Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Bern, 23. Februar 2022

Schutz der Patientendaten und Schutz der Versicherten

Ergänzender Bericht in Erfüllung des Postulates 08.3493 Heim vom 18.09.2008

Zusammenfassung

Im Jahre 2008 wurde der Bundesrat durch das überwiesene Postulat Heim (08.3493 – Schutz der Patientendaten und Schutz der Versicherten) beauftragt, in einem Bericht aufzuzeigen, welche Massnahmen gegen die Diskriminierung einzelner Patientengruppen durch die damals neu eingeführten besonderen Versicherungsmodelle (vgl. Art. 93 ff. KVV) und zum Schutz der Patientendaten bei den Krankenversicherern geplant sind.

Vom 4. Dezember 2007 – 16. Juni 2009 wurde die erste flächendeckende Datenschutzerhebung des BAG und des EDÖB durchgeführt. Dabei wurde festgestellt, dass der Schutz der Patientendaten grundsätzlich sichergestellt ist. Die Erhebung ergab aber auch, dass in einigen Bereichen noch Verbesserungsbedarf besteht. Am 16. Juni 2009 wurden die Ergebnisse veröffentlicht und es wurden auch Empfehlungen abgegeben.

In den Jahren 2011 – 2012 erfolgte die zweite umfassende Datenschutzerhebung betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer. Zudem wurden die Krankenversicherer sowohl durch den EDÖB wie auch durch das BAG in den im beiliegenden Bericht genannten Bereichen laufend beaufsichtigt.

Die Ergebnisse der zweiten Datenschutzerhebung von 2011 – 2012 belegen, dass die KVG-Versicherer frühere Mängel mehrheitlich behoben haben und professioneller mit dem Datenschutz umgehen als bei der ersten Erhebung.

Der Bundesrat stellte aufgrund dieser zweiten Erhebung und der Kontrolltätigkeit der Aufsichtsbehörden EDÖB und BAG in seinem Bericht vom 18. Dezember 2013 fest, dass die KVG-Versicherer mehrheitlich die nötigen Vorkehrungen für die Sicherstellung des Datenschutzes und der Datensicherheit getroffen haben. Der Bericht des Bundesrates stellte aber auch fest, dass gewisse Punkte nach wie vor nicht ganz erfüllt wurden.

Deshalb wurden das BAG und der EDÖB durch den Bundesrat verpflichtet, im Rahmen ihrer Aufsichtstätigkeit dafür zu sorgen, dass noch vorhandene Mängel in diesem Bereich korrigiert und die datenschutzrechtlichen Vorgaben umgesetzt werden. Der EDÖB und das BAG haben in der Folge in den Jahren 2013 - 2019 viele Prüfungen vorgenommen. Sie haben dabei die Vorgaben zum Datenschutz und zur Datensicherheit laufend intensiv kontrolliert und die Einhaltung der Eckpfeiler des Datenschutzes durchgesetzt.

Weil im Bericht des Bundesrates vom 18. Dezember 2013 festgestellt wurde, dass eine weitere Datenschutzerhebung und ein zusätzlicher Bericht des Bundesrates erarbeitet werden soll, wurde das Postulat Heim im Jahre 2014 nicht abgeschrieben. Aufgrund der intensiven Aufsichtstätigkeit des EDÖB und des BAG seit dem Jahr 2013 beinhaltet die dritte Datenschutzerhebung ausschliesslich Fragen zum Kernbereich des Postulates, dem «Datenschutz bei besonderen Versicherungsformen».

Für diese dritte Datenschutzerhebung wurden drei Fragen gestellt. Bei der ersten Frage geht es darum, welche Daten zu welchen Zwecken zwischen den involvierten Stellen (namentlich Gatekeeper/koordinierende Leistungserbringer, beauftragte Dritte und internen Abteilungen der Versicherer) bei besonderen Versicherungsformen ausgetauscht werden. Es wurde zudem gefragt, über welche Kanäle (insbesondere Portale/Plattformen) ein solcher Datenaustausch stattfindet und welche Datenflüsse insbesondere Überweisungen durch den Gatekeeper auslösen.

Zweitens wurde gefragt, welche technischen und organisatorischen Massnahmen die Versicherer zur Sicherung besonders schützenswerter Personendaten bei besonderen Versicherungsformen getroffen haben.

Drittens wurde gefragt, ob für den Versicherer die Möglichkeit besteht, auf die IT-Systeme (z.B. Praxis-Informationssystem) der Gatekeeper zuzugreifen, um Einsicht in medizinische Patientenakten zu erhalten.

Schutz der Patientendaten und Schutz der Versicherten

Die Ergebnisse zur Frage 1 zeigen, dass Bestandesdaten, Überweisungen (Zeitfenster) und Leistungsdaten zwischen den Krankenversicherern, allfälligen externen Dienstleistern und Gatekeepern ausgetauscht werden. Der Zweck des Datenaustauschs ist die Kontrolle und Durchsetzung der in den Versicherungsbedingungen der besonderen Versicherungsmodelle festgehaltenen Überweisungsregeln sowie die Steuerung durch die Leistungserbringer, wo das im Modell vorgesehen ist. Für die Übermittlung werden durchgehend gesicherte, d.h. verschlüsselte Kanäle eingesetzt (HIN, SFTP usw.). Nur in seltenen Ausnahmefällen geschieht noch eine Datenübermittlung in Papierform (vom Arzt an den Versicherer).

Die Ergebnisse zur Frage 2 zeigen, dass die eingesetzten technischen Massnahmen (Verschlüsselungen, Infrastruktur in geschützten Zonen, mit Zertifikaten geschützte Verbindungen usw.) durchgehend dem aktuellen Stand der Technik entsprechen. Der zugriffsberechtigte Personenkreis und die Umsetzung der Massnahmen bei den externen Dienstleistern wird durch die Krankenversicherer kontrolliert.

Als Ergebnis zur Frage drei kann festgehalten werden, dass in keinem Fall der Versicherer Einsicht in die Systeme der Gatekeeper hat.

Bei der Einreichung des Po. Heim im Jahre 2008 befand sich der Datenschutz noch im Stadium des Aufbaus. Mit der ersten und zweiten Datenschutzerhebung, dem Bericht des Bundesrates vom 18. Dezember 2013 sowie der dauernden Aufsichtstätigkeit des EDÖB und des BAG wurden die noch vorhandenen Mängel laufend korrigiert. Mehr und mehr wurden damit die datenschutzrechtlichen Vorgaben umgesetzt und grundsätzlich eingehalten. Mit der dritten Datenschutzerhebung wird die Lücke, die insbesondere den Kernbereich des Po. Heim betrifft, geschlossen.

Die Ergebnisse der dritten Datenschutzerhebung zeigen, dass die notwendigen Massnahmen getroffen wurden, um den Datenschutz im Bereich der besonderen Versicherungsformen grundsätzlich sicherzustellen. Die Beaufsichtigung der KVG-Versicherer durch den EDÖB und BAG ist ausreichend, um sicherzustellen, dass allfällige Lücken im Datenschutz festgestellt werden und die erforderlichen Massnahmen im Rahmen der geltenden Aufsichtskompetenzen ergriffen werden können.

Abkürzungsverzeichnis

ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts
BAG	Bundesamt für Gesundheit
BBl	Bundesblatt
DAS	Datenannahmestellen
DRG	Diagnosis Related Groups (Diagnosebezogene Fallgruppen)
DSG	Bundesgesetz über den Datenschutz
EDI	Eidgenössisches Departement des Innern
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
HA	Hausarzt
HAM	Health Maintenance Organization (Gesundheitserhaltungsorgansation)
HIN	Health Info Net (Verschlüsselung)
HMO	Hausarzt-Modell
ISO	Internationale Organisation für Normung
KVAG	Bundesgesetz betreffend die Aufsicht über die soziale Krankenversicherung
KVAV	Verordnung betreffend die Aufsicht über die soziale Krankenversicherung
KVG	Bundesgesetz über die Krankenversicherung
KVV	Verordnung über die Krankenversicherung
PV	Prämienverbilligung
RVK	Dienstleister im Schweizer Gesundheitsmarkt
SFTP	Secure File Transfer Protocol (Verschlüsselung)
SR	Systematische Rechtssammlung
SSL	Secure Sockets Layer (Verschlüsselung)
Telmed	Telefonische medizinische Beratungsstelle
VDSZ	Verordnung über die Datenschutzzertifizierungen

Inhaltsverzeichnis

1 Ausgangslage

Der Bundesrat wurde durch das überwiesene Postulat Heim (08.3493 – Schutz der Patientendaten und Schutz der Versicherten) im Jahre 2008 beauftragt, in einem Bericht aufzuzeigen, welche Massnahmen gegen die Diskriminierung einzelner Patientengruppen durch die damals neu eingeführten besonderen Versicherungsmodelle (vgl. Art. 93 ff. KVV) und zum Schutz der Patientendaten bei den Krankenversicherern geplant sind. In den Jahren 2007 – 2009 erfolgte eine erste Datenschutzerhebung des Bundesamtes für Gesundheit (BAG) mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bei den KVG-Versicherern.

Nach Erlass des Kreisschreibens 7.1 am 25. August 2011 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer erfolgte in den Jahren 2011 – 2012 die zweite Datenschutzerhebung. Die Ergebnisse stützen sich mehrheitlich auf Angaben der KVG-Versicherer. Es erfolgten aber zum Beispiel auch regelmässige Datenschutzkontrollen (Stichproben) vor Ort bei den KVG-Versicherern durch die Sektion Audit des BAG.

Mit dem Bericht des Bundesrates in Erfüllung des Postulats Heim vom 18. Dezember 2013 wurde umfassend über die damals aktuelle Situation des Schutzes der Patientendaten bei den Krankenversicherern informiert. Die Ergebnisse der zweiten Erhebung belegen, dass die KVG-Versicherer frühere Mängel mehrheitlich behoben haben und professioneller mit dem Datenschutz umgehen als bei der ersten Erhebung. Zahlreiche Punkte hatten sich im Vergleich zur ersten Datenschutzerhebung des BAG/EDÖB (2007-2009) verbessert, andere blieben aber nach wie vor nicht ganz erfüllt.

Deshalb wurde das BAG im Bericht des Bundesrates vom 18. Dezember 2013 beauftragt, im Rahmen seiner Aufsichtstätigkeit dafür zu sorgen, dass noch vorhandene Mängel korrigiert werden. Überdies wurde in diesem Bericht festgehalten, dass das BAG in den nächsten drei bis fünf Jahren einen weiteren Bericht erarbeiten soll. Dieser Bericht soll dem Bundesrat sowie dem Parlament zur Kenntnis gebracht werden. Aus diesem Grunde wurde das Postulat Heim vom Parlament noch nicht abgeschrieben.

Seit dem Bericht des Bundesrates vom 18. Dezember 2013 haben das BAG und der EDÖB die KVG-Versicherer regelmässig in den im beiliegenden Bericht genannten Bereichen beaufsichtigt und festgestellt, dass die nötigen Vorkehrungen für die Sicherstellung des Datenschutzes grundsätzlich getroffen wurden. Im Kernbereich des Postulats Heim, bei den besonderen Versicherungsformen, ist seit dem Bericht des Bundesrates von 2013 keine besondere zusätzliche Beaufsichtigung durch das BAG und den EDÖB erfolgt.

Aufgrund der Verpflichtung zu einer dritten Erhebung und einem weiteren Bericht haben das BAG zusammen mit dem EDÖB Fragen im Bereich dieser Lücke bei den besonderen Versicherungsformen vorbereitet und diese den Krankenversicherern unterbreitet. Aufgrund des Berichtes des Bundesrates vom 18. Dezember 2013 sowie der seit damals erfolgten intensiven Aufsichtstätigkeiten des EDÖB und des BAG wurden für den Ergänzungsbericht ausschliesslich Fragen zum Kernbereich des Postulates («Datenschutz bei den besonderen Versicherungsformen»), gestellt (vgl. unten Ziffer 6.1.).

Durch die Auswertung der Antworten auf die gestellten Fragen soll festgestellt werden, ob es noch immer offene Punkte gibt oder ob das Postulat Heim nun abgeschrieben werden kann.

2 Erste Datenschutzerhebung von 2007 -2009

Vom 4. Dezember 2007 – 16. Juni 2009 wurde die erste flächendeckende Datenschutzerhebung des BAG und des EDÖB durchgeführt. Diese hat ergeben, dass die Krankenversicherer für die Datenschutzproblematik sensibilisiert sind. Es wurde festgestellt, dass der Schutz der Daten trotz unterschiedlicher Organisationsstrukturen grundsätzlich sichergestellt ist. Diese erste Datenschutzerhebung ergab aber auch, dass in einigen sensiblen Bereichen noch Verbesserungsbedarf besteht. Mit der Veröffentlichung der Ergebnisse der Datenschutzerhebung am 16. Juni 2009 wurden auch Empfehlungen abgegeben.

3 Massnahmen des BAG seit der ersten Erhebung von 2007 - 2009

3.1 Kreisschreiben 7.1 vom 25. August 2011

Am 25. August 2011 wurde das Kreisschreiben betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer erlassen. Dieses wurde am 17. Juni 2013 aktualisiert. Dieses Kreisschreiben 7.1 schreibt den KVG-Versicherern vor, welche Vorkehrungen sie zum Schutz der Personendaten und vor allem der besonders schützenswerten Personendaten (insbesondere Gesundheitsdaten) treffen müssen.

Gleichzeitig kündigte das BAG den KVG-Versicherern an, sie einige Monate später gestützt auf das Kreisschreiben zu befragen, welche Vorkehrungen sie getroffen hätten und noch treffen würden, um die Empfehlungen und Vorgaben umzusetzen. Auch wurde mitgeteilt, dass die Vorgaben des Kreisschreibens namentlich im Rahmen regelmässiger Kontrollen und Stichproben durch die Sektion Audit des BAG geprüft würden.

3.2 Zweite Datenschutzerhebung von 2011 – 2012 betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer

Mit Schreiben vom 13. Dezember 2011 erhielten die KVG-Versicherer einen umfangreichen Fragebogen für die Kontrolle der Umsetzung des Kreisschreibens 7.1 zu folgenden Punkten: Stand der Datenschutz- und Datensicherheitskonzepte, Stand der Datenbearbeitungsreglemente, aktuelle Verzeichnisse der Datensammlungen und deren Registrierung beim EDÖB, ausgelagerte Dienstleistungen und datenschutzkonforme Datenbearbeitung durch die Dienstleister, strukturelle Unabhängigkeit des Vertrauensärztlichen Dienstes, verantwortliche Stelle für den betrieblichen Datenschutz und Datenschutzschulungen im Betrieb, Datenschutzmanagementsysteme und –zertifizierungen, Case Management und Inhalt der Vollmachten und Einwilligungserklärungen der Versicherten für die Weitergabe medizinischer Angaben an Dritte. Weitere Fragen betrafen den Datenaustausch zwischen den bei besonderen Versicherungsmodellen involvierten Stellen.

Fragen zur Sicherstellung des Datenschutzes und der Datensicherheit in Zusammenhang mit den Datenlieferungen der Leistungserbringer nach Einführung des Fallpauschalensystems Swiss DRG wurden von dieser zweiten Erhebung ausgeklammert, weil die Regelung für die Übermittlung der abrechnungsrelevanten medizinischen Daten zu jenem Zeitpunkt noch offen war.

3.3 Prüfungen der Krankenversicherer vor Ort durch die Sektion Audit des BAG zwischen 2009 und 2013

Im Rahmen seiner Aufsichtsfunktion führt das BAG regelmässig Audits durch. Ziel und Zweck dieser Kontrollen und Stichproben am Standort der KVG-Versicherer ist die Überwachung des

Schutz der Patientendaten und Schutz der Versicherten

Vollzugs des Bundesgesetzes über die Krankenversicherung (KVG; SR 832.10) und dessen Verordnungen sowie der vom BAG erteilten Weisungen. Das Prüfprogramm beinhaltet auch den Datenschutz. Seit 2012 stellt die Überprüfung des Datenschutzes eines der Schwerpunktthemen der Audits dar. Die Grundlage der Audit-Prüfung war das jeweils aktuell geltende Kreisschreiben des BAG.

Bei den Audits wird ermittelt, ob der KVG-Versicherer über eine datenschutzkonforme Organisation verfügt und ob die Abwicklung des Datenschutzes bei der Bearbeitung und Aufbewahrung von Daten und Akten (vor allem im vertrauensärztlichen Dienst) nach definierten Prozessen und entsprechend den gesetzlichen Bestimmungen nach dem Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG; SR 830.1), dem KVG sowie dem Bundesgesetz über den Datenschutz (DSG; SR 235.1) erfolgt.

Diese Audits vor Ort durch das BAG ersetzen aber in keiner Weise eine Zertifizierung nach Artikel 11 DSG und stellen auch keine Grundlage zu einer solchen Zertifizierung dar.

4 Ergebnisse der zweiten Datenschutzerhebung von 2011 – 2012 und Bericht des Bundesrates vom 18. Dezember 2013

Die Ergebnisse der zweiten Datenschutzerhebung von 2011-2012 beziehen sich auf folgende Themen: 1. Datenschutz- und Datensicherheitskonzepte der KVG-Versicherer, 2. Datenbearbeitungsreglemente und Konzepte für Zugriffsberechtigungen, 3. Register der Datensammlungen, 4. Outsourcing, 5. Vertrauensarzt und vertrauensärztlicher Dienst, 6. Betriebliche/r Datenschutzverantwortliche/r, 7. Datenschutzmanagementsystem und Datenschutzzertifizierungen, 8. Datenschutz bei der Durchführung besonderer Versicherungsformen (HMO- und Hausarztmodelle (Ärztenetzwerke(HAM) sowie Versicherungsmodell mit telemedizinischer Beratung), 9. Case Management, 10. Vollmachten und Einwilligungserklärungen.

Der Bericht listet für jedes dieser zehn Themen auf, was die durchgeführte Datenschutzerhebung ergeben hat.

Im Ergebnis kann zusammenfassend gesagt werden, dass die KVG-Versicherer frühere Mängel mehrheitlich behoben haben und professioneller mit dem Datenschutz umgehen als bei der ersten Erhebung. Im Hinblick auf die Durchführung von besonderen Versicherungsmodellen (Hauptfrage des Postulats Heim (08.3493)) wurden keine konkreten Hinweise für eine zweckfremde Bearbeitung medizinischer Daten gefunden. Zahlreiche Punkte haben sich im Vergleich zur ersten Datenschutzerhebung, welche das BAG zwischen 2007 und 2009 noch zusammen mit dem EDÖB durchführte, verbessert, andere bleiben aber nach wie vor nicht ganz erfüllt.

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

Das Parlament hat am 23. Dezember 2011 gestützt auf die parlamentarische Initiative 11.429 Tarmed. Subsidiäre Kompetenz des Bundesrates (vgl. BBl 2012 55) einen neuen Artikel 42 Absatz 3bis im KVG verabschiedet. Dieser Absatz sieht vor, dass die Leistungserbringer auf der Rechnung die Diagnosen und Prozeduren nach den aktuellen Klassifikationen kodiert aufführen. Ferner sieht dieser Absatz zusätzlich vor, dass der Bundesrat ausführende Bestimmungen zur Erhebung, Bearbeitung und Weitergabe der Daten unter Wahrung des Verhältnismässigkeitsprinzips erlässt. Nach Absatz 4 kann der Versicherer zusätzliche Auskünfte medizinischer Natur verlangen.

Schutz der Patientendaten und Schutz der Versicherten

Der Bundesrat hat anschliessend am 4. Juli 2012 in Artikel 59a KVV die Modalitäten der Datenweitergabe für DRG festgelegt, damit das Verhältnismässigkeitsprinzip gewahrt wird. Spätestens ab 2014 sollen die Spitäler die administrativen und medizinischen Angaben bei der Rechnungsstellung systematisch an eine vom KVG-Versicherer eingerichtete zertifizierte Datenannahmestelle übermitteln. Die Versicherer hatten bis Ende 2013 Zeit, eine Datenannahmestelle einzurichten und diese gemäss Artikel 11 DSG zertifizieren zu lassen. Es wurde festgelegt, dass die Zertifizierung vom EDÖB überwacht wird, der auch die Liste der zertifizierten Datenannahmestellen zu veröffentlichen hat.

Zudem hat das EDI am 20. November 2012 die gesamtschweizerisch einheitliche Struktur der Datensätze in Form einer Verordnung (Verordnung des EDI über die Datensätze für die Datenweitergabe zwischen Leistungserbringern und Versicherern; SR 832.102.14) festgelegt. Damit sind die Datensätze mit den administrativen und medizinischen Angaben schweizweit einheitlich definiert. Damit ist auch die Frage der Datenübermittlung – im Rahmen der Rechnungsstellung – zwischen den KVG-Versicherern und Spitälern definitiv geregelt. Die entsprechenden Änderungen des KVG (Art. 42 Abs. 3bis und 4) und der KVV (Art. 59 ff.) sowie die EDI-Verordnung sind per 1. Januar 2013 in Kraft getreten.

Der EDÖB und auch das BAG haben die Umsetzung dieser Bestimmungen durch die KVG-Versicherer in den letzten Jahren begleitet und kontrolliert.

4.2 Fazit des Berichts des Bundesrates vom 18. Dezember 2013

Der Bundesrat stellte aufgrund dieser zweiten Erhebung und der Kontrollmassnahmen der Aufsichtsbehörden BAG und EDÖB fest, dass die KVG-Versicherer mehrheitlich die nötigen Vorkehrungen für die Sicherstellung des Datenschutzes und der Datensicherheit getroffen haben. Frühere Mängel wurden überwiegend behoben. Der Umgang mit dem Datenschutz wurde gegenüber der ersten Erhebung professioneller.

Der Bericht des Bundesrates vom 18. Dezember 2013 stellt damit fest, dass sich zahlreiche Punkte im Vergleich zur ersten Datenschutzerhebung durch den EDÖB und das BAG in den Jahren 2007 – 2009 verbessert haben. Es wird aber auch festgestellt, dass gewisse Punkte nach wie vor nicht ganz erfüllt wurden.

Deshalb wurden das BAG und der EDÖB verpflichtet, im Rahmen ihrer Aufsichtstätigkeit dafür zu sorgen, dass die noch vorhandenen Mängel korrigiert werden und dass die datenschutzrechtlichen Vorgaben umgesetzt werden. Auch soll in den nächsten drei bis fünf Jahren ein weiterer Bericht erarbeitet und dem Bundesrat sowie dem Parlament zur Kenntnis gebracht werden. Es wurde auch festgestellt, dass die Aufsichtsbehörden BAG und EDÖB über eine Palette von Instrumenten verfügen, um bei Bedarf datenschutzspezifische Korrekturmassnahmen von den KVG-Versicherern zu fordern.

Diese Verpflichtung zu einer dritten Erhebung und einem weiteren Bericht ist Ausgangspunkt für den vorliegenden Ergänzungsbericht des Bundesrates.

5 Aufsicht des EDÖB und des BAG seit dem Bericht des Bundesrates vom 18. Dezember 2013

Wie in den Tätigkeitsberichten des EDÖB ab dem Jahre 2013 dargestellt wird, hat dieser in den vergangenen Jahren viele Bereiche des Datenschutzes bei den Krankenversicherern beaufsichtigt, so z.B. die Datenannahmestellen (inkl. Zertifizierung), die Bearbeitungsreglemente, die Rechnungsstellung nach Swiss DRG, die Auslagerung der Rechnungsstellung im medizinischen Bereich, die Auslagerung von Aufgaben der Krankenversicherer an branchen-

fremde Dienstleister, Datenbekanntgabe durch die Krankenversicherer im Rahmen der Prämienverbilligung (PV), Vollmachten im Krankenversicherungsbereich, die Leitfäden zu den technischen und organisatorischen Massnahmen des Datenschutzes und das Datenaustauschformat für DRG-Rechnungen.

Die Sektion Audit des BAG hat zwischen 2013 und 2018 im Prüfbereich Datenschutz 42 Audits durchgeführt. Dabei lag der Fokus auf der Prüfung der Einhaltung der Vorgaben zum Datenschutz und zur Datensicherheit gemäss dem Kreisschreiben 7.1. Ab 2017 und bis Anfang 2018 standen die Bereiche Datenschutzmanagementsystem, Umgang mit besonders schützenswerten Personendaten, Organisation des vertrauensärztlichen Dienstes und Prüfprozess SwissDRG ausserhalb der DAS-Zertifizierung im Vordergrund. Im 2018 kam schliesslich die Thematik «Outsourcing» hinzu. Dabei wurde aber weiterhin stets geprüft, ob die Vorgaben gemäss dem Kreisschreiben 7.1 eingehalten sind. In Bezug auf die erstellten Bearbeitungsreglemente wird deren Beurteilung gemäss Artikel 84b KVG durch den EDÖB vorgenommen. Die Aufsicht über die Zertifizierung der Datenannahmestelle obliegt nach Artikel 59a Absatz 7 KVV ebenfalls dem EDÖB. Die Sektion Audit hat dementsprechend keine detaillierten Prüfungen in diesen Bereichen vorgenommen.

Während das BAG die erste Erhebung in den Jahren 2007-2009 noch zusammen mit dem EDÖB gemacht hat, erfolgte nachher die Zusammenarbeit grundsätzlich nur noch in Form von Koordinationssitzungen, im Rahmen von Ämterkonsultationen usw. Wie dem Tätigkeitsbericht des EDÖB 2016/2017 (vgl. Ziff. 1.6.2., Seite 25) entnommen werden kann, war das Ziel dieser Sitzungen, die sich teilweise überschneidenden Aufsichtstätigkeiten der beiden Behörden zu koordinieren und offene Fragen zu diskutieren. Der EDÖB und das BAG gingen also in diesen Jahren von einer überschneidenden Zuständigkeit aus.

Die Grundlage der Audit-Prüfung des BAG ist das jeweils aktuell geltende Kreisschreiben 7.1 des BAG (vgl. KS 7.1 vom 25. August 2011; KS 7.1 vom 17. Juni 2013; KS 7.1 vom 1. November 2014 und KS 7.1 vom 17. Dezember 2015).

Das bis Ende 2021 geltende KS 7.1 vom 17. Dezember 2015 «Datenschutzkonforme Organisation und Prozesse der Krankenversicherer» wurde in den Jahren 2020 und 2021 grundlegend überarbeitet und durch das neue KS 7.1 «Aufsicht des BAG über datenschutzrelevante Bereiche gemäss KVAG, KVAV, KVG und KVV» ersetzt (Inkrafttreten 1. Januar 2022). Während dieser Zeit war die Finalisierung des Berichts sistiert. Die Überarbeitung des KS 7.1 erfolgte in enger Zusammenarbeit mit dem EDÖB. Dabei wurde die Gelegenheit genutzt, sich auch in Bezug auf die Zuständigkeiten der beiden Behörden zu verständigen. Im Zuge der Revision des KS 7.1 hat auch die Abgrenzung der Zuständigkeit bei der Aufsicht im Bereich Datenschutz zwischen dem EDÖB und dem BAG geklärt und bereinigt werden können.

6 Dritte Datenschutzerhebung von 2019

6.1 Fragen

6.1.1 Frage 1

Welche Daten werden zu welchen Zwecken zwischen den involvierten Stellen bei besonderen Versicherungsformen (KVG) ausgetauscht?

Über welche Kanäle (insbesondere Portale/Plattformen) findet ein solcher Datenaustausch statt?

Welche Datenflüsse lösen insbesondere Überweisungen durch den Gatekeeper aus?

Schutz der Patientendaten und Schutz der Versicherten

Bitte beziehen Sie sich insbesondere auf den Datenaustausch zwischen den involvierten Stellen (namentlich Gatekeeper/koordinierende Leistungserbringer, beauftragte Dritte [Dienstleister] und internen Abteilungen der Versicherer). Falls vorhanden, ersuchen wir Sie, ein Datenfluss-Schema beizulegen.

Ausserdem bitten wir Sie bei Ihrer Antwort zu unterscheiden nach: 1. HMO-Versicherungsmodelle, 2. Hausarzt-Versicherungsmodelle, 3. Versicherungsmodelle mit telemedizinischer Beratung, 4. Andere Versicherungsmodelle und 5. Gemeinschaftspraxen, an welchen Sie allenfalls beteiligt sind.

6.1.2 Frage 2

Welche technischen und organisatorischen Massnahmen haben Sie zur Sicherung besonders schützenswerter Personendaten bei besonderen Versicherungsformen getroffen?

6.1.3 Frage 3

Besteht für den Versicherer die Möglichkeit, auf die IT-Systeme (z.B. das Praxis-Informationssystem) der Gatekeeper zuzugreifen, um Einsicht in medizinische Patientenakten zu erhalten? Falls ja, in welchen Fällen (namentlich gemäss Aufzählung in Frage 2.1)?

6.2 Ergebnisse der dritten Datenschutzerhebung von 2019

6.2.1 Allgemeines

Alle Versicherer, welche besondere Versicherungsformen anbieten haben die drei Fragen beantwortet. Versicherungsgruppen haben grundsätzlich für alle beteiligten Versicherer nur eine Antwort abgegeben. Es sind somit für 50 Versicherer Antworten eingetroffen. Sieben Versicherer sind entweder reine Taggeldversicherer oder sie bieten keine besonderen Versicherungsformen an.

Die Antworten sind vorwiegend technischer Natur und werden im Bericht nicht vollständig wiedergegeben, da sie sich abhängig von den besonderen Versicherungsbedingungen und Versicherungsprodukte des jeweiligen Versicherers unterscheiden. Nachfolgend sind die Ergebnisse zusammengefasst und es werden ergänzend drei illustrative Beispiele von Antworten auf die Frage 1 und 2 ausgeführt, welche die Abläufe aufzeigen bei kleinen und mittelgrossen Versicherern, welche die Kontrollen zur Einhaltung der besonderen Versicherungsformen an externe Dienstleister ausgelagert haben oder Mittelgrosse, bzw. Grossversicherer, welche diese Kontrollen selbst durchführen. Die Antworten auf die Frage 3 sind bei allen Versicherern identisch ausgefallen.

6.2.2 Ergebnisse zur Frage 1

Allgemein kann zusammenfassend gesagt werden, dass Bestandesdaten, Überweisungen (Zeitfenster) und Leistungsdaten zwischen den Krankenversicherern, allfälligen externen Dienstleistern und Gatekeeper ausgetauscht werden, wo das im Modell vorgesehen ist. Für die Übermittlung werden durchgehend gesicherte, d.h. verschlüsselte Kanäle eingesetzt. Nur in seltenen Ausnahmefällen geschieht noch eine Datenübermittlung in Papierform (vom Arzt an den Versicherer).

Die Frage 1 wurde von je einem Versicherer der erwähnten Kategorie repräsentative Beispiele 1-3) wie folgt beantwortet:

Schutz der Patientendaten und Schutz der Versicherten

1. Beispiel (Outsourcing)

Der Krankenversicherer übermittelt dem Dienstleister (Outsourcingpartner: RVK) Bestandes- und Leistungsdaten. Dieser bereitet die Daten in seinem IT-System auf und sendet sie gebündelt nach Ärztenetzwerk oder Telefonanbieter an den von den Netzwerken gewünschten IT-Anbieter, welcher die Daten in seine Systeme importiert und den Ärzten, bzw. Telefonanbietern zur Verfügung stellt.

Die Betriebsgesellschaften (IT-Anbieter der Ärztenetzwerke / Telefonanbieter) übermitteln die von den Ärzten im System erfassten Überweisungen monatlich dem Dienstleister. Dieser liest sie wiederum gebündelt in sein IT-System ein und stellt die Daten dem Krankenversicherer zur Verfügung. In den von den Ärzten verwendeten Systemen werden ebenfalls Leistungsdaten bearbeitet. Um diese zu beurteilen, hat der Hausarzt die Möglichkeit, via Dienstleister eine Rechnungskopie zu bestellen. Dieser leitet die Bestellung an die Kasse weiter. Sobald der Dienstleister die Rechnungskopie hat, stellt er sie via Betriebsgesellschaft dem Arzt zur Verfügung.

Verstösse werden dem Dienstleister von den Betriebsgesellschaften monatlich zur Verfügung gestellt. Der Dienstleister importiert diese gebündelt in sein System und teilt diese der Kasse mit. Geahndete Verstösse meldet der Krankenversicherer den Betriebsgesellschaften, welche die angeschlossenen Ärzte darüber informieren.

Die Telefonanbieter erfassen ihre Überweisungen (Zeitfenster), welche je nach Wunsch der Krankenkasse (täglich, wöchentlich, zweiwöchentlich oder monatlich) dem Dienstleister übermittelt werden. Die Zeitfenster werden mit den Leistungsdaten zusammengeführt und in ein Filtersystem eingelesen. Somit können die Versicherer allfällige Verstösse ahnden und die Einhaltung der Versicherungsbedingungen sicherstellen.

2. Beispiel (eigene Überwachung, mittelgrosser Versicherer)

Der Krankenversicherer übermittelt den Gatekeeper/Leistungserbringern Administrativdaten (Versichertennamen, Adressen, Angaben zur Versicherungsdeckung). Zudem findet ein Austausch von Überweisungsdaten zwischen Leistungserbringern und Versicherern statt, sofern dies für die Abwicklung und das Verstossmanagement erforderlich ist. Der beschriebene Datenaustausch betrifft das Apothekermodell, das Telmedprodukt, das HMO-Versicherungsmodell, das Kombimodell /Telmed + HMO) sowie das HMO-Modell mit einer Gemeinschaftspraxis.

Im Hausarzt-Versicherungsmodell findet aktuell kein Datenaustausch statt. Die in Einzelfällen von den Gatekeepern übermittelten Überweisungsmeldungen, welche jedoch im Kernsystem speziell geschützt sind, lösen keine speziell definierten Datenflüsse aus und werden nicht weiterbearbeitet.

3. Beispiel (eigene Überwachung, Grossversicherer)

Die Krankenversicherer übermitteln den Telefonanbietern Administrativdaten zwecks Durchführung des Versicherungsproduktes insb. Identifikation des Versicherungsnehmers, Prüfung des Versicherers, Deckung. HMO-Praxen und Hausärzte erhalten Diagnose-, Behandlungs- und Rechnungsdaten zwecks Überprüfung der Einhaltung der produktspezifischen Voraussetzungen (wurde eine nicht-angeordnete Behandlung durchgeführt, besteht keine Leistungspflicht?).

Der Austausch der Administrativdaten mit Telefonanbietern erfolgt über zertifizierte Leitungen. Bei HMO- oder Hausarztmodellen erfolgt die Datenübermittlung via einen datenschutzgesi-

cherten Mailkanal, nur in Ausnahmefällen in Papierform. Überweisungen durch den Gatekeeper lösen folgende Datenflüsse aus: Der Hausarzt, HMO-Arzt oder Telefonanbieter beurteilt die medizinisch notwendigen Massnahmen aufgrund der Angaben der versicherten Person und ordnet allenfalls weitere medizinische Behandlungen an. Beim Telefonmodell werden dem weiterbehandelnden Leistungserbringer in der Regel keine medizinischen Daten bekannt gegeben. Die Datenweitergabe bei HMO-Anbietern oder Hausärzten liegt in deren Verantwortung und somit nicht in der Verantwortung des Versicherers.

6.2.3 Ergebnisse zur Frage 2

Generell kann zusammenfassend gesagt werden, dass Rechte und Pflichten betreffend Datenaustausch bzw. Datenschutz vertraglich mit den Leistungserbringern und den externen Dienstleistern geregelt sind. Nur spezifische Mitarbeitende haben Zugriff auf besonders schützenswerte Daten. Dies wird in Rollen- und Berechtigungskonzepten festgehalten. Die eingesetzten technischen Massnahmen (Verschlüsselungen, Infrastruktur in geschützten Zonen, mit Zertifikaten geschützte Verbindungen usw.) entsprechen durchgehend dem aktuellen Stand der Technik. Der zugriffsberechtigte Personenkreis und die Umsetzung der Massnahmen bei den externen Dienstleistern wird durch die Krankenversicherer kontrolliert.

Sowohl der externe Dienstleiser als auch die Versicherer selbst verfügen teilweise über entsprechende Zertifizierungen nach VDSZ:2014 bzw. über das Datenschutzgütesiegel GoodPriv@cy. Zudem sind teilweise auch deren IT-Infrastrukturen nach der Norm ISO 27001/2013 zertifiziert.

Die Frage 2 wurde von je einem Versicherer der erwähnten Kategorie (Beispiele 1-3) wie folgt beantwortet:

1. Beispiel (Outsourcing)

Der Austausch besonders schützenswerter Personendaten zwischen den Versicherern und dem Anbieter des Hausarztmodells erfolgt ausschliesslich über einen sicheren Kanal des Dienstleisters. Die mittels Client-Zertifikaten geschützten Verbindungen sind ausschliesslich auf den Rechnern und in den IT-Profilen der Personen installiert, welche Daten mit dem Dienstleister austauschen. Ein direkter Datenaustausch mit den Gatekeepern findet nicht statt.

Der Dienstleister (Outsourcingpartner: RVK) verwendet die Systeme exklusiv für das HMO-/Hausarztmodell und für Versicherungsmodelle mit telemedizinischer Beratung. Ein Zugriff ist nur über verschlüsselte Verbindungen möglich, welche über Benutzerzertifikate oder starke Passwörter geschützt sind. Über Zugriffsrechte verfügen nur diejenigen Mitarbeiter des Dienstleisters, die mit der Verarbeitung der Daten der erwähnten Versicherungsmodelle betraut sind, sowie die Mitarbeiter des Supports und die Entwickler der Software-Plattform (Zugriff nach Freigabe durch den Dienstleister). Alle unterstehen dem Datenschutzreglement des Dienstleisters.

Für die Datenaufbereitung und für den Transport der Daten von und zu den Versicherern werden getrennte Systeme eingesetzt. Die Leistungs- und Bestandesdaten der Versicherer werden durch den Dienstleister über eine verschlüsselte Verbindung abgeholt. Die dazu verwendeten Accounts sind ausschliesslich für HMO- und HA-Daten vorgesehen.

Der Austausch der Daten mit den Gatekeepern via deren Betriebsgesellschaft erfolgt ausschliesslich über die sichere Kommunikationsplattform HIN. Jede Betriebsgesellschaft wird individuell beliefert, so dass sie nur die Daten ihrer angeschlossenen Ärzte erhält.

Schutz der Patientendaten und Schutz der Versicherten

2. Beispiel (eigene Überwachung, mittelgrosser Versicherer)

Eine mehrstufige Firewall Infrastruktur mit Zonenkonzept sorgt für den Schutz der besonders schützenswerten Daten. Mittels Rollen- und Berechtigungskonzept werden die Zugriffe gesteuert und die Daten nur denjenigen Mitarbeitenden zugänglich gemacht, die diese Informationen für ihr Tagesgeschäft benötigen. Der zugriffsberechtigte Personenkreis wird regelmässig kontrolliert.

Der Datenaustausch erfolgt über gesicherte Kanäle und Schnittstellen.

3. Beispiel (eigene Überwachung, Grossversicherer)

Mit Sicherheits-, Datenschutz-, Informationssicherheits- und IT-Sicherheitsvorgaben wird der Schutz aller bearbeiteten Versichertendaten sichergestellt (umfassende Handlungsanweisungen und Verhaltensvorgaben). Zugriffskonzepte stellen sicher, dass nur diejenigen Mitarbeitenden Zugriffe auf Daten haben, welche diese auch benötigen.

Die Einhaltung dieser Vorgaben wird mit jährlichen Audits durch externe Zertifizierer überprüft. Im Sinne der kontinuierlichen Weiterentwicklung findet jährlich ein Aufrechterhaltungsaudit und nach 3 Jahren ein Rezertifizierungsaudit statt.

6.2.4 Ergebnisse zur Frage 3

Sämtliche Versicherer bestätigen, dass sie keine Einsicht in die Systeme der Gatekeeper haben.

7 Schlussfolgerung

Bei der Einreichung des Po. Heim im Jahre 2008 befand sich der Datenschutz noch im Stadium des Aufbaus. Die KVG-Versicherer wurden verpflichtet eine datenschutzkonforme Organisation und datenschutzkonforme Prozesse aufzubauen.

Bei der ersten Datenschutzerhebung wurde eine flächendeckende Erhebung durchgeführt und mit der Veröffentlichung der Ergebnisse wurden auch Empfehlungen abgegeben. Im Anschluss daran wurde auch ein Kreisschreiben erlassen und zwischen 2011 – 2012 wurde eine zweite, auch umfassende Datenschutzerhebung betreffend die datenschutzkonforme Organisation und Prozesse der KVG-Versicherer durchgeführt. Die Ergebnisse der zweiten Datenschutzerhebung belegen, dass sich zahlreiche Punkte im Vergleich zur ersten Erhebung verbessert haben, dass aber andere Punkte nach wie vor nicht ganz erfüllt waren.

In diesem Sinne zog auch der Bundesrat in seinem Bericht vom 18. Dezember 2013 das Fazit und verpflichtete das BAG und den EDÖB, im Rahmen ihrer Aufsichtstätigkeit dafür zu sorgen, dass die noch vorhandenen Mängel korrigiert werden und dass die datenschutzrechtlichen Vorgaben umgesetzt werden. Auch soll in den nächsten drei bis fünf Jahren ein weiterer Bericht erarbeitet und dem Bundesrat sowie dem Parlament zur Kenntnis gebracht werden. Es wurde aber im Bericht vom 18. Dezember 2013 auch festgestellt, dass die Aufsichtsbehörden BAG und EDÖB über eine Palette von Instrumenten verfügen, um bei Bedarf datenschutzspezifische Korrekturmassnahmen von den KVG-Versicherern zu fordern.

Im Anschluss an den Bundesratsbericht von 2013 erfolgte effektiv in den folgenden Jahren eine intensive Aufsichtstätigkeit durch den EDÖB und das BAG.

Mit der dritten Datenschutzerhebung wurde die Lücke bei den besonderen Versicherungsformen geschlossen. Die oben unter Ziffer 6.2 dargestellten Ergebnisse der dritten Datenschut-

zerhebung von 2019 zeigen, dass alle KVG-Versicherer über eine datenschutzkonforme Organisation bei den besonderen Versicherungsformen verfügen und dass die nötigen Massnahmen ergriffen wurden, um den Datenschutz auch in diesem Bereich zu gewährleisten.

Die Beaufsichtigung der KVG-Versicherer durch den EDÖB und BAG ist ausreichend, um sicherzustellen, dass allfällige Lücken im Datenschutz festgestellt werden und die erforderlichen Massnahmen im Rahmen der geltenden Aufsichtskompetenzen ergriffen werden können.

Zudem haben sich die beiden Behörden – wie oben in Ziffer 5 dargestellt – in Bezug auf ihre jeweiligen Zuständigkeiten abgestimmt und das BAG hat sein massgebendes KS 7.1 in enger Zusammenarbeit mit dem EDÖB entsprechend angepasst.

Es besteht deshalb kein zusätzlicher Handlungsbedarf.