dürfen nur für die Zwecke verwendet werden, welche für die betroffene Person erkennbar sind. Case Manager dürfen sich somit gegenüber der betroffenen Person nicht nur als «Wohltäter/in» in einer schwierigen Situation präsentieren, sondern müssen mit der notwendigen Aufklärung für Transparenz sorgen.

Die fachliche und organisatorische Unterstellung der Case Manager und ihrer Hilfspersonen ist bei vielen Krankenversicherern zu überprüfen und zu korrigieren. *Die Case Manager dürfen nicht mehr in der Leistungsabwicklung eingegliedert sein, sondern sind der Vertrauensärztin oder dem Vertrauensarzt zu unterstellen.* Es ist darauf zu achten, dass die Stellen der Case Manager sowie deren Hilfspersonen bezüglich ihrer fachlichen und organisatorischen Unterstellung sowie ihres Beschäftigungsgrades für das Case Management so konzipiert sind, dass sich daraus *keine Interessenkonflikte* für sie ergeben. Sie dürfen nicht mit verschiedenen Aufgaben betraut werden, die miteinander nicht kompatibel sind.

Anhang 6: Fragebogen zum Gesundheitszustand

BV 5 / KVG 4 Abs. 2 / KVV 6*a* Abs. 1

Fragen zum Gesundheitszustand von Personen, die einen Antrag auf Aufnahme in die obligatorische Krankenpflegeversicherung stellen, widersprechen dem KVG und dem Verhältnismässigkeitsprinzip. Auf diese Weise Gesundheitsdaten zu beschaffen, ist rechtswidrig.

Die Krankenversicherer dürfen sich bei der Aufnahme von versicherungspflichtigen Personen nicht über deren Gesundheitszustand informieren. Dieses Verbot ergibt sich aus der Pflicht nach Artikel 4 Absatz 2 KVG, jede versicherungspflichtige Person aufzunehmen, und aus dem Verhältnismässigkeitsprinzip gemäss Artikel 5 der Bundesverfassung (BV) vom 18. April 1999.

Fragen zum Gesundheitszustand dürfen bei der Aufnahme nur dann gestellt werden, wenn die versicherungspflichtige Person ausdrücklich ihr Interesse bekundet, eine Zusatzversicherung oder eine Taggeldversicherung abzuschliessen. Der entsprechende Fragebogen darf sich nur auf die nicht obligatorischen Versicherungen beziehen und muss dies klar angeben. Diese Beitrittsformulare mit Fragen zur Gesundheit sind strikt von den Beitrittsformularen für die obligatorische Krankenpflegeversicherung zu trennen.

Die Krankenversicherer müssen dafür sorgen, dass die von ihnen beauftragten Versicherungsvermittler sich nicht über den Gesundheitszustand von beitrittsinteressierten Personen informieren.

Wenn auf diese Weise bereits Gesundheitsdaten erhoben worden sind, sind die rechtswidrig beschafften Informationen und gegebenenfalls damit rechtswidrig betriebene Datensammlungen unverzüglich zu vernichten.

Anhang 7: Ermächtigungsklauseln / Generalvollmachten

StGB 321 / ATSG 28 Abs. 3, 33 und 43 Abs. 3 / DSG 3 Bst. c Ziff. 2, 4 Abs. 5 und 12ff / KVG 4 Abs. 2, 42 Abs. 3, 84*a* / KVV 6*a* Abs. 1

1. Vollmacht, Einwilligungsklauseln

Gemäss Artikel 33 ATSG haben die Versicherer gegenüber Dritten Verschwiegenheit zu bewahren. Sie dürfen Daten nur bekannt geben, wenn die in Artikel 84*a* KVG genannten Bedingungen erfüllt sind. Die Leistungserbringer und ihre Hilfspersonen unterstehen dem Berufsgeheimnis (Art. 321 StGB); die anderen Akteure im Gesundheitsbereich (andere Sozialversicherungen, Privatversicherer) unterliegen ebenfalls der Schweigepflicht (Art. 33 ATSG, Art. 12ff DSG). In der Praxis *verlangen viele Krankenversicherer von ihren Versicherten die Unterzeichnung einer Vollmacht, die sie ermächtigt, bei Dritten Informationen einzuholen oder Dritten Informationen bekannt zu geben. Eine solche Vollmacht muss die gesetzlichen Bedingungen einhalten, insbesondere Artikel 4 DSG.* Die Bearbeitung von Daten der versicherten Person ist also nur mit deren *freien und aufgeklärten Einwilligung* zulässig. Die Einwilligung ist aufgeklärt, wenn die Person zum Zeitpunkt der Einwilligung angemessen informiert worden ist, das heisst, wenn sie *in der Lage ist, die Tragweite ihrer Einwilligung abzuschätzen,* bzw. wenn sie erkennen kann, welche Daten weitergegeben werden können, welcher Personenkreis diese Informationen weitergeben darf und/oder welchem Personenkreis diese Informationen weitergegeben werden dürfen und was der Zweck der Datenweitergabe ist. Gesundheitsbezogene Daten sind *besonders schützenswerte Personendaten* im Sinne von Artikel 3 Buchstabe c Ziffer 2 DSG. Ihre Bearbeitung erfordert folglich die *ausdrückliche Einwilligung der versicherten Person* (Art. 4 Abs. 5 DSG).

2. Vollmacht zum Zeitpunkt des Beitritts

Gemäss Artikel 4 Absatz 2 KVG müssen die Krankenversicherer in ihrem Tätigkeitsbereich jede versicherungspflichtige Person aufnehmen, ohne ihren Gesundheitszustand zu berücksichtigen. Gesundheitsfragebogen sind verboten (siehe Anhang 6). Da die Versicherer ermächtigt sind, im Beitrittsformular alle Angaben zu verlangen, die für den Beitritt zur obligatorischen Krankenpflegeversicherung oder bei einem Wechsel des Versicherers erforderlich sind (Art. 6*a* Abs. 1 KVV), *ist eine Vollmacht überflüssig.* Der Versicherer muss alle benötigten Auskünfte von der versicherten Person selbst erhalten.

3. Vollmacht im Leistungsfall

Gestützt auf Artikel 28 Absatz 3 ATSG und vorbehältlich Artikel 42 Absatz 3 KVG *muss sich die Vollmacht immer auf einen bestimmten Leistungsfall beziehen.* Im Dokument, das der Versicherer der versicherten Person zur Unterschrift vorlegt, muss ausdrücklich der Versicherungsfall (Krankheit/Unfall, Datum) angegeben sein, für den die Vollmacht verlangt wird. Eine für zukünftige Leistungsfälle ausgestellte Vollmacht ist nicht gültig.

Die Vollmacht muss das Verhältnismässigkeitsprinzip einhalten: Der Krankenversicherer darf nicht mehr Informationen beschaffen, als er zur Ausübung seiner Aufgaben nach KVG benötigt. Ebenso darf er Dritten nicht mehr Daten bekannt geben, als diese tatsächlich benötigen.
Die Vollmacht kann durch die versicherte Person jederzeit widerrufen werden. Diese muss explizit über ihr Widerrufsrecht informiert werden.

In der Vollmacht anzugeben, dass ein Nichtunterschreiben des Dokuments die Einschränkung oder die Einstellung des Leistungsanspruchs zur Folge hat, ist nicht korrekt. Wenn die versicherte Person sich zu Unrecht weigert, die Vollmacht zu unterschreiben, muss der Versicherer sie schriftlich mah-

nen, um sie an ihre Mitwirkungspflicht zu erinnern und auf die Rechtsfolgen hinzuweisen. Der Versicherer räumt der versicherten Person eine angemessene Bedenkzeit ein (Art. 43 Abs. 3 ATSG).

4. Einwilligung bei Case Management

Bei Versicherungen mit Case Management (siehe Anhang 5) ist die Menge an Daten, die zwischen dem Versicherer, der die Behandlung steuert, und den Leistungserbringern ausgetauscht werden, grösser als bei anderen Versicherungen. Dafür muss die versicherte Person ihre *ausdrückliche Einwilligung* geben.

Die versicherte Person muss genau über die Daten, die weitergegeben werden, die Identität des Empfängers und den Zweck des Datenaustauschs informiert werden. Sie muss die *Einwilligung ausserdem jederzeit widerrufen können, und sie muss über dieses Recht informiert* sein.

Beilage 4

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Kranken- und Unfallversicherung

CH-3003 Bern, BAG

An die KVG-Versicherer

Referenz/Aktenzeichen:
Ihr Zeichen:
Unser Zeichen: Lp
Bern, 17. Juni 2013

Kreisschreiben 7.1, Datenschutzkonforme Organisation und Prozesse der Krankenversicherer

Sehr geehrte Damen und Herren

In der Beilage lassen wir Ihnen das aktualisierte Kreisschreiben 7.1 *Datenschutzkonforme Organisation und Prozesse der Krankenversicherer* und dessen Anhänge 1 - 8 zukommen. Es ersetzt das bisherige Kreisschreiben 7.1. vom 25. August 2011 und berücksichtigt die Änderungen des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung (Art. 42 Abs. 3^{bis} und 4 KVG; SR 832.10) und der Verordnung vom 27. Juni 1995 über die Krankenversicherung (Art. 59 ff KVV; SR 832.102) per 1. Januar 2013. Diese Anpassungen betreffen den Datenschutz im Rahmen der Rechnungsstellung bei einem Vergütungsmodell vom Typus DRG und werden auf den Seiten 2, 5, 6 und 7 des Kreisschreibens sowie in dessen Anhänge 4 und 8 erläutert.

Mit freundlichen Grüssen

Abteilung Versicherungsaufsicht
Die Leiterin

H. Portmann

Helga Portmann

Beilagen : Kreisschreiben 7.1 mit Anhängen 1 - 8

Bundesamt für Gesundheit
Patricia Leiber
Hessstrasse 27E, CH-3003 Bern
Tel. +41 31 322 92 23, Fax +41 31 323 00 60
Patricia.Leiber@bag.admin.ch
www.bag.admin.ch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Kranken- und Unfallversicherung

CH-3003 Bern, BAG

An die KVG Versicherer

Referenz/Aktenzeichen:
Ihr Zeichen:
Unser Zeichen: Lp/NME
Bern, 17. Juni 2013

Kreisschreiben Nr.:	**7.1**
Inkrafttreten:	**1. Juli 2013**

Datenschutzkonforme Organisation und Prozesse der Krankenversicherer

Dieses Kreisschreiben ersetzt das frühere Kreisschreiben 7.1 vom 25. August 2011, *Datenschutzkonforme Organisation und Prozesse der Krankenversicherer*, und berücksichtigt die Änderungen des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung (KVG; SR 832.10) und der Verordnung vom 27. Juni 1995 über die Krankenversicherung (KVV; SR 832.102) per 1. Januar 2013. Es erinnert die Krankenversicherer an die geltenden Datenschutzgrundsätze und -vorgaben. Es soll dazu beitragen, den Datenschutz und die Datensicherheit bei ihren Aktivitäten zu optimieren.

1. Ausgangslage

Die Datenschutzerhebung des BAG/des EDÖB vom 4. Dezember 2007 hat gezeigt, dass die Krankenversicherer für die Datenschutzproblematik sensibilisiert sind, und dass der Schutz der Daten trotz sehr unterschiedlicher Organisationsstrukturen über weite Strecken sichergestellt ist. Mit der Erhebung wurde aber auch festgestellt, dass in einigen sensiblen Bereichen noch Verbesserungspotential besteht. Mit der Veröffentlichung der Ergebnisse der Datenschutzerhebung wurden sinngemäss folgende Empfehlungen abgegeben:

Bundesamt für Gesundheit
Hessstrasse 27E, CH-3003 Bern
Postadresse: CH-3003 Bern
Tel. +41 31 323 70 66, Fax +41 31 323 00 60
www.bag.admin.ch

- Das BAG empfiehlt den Krankenversicherern, ein Datenschutzkonzept (eine Strategie) zu erarbeiten.
- Die Krankenversicherer sind verpflichtet, ein Verzeichnis der Datensammlungen zu unterhalten. Für jede Datensammlung mit besonders schützenswerten Personendaten ist ein Bearbeitungsreglement zu unterhalten (Beschreibung der Prozesse inkl. Verantwortlichkeiten, Berechtigungen, Datenfluss sowie der technischen Massnahmen zur Datensicherheit).
- Das BAG empfiehlt den Krankenversicherern, eine verantwortliche Person für den Datenschutz zu bezeichnen. Die Aufgaben dieses Verantwortlichen sind in einem Pflichtenheft zu umschreiben.
- Datenschutzverantwortliche müssen über die erforderlichen Fachkenntnisse verfügen.
- Es sollen von einer dafür spezialisierten Stelle regelmässig externe Datenschutzaudits durchgeführt und die Resultate den Aufsichtsbehörden unterbreitet werden.

Das BAG geht davon aus, dass die Krankenversicherer in der Zwischenzeit weitere Massnahmen zur Verbesserung der Datenschutzkonformität ihrer Organisation und / oder ihrer Prozesse eingeleitet haben bzw. dies noch tun werden. Zur Förderung dieser Entwicklung weist das vorliegenden Kreisschreiben und dessen Anhänge 1 - 8 die Krankenversicherer auf die für sie geltenden Datenschutzbestimmungen hin, welche sich aus den verschiedenen Bundeserlassen[1] ergeben. Neue Datenschutzbestimmungen sind mit fetter Schrift hervorgehoben.

In Zusammenhang mit der Einführung der diagnosebezogenen Fallpauschalen (SwissDRG) im Rahmen der neuen Spitalfinanzierung hat der Bundesrat am 4. Juli 2012, mit Inkrafttreten per 1. Januar 2013, die Artikel 59 ff KVV angepasst. Diese Anpassungen betreffen insbesondere den Datenschutz im Rahmen der Rechnungsstellung bei einem Vergütungsmodell vom Typus DRG und werden im neuen Anhang 8 erläutert.

2. Datenschutz- und Datensicherheitskonzept

KVG Art. **84*b*** (Inkrafttreten am 1.1.2012) / DSG 2, 3, 4, 5, 7/ VDSG 8 -10, 20 + 21

Das BAG empfiehlt allen Krankenversicherern, ein umfassendes ganzheitliches **Datenschutz- und Sicherheitskonzept** zu erarbeiten. Datensicherheit ist ein wesentlicher Bestandteil des Datenschutzes.

Ein Datenschutz- und Sicherheitskonzept gibt Auskunft über die mittel- und langfristige Strategie zur Umsetzung des Datenschutzes und der Datensicherheit im Betrieb. Es beschreibt die Organisation des Datenschutzes. Zudem leiten sich daraus insbesondere die Aufgaben der Personen ab, die innerhalb des Krankenversicherers für den Datenschutz verantwortlich und für die Datensammlungen zuständig sind.

Ein solches Konzept ist zwar gesetzlich nicht vorgeschrieben, es ist aber ein wichtiger Grundstein für den Datenschutz und die Datensicherheit im Betrieb. Gestützt darauf kann der Datenschutz betriebsintern in die Geschäftsabläufe integriert werden. Das Datenschutz- und Sicherheitskonzept bzw. Teile davon kann anschliessend in Richtlinien für die Mitarbeitenden, Sicherheits- und Informationsschutzrichtlinien für die Informatik und andere Bereiche sowie in *Bearbeitungsreglementen* (Art. 11 und 21 VDSG, Art. **84*b*** KVG) umgesetzt werden.

[1] Vgl. Anhänge 1 + 2

Die Umsetzung des Datenschutz- und Sicherheitskonzepts kann auch *technische und organisatorische Massnahmen* erfordern. Die Krankenversicherer müssen hierfür die erforderlichen Mittel bereitstellen (Art. 7 DSG).

Ein Leitfaden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes sowie Angaben, was in einem Bearbeitungsreglement aufgeführt werden muss, ist unter folgenden Link abrufbar:

http://www.edoeb.admin.ch/dokumentation/00445/00472/00935/index.html?lang=de

3. Bearbeitungsreglemente

KVG **84*b*** (Inkrafttreten am 1.1.2012) / VDSG 21

Artikel 21 VDSG schreibt den Krankenversicherern vor, *für automatisierte Datensammlungen*, die *besonders schützenswerte Daten und Persönlichkeitsprofile enthalten*, oder mit anderen Datensammlungen verknüpft sind, ein Bearbeitungsreglement zu erstellen. Dieses Reglement beinhaltet Angaben über die interne Organisation des Krankenversicherers, sowie über die Struktur, in welche die Datensammlung oder das automatisierte Bearbeitungssystem eingebettet ist. Es beschreibt die Datenbearbeitungs- und *Kontrollprozeduren*, und enthält alle Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung und der eingesetzten Informatikmittel. Es regelt namentlich *Art und Umfang der Zugriffsberechtigung auf Personendaten*. Das Reglement muss regelmässig angepasst bzw. nachgeführt werden und dem EDÖB in verständlicher Form jederzeit zur Verfügung stehen.

Das Sicherstellen der *Vollständigkeit* und der *Aktualität* der Bearbeitungsreglemente ist eine Hauptaufgabe der/des *Datenschutzbeauftragten* des Krankenversicherers und dient als eigentliche Grundlage für den gesetzeskonformen Betrieb bzw. die gesetzeskonforme Nutzung einer Datensammlung mit schützenswerten Personendaten.

Artikel **84*b*** KVG wiederholt und verdeutlicht diese bereits gemäss VDSG bestehenden Verpflichtungen der Krankenversicherer, präzisiert jedoch zusätzlich, dass die Bearbeitungsreglemente dem EDÖB *zur Beurteilung vorzulegen sind* und *öffentlich zugänglich* sein müssen.

Aufgrund dieser neuen Vorgaben müssen die Krankenversicherer ab dem 1. Januar 2012 ihre Bearbeitungsreglemente dem EDÖB *unaufgefordert zur Beurteilung vorlegen.* Das Bearbeitungsreglement ist aber bereits gültig, wenn der Krankenversicherer es für verbindlich erklärt hat.

Überdies müssen die Krankenversicherer die Bearbeitungsreglemente ab dem 1. Januar 2012 veröffentlichen. Sie haben diese den *interessierten Personen* mittels Publikation auf dem Internet oder in anderer Form zugänglich zu machen. Die Pflicht zur Veröffentlichung besteht dabei unabhängig von einer durch den EDÖB durchgeführten Beurteilung.

Ein Bearbeitungsreglement kann für mehrere Datensammlungen gültig sein, wenn das Reglement tatsächlich für die bezeichneten Datensammlungen zur Anwendung gelangt und für jede betreffende Datensammlung die Erfordernisse von Artikel 21 Absatz 2 VDSG erfüllt.

4. Verzicht auf die Anmeldung der Datensammlungen - Meldung einer für den Datenschutz verantwortlichen Person

DSG 11*a* Abs. 5 Bst. e / VDSG 12*a*

Das DSG ermöglicht die Selbstregulierung der Unternehmen im Bereich Datenschutz: Es liegt in der Verantwortung des Krankenversicherers, dafür zu sorgen, dass die Grundsätze und Vorgaben der Datenschutzgesetzgebung eingehalten werden. Der Krankenversicherer ist als Inhaber der Datensammlung von der Pflicht zur Anmeldung der Datensammlungen befreit, wenn er eine für den **betrieblichen Datenschutz verantwortliche Person** bezeichnet hat, die *unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht, Verzeichnisse der Datensammlungen führt* und diese Person *dem EDÖB gemeldet* hat.

Die für den betrieblichen Datenschutz verantwortliche Person ist entgegen der Bezeichnung nicht verantwortlich für den Datenschutz im Betrieb, sondern hat die *Rolle einer Beraterin oder eines Beraters*, bzw. einer Aufsichtsstelle (vgl. die französische Version im DSG: conseiller à la protection des données). Die Verantwortung für die Einhaltung der Bestimmungen zum Datenschutz bleibt in jedem Fall beim Inhaber der Datensammlung, also beim Krankenversicherer bzw. bei dessen leitenden Organ (Art. 16 Abs. 1 DSG).

Die oder der Datenschutzverantwortliche muss ihre/seine Funktion *organisatorisch und fachlich unabhängig* ausüben können, und ein möglicher Interessenkonflikt muss bereits durch ihre/seine organisatorische Stellung vermieden werden. Deshalb sollte ihre/seine Stelle ausserhalb der Linienverantwortlichkeit stehen. Empfohlen wird eine Stabstelle, eine Stelle in der Rechtsabteilung oder in der IT-Abteilung oder eine externe Stelle. Die Rolle und Funktion der für den Datenschutz verantwortlichen Person ist in einem *Pflichtenheft* zu definieren.

Weiterführende Informationen finden Sie im Anhang 3 und in den Empfehlungen des EDÖB unter folgenden Link:

http://www.edoeb.admin.ch/themen/00794/01609/01611/index.html?lang=de

5. Outsourcing

KVG 84 / DSG 10*a*

Outsourcing umfasst die Auslagerung von Dienstleistungen, die bisher von den Krankenversicherern selber erbracht wurden, sowie Dienstleistungen, welche die Krankenversicherer selber bisher nicht erbracht haben und die sie neu von einem Dienstleister beziehen.

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die *Daten nur so bearbeitet werden, wie es der Krankenversicherer selber tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht dies verbietet* (Art. 10*a* DSG). Artikel 84 KVG erlaubt den Krankenversicherern, Personendaten einschliesslich besonders schützenswerter Daten und Persönlichkeitsprofile durch Dritte bearbeiten zu lassen.

Der Krankenversicherer hat den Dienstleister sorgfältig auszuwählen, zu instruieren und zu überwachen. Schnittstellen, Verantwortlichkeiten, Zuständigkeiten und Haftungsfragen sind vertraglich genau zu regeln bzw. abzugrenzen. Die ausgelagerte Funktion ist in das interne Kontrollsystem des Krankenversicherers zu integrieren.

Im Vertrag ist der Bearbeitungszweck für die Daten genau zu umschreiben und der Dienstleister zu verpflichten, die Daten *nur zweck- und weisungsgebunden zu bearbeiten*. Damit ist die Verwendung für eigene oder fremde Zwecke des Dienstleisters ausgeschlossen. Der Dienstleister ist mitsamt den Mitarbeitenden funktionell in die *Schweigepflicht* und das bereichsspezifische Datenschutzrecht des Krankenversicherers einzubinden. Die Mitarbeitenden des Dienstleisters sind vertraglich und nötigenfalls einzelunterschriftlich zur Geheimhaltung zu verpflichten.

Der Krankenversicherer muss sich vergewissern, dass der Dienstleister die *Datensicherheit und den Datenschutz gewährleistet*. Die Sicherheitsstandards für den Datenaustausch und die Sicherheitsanforderungen, die der Dienstleister zu erfüllen hat, müssen schriftlich definiert werden. *Personendaten der Versicherten müssen durch angemessene, technische, personelle und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden*. Der Dienstleister muss den Datenschutz jederzeit gewährleisten können (vgl. Art. 7 DSG; Art. 8 und 9 VDSG). Der Vertrag muss die Konsequenzen bei Nichteinhaltung der Datenschutzklauseln und bei Auflösung des Vertrags enthalten (Konventionalstrafen, sofortige Sicherstellung von Daten, Auflösung des Vertrags, vollständige Vernichtung der Daten).

Der Dienstleister muss den Krankenversicherer regelmässig über die Datenbearbeitung informieren. Der auslagernde Krankenversicherer, dessen interne und externe Revisionsstelle sowie das BAG müssen den ausgelagerten Geschäftsbereich vollumfänglich, jederzeit und ungehindert einsehen und prüfen können. Der Krankenversicherer muss sich die Einsichts-, Weisungs- und Kontrollrechte vom Dienstleister vertraglich einräumen lassen, damit er ein ordnungsgemässes Controlling gegenüber dem Dienstleister wahrnehmen kann.

Die *Auskunftspflicht des Krankenversicherers* gegenüber den betroffenen Personen bleibt bestehen, da er auch Inhaber der Datenbank bleibt, wenn Personendaten durch einen Dritten bearbeitet werden (Art. 8 Abs. 4 DSG). Der Krankenversicherer muss deshalb jederzeit Zugriff auf die Daten haben, was durch den Dienstleister sicherzustellen ist.

Der Krankenversicherer muss sowohl im Vertrag über den vom Outsourcing betroffenen Bereich als auch im Sicherheitsdispositiv die nötigen Vorkehren treffen, die ihn vor einem plötzlichen und unerwarteten Ausstieg des Dienstleisters schützen und die Weiterführung des ausgelagerten Geschäftsbereichs mit der notwendigen Datensicherheit erlauben.

Aus diesem Grund ist, wenn immer möglich, auf das Outsourcing datensensibler Bereiche ins Ausland zu verzichten. Sollte dies ausnahmsweise der Fall sein, so ist Artikel 6 DSG besonders zu beachten (grenzüberschreitende Datenbekanntgabe nur unter bestimmten Voraussetzungen und unter Einbezug des EDÖB).

Der Krankenversicherer trägt als Inhaber der Datensammlung weiterhin die volle datenschutzrechtliche Verantwortung für den ausgelagerten Geschäftsbereich. Die Krankenversicherer müssen die Versicherten über ihre Outsourcingpraxis hinreichend informieren.

Diese Ausführungen gelten mit Ausnahme des Absatzes über die Einsichts- und Kontrollrechte des Versicherers insbesondere auch für einen Versicherer, welcher für die Umsetzung der Datenannahmestelle nach Art. **59*a*** KVV einen externen zertifizierten Dienstleister in Anspruch nimmt (vgl. Anhang 8). Die oben erwähnten Einsichts-, Weisungs- und Kontrollrechte des Versicherers gelten gegenüber der Datenannahmestelle nicht, da es sich nicht um ein freiwilliges Outsourcing des Versicherers, sondern um die Erfüllung einer gesetzlichen Pflicht zur Stärkung des Datenschutzes handelt. Der Versicherer kann gegenüber der Datenannahmestelle keine Weisungen bezüglich der Datenweitergabe auf einzelne Rechnungen erteilen. Daraus ergibt sich, dass der Versicherer nicht über Kontroll- oder Einsichtsrechte zu Daten kommen darf, deren Geheimhaltung durch die Datenannahmestelle sichergestellt wird.

6. Unabhängigkeit der Vertrauensärztin / des Vertrauensarztes und des vertrauensärztlichen Dienstes

STGB 321 / KVG 57, 56, 42 Abs. 5

Die Vertrauensärztin oder der Vertrauensarzt gemäss Artikel 57 KVG ist ein *besonderes Organ der sozialen Krankenversicherung*. Ihre/seine Aufgaben werden in Artikel 57 Absätze 4 und 5 KVG umschrieben. Danach berät sie/er den Versicherer in medizinischen Fachfragen sowie in Fragen der Vergütung und der Tarifanwendung. Zudem kommt ihr/ihm eine Überwachungs- und Kontrollfunktion zu. Sie/er überprüft die Voraussetzungen der Leistungspflicht des Versicherers (Art. 57 Abs. 4 KVG). Ihr/ihm obliegt die Kontrolle der Wirksamkeit, Zweckmässigkeit und Wirtschaftlichkeit der Behandlung im Sinn von Artikel 32 und Artikel 56 KVG. Ihre/Seine Kompetenz beschränkt sich auf die *Beantwortung medizinischer Fachfragen*. In fachlicher Hinsicht kann ihr/ihm der Versicherer nichts vorschreiben. In ihrem/seinem Urteil *unabhängig*, darf sie/er den zuständigen Stellen der Versicherer nur diejenigen Angaben weitergeben, die *notwendig* sind, um über die Leistungspflicht zu entscheiden, die Vergütung festzusetzen, den Risikoausgleich zu berechnen oder eine Verfügung zu begründen. Dabei wahrt sie/er die Persönlichkeitsrechte der Versicherten (Art. 57 **Abs. 7** KVG, Inkrafttreten am 1.1.2012). Der Leistungserbringer ist in *begründeten Fällen berechtigt* und auf Verlangen der versicherten Person *in jedem Fall verpflichtet,* medizinische Angaben *nur der Vertrauensärztin oder dem Vertrauensarzt* bekannt zu geben (Art. 42 Abs. 5 KVG).

Die gesetzlich vorgeschriebene Unabhängigkeit der Vertrauensärztin oder des Vertrauensarztes muss sich auch in der *Organisation des vertrauensärztlichen Dienstes (VAD)* niederschlagen. Diese Unabhängigkeit verlangt *eigene Bearbeitungsreglemente*, die klar umreissen, welche Kompetenzen und Aufgaben den einzelnen Vertrauensärztinnen und -ärzten und ihren Hilfspersonen zukommen.

Räumlich müssen Lokale des VAD genügend abgetrennt und abschliessbar sein. Die Post darf nur durch Stellen des VAD geöffnet werden und es muss jederzeit sichergestellt sein, dass besonders schützenswerte Personendaten den VAD nicht verlassen können. Ein unabhängiges Telefon- und Telefaxnetz ist unabdingbar. Das Informatiksystem muss physisch so organisiert werden, dass die vom VAD erstellten Dokumente nur auf eigenen Speichermedien archiviert werden, die wiederum nur den Mitarbeitern des VAD zugänglich sind. Der Vertrauensärztin oder dem Vertrauensarzt muss zudem die Kompetenz zur Anstellung ihres/seines Hilfspersonals zukommen. Sie/er hat darauf zu achten, dass die Stellen der Hilfspersonen bezüglich ihrer *fachlichen und organisatorischen* Unterstellung sowie ihres *Beschäftigungsgrades* für den VAD so konzipiert sind, dass sich daraus *keine Interessenkonflikte* für die Hilfspersonen ergeben. Die Hilfspersonen dürfen nicht mit verschiedenen Aufgaben betraut werden, die miteinander nicht kompatibel sind (z.B. für den VAD und die Leistungsabteilung).

Die Vertrauensärztin oder der Vertrauensarzt und ihre Hilfspersonen machen sich strafbar, wenn sie das Berufsgeheimnis gemäss *Artikel 321 des Strafgesetzbuchs (StGB)* verletzen. Benützt eine Hilfsperson die bei ihrer Tätigkeit für den Vertrauensarzt erhaltenen Personendaten für eine andere Tätigkeit beim selben oder bei einem anderen Versicherer, macht sie sich strafbar.

Vertrauensärzte und Vertrauensärztinnen nach Artikel 57 KVG sollten zur Vermeidung des Vorwurfs einer Risikoselektion keine Risikoprüfung bei neuen Versicherungsverträgen nach VVG vornehmen.

7. Substantiierung bei der Rechnungsstellung

KVG 42 **Abs. 3 - 5** / KVG 57 Abs. 4 und 6 / KVV **59**, ***59a***, ***59a*^bis**

Artikel 42 Absatz 3 KVG hält fest, dass der Leistungserbringer dem Schuldner eine detaillierte und verständliche Rechnung zustellen muss (Satz 1). Er muss ihm alle Angaben machen, die er benötigt, um die Berechnung der Vergütung und die Wirtschaftlichkeit der Leistung überprüfen zu können (Satz 2). Insbesondere verlangt Artikel 42 **Absatz 3^bis** KVG, dass die Leistungserbringer auf der Rechnung nach Absatz 3 die Diagnosen und Prozeduren nach den aktuellen Klassifikationen kodiert aufführen (für die Umsetzung dieser Bestimmung bezogen auf die Rechnungsstellung bei einem Vergütungsmodell vom Typus DRG vgl. Art. **59*a*** KVV und Anhang 8).

Für die systematische Übermittlung von Diagnosen und Prozeduren in anderen stationären Behandlungsbereichen und für den ganzen ambulanten Behandlungsbereich fehlen zurzeit die ausführenden Bestimmungen zur Erhebung, Bearbeitung und Weitergabe der Daten unter Wahrung des Verhältnismässigkeitsprinzips (Art. **59*a*^bis** KVV).

Im Weiteren sieht Artikel 42 Absatz 4 KVG vor, dass der Krankenversicherer zusätzliche Auskünfte medizinischer Natur verlangen kann. Nach Artikel 42 Absatz 5 KVG ist der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur der Vertrauensärztin oder dem Vertrauensarzt des Krankenversicherers bekannt zu geben. Dies setzt voraus, dass der Krankenversicherer die versicherte Person darüber informiert, dass er zusätzliche Auskünfte medizinischer Natur vom Leistungserbringer anfordern wird, welche der Leistungserbringer auf Verlangen der versicherten Person nur der Vertrauensärztin oder dem Vertrauensarzt des Krankenversicherers bekannt geben darf .

In diesen Fällen müssen die Leistungserbringer den Vertrauensärztinnen und –ärzten die zur Erfüllung ihrer Aufgaben notwendigen Angaben liefern (Art. 57 Abs. 6 Satz 1 KVG). Diese Aufgaben beinhalten insbesondere die Beratung des Versicherers in Fragen der Vergütung und Tarifanwendung sowie die Überprüfung der Voraussetzung der Leistungspflicht (Art. 57 Abs. 4 KVG). Gemäss Kommentarliteratur schreiben alle diese Bestimmungen gegenüber den Leistungserbringern eine Offenbarungspflicht sowie eine Offenbarungsermächtigung vor. Der Leistungserbringer wird bei den Tatbeständen von Artikel 42 Absatz 3 Satz 2, **Absatz 3^bis Satz 1** und **Absatz 4** KVG sowie Artikel 57 Absatz 6 Satz 1 KVG im Verhältnis zum Krankenversicherer von seinem Berufsgeheimnis befreit. Die Offenbarung steht nicht im Belieben des Leistungserbringers, sondern ist gegenüber dem Krankenversicherer gesetzliche Pflicht[2]. Diese Bestimmungen, welche die Leistungserbringer verpflichten, alle leistungsrechtlich relevanten Daten bekannt zu geben, haben eine grosse Tragweite. Die Krankenversicherer sind deshalb berechtigt, eine substantiierte Rechnungsstellung im Sinne dieser Ausführungen zu verlangen und bis zu deren Erhalt keine Zahlung zu leisten.

8. Weiteres Vorgehen

Das BAG wird die Einhaltung der Vorgaben zum Datenschutz und zur Datensicherheit gemäss diesem Kreisschreiben weiterhin im Rahmen regelmässiger Kontrollen durch die Sektion Audit prüfen. Im Hinblick auf die Einführung der Spitalfinanzierung sind zusätzliche Sonderaudits mit Stichproben zum Umgang der Krankenversicherer mit den diagnosebezogenen Personendaten ihrer Versicherten geplant.

Im Vorfeld dieser Untersuchungen weisen wir die Krankenversicherer speziell darauf hin, dass die

[2] Datenschutz im Gesundheitswesen, éditeur: B. Hürlimann/R. Jacobs/T. Poledna, Kapitel Datenschutz in der obligatorischen Krankenpflegeversicherung de G. Eugster/R. Luginbühl, p. 98 sv, Schulthess 2001

Verletzung der Schweigepflicht (Art. 33 ATSG) durch Personen, die an der Durchführung der sozialen Krankenversicherung beteiligt sind, als strafbares Verhalten (Vergehen) geahndet wird (Art. 92 Bst. c KVG) und dass die Missachtung gesetzlicher Datenschutzvorschriften nach Art und Schwere der Mängel Sanktionen nach Artikel 21 Absätze 5 und 5 ^{bis} KVG nach sich zieht. Dies beinhaltet auch die Möglichkeit zur Publikation der Massnahmen.

Direktionsbereich Kranken- und Unfallversicherung
Die Leiterin a.i.

Sandra Schneider

Abteilung Versicherungsaufsicht
Die Leiterin

H. Portmann

Helga Portmann

Beilagen: Anhänge 1 - 8

Anhang 1: Gesetzliche Grundlagen mit den massgebenden Datenschutzbestimmungen

- Bundesgesetz vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1)
- Verordnung vom 11. September 2002 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSV, SR 830.11)
- Bundesgesetz vom 18. März 1994 über die Krankenversicherung (KVG, SR 832.10)
- Verordnung vom 27. Juni 1995 über die Krankenversicherung (KVV, SR 832.102)
- Verordnung vom 12. April 1995 über den Risikoausgleich in der Krankenversicherung (VORA, SR 832.112.1)
- Verordnung vom 14. Februar 2007 über die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK; SR 832.105)
- Verordnung des Eidgenössischen Departements des Innern (EDI) vom 29. September 1995 über Leistungen in der obligatorischen Krankenpflegeversicherung (KLV, SR 832.112.31)
- Verordnung des EDI vom 20. März 2008 über die technischen und grafischen Anforderungen an die Versichertenkarte für die obligatorische Krankenpflegeversicherung (VVK-EDI, SR 832.105.1)
- **Verordnung des EDI vom 13. November 2012 über den Datenaustausch für die Prämienverbilligung (VDPV-EDI, SR 832.102.2)**
- **Verordnung des EDI vom 20. November 2012 über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern (SR 832.102.14)**
- Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1)
- Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11)
- Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (VDSZ, SR 235.13)

Anhang 2: Kommentar zu den massgebenden Datenbearbeitungsgrundsätzen und -vorgaben

ATSG 28, 31, 32, 33, 47 / ATSV 8, 9 / KVG 42 **Abs. 3-5**[3], 42*a*, **57 Abs**. 6, **7**[4] und 8, 82, **84**[5], **84*a***[6], **84*b***[7], 92 / KVV 6*a*, **28** und **28*a***[8], **59**[9], 59*a*[10] **ff,** 76, 120 / DSG 2, 3, 4, 5, 7, 8, **9**[11], 10*a*, 11, 11*a*, 16, 17, **18*a***[12], **18*b***[13], 19, 20, 22, 25, 27, 35 / VDSG 1, 2, 8, 9, 10, 12*a*, 12*b*, 16, 18, 20, 21, 22, 23, **24**[14], 28, 34, 35 / VDSZ

- Krankenversicherer, welche die obligatorische Krankenpflegeversicherung und die freiwillige Taggeldversicherung nach dem KVG durchführen, sind im Rahmen der gesetzlichen Bestimmungen befugt, besonders schützenswerte Personendaten[15] und Persönlichkeitsprofile[16] der Versicherten zu bearbeiten oder bearbeiten zu lassen. So z.B. gestützt auf Artikel **42 Absätze 3-5**, Artikel 42*a*, Artikel 56, Artikel 57 Absätze 4, 6 und 7, Artikel 58 Absatz 3, Artikel **59**, 82, 83, **84, 84*a*** und **84*b*** KVG. Dabei sind sie an die datenschutzrechtlichen Grundsätze wie das *Legalitätsprinzip*, das *Verhältnismässigkeitsprinzip*, das *Zweckbindungsgebot*, den *Grundsatz von Treu und Glauben*, das *Transparenzprinzip*, die *Datenrichtigkeit* und die *Datensicherheit* gebunden (Art. 4, 5, 7 DSG).

- Als Durchführungsorgane der sozialen Krankenversicherung nehmen die Versicherer eine öffentliche Aufgabe des Bundes im Sinne von Artikel 2 Absatz 1 Buchstabe b und Artikel 3 Buchstabe h DSG wahr und sind als solche dem **Legalitätsprinzip** unterstellt, das Folgendes vorsieht: Werden Personendaten durch die Versicherer bearbeitet, ist eine gesetzliche Grundlage nötig. *Besonders schützenswerte Personendaten und Persönlichkeitsprofile* im Sinn von Artikel 3 DSG dürfen nur bearbeitet werden, wenn ein formelles Gesetz dies ausdrücklich vorsieht. *Im Einzelfall* können solche Daten auch bearbeitet werden, wenn die betroffene Person *eingewilligt* hat oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 4 Abs. 1 und Art. 17 Abs. 2 Bst. c DSG). Im KVG bildet insbesondere Artikel **84** die formellgesetzliche Grundlage für die Datenbearbeitung. Demnach dürfen die Versicherer Personendaten nur im Rahmen der ihnen nach dem KVG übertragenen Aufgaben bearbeiten (Art. **84** KVG). Unter den nicht abschliessend aufgeführten Durchführungsaufgaben wird neu auch die Berechnung des verfeinerten Risikoausgleichs (Inkrafttreten per 1.1.2012) aufgeführt (Art. **84 Bst. i** KVG).

- Der **Grundsatz der Bearbeitung nach Treu und Glauben** (Art. 4 Abs. 2 DSG) erfordert, dass die Datenbearbeitung für die betroffene Person *transparent* sein muss, d.h. dass eine

---

[3] Art. 42 Abs. 3**bis** und 4 KVG: in Kraft seit 1.1.2013

[4] Art. 57 Abs. 7 KVG (Ergänzung): in Kraft seit 1.1.2012

[5] Art. 84 Einleitungssatz und Bst. i KVG (Ergänzung): in Kraft seit 1.1.2012

[6] Art. 84*a* Abs. 1 Einleitungssatz und Bst. f : in Kraft seit 1.1.2009

[7] Art. 84*b* KVG (neu): in Kraft seit 1.1.2012

[8] Art. 28 und 28*a* KVV: in Kraft seit 1.1.2009

[9] Art. 59 KVV, verschiedene Absätze in Kraft seit 1.1.2009 bzw. 1.1.2010 bzw. 1.1.2013

[10] Art. 59*a*, 59*a*bis, 59*a*ter, KVV: in Kraft seit 1.1.2013

[11] Art. 7*a* DSG (aufgehoben) und Art. 9 DSG (Änderung) per 1.12.2010

[12] Art. 18*a* DSG (neu):In Kraft seit 1.12.2010

[13] Art. 18*b* DSG (neu):In Kraft seit 1.12.2010

[14] Art. 24 VDSG (Änderung) per 1.12.2010

[15] Art. 3 DSG: Besonders schützenswerte Personendaten sind Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen.

[16] Art. 3 DSG: Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Datenbeschaffung und jede weitere Datenbearbeitung grundsätzlich für die betroffene Person *erkennbar* sein muss, die betroffene Person also aus den Umständen heraus damit rechnen musste oder sie entsprechend informiert bzw. aufgeklärt wird. Die betroffenen Personen sind über die Beschaffung und Bearbeitung von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen zu informieren (Art. **14** DSG).

- Das **Verhältnismässigkeitsprinzip** verlangt, dass nur diejenigen Personendaten beschafft und bearbeitet werden, welche *für einen bestimmten Zweck objektiv tatsächlich benötigt und geeignet* sind (Art. 4 Abs. 2 DSG). Daten dürfen nicht über den gesetzlich zugelassenen Umfang und die gesetzlich zulässige Dauer aufbewahrt werden.

- Personendaten dürfen *nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist* (**Zweckbindungsgebot**; Art. 4 Abs. 3 DSG). Die Personendaten dürfen nicht für andere als die ursprünglichen Zwecke bearbeitet werden.

- Wer Daten bearbeitet, hat sich zu vergewissern, dass diese richtig sind (**Wahrheitsgebot**; Art. 5 Abs. 1 DSG) und die von der Datenbearbeitung betroffenen Personen haben das *Recht, eine Berichtigung* von unrichtigen Daten zu verlangen (Art. 5 Abs. 2 DSG). Weiter haben diese das Recht, über *alle* diese Daten Auskunft zu verlangen (Art. 8 DSG). Die versicherte Person hat somit - unabhängig von einem Interessennachweis und jederzeit - das Recht, eine Kopie des gesamten Dossiers des Versicherers zu erhalten.

- Die Krankenversicherer müssen *ein Verzeichnis sämtlicher* ***Datenbanken*** *führen* und diese beim EDÖB *zur Registrierung anmelden* (Art. 11*a* DSG, Art. 16 VDSG). Sie sind von dieser Verpflichtung befreit, wenn sie eine für den *betrieblichen Datenschutz verantwortliche Person* bezeichnet haben, die *unabhängig* die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt[17], oder wenn sie aufgrund eines *Zertifizierungsverfahrens* nach Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben haben und das Ergebnis der Bewertung dem EDÖB mitgeteilt haben (Art. 11*a* Abs. 2 und 5 Bst. e und f DSG)[18].

- Das Personal der Krankenversicherer untersteht gemäss Artikel 33 ATSG der **Schweigepflicht**. Ein Verstoss gegen diese Norm hat strafrechtliche Konsequenzen zur Folge (Art. 92 Bst. c KVG). Zudem ist der Zugriff der berechtigten Angestellten des Krankenversicherers auf diejenigen Personendaten zu beschränken, welche diese zur Erfüllung ihrer klar umschriebenen Aufgaben benötigen (Art. 9 Abs. 1 Bst. g VDVG). Zusätzlich sind die *Vertrauensärztin oder der Vertrauensarzt und ihr Hilfspersonal* an die Schweigepflicht gemäss Artikel 321 des Strafgesetzbuchs (StGB; SR 311.0) und somit an das **Patientengeheimnis** gebunden.

- Die **Weitergabe von Personendaten** an externe Stellen ist nur in einem *sehr beschränkten Rahmen* zulässig. Zu beachten sind dabei die Artikel **84*a*** KVG (Datenbekanntgabe) in Abweichung von Artikel 33 ATSG (Schweigepflicht) und Artikel 82 KVG (besondere Amts- und Verwaltungshilfe) ebenfalls in Abweichung zu Artikel 33 ATSG, Artikel 120 KVV (Informationspflicht der Krankenversicherer über die Datenbekanntgabe und geleistete Amts- und Verwaltungshilfe), Art. 32 Abs. 2 ATSG (Amts- und Verwaltungshilfe) sowie Artikel 47 ATSG (Akteneinsicht). Artikel **84*a*** KVG regelt, unter welchen abschliessenden Voraussetzungen die in dieser Bestimmung genannten Organe (und nur diese) in Abweichung von der Schweigepflicht (Art. 33 ATSG) Personendaten genau definierten Dritten offenbaren dürfen. Eine andere Versicherungsgesellschaft, die die Versicherungen nach VVG anbietet, *ist eine Dritte* im Sinn von Art. 84*a* Abs. 5 KVG. Bietet der Krankenversicherer selber solche Versicherungen nach VVG

[17] Vgl. Anhang 3

[18] Vgl. Anhang 4

an, gelten die ob genannten Grundsätze, so insbesondere die Bearbeitung nach Treu und Glauben und das Zweckbindungsgebot. Dort, wo gleiche (automatisierte) Informationsflüsse für Personendaten aus der obligatorischen Krankenpflegeversicherung und den VVG-Versicherungen ein Datenmissbrauchspotential bergen, müssen *getrennte Bearbeitungswege* gewählt werden. Auch im Rahmen von Artikel **84*a*** KVG sind, soweit das KVG keine Ausnahme vorsieht, die ob genannten Regeln des DSG zu beachten.

- Im **Rahmen von Reorganisationen und Fusionen** besteht das Risiko, dass *Unberechtigte Zugriff a*uf personenbezogene Daten erhalten, dass zu viele Daten (zu früh oder den falschen Personen) bekannt gegeben werden, oder dass die Personendaten zweckentfremdet zum Einsatz kommen. Es ist deshalb während Reorganisationen und Fusionen in allen Phasen darauf zu achten, dass übertragene Personendaten weiterhin *nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen war (*Art. 4 *A*bs. 2 DSG*)*, und dass *nur berechtigte* Personen einen Zugriff auf die Daten erhalten. Entsprechende Empfehlungen des EDÖB zur Datenweitergabe im Rahmen von Unternehmenszusammenschlüssen finden Sie unter folgenden Link:

  http://www.edoeb.admin.ch/themen/00794/01609/01610/index.html?lang=de

Anhang 3: Checkliste Pflichtenheft der/des Datenschutzverantwortlichen

DSG 11*a* Abs. 5 Bst. e / VDSG 12*a* / DSG 8

1. Ziel der Funktion

- Sicherstellen der Einhaltung der gesetzlichen Bestimmungen zum Datenschutz im Krankenversicherungsunternehmen.
- Ansprechperson gegenüber dem EDÖB/BAG.

2. Kompetenzen und Verantwortung:

- Kontrolle der Bearbeitung von Personendaten.
- Vorschlagen von Massnahmen, falls die Gefahr besteht, dass Vorgaben bzw. Weisungen zum Datenschutz verletzt werden.
- Die/der betriebliche Datenschutzverantwortliche übt ihre/seine Funktion fachlich und organisatorisch unabhängig aus, ohne diesbezüglich Weisungen oder Sanktionen des Inhabers der Datensammlung zu unterliegen.
- Sie/er übt keine Tätigkeiten aus, die mit ihren/seinen Aufgaben als Datenschutzverantwortliche/n unvereinbar sind.
- Sie/er verfügt über die zur Erfüllung der Aufgaben erforderlichen Ressourcen.
- Sie/er hat Zugang zu allen Datensammlungen und Datenbearbeitungen sowie zu allen Informationen, die sie/er zur Erfüllung der Aufgaben benötigt: Umfassendes Einsichtsrecht in Dokumente, Vorführungsrecht im Hinblick auf Datenverarbeitungssysteme, Auskunftsrecht gegenüber sämtlichen für die Datenbearbeitungen verantwortlichen Personen.
- Rapportieren der Situation im Datenschutz gegenüber dem Inhaber der Datensammlung (leitendes Organ).

3. Hauptaufgaben:

- Prüfen aller Verträge und Vorhaben, die eine Bearbeitung von Personendaten beinhalten, auf Einhalten der gesetzlichen und der internen Bestimmungen zum Datenschutz. Durchführung einer Risikoanalyse (Risiko einer unbeabsichtigten oder unberechtigten Datenweitergabe, Datenlöschung oder Datenbearbeitung, eines Datenverlustes oder technischen Fehlers). Empfehlung von Korrekturmassnahmen bei Datenschutzverletzungen.
- Ständige Überprüfung und rechtliche Abgleichung der internen Datenschutzbestimmungen mit der Rechtsentwicklung.
- Schulen und Unterstützen der Mitarbeitenden in allen Fragen im Bereich Datenschutz. Sicherstellen eines schnellen Informationsflusses zwischen der/dem Datenschutzverantwortlichen und der betroffenen Abteilung bei Datenschutzverletzungen.
- Sicherstellen der termingerechten und korrekten Beantwortung von Auskunftsbegehren gemäss Datenschutzgesetzgebung.
- Sicherstellen der regelmässigen Aktualisierung der Bearbeitungsreglemente und der Datensammlungen mit besonders schützenswerten Personendaten.
- Führen des Inventars der Datensammlungen im Betrieb. Es wird empfohlen, mittels standardisierten Formulars sämtliche vorhandenen und geplanten Datensammlungen und Datenbearbeitungen zu erheben und damit Bestand, Mutationen und Löschungen der Datensammlungen zu überwachen. Die/der Datenschutzverantwortliche soll zu jeder Zeit einen Überblick darüber haben, welche Daten in welcher Abteilung bzw. in welchem Bereich bearbeitet werden. Das Inventar der Datensammlungen im Betrieb ist dem EDÖB oder betroffenen Personen, die ein entsprechendes Gesuch gemäss Art. 8 DSG stellen, zur Verfügung zu stellen.

Anhang 4: Datenschutzmanagementsysteme und Datenschutzzertifizierungen

KVV **59*a* Abs. 6** / DSG 11 + 11*a* Abs. 5 Bst. f / VDSZ

Um den Datenschutz und die Datensicherheit zu verbessern, können die Krankenversicherer bezüglich der Bearbeitung von Personendaten ihre Systeme, Verfahren und ihre Organisation einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen (Art. 11 DSG). Eine Datenannahmestelle im Sinne von Artikel **59*a* Absatz 4** KVV muss zertifiziert werden (Art. **59*a* Abs. 6** KVV). Diese Zertifizierungsstellen müssen von der Schweizerischen Akkreditierungsstelle SAS anerkannt sein (mehr hierzu im Anhang 8).

Die Zertifizierung von Organisation und Verfahren im Sinne der Verordnung über die Datenschutzzertifizierungen (VDSZ) ist in den Richtlinien des EDÖB über die Mindestanforderungen an das Datenschutzmanagementsystem (DSMS) (Art. 4 Abs. 3 VDSZ) und dem Leitfaden für das Datenschutzmanagement (Anhang zu den Richtlinien) ausgeführt, die unter folgender Adresse zugänglich sind:

http://www.edoeb.admin.ch/org/00828/index.html?lang=de

Die Richtlinien lehnen sich an die internationalen Normen für Managementsysteme, insbesondere ISO/IEC 27001:2005 (Informationssicherheit) an.

Die Zertifizierung im Sinne der VDSZ, das heisst also die Einführung und langfristige Aufrechterhaltung eines zuverlässigen und in die Unternehmensprozesse implementierten Datenschutzmanagementsystems (DSMS), führt in der Regel durch einen systematischen Ansatz bei der Bearbeitung von Personendaten zu einer Kostenreduktion. Ausserdem erhöht sie die Sicherheit bei der Verwendung von Personendaten (z.B. bei der Anwendung der Bestimmungen von Artikel **59 ff** KVV bezüglich der Bearbeitung und Aufbewahrung von diagnosebezogenen Daten) und gewährleistet eine konstante Überwachung der Unternehmensprozesse im Bereich des Datenschutzes im Hinblick auf deren kontinuierliche Verbesserung. Schliesslich kann eine Zertifizierung auch dem Image und dem Vertrauen von Partnern, Versicherten, Behörden und offiziellen Instanzen förderlich sein (Qualitätszeichen).

Zudem müssen die Versicherer ihre Datensammlungen nicht beim EDÖB anmelden, wenn sie aufgrund eines Zertifizierungsverfahrens nach Artikel 11 DSG ein Datenschutz-Qualitätszeichen erworben haben und das Ergebnis dem EDÖB mitgeteilt haben (Art. 11*a* Abs. 5 Bst. f DSG). Gerade den kleineren Krankenversicherern, welche nicht über einen betrieblichen Datenschutzverantwortlichen verfügen, ist ein Zertifizierungsverfahren zu empfehlen (im Bereich von Artikel 59a KVV besteht allerdings ein Zertifizierungsobligatorium, siehe Anhang 8).

Der Entscheid, eine Zertifizierung des Unternehmens als Ganzes oder bestimmter Verfahren bzw. Bereiche durchzuführen, obliegt dem Versicherer. Die Zertifizierung und die Aufrechterhaltung ihrer Gültigkeit erfordern einen gewissen finanziellen und personellen Aufwand.

Die Höhe der Investition für eine Zertifizierung hängt von deren Umfang (das ganze Unternehmen oder nur bestimmte Verfahren bzw. Bereiche) sowie der Grösse und der Organisation des Versicherers ab (2010: zwischen CHF 35'000.00 und CHF 120'000.00 für das Unternehmen als Ganzes und zwischen CHF 25'000.00 und CHF 35'000.00 für einzelne Bereiche). Hinzu kommen die personellen Ressourcen, die zur Ausarbeitung der Zertifizierungsdokumentation und zur Implementierung des Datenschutzmanagementsystems nötig sind (14 bis 45 Personentage für ein mittleres Unternehmen).

Für die Aufrechterhaltung der Gültigkeit ist mit den Kosten für die jährlichen Zwischenaudits (2010: zwischen CHF 8'000.00 und CHF 25'000.00 je nach Grösse des Unternehmens) und den Personalressourcen für die Durchführung der Zwischenaudits (zwischen 1 ½ und 4 ½ Personentage) sowie den Kosten für die regelmässige Aktualisierung der Dokumentation und die periodische Überwachung

der korrekten Verwendung des Datenmanagementsystems (internes Audit, Management Review usw. – 2 bis 5 Personentage pro Jahr) zu rechnen. Für die Ausführung dieser Aufgaben sollte der Krankenversicherer eine/n Datenschutzverantwortliche/n[19] bezeichnen (circa 10 bis 25 % Personentage pro Jahr).
Ausserdem dürfen die Kosten für die Rezertifizierung (alle drei Jahre) nicht vergessen werden.

Über den folgenden Link können Sie Zertifizierungsstellen suchen, die von der Schweizerischen Akkreditierungsstelle SAS für die Zertifizierung von Managementsystemen akkreditiert sind:

http://www.seco.admin.ch/sas/index.html?lang=de

[19] Vgl. Anhang 3

Anhang 5: Case Management

Sehr viele Personen sind bei Krankenversicherern versichert, die ein Case Management anbieten.

Im Rahmen eines Case Management werden besonders schützenswerte Personendaten bearbeitet. Da die Case Manager sowohl im Interesse der betroffenen Person als auch des Versicherers handeln und sich dabei Interessenskonflikte ergeben können, müssen die **Grundsätze der Transparenz und der Zweckbindung (Art. 4 Abs. 2 und 3 DSG)** besonders gewissenhaft beachtet werden. Speziell dabei ist, dass Case Manager von den Versicherern eingesetzt werden, um die durch einen Unfall oder eine Krankheit entstehenden Kosten möglichst gering zu halten, und um die betroffene Person so zu betreuen, dass sie möglichst rasch wieder gesund wird.

Damit die Case Manager die Datenbearbeitung legal vornehmen können, ist es besonders wichtig, dass sie die betroffene Person über ihre Rolle, ihre Ziele, den Zweck der Datenbearbeitung und ihren Auftraggeber, den Krankenversicherer, informieren. Die Personendaten dürfen nur für die Zwecke verwendet werden, welche für die betroffene Person erkennbar sind. Case Manager dürfen sich somit gegenüber der betroffenen Person nicht nur als «Wohltäter/in» in einer schwierigen Situation präsentieren, sondern müssen mit der notwendigen Aufklärung für Transparenz sorgen.

Die fachliche und organisatorische Unterstellung der Case Manager und ihrer Hilfspersonen ist bei vielen Versicherern zu überprüfen und zu korrigieren. *Die Case Manager dürfen nicht mehr in der Leistungsabwicklung eingegliedert sein, sondern sind der Vertrauensärztin oder dem Vertrauensarzt zu unterstellen.* Es ist darauf zu achten, dass die Stellen der Case Manager sowie deren Hilfspersonen bezüglich ihrer fachlichen und organisatorischen Unterstellung sowie ihres Beschäftigungsgrades für das Case Management so konzipiert sind, dass sich daraus *keine Interessenkonflikte* für sie ergeben. Sie dürfen nicht mit verschiedenen Aufgaben betraut werden, die miteinander nicht kompatibel sind. Ausserdem dürfen die Löhne (und Boni) der Case Manager nicht in einer Relation zu den für den Versicherer eingesparten Kosten stehen.

Anhang 6: Fragebogen zum Gesundheitszustand

BV 5 / KVG 4 Abs. 2 / KVV 6*a* Abs. 1

Fragen zum Gesundheitszustand von Personen, die einen Antrag auf Aufnahme in die obligatorische Krankenpflegeversicherung stellen, widersprechen dem KVG und dem Verhältnismässigkeitsprinzip. Auf diese Weise Gesundheitsdaten zu beschaffen, ist rechtswidrig.

Die Krankenversicherer dürfen sich bei der Aufnahme von versicherungspflichtigen Personen nicht über deren Gesundheitszustand informieren. Dieses Verbot ergibt sich aus der Pflicht nach Artikel 4 Absatz 2 KVG, jede versicherungspflichtige Person aufzunehmen, und aus dem Verhältnismässigkeitsprinzip gemäss Artikel 5 der Bundesverfassung (BV) vom 18. April 1999.

Fragen zum Gesundheitszustand dürfen bei der Aufnahme nur dann gestellt werden, wenn die versicherungspflichtige Person ausdrücklich ihr Interesse bekundet, eine Zusatzversicherung oder eine Taggeldversicherung abzuschliessen. Der entsprechende Fragebogen darf sich nur auf die nicht obligatorischen Versicherungen beziehen und muss dies klar angeben. Diese Beitrittsformulare mit Fragen zur Gesundheit sind strikt von den Beitrittsformularen für die obligatorische Krankenpflegeversicherung zu trennen.

Die Krankenversicherer müssen dafür sorgen, dass die von ihnen beauftragten Versicherungsvermittler sich nicht über den Gesundheitszustand von beitrittsinteressierten Personen informieren.

Wenn auf diese Weise bereits Gesundheitsdaten erhoben worden sind, sind die rechtswidrig beschafften Informationen und gegebenenfalls damit rechtswidrig betriebene Datensammlungen unverzüglich zu vernichten.

Anhang 7: Ermächtigungsklauseln / Generalvollmachten

StGB 321 / ATSG 28 Abs. 3, 33 und 43 Abs. 3 / DSG 3 Bst. c Ziff. 2, 4 Abs. 5 und 12 ff / KVG 4 Abs. 2, 42 Abs. 3, 84*a* / KVV 6*a* Abs. 1

1. Vollmacht, Einwilligungsklauseln

Gemäss Artikel 33 ATSG haben die Versicherer gegenüber Dritten Verschwiegenheit zu bewahren. Sie dürfen Daten nur bekannt geben, wenn die in Artikel 84*a* KVG genannten Bedingungen erfüllt sind. Die Leistungserbringer und ihre Hilfspersonen unterstehen dem Berufsgeheimnis (Art. 321 StGB); die anderen Akteure im Gesundheitsbereich (andere Sozialversicherungen, Privatversicherer) unterliegen ebenfalls der Schweigepflicht (Art. 33 ATSG, Art. 12 ff DSG). In der Praxis *verlangen viele Krankenversicherer von ihren Versicherten die Unterzeichnung einer Vollmacht, die sie ermächtigt, bei Dritten Informationen einzuholen oder Dritten Informationen bekannt zu geben. Eine solche Vollmacht muss die gesetzlichen Bedingungen einhalten, insbesondere Artikel 4 DSG*. Die Bearbeitung von Daten der versicherten Person ist also nur mit deren *freien und aufgeklärten Einwilligung* zulässig. Die Einwilligung ist aufgeklärt, wenn die Person zum Zeitpunkt der Einwilligung angemessen informiert worden ist, das heisst, wenn sie *in der Lage ist, die Tragweite ihrer Einwilligung abzuschätzen*, bzw. wenn sie erkennen kann, welche Daten weitergegeben werden können, welcher Personenkreis diese Informationen weitergeben darf und/oder welchem Personenkreis diese Informationen weitergegeben werden dürfen und was der Zweck der Datenweitergabe ist. Gesundheitsbezogene Daten sind *besonders schützenswerte Personendaten* im Sinne von Artikel 3 Buchstabe c Ziffer 2 DSG. Ihre Bearbeitung erfordert folglich die *ausdrückliche Einwilligung der versicherten Person* (Art. 4 Abs. 5 DSG).

2. Vollmacht zum Zeitpunkt des Beitritts

Gemäss Artikel 4 Absatz 2 KVG müssen die Versicherer in ihrem Tätigkeitsbereich jede versicherungspflichtige Person aufnehmen, ohne ihren Gesundheitszustand zu berücksichtigen. Gesundheitsfragebogen sind verboten (siehe Anhang 6). Da die Versicherer ermächtigt sind, im Beitrittsformular alle Angaben zu verlangen, die für den Beitritt zur obligatorischen Krankenpflegeversicherung oder bei einem Wechsel des Versicherers erforderlich sind (Art. 6*a* Abs. 1 KVV), *ist eine Vollmacht überflüssig.* Der Versicherer muss alle benötigten Auskünfte von der versicherten Person selbst erhalten.

3. Vollmacht im Leistungsfall

Gestützt auf Artikel 28 Absatz 3 ATSG und vorbehältlich Artikel 42 Absatz 3 KVG *muss sich die Vollmacht immer auf einen bestimmten Leistungsfall beziehen*. Im Dokument, das der Versicherer der versicherten Person zur Unterschrift vorlegt, muss ausdrücklich der Versicherungsfall (Krankheit/Unfall, Datum) angegeben sein, für den die Vollmacht verlangt wird. Eine für zukünftige Leistungsfälle ausgestellte Vollmacht ist nicht gültig.

Die Vollmacht muss das Verhältnismässigkeitsprinzip einhalten: Der Versicherer darf nicht mehr Informationen beschaffen, als er zur Ausübung seiner Aufgaben nach KVG benötigt. Ebenso darf er Dritten nicht mehr Daten bekannt geben, als diese tatsächlich benötigen.

Die Vollmacht kann durch die versicherte Person jederzeit widerrufen werden. Diese muss explizit über ihr Widerrufsrecht informiert werden.

In der Vollmacht anzugeben, dass ein Nichtunterschreiben des Dokuments die Einschränkung oder die Einstellung des Leistungsanspruchs zur Folge hat, ist nicht korrekt. Wenn die versicherte Person sich zu Unrecht weigert, die Vollmacht zu unterschreiben, muss der Versicherer sie schriftlich mah-

nen, um sie an ihre Mitwirkungspflicht zu erinnern und auf die Rechtsfolgen hinzuweisen. Der Versicherer räumt der versicherten Person eine angemessene Bedenkzeit ein (Art. 43 Abs. 3 ATSG).

4. Einwilligung bei Case Management

Bei Versicherungen mit Case Management (siehe Anhang 5) ist die Menge an Daten, die zwischen dem Versicherer, der die Behandlung steuert, und den Leistungserbringern ausgetauscht werden, grösser als bei anderen Versicherungen. Dafür muss die versicherte Person ihre *ausdrückliche Einwilligung* geben.

Die versicherte Person muss genau über die Daten, die weitergegeben werden, die Identität des Empfängers und den Zweck des Datenaustauschs informiert werden. Sie muss die *Einwilligung ausserdem jederzeit widerrufen können, und sie muss über dieses Recht informiert* sein.

Anhang 8: Rechnungsstellung bei einem Vergütungsmodell vom Typus DRG

KVG 42 **Abs. 3bis** / KVV **59, 59*a* und Übergangsbestimmung zur Änderung vom 4. Juli 2012 / Verordnung des EDI vom 20. November 2012 über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern /** VDSZ

1. Systematische Datenweitergabe

Mit Artikel 42 **Absatz 3bis** KVG wurde der Grundsatz für die systematische Datenweitergabe zwischen Leistungserbringern und Versicherern konkretisiert. Die Leistungserbringer haben auf den DRG-Rechnungen auch Diagnosen und Prozeduren anzugeben.

Damit ein Versicherer die medizinischen Angaben bei der Rechnungsstellung bei einem Vergütungsmodell vom Typus DRG systematisch empfangen darf, muss er eine zertifizierte Datenannahmestelle nach Artikel **59*a* Absatz 6** KVV bis am 31. Dezember 2013 errichten (**Absatz 1 der Übergangsbestimmung zur Änderung vom 4. Juli 2012**). Solange ein Versicherer nicht über eine zertifizierte Datenannahmestelle verfügt, können medizinische Angaben ausschliesslich an den Vertrauensarzt oder der Vertrauensärztin systematisch weitergegeben werden. Nach Ablauf dieser Frist ist jeder Versicherer verpflichtet, über eine zertifizierte Datenannahmestelle zu verfügen.

Das Zertifizierungsverfahren der Datenannahmestelle erfolgt nach Artikel 11 DSG und Artikel 4 VDSZ. Die Zertifizierung ist drei Jahre gültig. Der zertifizierte Bereich umfasst alle Datenbearbeitungsverfahren (auch externer Dienstleister), welche der Erfüllung von Artikel **59a** KVV dienen. Die Zertifizierungsstelle kann eine Zertifizierung sistieren oder entziehen, wenn schwere Mängel festgestellt werden, welche innert Frist nicht behoben werden (Art. 9 ff VDSZ). In einem solchen Fall wären die Voraussetzungen von Artikel **59*a* Absatz 6** KVV nicht mehr erfüllt und medizinische Angaben (MCD) dürften nicht mehr an den Versicherer übermittelt werden. Die systematische Übermittlung an den Vertrauensarzt oder die Vertrauensärztin ist ab dem 1. Januar 2014 nicht mehr zulässig. Der Empfang von Rechnungen des Typus DRG ist somit ab dem 1. Januar 2014 nur noch über die Datenannahmestelle möglich, ansonsten dürfen die DRG-Datensätze nicht mehr vollständig und systematisch dem Krankenversicherer übermittelt resp. von diesem empfangen werden. Das gleiche gilt im Falle eines Entzugs des Datenschutzzertifikats der Datenannahmestelle. In beiden Fällen ist es dem Versicherer ohne Datenannahmestelle nicht mehr möglich, eine systematische Rechnungsprüfung für das DRG-System vorzunehmen. Vorbehalten bleiben aufsichtsrechtliche Massnahmen des BAG nach Artikel 21 Absätze 5 und 5bis KVG.

Sowohl während der Übergangsfrist als auch dann, wenn der Versicherer eine zertifizierte Datenannahmestelle eingerichtet hat, müssen die Leistungserbringer dem Versicherer die administrativen und medizinischen Angaben gleichzeitig weiterleiten (Art. **59*a* Abs. 3** KVV). Damit die administrativen und medizinischen Datensätze nach einer Triage wieder zusammengeführt werden können, muss der Leistungserbringer sie mit einer Identifikationsnummer versehen (Art. **59*a* Abs. 1**).

2. Rechnungsinhalt

Nach Artikel 42 **Absatz 3bis** KVG i.V.m Artikel **59*a* Absatz 2** KVV haben die Leistungserbringer Diagnosen und Prozeduren entsprechend den Klassifikationen für die medizinische Statistik der Krankenhäuser nach Ziffer 62 des Anhangs der Verordnung vom 30. Juni 1993[20] über die Durchführung von statistischen Erhebungen des Bundes zu kodieren und kodiert auf der Rechnung aufzuführen.

In **Absatz 3** von Artikel **59*a*** KVV wird des Weiteren vorgeschrieben, dass die Leistungserbringer die

[20] SR 431.012.1

Datensätze mit den administrativen und medizinischen Angaben nach Artikel **59 Absatz 1** KVV gleichzeitig mit der Rechnung an die Datenannahmestelle des Versicherers übermitteln müssen. Im selben Artikel ist vorgesehen, dass der Versicherer sicherstellen muss, dass nur die Datenannahmestelle Zugang zu den medizinischen Angaben erhält.

Die einheitliche Struktur der Datensätze bzw. deren Umfang und Inhalt wird in der **Verordnung des EDI vom 20. November 2012 über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern** vorgegeben. Eine Rechnung bei einem Vergütungsmodell vom Typus DRG enthält daher die Angaben nach Artikel **59 Absatz 1** KVV sowie die Variablen des Anhangs zu **Artikel 1 dieser EDI-Verordnung**.

3. Datenannahmestelle

Jeder Versicherer ist verpflichtet, bis spätestens dem 31. Dezember 2013 eine zertifizierte Datenannahmestelle einzurichten (**Abs. 1 der Übergangsbestimmung zur Änderung vom 4. Juli 2012**).

Die zertifizierte Datenannahmestelle hat die Funktion, eine vollständig automatisierte Triage von Rechnungen mittels der Rechnungsdaten inklusive der medizinischen und administrativen Angaben durchzuführen. Die Triage erfolgt durch voreingestellte Parameter, welche der Versicherer festlegt. Die Parameter müssen so festgelegt werden, dass dem Aspekt der Verhältnismässigkeit im Sinne des DSG Rechnung getragen und anschliessend eine wirksame Rechnungs- und Wirtschaftlichkeitsprüfung ermöglicht wird.

Nach der Durchführung der Triage durch die zertifizierte Datenannahmestelle werden nur diejenigen Rechnungen, die gemäss dem voreingestellten Parameter auffällig waren, an die zuständige Stelle des Versicherers zur vertieften Überprüfung weitergeleitet. Während der Überprüfung durch die zuständige Stelle muss der Datenschutz im Sinne von Artikel **59a ter Absatz 1** KVV stets gewährleistet werden.

Alle unauffälligen Rechnungen werden zur Bezahlung freigegeben, wobei die medizinischen Angaben beim Versicherer verschlüsselt oder pseudonymisiert zu archivieren sind. Der Versicherer muss sicherstellen, dass nach erfolgter Triage die medizinischen Angaben für niemanden zugänglich sind und verschlüsselt oder pseudonymisiert archiviert werden. Nach erfolgter Archivierung kann nur der Vertrauensarzt oder die Vertrauensärztin die Verschlüsselung oder Pseudonymisierung aufheben (Art. **59*a*ter Abs. 2** KVV).

Nach vertiefter Überprüfung der auffälligen Rechnungen müssen die medizinischen Angaben ebenfalls verschlüsselt oder pseudonymisiert archiviert werden, wobei auch hier nur der Vertrauensarzt oder die Vertrauensärztin die Verschlüsselung oder Pseudonymisierung aufheben können (Art. **59*a*terAbs. 2** KVV).

Beilage 5

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Gesundheit BAG
Direktionsbereich Kranken- und Unfallversicherung

CH-3003 Bern, BAG

An die KVG-Versicherer

Referenz/Aktenzeichen:
Ihr Zeichen:
Unser Zeichen: Lp
Bern, 13. Dezember 2011

Erhebung über die datenschutzkonforme Organisation und Prozesse der Krankenversicherer Teil 1

Sehr geehrte Damen und Herren

Am 25. August 2011 haben wir Ihnen das Kreisschreiben 7.1 *Datenschutzkonforme Organisation und Prozesse der Krankenversicherer*, und dessen Anhänge 1 - 7 zugestellt, welches die für die Krankenversicherer geltenden Datenschutzgrundsätze und -vorgaben zusammenfasst. Das Kreisschreiben ist abrufbar unter
http://www.bag.admin.ch/themen/krankenversicherung/02874/02877/06501/index.html?lang=de.

Im Anschluss an das Kreisschreiben 7.1 und gestützt auf Artikel 21 Abs. 1 und 3 KVG befragen wir mit dem beiliegenden Fragebogen nochmals alle Krankenversicherer zum heutigen Stand ihrer Vorkehrungen zum Schutz der Versichertendaten (Datenschutz und Datensicherheit). Die Resultate dieser Erhebung werden in einen bundesrätlichen Bericht zur Erfüllung des Postulates Heim (P 08.3493, Schutz der Patientendaten. Schutz der Versicherten, Annahme NR 12.12.2008)[1] einfliessen. Zu einem späteren Zeitpunkt werden wir Sie noch befragen, wie Sie den Datenschutz und die Datensicherheit in Zusammenhang mit den Datenlieferungen der Leistungserbringer nach Einführung des Fallpauschalensystems Swiss DRG sicherstellen. Dies wird mit einem weiteren Fragebogen erfolgen, weil die Regelung für die Übermittlung der abrechnungsrelevanten Daten im Moment noch offen ist und von den Krankenversicherern umgesetzt werden muss.

[1] Das Postulat verlangt, dass der Bundesrat aufzeigt, welche Massnahmen gegen die Diskriminierung einzelner Patientengruppen und zum Schutz der Patientendaten bei den Versicherern geplant sind.

Bundesamt für Gesundheit
Patricia Leiber
Hessstrasse 27E, CH-3003 Bern
Postadresse: CH-3003 Bern
Tel. +41 31 322 92 23, Fax +41 31 323 00 60
Patricia.Leiber@bag.admin.ch
www.bag.admin.ch

Wir bitten Sie deshalb gestützt auf Artikel 21 Abs. 3 KVG, alle Auskünfte zu geben, welche im beiliegenden Fragebogen verlangt werden. Wir behalten uns vor, Sie für zusätzlich benötigte Angaben zu kontaktieren und Ihre Angaben im Rahmen der Kontrollen und Stichproben der Sektion Audit zu überprüfen.

Für Fragen steht Ihnen Frau Patricia Leiber (031 322 92 23, patricia.leiber@bag.admin.ch) zur Verfügung.

Bitte senden Sie den ausgefüllten Fragebogen mit Beilagen bis zum 31. Januar 2012 an das Bundesamt für Gesundheit, Sektion Rechtliche Aufsicht KV, zuhanden Patricia Leiber, Hessstrasse 27E, 3003 Bern, patricia.leiber@bag.admin.ch, zurück. Besten Dank !

Mit freundlichen Grüssen

Abteilung Versicherungsaufsicht
Die Leiterin

H Portmann

Helga Portmann

Beilage: Fragebogen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Bundesamt für Gesundheit BAG
Direktionsbereich Kranken- und Unfallversicherung

Fragen zur datenschutzkonformen Organisation und den datenschutzkonformen Prozessen der Krankenversicherer Teil 1

1. Datenschutzkonzept

1.1. Haben Sie ein Ihre ganze Organisation umfassendes Datenschutz- und Datensicherheitskonzept erstellt? Wenn ja, wann wurde es erstellt, bzw. aktualisiert?

1.2. Haben Sie ein Datenschutz- und Datensicherheitskonzept für einzelne Bereiche Ihrer Organisation erstellt?

a) Wenn ja, für welche Bereiche oder Aktivitäten wurde es erstellt und wann wurde es aktualisiert?

b) Welche Bereiche oder Aktivitäten sind noch nicht berücksichtigt?

2. Bearbeitungsreglemente

2.1. Haben Sie für jede automatisierte Datensammlung, die besonders schützenswerte Daten oder Persönlichkeitsprofile enthält oder mit anderen Datensammlungen verknüpft ist, ein Bearbeitungsreglement gemäss Artikel 21 der Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11) erstellt?

2.2. Haben Sie ein Konzept für die Zugriffsberechtigungen der Mitarbeitenden erstellt?

2.3. Haben Sie ein Bearbeitungsreglement für die Datenbearbeitung durch den Vertrauensarzt und den vertrauensärztlichen Dienst erstellt?

2.4. Wie oft überprüfen Sie die Bearbeitungsreglemente auf Aktualität und Vollständigkeit?

2.5. Haben Sie vor, die Bearbeitungsreglemente ab dem 1. Januar 2012 auf Ihrer Homepage zu veröffentlichen? Wenn nein, welche andere Publikationsform sehen Sie vor?

3. Datensammlungen

3.1. Führen Sie ein Verzeichnis sämtlicher personenbezogenen Datensammlungen gemäss Artikel 11a des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1) und Artikel 16 VDSG)?

3.2. Wenn ja, wann wurde es zum letzten Mal aktualisiert?

3.3. Haben Sie sämtliche personenbezogenen Datensammlungen beim EDÖB zur Registrierung angemeldet?

a) Ja

b) Wenn nein, warum nicht?

3.4. Verfügt der EDÖB über die aktuellsten Datensammlungen?

a) Ja

b) Wenn nein, warum nicht

4. Outsourcing

4.1. Welche von Ihnen beauftragte Dritte (Dienstleister) erhalten Personendaten Ihrer Versicherten? Zu welchen Zwecken erhalten sie diese Daten?

4.2. Beauftragen Sie ausländische Dienstleister mit der Bearbeitung von Personendaten Ihrer Versicherten? Wenn ja welche, in welchen Ländern? Zu welchem Zweck?

4.3. Sind die Dienstleister nach der Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (VDSZ, SR 235.13) zertifiziert?

4.4. Wie kontrollieren Sie die datenschutzkonforme Bearbeitung der Versichertendaten durch die Dienstleister?

4.5. Legen Sie bitte ein Muster oder eine Kopie eines solchen Zusammenarbeitsvertrages (mit Datenschutzklausel) Ihren Antworten bei.

5. Vertrauensarzt und Vertrauensärztlicher Dienst

5.1. Wo sind der Vertrauensarzt gemäss Artikel 57 des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung (KVG, SR 832.10) und der Vertrauensärztliche Dienst im Organigramm Ihres Unternehmens angesiedelt? Legen Sie bitte eine Kopie des Organigramms mit dem Vertrauensärztlichen Dienst Ihren Antworten bei.

5.2. Arbeiten die Hilfspersonen des Vertrauensarztes nur für ihn?

a) Ja

b) Wenn nein, welche zusätzlichen Aufgaben nehmen die Hilfspersonen wahr?

5.3. Verfügen die Hilfspersonen des Vertrauensarztes über ein schriftliches Pflichtenheft (vom Vertrauensarzt delegierte Kompetenzen)? Wenn ja, bitte legen Sie es Ihren Antworten bei.

5.4. Gelangt die Post (auch auf elektronischem Weg) direkt an den Vertrauensarzt?

5.5. Wie ist das Öffnen seiner Briefpost geregelt?

5.6. Wie ist der Zugriff auf seine elektronische Post geregelt?

5.7. Was passiert mit der für den Vertrauensarzt bestimmten Post, wenn diese infolge falscher Adressierung oder aus Versehen von einer anderen kasseninternen Stelle geöffnet wird?

5.8. Wie sind die Räumlichkeiten des Vertrauensarztes bzw. des Vertrauensärztlichen Dienstes in Bezug auf den Datenschutz und die Datensicherheit organisiert?

5.9. Wie ist die Ablage der besonders schützenswerten Daten organisiert (Klassifizierung je nach Grad der erhaltenen Daten, in Papierform und elektronisch)?

5.10. Wie sind die Zugriffe zu den besonders schützenswerten Daten geregelt, bzw. wer hat Zugriff zu diesen Daten (Papierdokumente und gescannte Dokumente)?

5.11. Wie gewährleisten Sie die Umsetzung von Artikel 57 Absatz 7 KVG?

6. Verantwortliche Stelle für den betrieblichen Datenschutz

6.1. Haben Sie für Ihr Unternehmen mind. eine für den betrieblichen Datenschutz verantwortliche Person gemäss Artikel 11*a* Absatz 5 Buchstabe e DSG bezeichnet?

6.2. Wo ist diese Stelle im Organigramm Ihres Unternehmens angesiedelt? Legen Sie bitte eine Kopie des Organigramms dieser Stelle Ihren Antworten bei.

6.3. Haben Sie eine externe Stelle mit dieser Aufgabe betraut? Wenn ja, welche externe Stelle?

6.4. Wie viele Stellenprozente setzen Sie dafür ein?

6.5. Üben die für den betrieblichen Datenschutz verantwortlichen Personen noch andere Aufgaben aus? Wenn ja, welche?

6.6. Haben Sie die für den betrieblichen Datenschutz verantwortlichen Personen dem EDÖB gemeldet?

6.7. Verfügen die für den betrieblichen Datenschutz verantwortlichen Personen über ein schriftliches Pflichtenheft? Wenn ja, bitte legen Sie es Ihren Antworten bei.

6.8. Haben diese Personen eine datenschutzspezifische Ausbildung absolviert?

6.9. Bilden sie sich im Bereich Datenschutz laufend weiter?

6.10. Führt die für den betrieblichen Datenschutz verantwortliche Stelle Datenschutzschulungen für die Mitarbeitenden durch? Wenn ja, wie oft? Ist die Teilnahme an den Schulungen für alle Mitarbeitenden des Unternehmens obligatorisch?

7. Datenschutzmanagement, Informations- und Datensicherheits-System Datenschutz-Zertifizierung

7.1. Haben Sie Ihre Datenbearbeitungssysteme und -verfahren sowie Ihre Organisation als Ganzes einem Datenschutz-Zertifizierungsverfahren nach der VDSZ unterstellt?

a) Ja: Zertifizierungsstelle:

b) Nein: Gründe:

7.2. Haben Sie nur einzelne Bereiche und nur bestimmte Verfahren einem Datenschutz-Zertifizierungsverfahren unterstellt?

Wenn ja, welche Bereiche und Verfahren und bei welcher Zertifizierungsstelle?

7.3. Wird die Einhaltung der Vorgaben für den Datenschutz innerhalb Ihres Unternehmens geprüft (interne Audits)?

7.4. Durch welche Stelle, wie und wie oft?

7.5. Wer ist der Auftraggeber und wie werden die Ergebnisse mitgeteilt?

8. HMO- und Hausarztmodelle sowie Versicherungsmodell mit telemedizinischer Beratung

8.1. Welche technischen und organisatorischen datensichernden Massnahmen haben Sie für den Datenaustausch zwischen den involvierten Stellen (Gatekeeper/koordinierende Leistungserbringer, beauftragten Dritte (Dienstleister) und internen Kassenstellen inkl. Vertrauensärztliche Dienst) getroffen?

8.2. Welche Daten werden zwischen den involvierten Stellen ausgetauscht?

8.3. Wie ist die Zugriffsberechtigung auf ein Dossier der versicherten Person geregelt?

9. Case Management durch den Krankenversicherer

9.1. Wo ist ein allfälliges Case Management[1] im Organigramm Ihres Unternehmens angesiedelt? Legen Sie bitte eine Kopie des Organigramms mit dieser Stelle Ihren Antworten bei.

9.2. Beschreiben Sie den Prozessablauf eines Case Managements, die Zusammenarbeit mit der versicherten Person, dem Vertrauensarzt bzw. Vertrauensärztliche Dienst und den Leistungserbringern, und legen Sie ein Muster der Einwilligungserklärung der versicherten Person bei.

9.3. Wie ist die Zugriffsberechtigung auf ein Case Management-Dossier geregelt?

[1] Gemeint sind alle Arten von Case Management, welche der Krankenversicherer in der obligatorischen Krankenpflegeversicherung als Massnahme zur Optimierung der Leistungen, zur Kostenkontrolle und zur Kostenminimierung anbietet.

10. Risikoausgleich

10.1. Welche technischen und organisatorischen datensichernden Massnahmen haben Sie als Vorversicherer in Bezug auf die Datenbearbeitung und –weitergabe der für die Zentrale Meldestelle Risikoausgleich (ZEMRA) bestimmten Daten der Versichererwechsler für die Berücksichtigung des erhöhten Krankheitsrisikos im neuen Risikoausgleich gemäss KVG-Änderung vom 21. Dezember 2007 getroffen?

10.2. Welche technischen und organisatorischen datensichernden Massnahmen haben Sie als Nachversicherer in Bezug auf die Datenbearbeitung der von der Zentralen Meldestelle Risikoausgleich (ZEMRA) erhaltenen Daten der Versichererwechsler für die Berücksichtigung des erhöhten Krankheitsrisikos im neuen Risikoausgleich gemäss KVG-Änderung vom 21. Dezember 2007 getroffen?

11. Vollmachten und Einwilligungserklärungen

11.1. Bitte legen Sie dem Fragebogen ein Muster aller Vollmachts- und Einwilligungserklärungen bei, welche den Versicherten unterbreitet werden und den Krankenversicherer ermächtigt, medizinische Angaben von Dritten einzuholen. Es sind auch diejenigen Muster beizulegen, welche Daten der obligatorischen Krankenpflegeversicherung betreffen, wenn sie für Zusatzversicherungen eingeholt werden.

12. Zusätzliche Bemerkungen

12.1. Haben Sie zusätzliche Bemerkungen und Zusatzinformationen?

13. **Adresse** der zuständigen Person für Rückfragen des BAG

Herr/Frau ….....
Tel. ….....
Email ….....
Funktion ….....

Vielen Dank für Ihre Antworten !