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.