Eidgenössischer Datenschutzbeauftragter
Préposé fédéral à la protection des données
Incaricato federale per la protezione dei dati
Incumbensà federal per la protecziun da datas

Stellungnahme des EDSB zum Berichtsentwurf zu den Regelungslücken im medizinischen Datenschutz in den Sozialversicherungen

a. Ausgangspunkt des vorliegenden Berichts ist das Postulat der Kommission für Rechtsfragen NR (99.093), welches „einen umfassenden, alle Sozialversicherungsbereiche umfassenden Bericht über Regelungslücken im medizinischen Datenschutz" verlangt. Dabei ist insbesondere die technologische Entwicklung und die damit zusammenhängende Missbrauchsgefahr unter Einbezug des Patientengeheimnisses nach Art. 321 StGB zu berücksichtigen.

Die enorme Anhäufung von Gesundheitsdaten – bedingt durch den Kostendruck und die technologische Entwicklung - erhöht die Gefahr von Persönlichkeitsverletzungen sowie Diskriminierungen aufgrund bestimmter Gesundheitsdispositionen. Dies gilt vor allem für den KVG-, UVG- und IV-Bereich. Im Bereich des Gesundheitswesens herrscht seit Jahren ein datenschutzrechtlicher Vollzugsnotstand. Es geht somit darum, die notwendigen Massnahmen zu treffen, damit das informationelle Selbstbestimmungsrecht bzw. das Patientengeheimnis nicht vollends zur Makulatur wird. Sowohl jetzt als auch in Zukunft besteht ein offensichtlicher Handlungsbedarf, den Persönlichkeitsschutz im Gesundheitswesen durch geeignete juristische und vor allem technisch-organisatorische Massnahmen zum Durchbruch zu verhelfen. Dazu bedarf es einer vertieften Analyse (vgl. auch unser Schreiben [A2001.10.04-0009/HO] vom 8.10.2001 an das BSV). Es sei vorliegend daran erinnert, dass im Gesundheitswesen besonders schützenswerte Personendaten bearbeitet werden, welche die gesamte Bevölkerung betreffen. Tatsächlich ist es bereits schon zu Diskriminierungen aufgrund schlechter Gesundheitsdispositionen gekommen (vgl. „Visana: Kundendienst nach Noten" in: Beobachter 6/02).

Insbesondere ist zu untersuchen,

- ob die gegenwärtigen Prozesse im Sozialversicherungsbereich (AHVG, IVG, ELG, BVG, FZG, KVG, UVG, MVG, EOG, AVIG) mit dem Datenschutzgesetz im Einklang sind oder allenfalls die geltenden Datenschutzbestimmungen in den einzelnen Sozialversicherungserlasse angepasst werden müssen; die zukünftige Entwicklung im Sozialversicherungsbereich und im medizinischen Datenschutz im Besonderen soll dabei miteinbezogen werden (Case Management, E-Health, Computerbasierte Patientendossier, Gesundheitskarte etc.); **die Missbrauchsgefahr sowie der jeweilige Regelungsbedarf sollen konkret aufgezeigt werden**; zu berücksichtigen ist dabei auch die Entwicklung auf internationaler Ebene; im Übrigen verweisen wir auf die Praxis (Beispiel TARMED) und die entsprechende Fachliteratur.
- ob die Grundsätze der Datensicherheit (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) im Sozialversicherungsbereich eingehalten werden; die Missbrauchsgefahr diesbezüglich darlegen bzw. aufzeigen, **ob und welche Möglichkeiten bzw. technische Lösungen Risiken vermindern helfen können** („Datenschutz durch Technik" wie Privacy Enhancing Technologies {PET}, Pseudonymisierung, Kryptotechniken, digitale Signatur etc.); die technologische Entwicklung im medizinischen Datenschutz soll dabei soweit wie möglich miteinbezogen werden; zu untersuchen ist auch, ob die technischen und organisatorischen Massnahmen im Sinne der geltenden Datenschutzgesetzgebung eingehalten sind (Beispiel: Bearbeitungsreglement nach Art. 21 VDSG, SR 235.11)
- ob und auf welche Weise einheitliche und verbindliche Datensicherheitsstandards für den gesamten Sozialversicherungsbereich eingeführt werden sollen; insbesondere ist zu

prüfen, ob dafür eine staatliche Koordinationsstelle und / oder eine Zertifizierung für Informatikprodukte sinnvoll ist.

- wie das informationelle Selbstbestimmungsrecht der Versicherten / Patienten verbessert werden soll; die Literatur spricht von „Patient Empowerment", welches vom selbstbestimmten Patienten ausgeht, der z. B. selber bestimmt, wer zu welchem Zweck Zugriff auf seine Daten haben soll. Das informationelle Selbstbestimmungsrecht spielt insbesondere dann eine wichtige Rolle, wenn eine Versicherten- oder gar Gesundheitskarte eingeführt werden soll.
- **welche konkreten Massnahmen zu treffen sind**, wie die Transparenz der Datenbearbeitung im Gesundheits- bzw. Sozialversicherungsbereich für die Versicherten erhöht werden soll; diesbezüglich wird auf die Schlussfolgerungen der Expertenkommission für den Persönlichkeitsschutz in der sozialen und privaten Kranken- und Unfallversicherung (Bericht Geiser) verwiesen, welche die mangelnde Transparenz der Datenbearbeitung festgestellt hat. Diesbezüglich ist insbesondere darzulegen, wie die betroffenen Personen ihre Rechte besser wahrnehmen können.
- ob und inwiefern die technologische Entwicklung im Sozialversicherungs- und im Gesundheitsbereich im Besonderen, welche vor allem vom Effizienzgedanken geprägt ist, nicht zulasten des Patienten / Versicherten geht; insbesondere ist zu prüfen, ob die technologische Entwicklung im Gesundheitswesen zu Missbräuchen und möglichen Diskriminierungen von bestimmten Gruppen führen kann.
- **ob die Datenbeschaffung und Datenweitergabe durch die Sozialversicherer datenschutzkonform sind und die möglichen Missbrauchsgefahren aufzeigen** (Schnittstellen zwischen Sozialversicherern und Spitälern, anderen Sozialversicherern, Zusatz-, Lebens-, Haftpflichtversicherern etc.).
- ob und inwiefern die gesetzlichen und beruflichen Schweigepflichtbestimmungen durch die technologische Entwicklung im medizinischen Datenschutz in Gefahr sind, unter spezieller Berücksichtigung des Patientengeheimnisses nach Art. 321 StGB.
- ob und inwiefern die geltenden Rechtsgrundlagen angepasst werden müssen bzw. können (föderalistische Strukturen im Sozialversicherungs- und Gesundheitsbereich); Handlungsbedarf aufzeigen und ev. verschiedene Szenarien ausarbeiten.

b. Im Gegensatz zum Vorentwurf kommt das BSV nicht mehr zum Schluss, dass die Selbstregulierung (autorégulation) durch die Versicherer genüge. Hingegen ist das beauftragte „Institut de droit de la santé" (IDS) weiterhin der Ansicht, dass die Selbstregulierung durch die Versicherer möglich und nützlich sei (siehe Bericht IDS, S. 159). Der Berichtsentwurf verlangt hingegen, dass „*die zuständigen Bundesstellen zusammen mit den interessierten Kreisen die Ausarbeitung von Richtlinien und Verordnungs- und Gesetzesbestimmungen einleiten oder weiterverfolgen sowie andere Massnahmen einführen müssen*." (vgl. Entwurf zum Bericht des Bundesrats für die Konsultation der Organisationen: „Regelungslücken im medizinischen Datenschutz in den Sozialversicherungen", S. 68).

Aus verschiedenen Gründen kann sich der Eidgenössische Datenschutzbeauftragte (EDSB) dieser Schlussfolgerung nicht anschliessen. **Es ist offensichtlich, dass die Selbstregulierung in der Praxis nicht funktioniert.** Selbstregulierungsinstrumente (Weisungen, Richtlinien etc.) existieren z. T. schon. Das Hauptproblem – dies wurde im Bericht zum Teil erkannt – liegt in der Umsetzung dieser Regeln bzw. im Vollzug. Im Weiteren ist Selbstregulierung nichts Neues, da die verschiedenen Sozialversicherer bereits heute für den Datenschutz verantwortlich sind und somit den gesetzmässigen Zustand garantieren müssen (vgl. auch Art. 16 DSG).

Im Weiteren sind die Schlussfolgerungen im Berichtsentwurf sehr vage und nicht konkret. Gerade der Ist-Zustand und die alltägliche Praxis zeigen deutlich auf, dass die Bereitschaft der zuständigen Aufsichtsbehörde und der Versicherer eher gering ist, die datenschutzrechtlichen Vollzugsprobleme wirklich zu lösen. So wurden etwa die Empfehlungen im „Bericht Geiser" bis heute nicht umgesetzt.

Auf der anderen Seite sind die Sanktionsmöglichkeiten des EDSB von Gesetzes wegen eher beschränkt; z. B. kann der EDSB – im Gegensatz zur zuständigen Aufsichtsbehörde - keine Verfügungen erlassen, sondern nur Empfehlungen. Auch sind für die Versicherer verbindliche Richtlinien/Weisungen durch den EDSB nicht möglich.

Es sind somit andere Empfehlungen bzw. Massnahmen auszuarbeiten, welche die Versicherer zur konsequenten Umsetzung der bestehenden Datenschutzregelungen verpflichten (inkl. Sanktionen). Denn nur so lassen sich die festgestellten Mängel /Lücken korrigieren. Denkbar wäre etwa die Verpflichtung der Versicherer, Audits bzw. Zertifizierungsverfahren betreffend die Datenbearbeitung durchzuführen, welche noch im Detail zu konkretisieren wären. Auch eine stärkere Beteiligung der Aufsichtsbehörde, welche ihrerseits Massnahmen gegen fehlbare Versicherer treffen könnte, wäre zu prüfen.

Für den EDSB ist es sehr schwierig, zum vorliegenden Bericht materiell Stellung zu nehmen. Dies vor allem deshalb, weil **viele Passagen vage und unklar sind**. Insbesondere fehlen konkrete Massnahmen zu den verschiedenen Problembereichen. Die im Bericht aufgeführten Mängel und Lücken sollten daher noch vertieft abgeklärt werden. Klare Vorgaben an den Bundesrat bzw. das Parlament sind nicht vorhanden. Auch wurden die verschiedenen **Problembereiche in den einzelnen Sozialversicherungen nicht differenziert dargestellt.** Themen- bzw. Problembereiche, welche im Bericht erwähnt werden, finden am Ende des Berichts z. T. keine Würdigung bzw. es werden diesbezüglich **keine konkreten Massnahmen vorgeschlagen** (Beispiel: Privatdetektive S. 30/31). Der **Inhalt** und insbesondere die **Schlussfolgerungen bleiben im Wesentlichen abstrakt** und spiegeln die langjährige Erfahrung des EDSB im Gesundheitswesen nicht wieder.

Für den EDSB sind folgende Punkte von Relevanz (eine umfassende Aufzählung ist aus Kapazitätsgründen nicht möglich):

- *Gesetzliche Grundlagen im Sozialversicherungsbereich*: Das BSV geht in seinem Bericht grundsätzlich davon aus, dass die gesetzlichen Grundlagen hinsichtlich des Datenschutzes im Sozialversicherungsbereich genügen (vgl. S. 48 ff des Berichtsentwurfs). Diese Aussage steht aber im Widerspruch zu den Erwägungen des IDS, welches selbst davon ausgeht, dass gewisse gesetzliche Grundlagen zu allgemein abgefasst sind (vgl. S. 159 der Studie des IDS). Tatsächlich gibt es aber Auslegungsprobleme in der Praxis (Beispiele: Art. 42 und Art. 84 KVG). Andere Bereiche wie das dem BSV seit Jahren bekannte und bis anhin ungelöste Problem der Aufsicht/Statistik finden überhaupt keine Erwähnung im Bericht.

  Weiterhin nicht gelöst ist die Frage, wann die Einwilligung oder die gesetzliche Grundlage als Rechtfertigungsgrund gelten soll: vor allem im Invaliden- und Unfallversicherungsbereich stellt sich diese Frage bei der Datenbeschaffung; unklar ist etwa, wann Art. 28 Abs. 3 ATSG, welcher die Einwilligung der Versicherten für die Datenbeschaffung im Einzelfall verlangt, zu Anwendung kommt und wann nicht (vgl. auch S. 57 ff des Berichtsentwurfs).

  Auch wird festgestellt, dass im UVG-Bereich vermehrt Privatdetektive - ohne gesetzliche Grundlage - eingesetzt werden. Es wird aber nicht untersucht, ob dafür allenfalls die

notwendigen gesetzlichen Grundlagen geschaffen werden müssten (vgl. Berichtsentwurf, S. 30/31).

- *Vollzugsprobleme:* Der Bericht hält fest, dass es Vollzugsprobleme im medizinischen Datenschutz gibt; insbesondere werde das Verhältnismässigkeitsprinzip verletzt (vgl. 50/51 des Berichts). Tatsächlich werden aber für die einzelnen Themenbereiche **keine konkreten Massnahmen vorgeschlagen, welche die Missstände lösen helfen**. Als Beispiel sei das Problem der Postadressierung an die Vertrauensärzte im KVG-Bereich erwähnt; nach Ansicht des BSV sollen Richtlinien ausgearbeitet werden, welche die interne Weiterleitung der Post regeln (vgl. S. 50/51 des Berichtsentwurfs). Unklar bleibt aber, wer die Richtlinien ausarbeiten soll. Dass die Versicherer jedoch grundsätzlich nicht bereit sind, Richtlinien zu erstellen bzw. die Namen der Vertrauensärzte den Leistungserbringern bzw. Patienten bekannt zu geben, zeigt die Praxis jeden Tag. Es sind daher andere griffigere Massnahmen vorzuschlagen, um die Vollzugsprobleme zu lösen.

- *Technisch-organisatorische Aspekte*: **Die neueren Entwicklungen im Bereich der Datensicherheit werden kaum erwähnt im Bericht**. Tatsächlich existieren bereits heute datenschutzfreundliche Technologien, welche eingesetzt werden können („Datenschutz durch Technik").

  Im Rahmen der Wirtschaftlichkeitskontrolle durch die Versicherer wäre es etwa denkbar, die Versichertendaten durch geeignete technische Verfahren zu pseudonymisieren. Immerhin hat sich das IDS in diesem Sinne zu TARMED inkl. gesetzgeberischer Handlungsbedarf geäussert (vgl. Bericht IDS, S. 154 ff); leider wurden die Schlussfolgerungen im Bericht des BSV nicht übernommen. Im Bericht wird hingegen darauf hingewiesen, dass im Zusammenhang mit TARMED die Festlegung eines Codes von zentraler Bedeutung sei und der EDSB Informationen über diesen Code verlangt habe (vgl. Bericht, s. 60). Für den EDSB steht aber nicht der Code bzw. dessen Zusammensetzung im Vordergrund, sondern die Methodik der Datenbearbeitung (Anonymisierung bzw. Pseudonymisierung). Im Übrigen verweisen wir auf unseren Bericht zu TARMED, welcher am 25 Juni 2004 publiziert wurde (mehr dazu unter www.edsb.ch).

- *Transparenz:* Grundsätzlich wird im Bericht anerkannt, dass die Transparenz der Datenbearbeitung für die Versicherten verbessert werden muss (vgl. S. 49 des Berichtsentwurfs). Konkrete Vorschläge fehlen leider.

  Es wird z. B. erwähnt, dass für die Information der Versicherten im Rahmen der Datenbekanntgabe Verordnungsregelungen und Weisungen geeignet seien (vgl. S. 65 des Berichts). Einerseits fehlen aber konkrete Beispiele dafür. Andererseits wäre der Bundesrat schon seit einigen Jahren dazu verpflichtet, die Information der Versicherten auf Verordnungsstufe zu normieren (Beispiel: Art. 84a Abs. 7 KVG). Es wäre mindestens im Rahmen des vorliegenden Berichts an der Zeit gewesen, konkrete Vorschläge zu machen.

  Auf Versichererseite wird zudem die Notwendigkeit eines vermehrten Datenaustausches propagiert. Dies betreffe den Datenaustausch innerhalb einer Versicherungsgesellschaft als auch den Datenaustausch zwischen den Sozialversicherern einerseits und den Sozial- und Privatversicherern andererseits (vgl. Berichtsentwurf, S. 44-47). Im Rahmen der interinstitutionellen Zusammenarbeit zwischen der Invaliden- und Arbeitslosenversicherung ist sogar ein mündlicher Datenaustausch möglich (vgl. Berichtsentwurf, S. 63). Auch wenn ein vermehrter Datenaustausch nötig sein mag, sind auf der anderen Seite aber gleichzeitig die Persönlichkeitsrechte der Versicherten zu stärken. Dies bedeutet, dass die Versicherten über den Datenaustausch informiert werden müssen, um allenfalls ihr Sperrrecht geltend machen zu können. Diesbezügliche konkrete Vorschläge fehlen jedoch im Berichtsentwurf.

- *Rechte der betroffenen Personen:* Die im Bericht erwähnten Vollzugsprobleme (Auskunftsrecht, mangelnde Transparenz etc.) sind in konkrete Lösungen umzusetzen. Insbesondere ist das informationelle Selbstbestimmungsrecht der Versicherten zu stärken. Es sind Verfahren auszuarbeiten, welche die Rechte der Versicherten vermehrt berücksichtigen (Patient Empowerment). So wird etwa anerkannt, dass das Auskunftsrecht in der Praxis nicht immer gewährt wird; konkrete Massnahmen, welche diesen Zustand ändern könnten, fehlen jedoch (vgl. Berichtsentwurf, S. 64/65).

- *Vertrauensarzt-Problematik:* Im Bericht werden die verschiedenen Funktionen der Ärzte in den einzelnen Sozialversicherungen nicht klar dargelegt. Das Institut des Vertrauensarzt existiert tatsächlich nur für den KVG-Bereich (Kreisärzte, medizinischer Dienst im UVG-Bereich; regionale ärztliche Dienste im IVG-Bereich, medizinischer Dienst im BVG-Bereich).

  Obwohl Literatur sowie die Praxis die Frage diskutieren, ob die **„Filterfunktion" des Vertrauensarzt nach KVG** auch auf andere Sozialversicherer ausgedehnt werden könnte, **wird sie im Bericht leider nicht konkretisiert** (S. 53 des Berichtsentwurfs). Denkbar wäre z. B., dass der Kreisarzt der SUVA oder der regionale ärztliche Dienst der IV eine erste Anlaufstelle für sehr heikle medizinische Informationen sein könnte, wenn der Versicherte dies wünscht. Auf keinen Fall dürfen Informationen, welche die Versicherungsverwaltung für die Aufgabenerfüllung nicht benötigt, an diese weitergeleitet werden (Prinzip der Verhältnismässigkeit).

- *Datenbearbeitung im Auftrag* (vgl. S. 55 des Berichtsentwurfs): Tatsächlich macht die Datenbearbeitung im Auftrag bzw. das „Outsourcing" von staatlichen Tätigkeiten an Private in der Praxis vermehrt Probleme in der Praxis. Insbesondere im KVG-Bereich besteht die Tendenz, dass auch materielle Aufgaben im Sinne des KVG an Private delegiert werden (vgl. auch Gutachten Poledna). Auch die Einhaltung der datenschutzrechtlichen Grundsätze beim Outsourcing wirft Fragen auf. **Die Frage der Datenbearbeitung im Auftrag im Sozialversicherungsbereich ist daher vertieft zu analysieren, und es sind konkrete Lösungsvorschläge auszuarbeiten.**

Fazit:

Im Berichtsentwurf wird erkannt, dass im Sozialversicherungsbereich in erster Linie ein datenschutzrechtlicher Vollzugsnotstand existiert. Tatsächlich gibt es in einzelnen Bereichen auch einen Regelungsbedarf (Beispiel: Einsatz von Privatdetektiven).

Hingegen fehlen im Berichtsentwurf konkrete Lösungsvorschläge bzw. Massnahmen und Sanktionen. Die Schlussfolgerungen sind sehr vage und abstrakt bzw. es ist nicht ausreichend, nur Lösungsansätze aufzuführen. Insbesondere bleibt offen, wer wann welche Massnahmen treffen soll. Denn es besteht – der EDSB hat in seinen Tätigkeitsberichten mehrmals darauf aufmerksam gemacht - schon seit Jahren ein echter Handlungsbedarf betreffend den Datenschutz im Sozialversicherungsbereich. Denkbar wäre etwa, im Sozialversicherungsbereich Audits und Zertifizierungsverfahren von Gesetzes wegen einzuführen.

Zudem erhöht die technologische Entwicklung bereits heute die Missbrauchsgefahr und stellt eine Bedrohung für das Patientengeheimnis dar. Auf der anderen Seite können gerade datenschutzfreundliche Technologien die Persönlichkeitsrechte der Betroffenen schützen. Leider gibt der Bericht diesbezüglich auch keine konkreten Lösungsvorschläge.

EIDGENÖSSISCHER
DATENSCHUTZBEAUFTRAGTER