Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

CH-3003 Bern
BAG

An die KVG Versicherer und ihre
Rückversicherer

Referenz/Aktenzeichen:
Unser Zeichen:
Sachbearbeiterin: Lp
Bern, 14. Oktober 2014

Kreisschreiben Nr.:	**7.1**
Inkrafttreten:	**1. November 2014**

Datenschutzkonforme Organisation und Prozesse der Krankenversicherer

1. Ausgangslage

Die bisherigen Datenschutzerhebungen und Kontrollmassnahmen des BAG haben gezeigt, dass die Krankenversicherer den Datenschutz trotz sehr unterschiedlicher Organisationsstrukturen über weite Strecken sicherstellen. Es wurde aber auch festgestellt, dass in einigen sensiblen Bereichen noch Verbesserungspotential besteht. Früher abgegebene Empfehlungen sind deshalb immer noch gültig:

- 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 erstellen (Beschreibung der Prozesse inkl. Verantwortlichkeiten, Berechtigungen, Datenfluss sowie der technischen Massnahmen zur Datensicherheit). Das Bearbeitungsreglement muss regelmässig aktualisiert werden.
- Das BAG empfiehlt den Krankenversicherern, eine verantwortliche Person für den Datenschutz zu bezeichnen. Die Aufgaben dieses Datenschutzverantwortlichen sind in einem Pflichtenheft zu umschreiben.
- Datenschutzverantwortliche müssen über die erforderlichen Fachkenntnisse verfügen.

Bundesamt für Gesundheit
Hessstrasse 27E, CH-3003 Bern
Tel. +41 58 463 70 66, Fax +41 58 463 00 60
www.bag.admin.ch

- Es sollen von einer dafür spezialisierten Stelle regelmässig externe Datenschutzaudits durchgeführt und die Resultate den Aufsichtsbehörden unterbreitet werden.

Das BAG empfiehlt den Krankenversicherern laufend weitere Massnahmen zur Verbesserung der Datenschutzkonformität ihrer Organisation und / oder ihrer Prozesse einzuleiten und umzusetzen. Zur Förderung dieser Entwicklung weist das vorliegende Kreisschreiben und dessen Anhänge 1 - 8 die Krankenversicherer auf die für sie geltenden Datenschutzbestimmungen hin, welche sich aus den verschiedenen Bundeserlassen[1] ergeben. Neuere Datenschutzbestimmungen sind mit fetter Schrift hervorgehoben.

In Zusammenhang mit der Einführung der diagnosebezogenen Fallpauschalen (SwissDRG) im Rahmen der neuen Spitalfinanzierung hat der Bundesrat 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 Anhang 8 erläutert.

2. Datenschutz- und Datensicherheitskonzept

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

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, beschreibt die Organisation des Datenschutzes sowie die datenschutzkonforme Ausgestaltung der Datenflüsse. 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.

Die Umsetzung des Datenschutz- und Sicherheitskonzepts erfordert auch technische und organisatorische Massnahmen. Die Krankenversicherer müssen die erforderlichen Mittel zur Umsetzung der technischen und organisatorischen Massnahmen 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/datenschutz/00628/00629/00636/index.html?lang=de

[1] Vgl. Anhänge 1 + 2

3. Bearbeitungsreglemente

Art. **84*b*** KVG / Art. 21 VDSG

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 *Kontrollprozesse*, 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. Eine Reglementsanpassung ist insbesondere in Bezug auf die Verfahren für die Bearbeitung und Kontrolle der Rechnungen bei einem Vergütungsmodell vom Typus DRG vorzunehmen (vgl. dazu Anhang 8).

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 Vorgaben müssen die Krankenversicherer ihre Bearbeitungsreglemente dem EDÖB *unaufgefordert zur Beurteilung vorlegen.* Dies gilt ebenfalls für angepasste Bearbeitungsreglemente in Bezug auf die Verfahren für die Bearbeitung und Kontrolle der Rechnungen bei einem Vergütungsmodell vom Typus DRG. Das Bearbeitungsreglement ist aber bereits gültig, wenn der Krankenversicherer es für verbindlich erklärt hat.

Überdies müssen die Krankenversicherer die Bearbeitungsreglemente veröffentlichen. Sie haben diese den *interessierten Personen* mittels Publikation auf dem Internet oder in anderer Form zugänglich zu machen. Die Pflicht zur Veröffentlichung besteht unabhängig von einer durch den EDÖB durchgeführten Beurteilung. Eine Bekanntgabe des Bearbeitungsreglements auf Anfrage genügt nicht. Der Krankenversicherer kann Geschäftsgeheimnisse von der Veröffentlichung ausnehmen.

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

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

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 seinem leitenden Organ (Art. 16 Abs. 1 DSG).

Die oder der Datenschutzverantwortliche muss ihre/seine Funktion *organisatorisch und fachlich unabhängig* ausüben können. Ein möglicher Interessenkonflikt muss bereits durch ihre/seine organisatorische Stellung innerhalb des Krankenversicherers 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/datenschutz/00626/00743/00874/01051/index.html?lang=de

5. Outsourcing

Art. 84 KVG / Art.10*a* DSG

Outsourcing umfasst die Auslagerung von Dienstleistungen, die bisher von den Krankenversicherern selber erbracht wurden oder die sie gemäss gesetzlichen Vorgaben erbringen müssen, auf einen externen Dienstleister (unternehmensexternes Outsourcing) oder auf eine Gesellschaft derselben Versicherungsgruppe (unternehmensinternes Outsourcing).

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). Dies ist im Outsourcingvertrag schriftlich festzuhalten. 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. Er hat die Dienstleister regelmässig zu auditieren. Schnittstellen, Verantwortlichkeiten, Zuständigkeiten und Haftungsfragen sind vertraglich 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, Hilfspersonen und beigezogenen Dritten funktionell in die *Schweigepflicht* und das bereichsspezifische Datenschutzrecht des Krankenversicherers einzubinden. Die Mitarbeitenden des Dienstleisters, Hilfspersonen und beigezogene Dritte sind vertraglich und nötigenfalls einzelunterschriftlich zur Geheimhaltung zu verpflichten. Werden die Aufgaben des Vertrauensarztes ausgelagert, so sind die Mitarbeitenden des beigezogenen Dienstleisters mittels Geheimhaltungserklärung mit Einzelunterschrift in die Geheimhaltungsverpflichtungen des Vertrauensarztes einzubinden.

Auch bei Mitarbeitenden von externen Dienstleistern im IT-Bereich mit umfassenden Einsichts- oder Bearbeitungsrechten (z.B. Datenbank- oder Netzwerkadministratoren) sind die Geheimhaltungsverpflichtungen mittels Einzelunterschrift zu regeln.

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. Der Krankenversicherer muss die ihm vertraglich zugesicherten Controlling-Möglichkeiten tatsächlich regelmässig z.B. in Form eines Audits wahrnehmen.

Die *Auskunftspflicht des Krankenversicherers* gegenüber den betroffenen Personen bleibt bestehen, da er auch Inhaber der Datensammlung 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.

Auf das Auslagern der Bearbeitung von besonders schützenswerten Personendaten ins Ausland ist, wenn immer möglich, zu verzichten. Sollte dies ausnahmsweise der Fall sein, so ist Artikel 6 DSG besonders zu beachten. Die grenzüberschreitende Datenbekanntgabe ist nur unter bestimmten Voraussetzungen und unter Einbezug des EDÖB zulässig. Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend ge-

fährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet (Art. 6 Absatz 1 DSG). Eine Staatenliste finden Sie unter:

http://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=de

Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können nach Artikel 6 Absatz 2 Bst. a-g DSG Personendaten nur dann ins Ausland bekannt gegeben werden, wenn alternative Voraussetzungen erfüllt sind.

Besondere Vorsicht besteht bei der Nutzung von echten Clouddiensten. Weitere Angaben finden Sie auf der Internetseite des EDÖB:

http://www.edoeb.admin.ch/datenschutz/00626/00876/index.html?lang=de

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 nur beschränkt. Der Versicherer darf nicht über Kontroll- oder Einsichtsrechte zu Daten kommen, deren Geheimhaltung durch die Datenannahmestelle sichergestellt wird.

Auch für das Umsetzen des Auskunftsrechts gemäss Art. 8 DSG ist ein Bearbeitungsablauf zu installieren, welcher garantiert, dass der Versicherer über diesen Weg nicht zu Informationen gelangen kann, die ihm nicht zustehen.

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

Art. 321 StGB / Art. 57, 56, 42 Abs. 5 KVG

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). 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 medizinische Informationen 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. Den bei der Rechnungskontrolle der Rechnungen des Typus DRG eingesetzten Spezialistinnen und Spezialisten (z.B. medizinische Codiererinnen und Codierer), die ihre Aufgaben sowohl für die Leistungsabteilung als auch den VAD ausüben, sind Arbeitsplätze in der Leistungsabteilung und im VAD einzurichten. Nur so kann sichergestellt werden, dass für den VAD bestimmte medizinische Informationen diesen nicht verlassen.

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. Der Versicherer muss die als Hilfspersonen des Vertrauensarztes eingesetzten Mitarbeitenden ausdrücklich bezeichnen (Liste) und sie ausdrücklich auf ihre Position und rechtlichen Pflichten hinweisen. Geheimhaltungserklärungen mit Unterschrift der/des Mitarbeitenden sind zu begrüssen.

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

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

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). Diese Bestimmung ist derzeit aber nur im Bereich der stationären akutsomatischen Spitalbehandlungen anwendbar.

Die systematische Übermittlung von Diagnosen und Prozeduren ist derzeit nur im akutsomatischen stationären Bereich zulässig, da in den anderen stationären Behandlungsbereichen zurzeit die ausführenden Bestimmungen zur Erhebung, Bearbeitung und Weitergabe der Daten unter Wahrung des Verhältnismässigkeitsprinzips (Art. **59*a*^bis** KVV) fehlen. Im ambulanten Bereich gelten die Bestimmungen des jeweils anzuwendenden Tarifvertrags (z.B TARMED).

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, soweit es für den konkreten Fall notwendig ist. 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 regelmässigen Prüfungen durch die Sektion Audit unterziehen. Es sind weiterhin Sonderaudits mit Stichproben zum Umgang der Krankenversicherer mit den diagnosebezogenen Personendaten ihrer Versicherten geplant.

---

[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

Im Vorfeld dieser Prüfungen 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 5 ^{bis} KVG nach sich zieht. Dies beinhaltet auch die Möglichkeit zur Publikation der Massnahmen.

Das vorliegende Kreisschreiben enthält formelle und redaktionelle Änderungen in allen Ziffern.
Dieses Kreisschreiben ersetzt das Kreisschreiben 7.1 vom 17. Juni 2013 „Datenschutzkonforme Organisation und Prozesse der Krankenversicherer".

Oliver Peters
Vizedirektor
Leiter Direktionsbereich Kranken- und Unfallversicherung

Helga Portmann
Leiterin Abteilung
Versicherungsaufsicht

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

Art. 28, 31, 32, 33, 47 ATSG / Art. 8, 9 ATSV / Art. 42 **Abs. 3-5**[3], 42*a*, **57 Abs**. 6, **7**[4] und 8, 82, **84**[5], **84*a***[6], **84*b***[7], 92 KVG / Art.6*a*, **28** und **28*a***[8], **59**[9], 59*a*[10] **ff,** 76, 120 KVV / Art.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 DSG / Art.1, 2, 8, 9, 10, 12*a*, 12*b*, 16, 18, 20, 21, 22, 23, **24**[14], 28, 34, 35 VDSG / 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 auch die Berechnung des verfeinerten Risikoausgleichs 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 Ausnahmen sind in Artikel 9 DSG geregelt.

- 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[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].

- Sämtliche Mitarbeitenden eines Krankenversicherers unterstehen 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 Mitarbeitenden des Krankenversicherers auf diejenigen Personendaten zu beschränken, welche diese zur Erfüllung ihrer klar umschriebenen Aufgaben benötigen (Art. 9 Abs. 1 Bst. g VDSG). 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 Versiche-

[17] Vgl. Anhang 3

[18] Vgl. Anhang 4

rungsgesellschaft, die Versicherungen nach VVG anbietet und der gleichen Versicherungsgruppe angehört wie der Krankenversicherer, *ist eine Dritte* im Sinn von Art. 84*a* Abs. 5 KVG. Bietet der Krankenversicherer selber solche Versicherungen nach VVG an, gelten die oben 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* auf 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/datenschutz/00626/00743/00746/index.html?lang=de

Anhang 3: Checkliste Pflichtenheft der/des Datenschutzverantwortlichen

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

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.
- Empfehlung 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.
- Erlass von Weisungen und Richtlinien zum Datenschutz und zur Datensicherheit, regelmässige Aktualisierung der Bearbeitungsreglemente und der Datensammlungen mit besonders schützenwerten Personendaten.
- 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.
- Führen des Inventars der Datensammlungen im Unternehmen. 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

Art. **59*a* Abs. 6** KVV / Art. 11 + 11*a* Abs. 5 Bst. f DSG / 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 neuen 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/datenschutz/00756/00974/index.html

Die Richtlinien lehnen sich an die internationalen Normen für Managementsysteme, insbesondere ISO/IEC 27001:2013 (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. Hinzu kommen die personellen Ressourcen, die zur Ausarbeitung der Zertifizierungsdokumentation und zur Implementierung des Datenschutzmanagementsystems nötig sind.

Für die Aufrechterhaltung der Gültigkeit ist mit den Kosten für die jährlichen Zwischenaudits und den Personalressourcen für die Durchführung der Zwischenaudits sowie den Kosten für die regelmässige Aktualisierung der Dokumentation und die periodische Überwachung der korrekten Verwendung des Datenmanagementsystems (internes Audit, Management Review usw.) zu rechnen. Für die Ausfüh-

rung dieser Aufgaben sollte der Krankenversicherer eine/n Datenschutzverantwortliche/n[19] bezeichnen. 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/00206/index.html?lang=de

[19] Vgl. Anhang 3

Anhang 5: Case Management

Verschiedene Krankenversicherer bieten ein Case Management an.

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

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

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

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

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 erfüllen, 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

Art. 42 **Abs. 3bis** KVG / Art.**59, 59*a*** KVV **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 Datenweitergabe bei einem Vergütungsmodell vom Typus DRG ist mit den Bestimmungen von Art. 59a KVV näher ausgeführt worden. Die Leistungserbringer haben auf der Rechnung die Diagnosen und Prozeduren nach den Klassifikationen in den jeweiligen vom zuständigen Departement herausgegebenen schweizerischen Fassungen codiert aufzuführen.

Damit ein Versicherer die Rechnungen sowie die administrativen und medizinischen Datensätze bei einem Vergütungsmodell vom Typus DRG empfangen darf, muss er zwingend über eine zertifizierte Datenannahmestelle nach Artikel **59*a* Absatz 6** KVV verfügen.

Das Zertifizierungsverfahren der Datenannahmestelle erfolgt nach Artikel 11 DSG und Artikel 4 VDSZ. Das Zertifikat ist drei Jahre gültig. Der zertifizierte Bereich umfasst alle Datenbearbeitungsverfahren, welche der Erfüllung von Artikel **59a** KVV dienen. Das heisst, dass sowohl die elektronischen Datenbearbeitungsverfahren als auch der Papierprozess, welche mit der systematischen Weiterleitung der Datensätze sowie der Rechnung im Zusammenhang stehen, zertifiziert werden müssen. Werden solche Datenbearbeitungsverfahren von externen Dienstleistern ausgeführt, so sind auch diese zu zertifizieren.

Die Zertifizierungsstelle kann eine Zertifizierung sistieren oder entziehen, wenn schwere Mängel festgestellt werden (Art. 9 ff VDSZ). In beiden Fällen wären die Voraussetzungen von Artikel **59*a* Absatz 6** KVV nicht mehr erfüllt, und die DRG-Rechnungen dürften nicht mehr an den Versicherer übermittelt werden. Der Versicherer könnte auch nicht etwa deren Übermittlung an die Vertrauensärztin oder den Vertrauensarzt verlangen: Die Übermittlung von DRG-Rechnungen an den Vertrauensarzt oder die Vertrauensärztin ist seit dem 1. Januar 2014 nicht mehr zulässig. Vorbehalten bleiben aufsichtsrechtliche Massnahmen des BAG nach Artikel 21 Absätze 5 und 5bis KVG.

Die Leistungserbringer müssen der Datenannahmestelle des Versicherers die administrativen und medizinischen Angaben gleichzeitig mit der Rechnung 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** KVV).

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 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

[20] SR 431.012.1

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.

3. Datenannahmestelle

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. Bevor die Datenannahmestelle die für die Triage notwendige Auswertung des MCD vornimmt, muss durch die Datenannahmestelle sichergestellt sein, dass das MCD zu einer Rechnung gehört, welche tatsächlich eine beim jeweiligen Versicherer versicherte Person betrifft.

Alle unauffälligen Rechnungen werden zur Bezahlung freigegeben, wobei die medizinischen Angaben beim Versicherer verschlüsselt zu archivieren sind. Sofern die medizinischen Angaben nicht verschlüsselt aufbewahrt werden, müssen die Personalien der Versicherten zur Aufbewahrung dieser Angaben pseudonymisiert werden. Der Versicherer muss sicherstellen, dass die Bearbeitung der medizinischen Angaben nach Artikel 59 Absatz 1 KVV datenschutzkonform zu erfolgen hat (Artikel 21 und 22 VDSG).

Alle durch die Datenannahmestelle für eine vertiefte Überprüfung ausgelenkten Rechnungen müssen durch den Versicherer tatsächlich einer vertieften Kontrolle unterzogen werden. Es darf nicht zu einer «Auslenkung auf Vorrat» kommen.

Nach vertiefter Überprüfung der auffälligen Rechnungen müssen die medizinischen Angaben ebenfalls verschlüsselt oder pseudonymisiert archiviert werden.

Nach erfolgter Archivierung kann nur der Vertrauensarzt oder die Vertrauensärztin die Verschlüsselung oder Pseudonymisierung aufheben (Art. **59a ter Abs. 2** KVV).