



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Der Beauftragte

Datenbearbeitung im vertrauensärztlichen Dienst der CSS Kranken-Versicherung AG

Schlussbericht

(anonymisiert am 01.06.2007)

vom 17. April 2007

**der Sachverhaltsabklärung des
Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)
gemäss Art. 27 des Bundesgesetzes über den Datenschutz (DSG)**



1. Ausgangslage

Im Februar 2006 teilte der Beobachter in seinem Artikel „Einblicke in den Intimbereich“ mit, ihm lägen Dokumente vor, die zeigten, dass rund 400 CSS-Mitarbeiterinnen und Mitarbeiter – unter ihnen auch Mitarbeitende der Administration – auf das elektronische System „Anfragebewirtschaftung vertrauensärztlicher Dienst“ (AVD) Zugriff hätten. Dieser Beitrag blieb nicht unbeachtet. Er gab verschiedensten Medien Anlass zu einer Berichterstattung über einen „unzureichenden Datenschutz“ bei der CSS. Er veranlasste das Bundesamt für Gesundheit (BAG) im Rahmen seiner Aufsichtspflichten zum Handeln. In Zusammenarbeit mit dem Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragten (EDÖB) wurden Vorabklärungen durchgeführt, in deren Verlauf dem BAG und dem EDÖB ein interner Revisionsbericht der CSS vom 2.5.06 zugestellt wurde. Wegen des Verdachts auf Verletzung beruflicher Geheimhaltungspflichten hat das BAG am 15.5.06 eine Strafanzeige gegen die CSS eingereicht. Der EDÖB hat seinerseits die CSS mit Brief vom 23.5.06 darüber in Kenntnis gesetzt, dass er sich entschieden habe, im Rahmen seiner Aufsichtstätigkeit eine Sachverhaltsabklärung im Sinne von Art. 27 des Datenschutzgesetzes (DSG, SR 235.1) durchzuführen.

2. CSS-interner Revisionsbericht

Im Bericht der internen Revision der CSS wird zunächst festgestellt, dass der AVD in drei Bereiche unterteilt sei: Basic, Control, Medical. Im Bereich Basic könnten Anfragen an den Vertrauensarzt formuliert und Empfehlungen entgegengenommen werden. Im Bereich Control könnten zusätzliche medizinische Dokumente (zum Beispiel Arztberichte) bewirtschaftet werden, welche für die Beurteilung einer Sachlage und die Formulierung einer Empfehlung für den Vertrauensärztlichen Dienst (VAD) und die Experten notwendig seien. Zudem bestehe in diesem Bereich die Möglichkeit vertraulich medizinische Texte zu hinterlegen. Im Bereich Medical könnten zusätzlich eingescannte Fotos abgelegt werden.

Der Bericht der internen Revision weist ferner darauf hin, dass entgegen den Behauptungen in den Medienberichten nicht 400 Personen „uneingeschränkter Zugang zum AVD“ gehabt hätten. Zum Bereich Medical hätten ausschliesslich die Vertrauensärzte und deren Hilfspersonen (total 25 Personen) Zugang gehabt. Bis zum 22. Februar 2006 hätten ausserdem „gut 150 Personen“ Zugang zum Bereich Control gehabt. Inzwischen habe der VAD Massnahmen getroffen, um die Anzahl der Benutzer mit Control-Berechtigung anhand ihrer Zugriffshäufigkeit zu reduzieren. Der Kreis habe auf ungefähr 120 Personen eingeschränkt werden können. Parallel dazu habe die Interne Revision eine Analyse der internen Prozesse vorgenommen und daraus die Benutzer abgeleitet, die auf Zugriff zum Control-Bereich verzichten könnten. Im Bericht wird festgehalten, dass die von der Internen Revision festgehaltenen Benutzer sich weitestgehend mit denjenigen Personen decken würde, deren Berechtigung zwischenzeitlich bereits vom VAD eingeschränkt worden sei. Hinsichtlich der Berechtigungsvergabe stellte der Bericht fest, dass zum Zeitpunkt der Revision „in Bezug auf AVD kein standardisiertes Verfahren für das Beantragen, das Bewilligen und Dokumentation von Berechtigungen“ existierte. Daraus zieht der Bericht den Schluss: „.....“¹

Aus Sicht des EDÖB hat der Revisionsbericht gravierende Mängel beim VAD der CSS zu Tage geför-

¹ Aufgrund überwiegender Interessen der CSS an der Vertraulichkeit dieser Schlussfolgerung (Geschäftsgeheimnisse) wurde die entsprechende Passage für die Publikation aus dem Bericht herausgenommen.



dert. Die Analyse der internen Prozesse führte zu einer deutlichen Reduktion der Zugriffsberechtigungen zum heiklen Bereich der medizinischen Informationen. Wegen des fehlenden standardisierten Verfahrens für die Berechtigungsvergabe kann rückwirkend nicht mehr festgestellt werden, ob auch Unberechtigte Zugang zum sensiblen Bereich des VAD erhielten. Das ist im Rahmen des vom BAG eingeleiteten Strafverfahrens abzuklären.

3. Umfang der Sachverhaltsabklärung

Gemäss Art. 27 DSG überwacht der Datenschutz- und Öffentlichkeitsbeauftragte die Einhaltung dieses Gesetzes und der übrigen Datenschutzvorschriften des Bundes durch die Bundesorgane. Der Datenschutzbeauftragte klärt von sich aus oder auf Meldung Dritter hin den Sachverhalt näher ab. Bei der Abklärung kann er Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen. Die Bundesorgane müssen bei der Feststellung des Sachverhalts mitwirken. Das Zeugnisverweigerungsrecht nach Artikel 16 des Verwaltungsverfahrensgesetzes (VwVG, SR 172.021) gilt sinngemäss. Dem EDÖB stehen in einer angeordneten Sachverhaltsabklärung keine strafprozessualen Untersuchungsmassnahmen zu. Er kann weder Zeugen noch Auskunftspersonen vorladen. Ebenso wenig ist er befugt, aussagewillige Drittpersonen vom Berufsgeheimnis zu entbinden.

In verschiedenen Medienberichten wurden die Vorwürfe an die Adresse der CSS mit konkreten Beispielen von Datenschutzverletzungen untermauert. Wie unter Ziffer 2 ausgeführt, kann nicht ausgeschlossen werden, dass sich mit Bezug auf diese Beispiele Unberechtigte Zugang zu sensiblen Daten im VAD verschafften. Das BAG hat deshalb eine Strafuntersuchung veranlasst. Es obliegt dem Untersuchungsrichter abzuklären, inwieweit sich im Zusammenhang mit diesen Beispielen bei der CSS strafrechtlich relevante Sachverhalte ereignet haben.

Der EDÖB kontrollierte die aktuelle Datenbearbeitung im vertrauensärztlichen Dienst (nachfolgend VAD) der CSS Kranken-Versicherung AG (nachfolgend CSS KVG). In Art. 57 des Bundesgesetzes über die Krankenversicherung (KVG, SR 832.10) ist die gesetzliche Grundlage für Vertrauensärzte und Vertrauensärztinnen zu finden. Gemäss Art. 42 Abs. 5 KVG ist der Leistungserbringer in begründeten Fällen berechtigt und auf Verlangen der versicherten Person in jedem Fall verpflichtet, medizinische Angaben nur dem Vertrauensarzt oder der Vertrauensärztin des Versicherers nach Artikel 57 bekannt zu geben. Geprüft wurden im VAD deshalb insbesondere sämtliche Datenflüsse wie auch die Datenweitergabe an die Administration von CSS KVG.

4. Grundlage

Eine wichtige Grundlage der Sachverhaltsabklärung bildet zunächst der interne Revisionsbericht der CSS vom 2.5.06. Nach Überprüfung des AVD wurden in Bezug auf den Datenschutz CSS-intern punktuelle Optimierungen empfohlen. Insbesondere wurde veranlasst, dass die Anzahl Personen, die die Zugriffsberechtigungen erteilen können, möglichst klein zu halten sei, und dass die systemtechnische Zuteilung von Zugriffsberechtigungen nur den Mitgliedern des VAD zustünde. Im Rahmen der Sachverhaltsabklärung wurden sodann durch den EDÖB umfangreiche Dokumente über Organisation und interne Datenflüsse eingeholt. Anlässlich eines Augenscheins bei der CSS konnten die Räumlichkeiten und die Zugangskontrolle begutachtet sowie ausstehende Fragen in Bezug auf den VAD vor Ort geklärt werden.



Die daraus resultierende Sachverhaltsfeststellung des EDÖB wurde von der CSS bestätigt und in bereinigter Form verfasst (24.1.2007). Ergänzend wurde von Anfang an eine enge Zusammenarbeit mit dem BAG angestrebt und gepflegt.

5. Ablauf der Sachverhaltsabklärung

5.1. Dokumente

Mit Schreiben vom 23. Mai 2006 hat der EDÖB seine Sachverhaltsabklärung beim VAD der CSS KVG angekündigt. Im Rahmen der Sachverhaltsabklärung hat er schwergewichtig Dokumente über die Datenbearbeitung, die einzelnen Prozesse sowie die entsprechenden Datenflüsse einverlangt. Nach gewährter Fristerstreckung wurden diese Dokumente mittels Schreiben vom 6. Juli 2006 eingereicht. Der EDÖB unterzog diese einer eingehenden Analyse.

Aufgrund der gewonnenen Erkenntnisse wurden anlässlich des Augenscheins weitere Dokumente angefordert. Sie wurden mit Datum vom 20. November zugestellt. Eine letzte Dokumenteneingabe erfolgte am 3. Januar 2007.

5.2. Augenschein

Der Augenschein beim VAD der CSS KVG erfolgte am 30. Oktober 2006 in Anwesenheit der verantwortlichen Mitarbeiterinnen und Mitarbeiter der CSS und des EDÖB.

Anlässlich des Augenscheins wurden zunächst die Aufgaben der anwesenden Personen erläutert und Fragen zur Struktur der CSS Versicherung erörtert. In einem zweiten Schritt wurde die Datenbearbeitung im VAD vor Ort erklärt. Die Vorführung erfolgte dem zeitlichen Ablauf entsprechend, vom Eingang der Daten mit der Post bis zu deren Archivierung. Die mit den einzelnen Teilaufgaben der Datenbearbeitung betrauten Personen wurden während des Rundgangs vorgestellt. Insgesamt wurde ein gut strukturierter Einblick in die Datenflüsse und in die einzelnen Prozesse der Datenbearbeitung vermittelt.

5.3. Sachverhaltsfeststellung

Die durch den EDÖB erstellte Sachverhaltsfeststellung stützt sich auf die vor Ort gewonnenen Erkenntnisse sowie auf die von der CSS zugestellten Dokumente ab. Am 6. Dezember 2006 wurde sie dem VAD zur Stellungnahme zugestellt. Mit Korrekturen und Ergänzungen hat sie dieser am 3. Januar 2007 zurückgesandt. Die anschliessend bereinigte Version wurde dem VAD am 15. Januar 2007 zur erneuten Einsicht zugestellt. Der VAD hat sie mit letzten Korrekturen am 24. Januar 2007 zurückgeschickt. Sie flossen in die definitive Sachverhaltsfeststellung ein, welche dem EDÖB u.a. als Grundlage für vorliegenden Bericht dient.



6. Sachverhalt

6.1. Struktur CSS

Der CSS Verein ist Alleinaktionär der CSS Holding AG. Die Mitglieder des CSS Vereins werden durch einen 40-köpfigen Mitgliederrat vertreten. Die CSS Holding AG befindet sich als Dachgesellschaft und Finanzholding aller operativen Gesellschaften an der Spitze der CSS Gruppe.

Die CSS Gruppe besteht aus:

- CSS Kranken-Versicherung AG (KVG)
- Arcosana AG (KVG)
- Auxilia (KVG)
- CSS Versicherung AG (VVG) + Tochtergesellschaft: vivit gesundheits ag

Die oberste Leitung der CSS Gruppe übt der Verwaltungsrat aus. Die operative Leitung der CSS Gruppe obliegt der Geschäftsleitung.

Die Organe der Gesellschaft sind:²

6.2. Struktur VAD

Der VAD umfasst den Leiter des VAD (nachfolgend L-VAD), die Vertrauensärzte (nachfolgend VA) sowie die VertrauensarztassistentInnen (nachfolgend VA-Assistent).

Im VVG-Bereich fungiert der VAD als gesellschaftsärztlicher Dienst. Im VVG hat der Gesellschaftsarzt nur eine beratende Funktion, die Entscheidung liegt bei den entsprechenden Stellen der Administration.

Abgrenzung zwischen den einzelnen KVG-Versicherern

Es gibt einen VAD für die CSS KVG, die Arcosana AG sowie die Auxilia. Zwischen diesen drei Krankenversicherungen nach KVG gibt es den VAD betreffend keine Trennung. Die Mitarbeiter des VAD CSS KVG sind für alle drei Kassen zuständig.

Im Bereich der Administration gibt es gemäss CSS eine Trennung zwischen CSS Kranken-Versicherung, Arcosana und Auxilia durch die verschiedenen IT-Systeme. Die Versicherten der Arcosana und Auxilia sind von der CSS darauf aufmerksam gemacht worden, dass die Durchführung und die Bearbeitung der Daten durch Mitarbeiter der CSS Kranken-Versicherung AG erfolgt.

Innerhalb der Applikation AVD gibt es nach Versicherung unterteilte Datenbanken: CSS, Arcosana, Auxilia, Personal.

² Aufgrund überwiegender Interessen der CSS an der Vertraulichkeit dieses Inhalts (Geschäftsgeheimnisse) wurden die entsprechenden Angaben für die Publikation aus dem Bericht herausgenommen.



Abgrenzung zwischen KVG und VVG

Für KVG und VVG gibt es getrennte Policen. Es wird bei KVG-Anmeldungen auch kein Fragebogen verteilt. Im VVG-Vertrag ist aber geregelt, dass der Versicherer in die KVG-Unterlagen Einsicht nehmen darf.

90% der Anfragen betreffen die Leistung und somit den KVG Bereich.

10% der Anfragen betreffen das Taggeld und die Antragsgeschäfte und somit nur den VVG Bereich.

In Bezug auf die logische Trennung von KVG und VVG ist gemäss CSS zu bemerken, dass die meisten Versicherten der CSS beide Versicherungsarten bei der CSS abgeschlossen haben. Die Leistungserbringer stellen keine getrennten Kostengutsprache gesuche oder Rechnungen etc. zu. Eine Trennung dieser Bereiche wäre unverhältnismässig und für die Versicherten unverständlich. Es sind keine Fälle bekannt, in denen ein Versicherter eine getrennte Rechnungsstellung beim Leistungserbringer verlangt hätte.

Für den Bereich VVG besteht ein AVD-Zugriff auf dem Niveau Control, aber ohne Einsicht in die obligatorische Krankenpflegeversicherung (OKP). Die Mitarbeiter, die nur im VVG arbeiten, haben keinen Zugriff auf VAD-Daten von nur OKP-Versicherten.

Falls der Versicherte nur das KVG bei der CSS hat, wird bei Anfragen des VVG-Versicherers eine Vollmacht der versicherten Person verlangt.

Einen Zugriff auf die Berechtigungsstufe Basic reicht nicht, da die Mitarbeiter Empfehlungen machen müssen (vgl. auch die Kapitel Berechtigungsstufen und Zugriffsberechtigungen).

6.3. Abläufe im VAD

Die Abläufe im VAD werden in zeitlicher Folge aufgeführt und erläutert: vom Posteingang der Daten bis zu deren Archivierung. Abschliessend folgt ein Kapitel zum AVD-System.

6.3.1. Der Posteingang

6.3.1.1. Mail Source

Die Verarbeitung der Post (Eingang/Ausgang) wurde an die *Mail Source* – Tochtergesellschaft der Post – ausgegliedert.

Der eigentliche Posteingang der CSS erfolgt demnach bei *Mail Source*. Ihre Mitarbeitende unterziehen die eingehende Post vorschriftsgemäss einer Triage. Für den VAD gibt es ein separates Fach. *Mail Source* überbringt die Briefe sodann persönlich in das Sekretariat des VAD.

Werden von CSS Dokumente zuhanden des VAD eingeholt, wird ein Umschlag mit Anschrift des VAD bzw. des betroffenen Vertrauensarztes mitgeschickt.

Ist nicht ersichtlich, ob ein Umschlag für den VAD bestimmt ist, so wird er von *Mail Source*-Mitarbeitenden geöffnet. Die Triage erfolgt aufgrund des Inhalts. Bestehen Unsicherheiten, wird beim VAD direkt nachgefragt. Eine Mitarbeiterin ist Ansprechperson in Bezug auf die Triage aller Bereiche.

Mail Source-Mitarbeiter unterstehen dem Postgeheimnis.

Für die Postverteilung haben die Mitarbeiter von *Mail Source* Zugang zu den Räumlichkeiten der CSS. Beim VAD wird die Post nur an Anwesende des Sekretariats oder aber direkt an einen Vertrauensarzt verteilt. Bei Abwesenheit nimmt *Mail Source* die für den VAD bestimmte Post zurück.



Die Postverteilung erfolgt dreimal täglich: morgens (08.00), mittags (12.30) und abends (16.00).

Mail Source ist verantwortlich für die Post bis und mit Übergabe an die verschiedenen Bereiche von CSS.

6.3.1.2. Der Posteingang im Service-Center

An das Service-Center adressierte Postsendungen gelangen über den internen Postdienst des Leistungsbereichs CSS in den Posteingang des Service-Centers.

Das Service-Center umfasst die Sachbearbeiter Service-Center sowie die medizinischen Experten, nicht aber die Risikoprüfer/Risikoexperten oder die Taggeldsachbearbeiter und die Taggeldexperten, die in die Geschäftsbereiche Entwicklung & Innovation (respektive Markt) eingeordnet sind.

Im Service-Center wird eingegangene Post geöffnet und einer Triage unterzogen. Auch hier kann noch für den VAD bestimmte Post auftauchen, die irrtümlich nur mit Service-Center angeschrieben war. Dies geschieht täglich. Absender sind mehrheitlich Ärzte.

Für die Weiterleitung solcher Briefe an den VAD bestehen mündliche Richtlinien. Gemäss Art. 33 des Bundesgesetzes vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1) unterstehen alle Mitarbeiter der CSS der Schweigepflicht. Sie haben ein entsprechendes Formular zu unterschreiben.

6.3.2. Der vertrauensärztliche Dienst

6.3.2.1. Die Unabhängigkeit des VAD in Bezug auf das Budget

Der Vertrauensarzt (VA) hat die Vertraulichkeit aller ihm zur Verfügung gestellten medizinischen Informationen zu wahren (Art. 83 und 84 KVG). Gemäss Art. 5 Abs. 3 des Vertrauensarztvertrages zwischen santésuisse und FMH (nachfolgend VA-Vertrag) haben Versicherer die Stellung des Vertrauensarztes so zu organisieren, dass dessen Unabhängigkeit gewahrt wird und keine Interessenkonflikte entstehen. Insbesondere ist eine Leistungshonorierung nach dem Geschäftsergebnis des Versicherers unzulässig. Damit soll verhindert werden, dass Leistungseinsparungen über den VAD erfolgen. Entsprechend dürfen keine Budgetvorgaben gemacht werden. Auch die CSS hat ihren VAD dementsprechend organisiert. Wie jede andere Abteilung bei der CSS erhält der VAD ein Verwaltungsbudget. Dieses untersteht aber keinen Leistungseinsparungszielen. Die Stellenbewirtschaftung und Administration im VAD werden allein nach den anfallenden Tätigkeiten vorgenommen.

In Bezug auf die administrative Führung ist einzig der Geschäftsbereichsleiter Leistung berechtigt, Entscheide zu fällen. In dem vom Gesetz und vom VA-Vertrag vorgegebenen Aufgabenbereich ist der VAD laut eigenen Angaben unabhängig und nicht weisungsgebunden. Die organisatorische Einbindung des VAD in unmittelbarer Nähe zum Service Center wurde in der CSS einzig aus prozessökonomischen Gründen gewählt. Damit werde eine rasche und effiziente Abwicklung garantiert. Ebenso könne der VA die Einhaltung der Datenschutzbestimmungen besser kontrollieren. Insbesondere werde vermieden, dass zusätzliche Stellen im Informationsfluss eingeschaltet werden.

6.3.2.2. Die Räumlichkeiten

Der VAD ist zusammen mit anderen Büros im 3. Stock des alten CSS-Gebäudes untergebracht. Dort befindet sich ebenfalls das Service-Center. Die Büros der Mitarbeiter des VAD (VA und VA-Assistenz) sind von den anderen Büros auf dem 3. Stock räumlich nicht abgetrennt. Die VAD-Büros sind bei Verlassen abzuschliessen.



Die Büros der medizinischen Experten (nachfolgend MedEx) befinden sich ausserhalb des VAD. Beim Verlassen der Büros haben die medizinischen Experten alle medizinischen und vertraulichen Unterlagen in Schränken einzuschliessen. Die Büros werden aber nicht abgeschlossen. Obschon die medizinischen Experten nicht Mitarbeiter des VAD sind, werden sie zur Bearbeitung von leichten Fällen beigezogen (vgl. hierzu das Kapitel Mitarbeiter und Triage). Aus diesem Grund werden sie hier aufgeführt.

6.3.2.3. Das Sekretariat

Die Post gelangt grundsätzlich ungeöffnet zum VAD-Sekretariat. Nur falsch oder fehlerhaft adressierte Post, die nicht eindeutig dem VAD zugewiesen werden konnte, wird geöffnet übergeben. Sämtliche Posteingänge werden im Sekretariat mit einem Eingangsstempel versehen und den 15 VA-Assistenten zur weiteren Bearbeitung zugeteilt. Die Dokumente werden registriert (vgl. weiter hinten die Erklärung des AVD) und vor der weiteren Bearbeitung einer Triage unterzogen.

6.3.2.4. Die Mitarbeiter

Der Leiter Vertrauensärztlicher Dienst

Der L-VAD hat einen Anstellungsvertrag mit der CSS Kranken-Versicherung AG. Seine Fachaufgaben sind in einer Stellenbeschreibung zusammengefasst. Er ist dem Leiter Geschäftsbereich Leistung direkt unterstellt. Zu den Fachaufgaben des L-VAD gehören unter anderem die Beratung im Bereich Leistungsabwicklung (KVG) und Antragsbearbeitung (VVG).

Im VVG-Bereich ist der VA als Gesellschaftsarzt tätig.

Die CSS setzt für die Bereiche des KVG und VVG die gleichen Datenschutznormen ein.

Auch im Antragsbereich hat der VA (Gesellschaftsarzt) keine Entscheidungsbefugnis. Diese liegt bei der Administration.

Für die Funktion als Gesellschaftsarzt gibt es keine separate Stellenbeschreibung.

Die Stellung des L-VAD als Kader oder als Mitglied der Direktion hat gemäss CSS keinen Einfluss auf die Budgetfragen des VAD oder Vorgaben für Leistungseinsparungen.

Kader- und Direktionsmitglieder haben einen gewissen Informationsvorsprung gegenüber anderen Mitarbeitern der CSS. Ebenfalls ist die Arbeitszeit anders geregelt.

Der L-VAD ist gemäss Stellenbeschreibung zuständig für den Ablauf im VAD und zwischen Versicherten, Leistungserbringern und den zuständigen Mitarbeitern der Administration CSS.

Die zuständigen Mitarbeiter sind diejenigen der Expertengruppe, die zahlenmässig beschränkt und speziell geschult sind. Es soll verhindert werden, dass der VA von allen Sachbearbeitern kontaktiert werden kann. Zudem haben die Experten eine spezielle Schweigepflichtserklärung zu unterzeichnen.

Einer der Leistungsmassstäbe des Leiter-VA ist das Budget VAD. Leistungsmassstab ist, dass der VA sein Budget unter geordneten Verhältnissen einhalten kann und seine Ressourcen danach richtet.



Die Vertrauensärzte

Die VA haben Anstellungsverträge mit der CSS Kranken-Versicherung AG. Ihre Fachaufgaben sind in einer Stellenbeschreibung zusammengefasst. Sie sind dem L-VAD direkt unterstellt. Als Mitglieder des Kaders sind sie zuständig für die Leitung der ihnen zugeteilten VA-Assistenten. Gemäss Stellenbeschreibung haben sie die gleichen Fachaufgaben wie der L-VAD.

Die VA-Assistenten

Die VA-Assistenten haben Anstellungsverträge mit der CSS Kranken-Versicherung AG. Ihre Fachaufgaben sind in einer Stellenbeschreibung zusammengefasst. Sie sind den VA direkt und dem L-VAD indirekt unterstellt. Die VA-Assistenten haben keine zusätzlichen Funktionen oder Verträge mit Dritten (innerhalb oder ausserhalb CSS Kranken-Versicherung AG).

Die medizinischen Experten

Die MedEx haben Anstellungsverträge mit der CSS Kranken-Versicherung AG. Ihre Fachaufgaben sind in einer Stellenbeschreibung zusammengefasst. Sie sind der/dem Leistungsexperten/In Service Center unterstellt.

Der MedEx fungiert als Schnittstelle zwischen dem VAD und dem Service Center.

Der MedEx ist für die Empfehlung leichter Fälle verantwortlich, die nach Art. 42 Abs. 4 und 5 KVG direkt an den Versicherer gelangen. In diesen leichten Fällen ist weder eine Begründung für die Zustellung an den VAD ersichtlich noch wurde eine solche vom Versicherten verlangt.

In der ohnehin kleinen Gruppe der MedEX sind zusätzlich „Spezialisten“ integriert, die von der Sache her ein medizinisches Urteil abgeben können. Diese sind auch zuständig für die Korrespondenz bei Ablehnung mit medizinisch-administrativen Begründungen. Sie haben eine **separate Datenschutzvereinbarung** unterschrieben. Bei nicht standardisierten Abklärungen in Leistungsfragen bei Leistungserbringern stehen sie mit ihren Spezialkenntnissen den Sachbearbeitern im Service Center zur Verfügung. Damit wird gewährleistet, dass die CSS die Kostengutsprache und die Leistungsentscheide innerhalb der sachgerechten Frist und damit auch innerhalb der gesetzlichen Frist vollziehen kann.

6.3.2.5. Die Triage

Die VA-Assistenten nehmen eine Triage der eingegangenen Dokumente vor und verteilen diese zur medizinischen Beurteilung wie folgt:

- Fälle die keiner medizinischen Beurteilung bedürfen, werden direkt an den Versicherer weitergeleitet.
- **Leichte Fälle:** die Dossiers enthalten lediglich den Inhalt, welcher der VAD dem Versicherer zur Überprüfung der Leistungspflicht mitteilen muss. Die Bearbeitung erfolgt durch medizinische Experten.
- **Mittelschwere Fälle:** die Dossiers enthalten mehr medizinische Daten als der Versicherer zur Beurteilung der Leistungspflicht benötigt. Die Bearbeitung erfolgt durch VA-Assistenten.



- **Schwere Fälle und Fälle von hohem Geheimhaltungsgrad:** die Beurteilung dieser Fälle erfordert ein hohes medizinisches Wissen. Zu beurteilen sind Neubeurteilungen, Berichte von bekannten Personen und Beratung in Rechtsfällen. Die Bearbeitung erfolgt ausschliesslich durch Vertrauensärzte.

Die VA und VA-Assistenten

Muss die Empfehlung mittelschwerer Fälle dem externen Antragsteller (i.d.R. ein Leistungserbringer) kommuniziert werden, erfolgt die Unterschrift durch einen VA.

Der Entscheid erfolgt durch die CSS Administration. Da der VA nur befugt ist, Empfehlungen abzugeben, werden Leistungserbringer wie Versicherte überwiegend direkt durch die Administration informiert. Ein direkter Kontakt zwischen VA und Leistungserbringer beschränkt sich auf Empfehlungen.

Wer als Patient oder versicherte Person darauf Wert legt, dass seine Unterlagen nur dem VA oder dem VAD ausgehändigt werden, muss dies auf dem Umschlag ausdrücklich vermerken.

Bei seiner medizinischen Beurteilung hat der VA eine Prüfung zum Krankheitswert und zu Wirtschaftlichkeit, Zweckmässigkeit sowie Wirksamkeit (nachfolgend WZW) vorzunehmen. Zu prüfen ist dabei primär, ob die vorgesehene Behandlung wirksam und zweckmässig ist. Die WZW ist vom Gesetzgeber wie der Rechtssprechung vorgegeben.

Fallbezogene Besprechungen erfolgen stets zwischen dem VA und der VA-Assistenz oder dem VA und einem MedEx, nicht aber zwischen dem VA und einem Sachbearbeiter der Administration.

Betreffen Anfragen die Mitarbeiterinnen und Mitarbeiter der CSS (ca. 2000) ist nur der VAD (VA / VA-Assistenz), nicht aber der MedEx zuständig. Es ist vorgesehen, die medizinische Beurteilung an einen externen VA auszulagern. In der CSS-Administration ist ein beschränkter Kreis von Mitarbeitenden in einem separaten Büro ausschliesslich für die Fälle „Personal“ zuständig (keine Vermischung).

Die medizinischen Experten

Wie die Risikoexperten (nachfolgend REX), Case Manager und Taggeldexperten (nachfolgend TEX) gehören die MedEx der Expertengruppe an. Sie sind beim Service-Center und somit beim Geschäftsbereich Leistung angegliedert und nicht im VAD integriert. Sie walten als Bindeglied zwischen VAD und Sachbearbeiter. Im Gegensatz zum VAD sind sie nicht nur befugt, Empfehlungen abzugeben, sondern auch Entscheide zu fällen. Medizinische Experten erhalten nur im Einzelfall und nach ausdrücklicher Erlaubnis des VA Zugriff auf das AVD. Der VAD hingegen darf nur empfehlen.

Anlässlich des Augenscheins wurde dem EDÖB anhand eines Reha-Gesuches das Vorgehen erläutert. Vorab wird stets die Versicherungsdeckung des Gesuchstellers geprüft. Es folgt eine medizinische Beurteilung. Nach eingehender Begründung hat die medizinische Expertin schliesslich empfohlen, das Gesuch gutzuheissen.

Die Sachbearbeiter erhalten eine Empfehlung für eine Kostengutsprache in der Regel per E-Mail. *Den Link können aber nur die Berechtigten öffnen.* Die Sachbearbeiter übermitteln die Kostengutsprache dem Leistungserbringer bzw. der versicherten Person. Diese Mitteilung kann auch durch einen MedEx erfolgen. Das Schreiben wird sowohl vom Gruppenleiter als auch vom Sachbearbeiter unterschrieben.

Ein Gesuch um Kostengutsprache kann nur von einem MedEx abgelehnt werden, da der Sachbearbeiter im AVD keine Einsicht in die medizinische Begründung hat.



6.3.3. Das Archiv des VAD

Das Papierarchiv

Dossiers *sind nach Eröffnungsdatum* im AVD in einem separaten, abgeschlossenen und nur für Mitarbeiter des VAD zugänglichen Archiv *alphabetisch* abgelegt. Diese Dossiers werden 10 Jahre aufbewahrt und dann gesichert entsorgt.

Das elektronische Archiv im AVD

Nach 15 Monaten ohne neuen Eintrag wird auch das elektronische Dossier archiviert, während 10 Jahren aufbewahrt und anschliessend *gesichert* gelöscht.

Einen Zugriff zum Archiv haben:

- Die VA
- Die VA-Assistenten
- Die MedEx unter Aufsicht eines VA-Assistenten

6.3.4. Das AVD System

Beim AVD handelt es sich um eine Lotus Notes Applikation. Das User/ID-Management erfolgt über SAP im Rahmen des HR-Management CSS. Die Systeme werden durch die Informatik CSS betreut. Die Clients sind mit Citrix Metaframe angebunden. Der Passwortwechsel für den Zugriff auf das AVD wird alle drei Monate forciert. Die Zugriffsberechtigung auf das AVD wird nach Vorschlag des direkten Vorgesetzten des Mitarbeiters und nach Überprüfung VAD-NAV durch den VAD-NAV vergeben und periodisch überprüft.

Eine allgemeine Überprüfung der Zugriffsberechtigungen findet monatlich statt. Zwischenzeitliche Mutationen erfolgen bei Änderung des Berechtigungsgrades, bei Neueintritten wie Austritten.

6.3.4.1. Die Klassifikation der Daten

Die Daten werden aufgrund folgender Kriterien drei Klassen zugeordnet:

- datenschutzrechtliche Relevanz
- Vertraulichkeit
- Archivierungspflicht

Die Daten in den einzelnen Klassen werden entsprechend ihrer Eigenschaft in Stufen eingeteilt. Für die Datensammlungen im VAD ergeben sich somit folgende Klassifikationen:

- **Stammdaten:** Personendaten, Vertraulich, gesetzliche Archivierungspflicht
- **Vorschlag:** besonders schützenswerte Personendaten, Vertraulich, gesetzliche Archivierungspflicht
- **Empfehlung:** besonders schützenswerte Personendaten, Vertraulich, gesetzliche Archivierungspflicht
- **Entscheidung:** besonders schützenswerte Personendaten, Vertraulich, gesetzliche Archivierungspflicht
- **Medizinische Stammdaten:** besonders schützenswerte Personendaten, Vertraulich, gesetzliche Archivierungspflicht



6.3.4.2. Die Berechtigungsstufen / Funktionen

Für die einzelnen Datenfelder im AVD gibt es **drei Berechtigungsstufen**.

- **Basic**
- **Control**
- **Medical**

Wer über Control-Rechte verfügt, hat keine zusätzlichen Funktionen oder Verträge mit Dritten (innerhalb oder ausserhalb CSS Kranken-Versicherung AG).

CaseManager und Underwriting haben keinen Zugriff auf Daten von nur KVG-Versicherten.

Neben den drei Berechtigungsstufen gibt es:

Administrationsrechte

Die Notes-Administratoren sind befugt, die Benutzungsrechte zu überprüfen und zu vergeben. Sie stellen gleichzeitig die Schulung sicher. Zusätzlich holen sie die jeweils notwendige Unterschrift für die verschärfte Datenschutzbestimmung ein, die im Personaldossier abgelegt wird.

Die NAV-AdministratorInnen sind primär VA-AssistentInnen.

Funktionen	Beschreibung	Rechte	Anzahl
SB (Sachbearbeiter)	<ul style="list-style-type: none">- Macht Anfrage an den Leistungserbringer (LERB) bei für die Leistungskontrolle unerlässlichen medizinischen Fragestellungen- Kommuniziert Entscheidungen bei Zustimmungen und nur administrative begründeten Ablehnungen.	Basic	³
EXP (Experten)	<ul style="list-style-type: none">- medizinische Experten: Zuständig für die medizinische Beurteilung von leichten Fällen (mit Unterstützung durch den VAD), arbeiten ausschliesslich mit dem VAD zusammen; kommunizieren medizinisch begründete ablehnende Entscheidungen (siehe Bericht interne Revision, Punkt 2.2)	Control	

³ Aufgrund überwiegender Interessen der CSS an der Vertraulichkeit der genauen Anzahl Sachbearbeiter (Geschäftsgeheimnisse) wurden in der Tabelle die entsprechenden Zahlen für die Publikation aus dem Bericht herausgenommen.



	<ul style="list-style-type: none"> - Fachspezialisten, die für Leistungen in einem bestimmten, abgegrenzten Gebiet (Unfall, Zahnbehandlung, Spitalspezialisten, Abrechnungen von Leistungen, die im Ausland erbracht werden etc.) zuständig sind. 		
Care Manager	Fallspezialisten. Sie begleiten und beraten die Versicherten individuell in komplexen Fällen. Sie arbeiten mit Vollmacht der Versicherten (Einsichtsrecht in vertrauensärztliche Unterlagen).	Control	
Taggeld Case Manager	Fallspezialisten für Taggeld nach VVG. Begleiten und kontrollieren Versicherte mit längerer Arbeitsunfähigkeit	Control: kein Zugriff auf nur OKP- Versicherte (siehe Bericht interne Revision, Punkt 2.3)	
Underwriting	Risikoexperten für VVG-Anträge. Eine Vollmacht der Versicherten liegt vor.	Control: kein Zugriff auf nur OKP- Versicherte (siehe Bericht interne Revision, Punkt 2.3)	
Vertrauensarzt	Zuständig für die medizinische Beurteilung von schwierigen Fällen	Medial	
VA-Assistenz	Zuständig für die medizinische Beurteilung von Fällen mittleren Schwierigkeitsgrads und Fällen erhöhter Geheimhaltungspflicht (z.B. Fotos)	Medical	
Notes-Administratoren (NAV)	Definierte Einzelpersonen innerhalb des VAD, welche Benutzerberechtigungen auf Antrag erteilen und entziehen	Administratorenrechte	
IT-Administratoren	Definierte Einzelpersonen, welche aus technischen Gründen Zugriff auf die Datenbanken benötigen, nicht aber auf die Applikation AVD	Systemrechte	
Controller	Einzelperson, die Kennzahlen aus dem AVD ableitet	Hat zur Zeit keine Berechtigung, neuer Zugriff in Erarbeitung (siehe Bericht interne Revision, Punkt 2.4)	

Zur Tabelle: sie entspricht derjenigen, welche der Leiter Recht & Compliance mit Brief vom 6.7.06 dem EDÖB zu den Akten der Sachverhaltsabklärung zugesandt hat. Darin wird ausdrücklich darauf hingewiesen, dass die Anzahl der Berechtigten aufgrund von Ein- und Austritten variiere.



6.3.4.3. Die Zugriffsberechtigungen

Im AVD werden die Zugriffsberechtigungen auf die elektronisch erfassten Daten des VAD den drei Kategorien **Basic**, **Control** und **Medical** zugeordnet.

Die in folgender Tabelle zusammengefasste Anzahl der Zugriffsberechtigten ergibt sich aus obiger Tabelle. In der Antwort der CSS vom 3.1.07 auf den Sachverhaltsfeststellungsentwurf des EDÖB vom 6.12.06 wurde bei der Berechtigungsstufe Control die Zahl der Zugriffsberechtigten mit total + / - 130 Personen angegeben.

Der Vorgesetzte stellt Antrag auf die Zugriffsberechtigung. Mit den Kategorien wird der Umfang der zur Bearbeitung zur Verfügung stehenden Information definiert. Ein Mitarbeiter, der Zugriff auf Daten des AVD hat, erhält eine dieser Berechtigungsstufen. In den vier Kernfunktionen Eröffnung, Vorschlag, Empfehlung und Entscheidung können zuständige Mitarbeiter gemäss ihrer Zugriffsberechtigung auf den gesamten oder nur einen Teil der Daten innerhalb eines Falls zugreifen. Die Zugriffsberechtigungen⁴ sind fest vergeben:

Basic	Control	Medical
SB⁵	MedEx, REX, TEX, CareManager, CaseManager, Underwriting	VA, VA-Ass

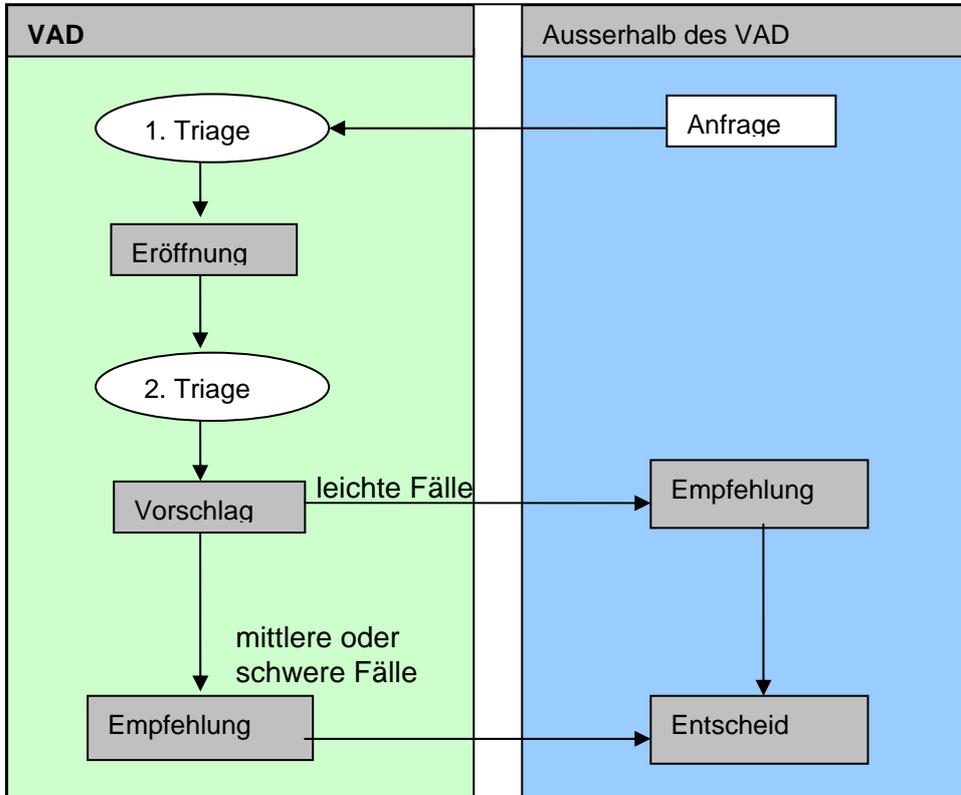
6.3.4.4. Der zentrale Datenfluss

Im VAD haben total 25 Mitarbeiter (VA 9, VA-ASS 15) Medicalrechte, ausserhalb des VAD 621 Mitarbeiter (Experten 61, Sachbearbeiter 560) Control und Basicrechte. Mit diesen Rechten können sie in unterschiedlichem Umfang auf Daten im AVD zugreifen.

Besondere Aufmerksamkeit muss der Datenbearbeitung ausserhalb des VAD gewidmet werden. Dort werden mit der Empfehlung und dem Entscheid Daten des Versicherten, welche an den VAD geschickt wurden, durch Mitarbeiter ausserhalb des VAD bearbeitet. Mit dem Vorschlag und der Empfehlung stehen Gesundheitsdaten des Versicherten auch Mitarbeitern mit Control und Basic Rechten zur Verfügung.

⁴ Die Zugriffsrechte für die System- und Anwendungsadministration werden an dieser Stelle nicht berücksichtigt.

⁵ Aufgrund überwiegender Interessen der CSS an der Vertraulichkeit der genauen Anzahl Sachbearbeiter (Geschäftsgeheimnisse) wurden in der Tabelle die entsprechenden Zahlen für die Publikation aus dem Bericht herausgenommen.



⁶	Basic	Control	Medical
Eröffnung	Alles	Alles	Alles
Vorschlag	Ohne Fotos und medizinische Dokumentation	Ohne Fotos	Alles
Empfehlung	Ohne Angaben zum Autor der Empfehlung, der Begründung, dem Vorschlag für die Begründung und dem vertraulichen Text.	Ohne vertraulichen Text	Alles
Entscheid	Alles	Alles	Alles

Bei der **Eröffnung** werden die administrativen Daten des Versicherten bearbeitet. Kritisch könnte lediglich das Datenfeld „Text der externen Anfrage“ sein. Wenn der Text heikle Informationen enthält sind diese auch für Control und Basic sichtbar.

⁶ Aufgrund überwiegender Interessen der CSS an der Vertraulichkeit der genauen Anzahl Sachbearbeiter (Geschäftsgeheimnisse) wurden in der Tabelle die entsprechenden Zahlen für die Publikation aus dem Bericht herausgenommen.



Bei der Erarbeitung des **Vorschlags** werden neben administrativen auch medizinische Daten eines Versicherten bearbeitet. Bildmaterial zu einem Fall kann nur von Mitarbeitern mit Medical bearbeitet werden. Weder Control noch Basic haben Zugriff auf diese besonders sensible Information. Anders verhält es sich beim Datenfeld Zeugnistext. Auf dieses haben neben Medical auch Control und Basic Zugriff. Wohingegen auf das Datenfeld medizinische Dokumentation Basic der Zugriff verwehrt bleibt.

Die **Empfehlung** beinhaltet Datenfelder, die dazu geeignet sein können, besonders schützenswerte Informationen über einen Versicherten zu enthalten. Hier handelt es sich um Felder zur Anfrage/Diagnose, Vorschlag für Empfehlung und Attachments. Der Inhalt der Felder wird durch den Verfasser der Empfehlung bestimmt. Er entscheidet, welche Information über den Versicherten Mitarbeitern der CSS mit Control und Basic sichtbar gemacht werden.

Bei der **Entscheidung** gibt es keinen Unterschied in den Zugriffsberechtigungen. Lediglich das Feld mit dem Text der Entscheidung kann Gesundheitsdaten enthalten.

Der Controller kann als einzige Stelle **ausserhalb des VAD** direkt auf die Daten des VAD zugreifen. Der Zugriff wird ihm nur ad hoc und unter Kontrolle der Notes-Applikations-Verantwortlichen gewährt. Aufgrund der monatlichen Kennzahlen erhebt er die Durchlaufzeit und die Anzahl der Empfehlungen.

7. Datenschutzrechtliche Beurteilung

7.1. Einleitung

Im Bereich des Gesundheitswesens ist das Bearbeiten von besonders schützenswerten Personendaten an der Tagesordnung. Mit der elektronischen Datenbearbeitung hat sich die Datenschutzproblematik zugespitzt. Die enorme Anhäufung von Gesundheitsdaten – bedingt durch den Kostendruck und die technologische Entwicklung – erhöht die Gefahr von Persönlichkeitsverletzungen sowie Diskriminierung aufgrund bestimmter Gesundheitsdispositionen. Das Schlagwort vom gläsernen Patienten macht die Runde. Im Spannungsfeld stehen sich auf der einen Seite Datenschutz und Datensicherheit der versicherten Personen und auf der anderen Seite die Interessen der Versicherer gegenüber. *Kurz und bündig* zusammengefasst: „Im Krankenversicherungswesen müssen die Versicherten wirksam vor der Gefahr des Datenmissbrauchs geschützt werden. Ebenso in ihrem Interesse liegt allerdings eine effektivere Wirtschaftlichkeitsprüfung von Seiten der Versicherer, denn die medizinische Leistung kann nur anhand ausreichender Informationen überprüft werden. Auch die Versicherten profitieren davon, wenn die Leistungserbringer die Qualität und Wirtschaftlichkeit ihrer Leistungen verbessern und die Versicherer gleichzeitig ihre internen Abläufe rationalisieren.“⁷ Soweit die Zuständigkeit des EDÖB gegeben ist, greift er im Rahmen seiner Ressourcen ein, wenn er den Datenschutz und die Verhältnismässigkeit der Datenbearbeitung schwerwiegend verletzt sieht.

7.2. Zuständigkeit des EDÖB

Die Krankenversicherer erfüllen im Bereich des KVG eine öffentliche Aufgabe. Sie gelten diesbezüglich als Bundesorgane im Sinne von Art. 3 lit. h des DSG. Der Geltungsbereich des DSG gilt für das Bearbeiten von Daten natürlicher Personen durch Bundesorgane (Art. 2 lit. b DSG). Die Zuständigkeit des EDÖB ist gemäss Art. 27 DSG gegeben. Ihm obliegt danach die Aufsicht über Bundesorgane.

⁷ PD Dr. iur. Isabelle Häner, Datenschutz in der Krankenversicherung, digma 2003.4, S. 147



7.3. Zweck der Sachverhaltsabklärung

Mit der vorliegenden Sachverhaltsabklärung bezweckt der EDÖB die Überprüfung des **internen** Datenschutzes im VAD der CSS.

Die Datenbearbeitung hat den Grundsätzen der Verhältnismässigkeit und der Zweckmässigkeit zu gehorchen. Für die Bearbeitung von besonders schützenswerten Personendaten sind hohe Hürden zu setzen. Zugang zu diesen Daten darf nur erhalten, wer diese zur Erfüllung seiner Aufgaben unbedingt benötigt. Je durchdachter die interne Organisation des Datenschutzes eingegrenzt und geregelt ist, desto geringer ist die Gefahr von systemimmanenten Datenschutzverletzungen.

8. Würdigung der Ergebnisse aus der Sachverhaltsabklärung

8.1. Allgemeines

Im Zusammenhang mit den eingangs erwähnten Presseberichten über die angeblichen Datenschutzverletzungen in der CSS und infolge der Sachverhaltsabklärung durch den EDÖB hat die CSS ihr AVD einer intensiven internen Überprüfung unterzogen und aus Sicht des EDÖB notwendige Korrekturen bereits angebracht (vgl. oben Ziffer 2).

Nach durchgeführter Sachverhaltsabklärung sind aus Sicht des EDÖB weitere Verbesserungen besonders mit Blick auf das neue AVD-System erforderlich, weshalb der CSS die nachfolgenden Empfehlungen unterbreitet werden.

8.2. Zugangskontrolle und Räumlichkeiten

Beurteilung aus Sicht des EDÖB:

Die weit überwiegende Anzahl von Patientendossiers wird auch heute noch in Papierform bearbeitet und entsprechend aufbewahrt. Die Räumlichkeiten der VAD-Mitarbeiter sind von den Arbeitsplätzen der übrigen CSS-Mitarbeiter nicht getrennt, sodass auch keine systematische Zugangskontrolle erfolgt. Umfangreiche Dossiers können nicht stets von allen neugierigen Blicken geschützt werden. Es ist auch nicht zu verhindern, dass bisweilen Teile eines Dossiers – Fotos, wichtige Daten – Unbefugten zur Kenntnis gelangen.

Empfehlung des EDÖB:

Eine höhere Sicherheit vor unbeabsichtigt neugierigen Blicken wie vor Missbrauch kann nur durch eine konsequente räumliche Abtrennung des VAD-Bereichs erzielt werden. Dem vertrauensärztlichen Dienst müssen die notwendigen **eigenen Räumlichkeiten und Infrastrukturmittel** zur Verfügung gestellt werden. Die Ausgestaltung hat so zu erfolgen, dass die Daten des VAD gegenüber der Versicherung und gegenüber Dritten stets vertraulich gehalten werden können.



8.3. Der Vertrauensärztliche Dienst (VAD)

Beurteilung aus Sicht des EDÖB:

Der VAD der CSS kommt nicht nur in der Grundversicherung (KVG) zum Einsatz sondern wird auch für Fälle im Bereiche der Zusatzversicherungen (VVG) als gesellschaftsärztlicher Dienst beigezogen. Während der Vertrauensarzt im Bereiche des KVG gegenüber der Versicherung seine Unabhängigkeit zu bewahren hat, geniesst er als Gesellschaftsarzt im Bereiche des VVG diesen Status nicht. Es besteht die Gefahr, dass der VAD sein Wissen aus der obligatorischen Versicherung wegen des Unterstellungsverhältnisses im VVG-Bereich der Versicherung nicht vorenthalten kann. Diese Interessenkollision kann dazu führen, dass die vorgeschriebene Unabhängigkeit im Bereiche der Grundversicherung nicht genügend gewahrt werden kann. Der EDÖB erachtet deshalb eine strikte personelle Trennung des VAD gemäss KVG vom Gesellschaftsarzt gemäss VVG für unerlässlich.

Empfehlung des EDÖB:

Der Gesellschaftsarzt gemäss VVG ist vom VAD gemäss KVG personell zu trennen.

8.4. Leiter vertrauensärztlicher Dienst (L-VAD)

Beurteilung aus Sicht des EDÖB:

Der L-VAD ist gemäss Stellenbeschreibung direkt dem Leiter Geschäftsbereich Leistung unterstellt. Eine andere Unterstellung des L-VAD drängt sich allein schon im Hinblick auf dessen unabdingliche Unabhängigkeit förmlich auf.

Empfehlung des EDÖB:

Der L-VAD ist direkt der Geschäftsleitung als Stabstelle beizuordnen.

8.5. Berechtigungskonzept

8.5.1. Bereich Medical

Beim bestehenden Berechtigungskonzept ist der Bereich Medical als unbedenklich zu bewerten. Auf diesen Bereich haben lediglich der Leiter des VAD, die Vertrauensärzte und die VertrauensarztassistentInnen Zugriff (24 Personen).

Beurteilung aus Sicht des EDÖB:

Keine Verbesserungen notwendig.

8.5.2. Bereich Basic

Beurteilung aus Sicht des EDÖB

Im Bereich Basic ist mit grösster Sorgfalt darauf zu achten, dass in den Textfeldern des Vorschlags oder der Empfehlung keine Angaben über den Versicherten gemacht werden, die den vertrauensärztlichen Bereich nicht verlassen dürften. Im internen Revisionsbericht wird festgehalten, dass die Empfehlungsbegründung, insbesondere bei Ablehnungen, sensitive Informationen über Versicherte beinhalten kann. Gemäss Bericht sollen nach der Zusammenführung der Service Center Luzern und Zü-



rich (wann?) sämtliche Ablehnungsentscheide ausschliesslich durch medizinische Experten, welche Zugriff zum Bereich Control verfügen, formuliert werden.

Empfehlung des EDÖB:

Bis zur Zusammenführung der Service Center Luzern und Zürich dürfen bei Ablehnungsentscheiden keine sensitiven Informationen über Versicherte Personen zugänglich gemacht werden, die lediglich über die Berechtigung Basic verfügen.

8.5.3. Bereich Control

Beurteilung aus Sicht des EDÖB:

Nach den erwähnten Medienberichten hat die CSS im Rahmen ihrer internen Revision im Bereich Control feststellen müssen, dass die Zugriffsberechtigung auf Daten der Versicherten zu wenig genau definiert war. Die ungenaue Zugriffs-Definition und -Abgrenzung hatte zur Folge, dass die Anzahl der Mitarbeiter mit Zugriffsrecht Control als zu hoch gewertet werden musste. Die CSS sah sich deshalb veranlasst, die Anzahl der Mitarbeiter mit Zugangsberechtigung Control von „gut 150 Benutzern“ zu reduzieren. Die CSS hat in ihrer Antwort vom 3.1.07 auf den Sachverhaltsfeststellungsentwurf des EDÖB (6.12.06) die Zahl der Zugriffsberechtigten mit Berechtigungsstufe Control auf total + / - 130 Personen festgesetzt. Der EDÖB erachtet diese Bandbreite als zu hoch, sieht er doch im Bereich Control das eigentliche Risikopotential für Datenschutzverletzungen im Zusammenhang mit der Bearbeitung von Versichertendaten durch den vertrauensärztlichen Dienst. Zwar umfasst die Gruppe mit den Rechten Control gemäss obiger Tabelle momentan „lediglich“ 115 Zugangsberechtigte. Aufgrund der Systematik und der Tatsache, dass die Anzahl der Berechtigten infolge von Ein- und Austritten variiert, ist jedoch nicht auszuschliessen, dass diese Gruppe in der täglichen Anwendung des Systems wieder wächst.

Empfehlung des EDÖB:

Die Aufgaben und Pflichten der Mitarbeiter der Gruppe Control sind möglichst detailliert zu beschreiben. Die **Zugriffsberechtigung** auf die einzelnen Datenfelder, insbesondere in der Empfehlung, müssen auf ein absolutes Minimum reduziert werden. Bei den als leicht eingestufteten Fällen sind die Zeugnistexte für Basic zu sperren, wenn diese Angaben enthalten, die aus vertrauensärztlicher Sicht für die Erstellung des Entscheids nicht nötig sind. Die **Anzahl der Zugangsberechtigten** mit Zugriffsrecht Control ist möglichst klein zu halten und ständig zu überprüfen.

8.5.4. Zahl der Zugangsberechtigten zum VAD

Beurteilung aus Sicht des EDÖB:

Die von der CSS angegebene Anzahl von +/- 130 Zugriffsberechtigten zum sensiblen Bereich des VAD erscheinen dem EDÖB nach wie vor zu hoch. Die mit Blick auf die Verhältnismässigkeit und Zweckmässigkeit richtige Zahl kann nur durch eine detaillierte und fundierte Analyse der internen Prozesse festgelegt werden. Eine solche Überprüfung ist wegen der Komplexität der Sache, der möglichen Veränderungen und dem hohen Gefährdungspotential in regelmässigen zeitlichen Abständen zu wiederholen. Derartige Überprüfungen und Revisionen sind im Rahmen von Audits bzw. Zertifizierungsverfahren, wie sie das neue DSG vorsieht, an die Hand zu nehmen. Insbesondere mit der bevorstehenden **Einführung der vollelektronischen Dossiers** wird die konsequent durchorganisierte,



dem Datenschutz vollauf gerecht werdende Architektur der entsprechenden AVD-Software unabdingbar. Die CSS konnte während der Sachverhaltsabklärung weder über die effektive noch über die notwendige Anzahl Zugriffsberechtigungen genauen Angaben liefern. Deshalb verlangt der EDÖB von der CSS, sich einer externen und systematischen Untersuchung (Audit) unterziehen zu lassen, um die Erforderlichkeit und die Zweckmässigkeit der Anzahl von Zugriffsberechtigungen zu überprüfen.

Empfehlung des EDÖB:

Die CSS lässt ihren VAD **im Rahmen eines externen Audits** auf dessen Datenschutzkonformität hin überprüfen.

9. Die neue Version AVD

Wie aus den obigen Darlegungen ersichtlich, werden die medizinischen Dossiers bei der CSS schwerpunktmässig in Papierform bearbeitet und archiviert. Lediglich die Administrationsdaten (wer bearbeitet gerade das Patienten-Dossier X, wo befindet es sich zum Zeitpunkt usw.) werden elektronisch erfasst. So kann jederzeit über jedes Dossier eine „History“ aller Bearbeitungszyklen eingesehen werden. Dieses papierlastige AVD-System soll möglichst umgehend durch eine vollelektronische neue Version abgelöst werden. Sie befindet sich zur Zeit in der Planungsphase. Vorgesehen ist die elektronische Bearbeitung und Archivierung sämtlicher medizinischer Patientendaten samt der dazugehörigen Administrationsdaten. Die Aufbewahrungszeit umfasst 10 Jahre und sieht danach eine gesicherte Löschung vor. Das neue System ist bis heute weder vom internen Datenschutz der CSS noch von Recht&Compliance abgenommen worden. Für die Umsetzung wird der Bericht des EDÖB abgewartet.

10. Schlussfolgerungen

10.1. Bezüglich der Kontrolle

Im Rahmen seiner Sachverhaltsabklärung bei der CSS musste der EDÖB feststellen, dass sich der VA mit Datenschutzproblemen konfrontiert sieht. Dabei hat sich einmal mehr bewahrheitet, dass der Datenschutz nicht nur eine Frage von gesetzlichen Vorschriften und internen Weisungen ist, sondern vor allem Sache des Verhaltens der einzelnen Personen, die mit der Bearbeitung der Daten beauftragt sind. Nach den Presseberichten und der Sachverhaltsabklärung des EDÖB hat die CSS unverzüglich die notwendigen organisatorischen wie technischen Massnahmen getroffen und durch eine sofortige **interne Analyse selbst Massnahmen zur Verbesserungen** vorgenommen. Die CSS behauptet, dass zu keinem Zeitpunkt die hohe Zahl von 400 CSS Mitarbeiterinnen und Mitarbeiter auf das elektronische System „Anfragebewirtschaftung vertrauensärztlicher Dienst“ (AVD) Zugriff hatten, sondern lediglich rund 150 Personen. Ob allerdings auch nicht Zugriffsberechtigte Zugang zum sensiblen Bereich des VAD hatten (vgl. oben Ziffer 2), ist im Rahmen des vom BAG angehobenen Strafverfahrens abzuklären. Immerhin stellt der interne Revisionsbereich der CSS selber fest, dass rückwirkend nicht mehr feststellbar sei, welcher Mitarbeiter zu welchem Bereich zu welchem Zeitpunkt Zugriffsberechtigung hatte.

Die **fehlende räumliche Abgrenzung des VAD** von den übrigen Versicherungsteilen und die papierlastige Dossierverwaltung haben auf ein Problem hingewiesen, das wohl in ähnlichem Ausmass auch bei anderen Krankenversicherern auszuloten wäre. Gegen das Führen einer Datenbank mit heiklen



Patientendaten für eine vertrauensärztliche Abklärung ist nichts einzuwenden. Die darin enthaltenen Informationen müssen jedoch **zwingend im Kreis des vertrauensärztlichen Dienstes** bleiben. Solange Patientendossiers überwiegend in Papierform behandelt werden, kann besagter Kreis – wie empfohlen – nur durch eine konsequente räumliche Abtrennung des VAD von den übrigen Bereichen erreicht werden.

Es wird immer wieder betont, dass der Vertrauensarzt eine Scharnierfunktion zwischen Patient, behandelndem Arzt und Versicherung innehat. Scharniere sind allgemein grosser Belastung unterworfen. Mehr oder weniger ständig in Bewegung, bedürfen sie regelmässigen Unterhalts. Sind Scharniere zu schwach dimensioniert, führt dies früher oder später zu Funktionsstörungen. Tatsache bleibt, dass an den Scharnieren, an den Schnittstellen der AVD-Abläufe die grösste Gefahr von Lücken im System besteht. Die **Stellung des L-VAD** ist deshalb zu stärken. Er muss direkt der Geschäftsleitung unterstellt werden. Seine Unabhängigkeit ist auch dadurch zu stärken, dass er nicht gleichzeitig mit Aufgaben eines Gesellschaftsarztes für den Bereich des VVG belastet wird. Eine Stärkung seiner Stellung kann auch durch Datenschutzaudits erfolgen.

10.2. Verfahren und weiteres Vorgehen

In Anbetracht der Tatsache, dass auch andere Krankenkassen im Bereich des vertrauensärztlichen Dienstes sich mit den gleichen Abgrenzungsschwierigkeiten konfrontiert sehen, erweist sich die vorliegende Kontrolle als richtungsweisend für weitere Anwender (Krankenkassen). Aus besagtem Grund besteht ein grundsätzliches Interesse daran, die Öffentlichkeit für diese Art der Datenerhebung zu sensibilisieren und sie insbesondere über die erfolgte Datenschutzkontrolle bei der CSS und die diesbezüglichen Ergebnisse zu informieren. Gestützt auf Art. 30 Abs. 2 DSG wird der EDÖB daher den vorliegenden Kontrollbericht sowie die daraus resultierende Empfehlung betreffend der Organisation des AVD bei der CSS in einer angepassten Version **der Öffentlichkeit zugänglich machen** und diese Dokumente auf seiner Website (www.edoeb.admin.ch) publizieren. Selbstverständlich erfolgt die Publikation unter dem Vorbehalt, dass aus Sicht von CSS keine vertraulichen Daten, welche Geschäftsgeheimnisse offenbaren oder die Konkurrenzfähigkeit beeinflussen könnten, bekannt gegeben werden. Die CSS wird daher aufgefordert, den Kontrollbericht und die Empfehlung auf solche vertraulichen Inhalte hin zu überprüfen und dem EDÖB **mit Frist von 30 Tagen** entsprechend schriftliche Rückmeldung zu erstatten.

Der vorliegende Kontrollbericht enthält eine Reihe von Feststellungen, welche auf der vom EDÖB durchgeführten Kontrolle basieren. Die CSS wird gebeten, vorliegenden Kontrollbericht sowie die darin enthaltenen Feststellungen zur Kenntnis zu nehmen und den EDÖB **mit Frist von 30 Tagen** darüber zu informieren, ob von Seiten CSS irgendwelche Bemerkungen dazu vorliegen und ob, und wenn ja, welche Massnahmen zur Verbesserung sie in der Zwischenzeit zusätzlich selbst getroffen oder in die Wege geleitet hat

Darüber hinaus enthält der vorliegende Kontrollbericht **sechs Empfehlungen** im Sinne des Art. 27 Abs. 4 DSG, welche sich an die CSS Versicherung, Geschäftsleitung, Tribschenstrasse 21, Postfach 2568, 6002 Luzern richtet. Die CSS teilt dem EDÖB **mit Frist von 30 Tagen** mit, ob sie diese Empfehlung akzeptiert oder nicht. Falls die Empfehlung abgelehnt oder nicht befolgt wird, kann der EDÖB die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorlegen (Art. 27 Abs. 5 DSG).



Bern, den 17. April 2007

**EIDGENÖSSISCHER
DATENSCHUTZ- UND ÖFFENLICH-
KEITSBEAUFTRAGTER**

Der Beauftragte:

Hanspeter Thür