

HCS Health Communication Service GmbH
Maiss 48
A-3033 Altengbach

**Gutachten zur Gesetzeskonformität des Systems
Praxisnetzwerk**

18.05.2005

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

Inhalt

1	Auftrag.....	3
2	Befund.....	3
2.1	Gegenstände der Befundaufnahme	3
2.2	Befundaufnahme	3
3	Rechtsgrundlagen	13
3.1	Datenschutzgesetz(DSG).....	13
3.1.1	Grundsätzliches	13
3.1.2	Beteiligte	14
3.1.3	Meldung, Registrierung, Zulassung.....	15
3.1.4	Art der Datenanwendung	16
3.1.5	Zulässigkeit der Übermittlung.....	17
3.1.5.1	Zulässige Datenanwendung.....	18
3.1.5.2	Befugnis des Empfängers	18
3.1.5.3	Schutzwürdige Geheimhaltungsinteressen.....	19
3.1.6	Freigeben von Befunden	19
3.1.7	Datensicherheit	20
3.2	Gesundheitstelematikgesetz (GTelG)	21
3.3	Ärztegesetz	23
3.4	Bundesgesetz über Krankenanstalten und Kuranstalten (KAKuG)	23
3.5	Oö Krankenanstaltengesetz 1997 (Oö KAG)	25
3.6	NÖ Krankenanstaltengesetz (NÖ KAG)	27
3.7	Wiener Krankenanstaltengesetz 1987 (Wr. KAG)	28
3.8	Steiermärkisches Krankenanstaltengesetz 1999 (KALG).....	29
3.9	Kärntner Krankenanstaltenordnung.....	30
3.10	Salzburger Krankenanstaltengesetz 2000 (SKAG)	31
3.11	Tiroler Krankenanstaltengesetz (Tir KAG).....	32
3.12	Zusammenfassung.....	33
4	Gutachten.....	34
4.1	Einhaltung des DSG.....	34
4.1.1	Zulässigkeit der Nutzung des Systems gemäß DSG	34
4.1.2	Registrierungspflicht, Vorabkontrolle gemäß DSG.....	34
4.1.3	Datensicherheitsmaßnahmen	35
4.2	Einhaltung der Vorgaben des GTelG	36
4.2.1	Nachweis von Identität und Rolle	36
4.2.2	Benutzeridentifikation bei Nutzung des Systems	37
4.2.3	Vertraulichkeit - Verschlüsselung.....	37
4.2.4	Sicherstellung der Integrität (Unverfälschbarkeit) der Befunddaten	37
4.2.5	Dokumentation	37

1 Auftrag

Am 25.04.2005 wurde ich von Herrn Eduard Schebesta, Geschäftsführer der HCS Health Communication Service GmbH, beauftragt, die Gesetzeskonformität des internetbasierten Dienstes „Praxisnetzwerk“ (bestehend aus den Produkten „medView“ und „medIndex“) in Hinblick auf das österreichische Gesundheits- und Datenschutzrecht zu begutachten.

2 Befund

2.1 Gegenstände der Befundaufnahme

Einsicht genommen wurde in folgende Unterlagen:

Datenschutzgesetz 2000 (DSG 2000)
Gesundheitstelematikgesetz (GTelG)
Ärztegesetz
Bundesgesetz über Krankenanstalten und Kuranstalten (KAKuG)
Oö Krankenanstaltengesetz 1997 (Oö KAG)
NÖ Krankenanstaltengesetz (NÖ KAG)
Wiener Krankenanstaltengesetz 1987 (Wr. KAG)
Steiermärkisches Krankenanstaltengesetz 1999 (KALG)
Kärntner Krankenanstaltenordnung
Salzburger Krankenanstaltengesetz 2000 (SKAG)
Tiroler Krankenanstaltengesetz (Tir KAG)

Richtlinien der Österreichischen Ärztekammer für die Übertragung medizinischer Daten

2.2 Befundaufnahme

Bei der Befundaufnahme am 25.04.2005 in den Räumen des SV und im Rechenzentrum der Health Communications Service in 1210 Wien, Brünner Strasse 20, war neben dem Sachverständigen Herr Eduard Schebesta anwesend.

Bei der Befundaufnahme im Büro des SV wurden an einem ans Internet angeschlossenen PC folgende Tätigkeiten mit dem System abgewickelt:

Zu Beginn wurde versucht, www.praxisnetzwerk.at mit dem Web-Browser Internet Explorer zu öffnen. Dabei wurde allerdings angezeigt, dass das root-Zertifikat für die

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

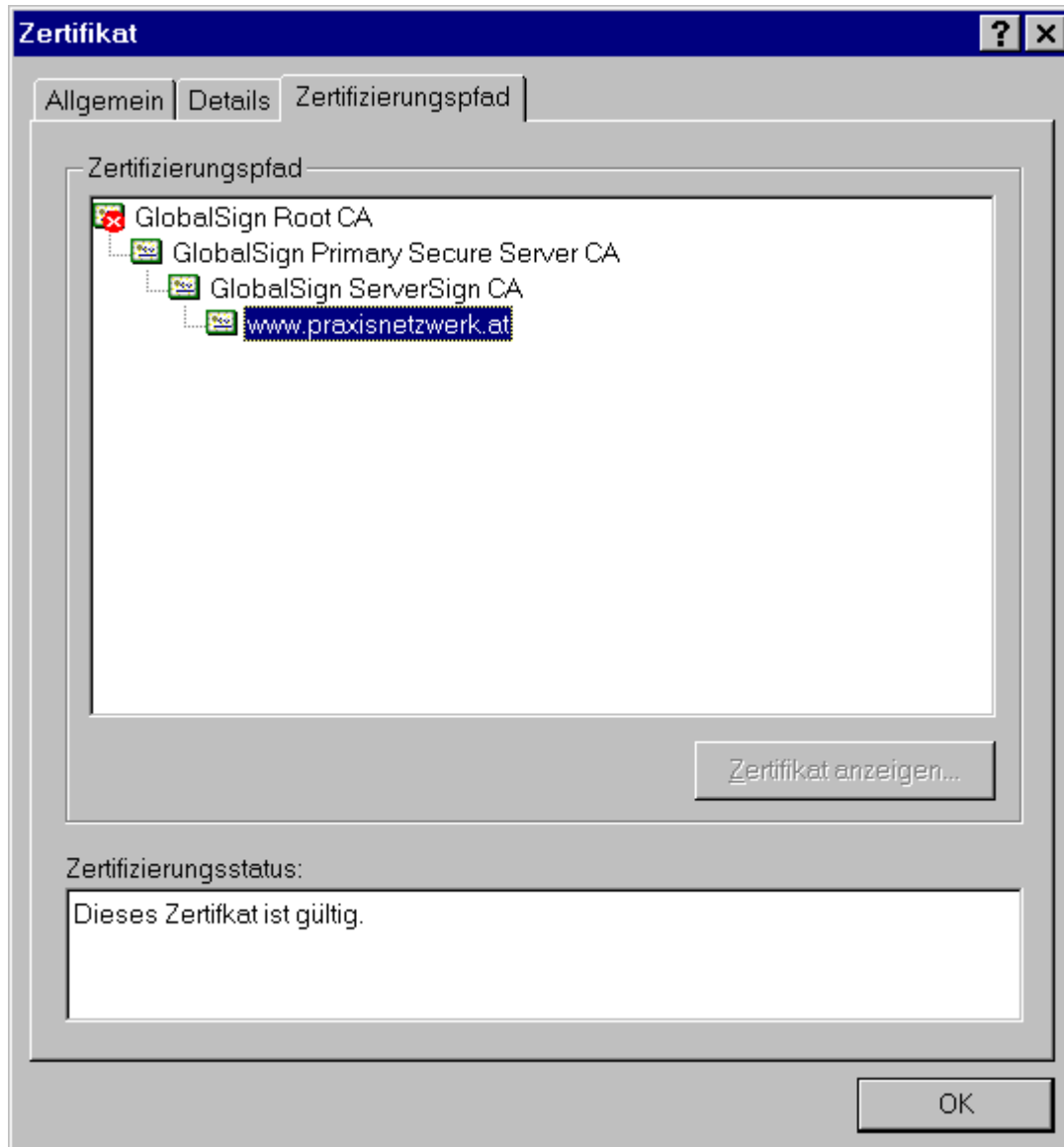
Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

SSL-Verschlüsselung fehle. Nach einem Umstieg auf eine neuere Version von Mozilla trat diese Frage nicht mehr auf, da diese Version das root-Zertifikat von Global Sign schon installiert hatte. Der Test bewies allerdings eindeutig, dass das System mittels SSL verschlüsselt überträgt.



Die Anmeldung am System ist durch Eingabe von Username, PIN-Code, sowie eines nur ca 1 min gültigen Kennworts, generiert mit einem Cryptomodul von RSA Inc gesichert.

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation
IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung
Universitätslektor im Fach EDV- und Fernmelderecht
Steigentesch. 13/3/2, A-1220 Wien
Telefon: 203 53 81-0, Fax: 203 53 81-5
E-Mail: walter.jaburek@edv-concept.at

Die Web-Oberfläche ähnelt einem Webmail-Interface. Es gibt ein Postfach für gelesene und eines für ungelesene Befunde.



Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

Für jeden Patienten können die zugehörigen Befunde samt Anhängen wie zB Röntgenbilder aufgerufen werden:





Befunde können, wie in jedem Mail-System, an andere Benutzer des Praxisnetzwerks weitergeleitet werden.

Außerdem bietet das Praxisnetzwerk die derzeit nur für den Testbetrieb eingerichtete Möglichkeit, die Befunde für Gruppen anderer Benutzer im Netz freizugeben. In der selben Eingabemaske kann die Freigabe auch wieder rückgängig gemacht werden, indem man „nicht freigeben“ auswählt.

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

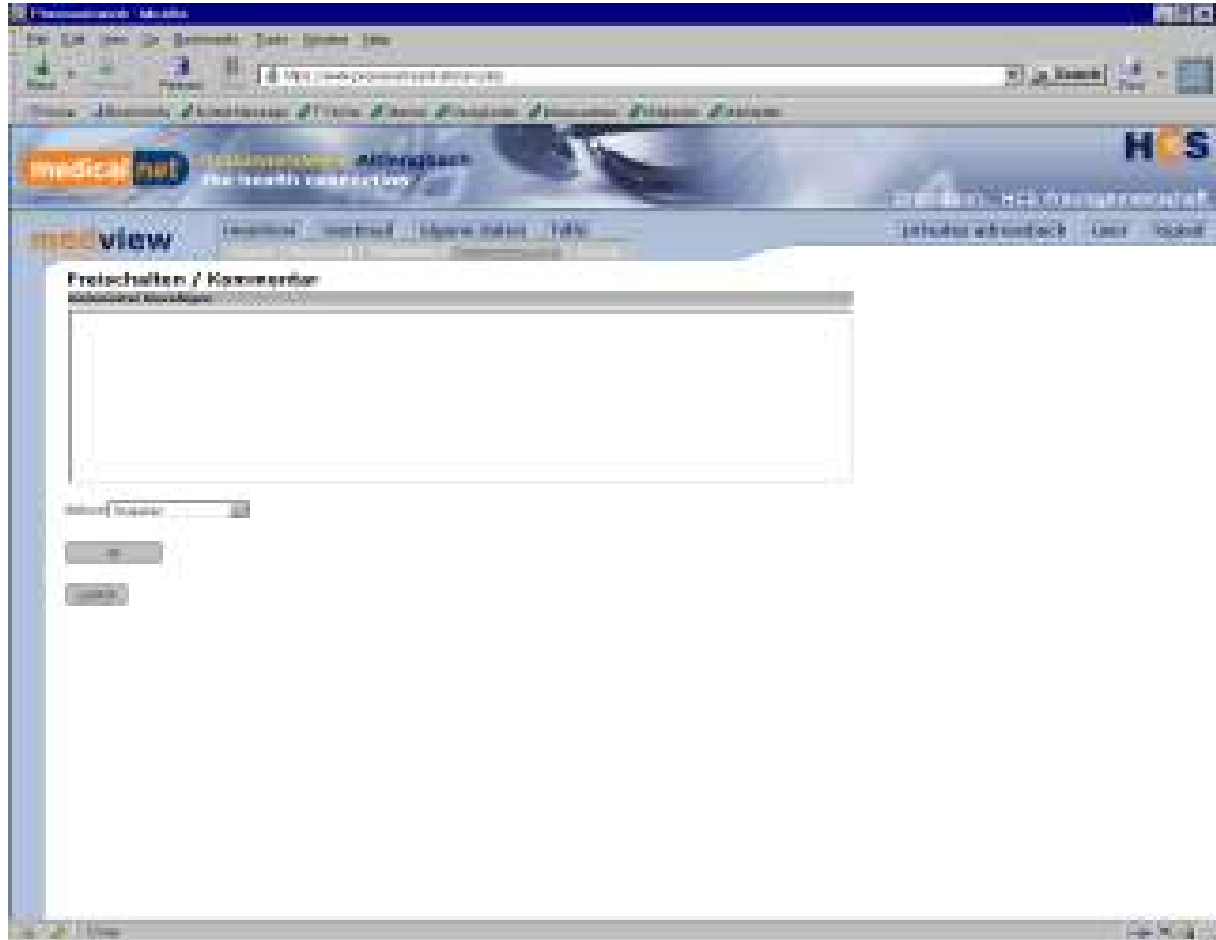
IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steingteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at



Ebenso ist es möglich, das Praxisnetzwerk nach von anderen Benutzern freigegebenen Befunden zu durchsuchen und sich diese anzeigen zu lassen.

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation
IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung
Universitätslektor im Fach EDV- und Fernmelderecht
Steigenteschg. 13/3/2, A-1220 Wien
Telefon: 203 53 81-0, Fax: 203 53 81-5
E-Mail: walter.jaburek@edv-concept.at



Laut Hr Schebesta ist vorgesehen, die Einwilligung des Patienten für jeden einzelnen Befund durch Ausdruck eines Mustertextes und Unterschrift des Patienten einzuholen.

Ein automatischer Abbau der Verbindung bei längerer Untätigkeit des Benutzers am Bildschirm („Timeout“) wird derzeit gerade realisiert.

Der zweite Teil der Befundaufnahme fand im Rechenzentrum an der Adresse 1210 Wien, Brünner Strasse 20 statt.

Zur Ausstattung des Rechenzentrums gehören gesicherte Türen, sowie eine Brandmelde- und Löschanlage. Bei dem Mailserver handelt es sich um einen Rechner mit der Software Gordano Messaging Server. Ein Windows 2000-Server fungiert als Client, der die E-Mails vom Mailserver abholt.

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

Der Server befindet sich hinter einer Fortinet FortiGate 200A Antivirus Firewall, die eine Intrusion Detection und einen Virensan beinhaltet.

Die Mailclient-Software von HCS HEALTH COMMUNICATION SERVICE GMBH trägt den Namen „medsecure+“ und wurde in Delphi/C++ geschrieben. Sie enthält eine Verschlüsselung mit 3DES, sowie eine Prüfung von RSA Signaturen.

Der Client speichert die E-Mails in ein Verzeichnis auf dem Client-Rechner. Danach werden die E-Mails in eine MySQL-Datenbank auf einem weiteren Windows-Rechner geschrieben.

Auf dem Client-Rechner läuft Apache. Der Zugriff ist mit SSL (Zertifikat von Global Sign) und dem oben beschriebenen UserID/ PIN/ zeitlich begrenzt gültiges Passwort gesichert.

Im internen Netzwerk wird der IP-Adressbereich 192.168.*.* verwendet. Ein irrtümliches Routen des internen Netzwerkverkehr ist also ausgeschlossen. Außerdem existiert eine DMZ zwischen internem und externem Netz.

Der Webserverzugang erfolgt über eine andere Firewall.

Zum Test der Forderung des Gesundheitstelematikgesetzes, dass Befunde mit kompromittierter Signatur nicht weitergeleitet werden dürfen, wurden Testnachrichten im Rohformat der Inbox des Gordano-Rechners (attachement content-type: application/x-pkcs7-mime ; die Dateierdung ist : .p7m) willkürlich in einem Zeichen geändert. Die geänderten Nachrichten wurden anschließend vom Client abgeholt. Dieser brachte beim ersten Test die Fehlermeldung: „ASN1 Fehler“, „message was encrypted but not signed“.

Bei einem zweiten Test wurde eine Änderung eher am Ende der Nachricht durchgeführt. Die Fehlermeldung des Clients lautete diesmal: „decrypted“, aber „Signatur invalid“. In jedem Fall wurde die Nachricht nach Protokollierung des Fehlers nicht in die Inbox des Empfängers weitergeleitet.

3 Rechtsgrundlagen

3.1 Datenschutzgesetz(DSG)

3.1.1 Grundsätzliches

§ 1 Abs 1 DSG normiert:

„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. (...)“
(Grundrecht auf Datenschutz)

Nach § 4 Z 1 DSG sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist, „**Daten**“ („**personenbezogene Daten**“).

Nur „**indirekt personenbezogen**“ sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.

Die **medizinischen Daten der Patienten** sind direkt personenbezogene Daten, da zB auf Befunden immer der Name des Patienten vermerkt ist.

Das DSG unterscheidet zwischen zwei Datenklassen, sensiblen und nicht-sensiblen Daten. Die Verwendung nicht-sensibler Daten wird in § 8 DSG geregelt, jene sensibler Daten in § 9 DSG.

Nach § 4 Z 2 DSG sind Daten natürlicher Personen über ihre

- rassische und ethnische Herkunft,
- politische Meinung,
- Gewerkschaftszugehörigkeit,
- Religiöse und philosophische Überzeugung,
- Gesundheit
- oder ihr Sexualleben

sensible Daten („besonders schutzwürdige Daten“).

Die Befunddaten der Patienten betreffen deren Gesundheitszustand und sind somit eindeutig sensible Daten iSd DSG.

Im § 6 DSG sind **Grundsätze für die Verwendung von Daten** normiert:

„§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
 2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
 3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
 4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
 5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.
- (2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.
(...)“

Gemäß § 7 Abs 1 DSGVO **dürfen Daten nur verarbeitet werden**, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

Weiters ist die Übermittlung sensibler Daten ausschließlich in den in § 9 Z 1-13 DSGVO genannten Fällen zulässig.

3.1.2 Beteiligte

Auftraggeber einer Anwendung des Systems Praxisnetzwerk iSd § 4 Z 4 DSGVO sind die beteiligten **Krankenanstalten, Ärzte und medizinischen Labors**. Krankenanstalten sind idR in Formen des öffentlichen Rechts eingerichtet. Labors unterstehen einem Arzt und werden daher in der Folge datenschutzrechtlich wie Arztpraxen behandelt.

Eine geplante Anwendung des Systems Praxisnetzwerk ist daher gemäß § 5 DSGVO dem **öffentlichen Bereich** zuzurechnen, wenn sie für Zwecke auch nur eines Auftraggebers des öffentlichen Bereiches nach §5 Abs 2 Z 1 durchgeführt werden soll, sonst dem **privaten Bereich**. Diese Unterscheidung spielt allerdings seit dem DSGVO 2000 kaum mehr eine Rolle.

Der Betreiber von Praxisnetzwerk ist als **Dienstleister** iSd § 2 Z 5 zu qualifizieren, da er Daten verwendet, die ihm zur Herstellung eines aufgetragenen Werkes (Errichtung und Betrieb von Praxisnetzwerk) überlassen wurden.

3.1.3 Meldung, Registrierung, Zulassung

Es gibt nach DSGVO prinzipiell drei verschiedene Möglichkeiten. Eine Datenanwendung kann meldefrei sein, sie kann meldepflichtig bei der Datenschutzkommission sein oder sie unterliegt einer Vorabkontrolle durch die Datenschutzkommission. In letztgenanntem Fall darf sie erst nach einer Prüfung durch die Datenschutzkommission in Betrieb genommen werden.

Vor Aufnahme einer Datenanwendung hat ein Auftraggeber gemäß § 17 Abs 1 DSGVO **Meldung an die Datenschutzkommission** zu erstatten. Davon sind Datenanwendungen ausgenommen, die den Erfordernissen von § 17 Abs 2, bzw 3 entsprechen.

Meldepflichtige Datenanwendungen dürfen gemäß § 18 Abs 1 DSGVO unmittelbar nach Abgabe der Meldung aufgenommen werden. Sollten jedoch die Voraussetzungen des § 18 Abs 2 DSGVO vorliegen, dann darf die Datenanwendung erst nach ihrer Prüfung durch die Datenschutzkommission aufgenommen werden (Vorabkontrolle).

Eine Meldung im Sinne des § 17 DSGVO ist insbesondere dann nicht notwendig, wenn die Datenanwendung einer Standardanwendung entspricht (§ 17 Abs 2 Z 6 DSGVO). Eine Aufzählung aller Datenanwendungen, die als Standardanwendungen zu qualifizieren sind, findet sich in Anlage 1 der Standard- und Muster-Verordnung 2004 (StMV 2004). In dieser Anlage wird unter SA024 Patientenverwaltung und Honorarabrechnung die Führung von Patientenkarteen zur Dokumentation (§ 51 ÄrzteG 1998), Erstellung von medizinischen Gutachten und Honorarverrechnung durch Ärzte, Zahnärzte und Dentisten, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) in diesen Angelegenheiten zur Standardanwendung erklärt. Zu den Empfängerkreisen dieser Standardverarbeitung gehören ua andere Ärzte, Vertreter von sonstigen Gesundheitsberufen und medizinische oder soziale Einrichtungen, in deren Behandlung der Patient steht, sowie Apotheken, mit Zustimmung des Patienten.

Meldepflichtige Anwendungen können allerdings gemäß § 18 einer Vorabkontrolle durch die Datenschutzkommission unterliegen, wenn sie

- a) keiner Musteranwendung entsprechen und
- b) sensible Daten enthalten oder in Form eines Informationsverbundsystems durchgeführt werden sollen.

Ad a) Eine Aufzählung aller Datenanwendungen, die als Musteranwendungen zu qualifizieren sind, findet sich in Anlage 2 der Standard- und Muster-Verordnung 2004 (StMV 2004).

Ad b) Ein Informationsverbundsystem wird in § 4 Z 13 DSG wie folgt definiert: „die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;“

Meldepflichtige Informationsverbundsysteme, die keiner Musteranwendung entsprechen, müssen daher vor ihrer Inbetriebnahme von der Datenschutzkommission geprüft werden.

Anders stellt sich allerdings die Situation dar, wenn ein bereits bestehendes Informationsverbundsystem weiterbetrieben wird:

§ 61 DSG:

„(1) Meldungen, die vor Inkrafttreten dieses Bundesgesetzes an das Datenverarbeitungsregister erstattet wurden, gelten als Meldungen im Sinne des § 17, soweit sie nicht im Hinblick auf das Entfallen von Meldepflichten gemäß § 17 Abs. 2 oder 3 gegenstandslos geworden sind. Desgleichen gelten vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen als Registrierungen im Sinne des § 21.“

Datenanwendungen - und damit auch Informationsverbundsysteme - , die vor dem Inkrafttreten des DSG 2000 dem Datenverarbeitungsregister gemeldet wurden und im Datenverarbeitungsregister registriert wurden, sind daher nicht neu zu melden und zu registrieren.

Für diese Datenanwendungen ist daher eine Vorabkontrolle durch die Datenschutzkommission nicht notwendig, da ja die Registrierung im Datenverarbeitungsregister, die das Ergebnis der Vorabkontrolle wäre, schon vorhanden ist.

3.1.4 Art der Datenanwendung

Der Ansatzpunkt für die rechtliche Beurteilung ist zunächst einmal Ausmaß und Natur der geplanten Datenanwendung.

Die **Datenanwendung** ist die

- Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die
- zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

- zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).“ (§ 4 Z 7 DSGVO).

Die Tätigkeit von Praxisnetzwerk lässt sich in 2 grundlegend verschiedene Bereiche unterteilen.

- Einerseits wird eine bloße Versendungsmöglichkeit von Befunden angeboten, die einem herkömmlichen E-Mail-System nicht unähnlich ist.
- Andererseits gibt es auch die Möglichkeit, eigene Befunde für andere Ärzte freizugeben und diesen zugänglich zu machen.

Versenden von Befunden:

Praxisnetzwerk bietet lediglich die Infrastruktur, die Patientendaten und Befunde werden von Ärzten oder Krankenanstalten an andere Ärzte/Krankenanstalten versendet. Das E-Mail System dient nur der Durchleitung von Daten, die Betreiber von Praxisnetzwerk haben keinen direkten Einfluss auf die Übermittlung.

Freigeben von Befunden:

Die Verwendungsschritte zum Erreichen des Ergebnisses umfassen die Übertragung von Befunddaten zum und vom zentralen Server. Praxisnetzwerk ermöglicht den Upload von Befunddaten, die Speicherung, sowie den Download durch einen Benutzer des Systems.

3.1.5 Zulässigkeit der Übermittlung

Zu prüfen ist die Zulässigkeit der Übermittlung von Daten zwischen Ärzten, Krankenanstalten und Labors.

§ 7 Abs 2 DSGVO nennt dazu drei Voraussetzungen:

- Die Daten müssen aus einer **zulässigen Datenanwendung** stammen.
 - Der Empfänger muss dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder **rechtliche Befugnis** - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft machen.
 - Durch Zweck und Inhalt der Übermittlung dürfen die **schutzwürdigen Geheimhaltungsinteressen** des Betroffenen nicht verletzt werden.
-

3.1.5.1 Zulässige Datenanwendung

Die Zulässigkeit der Datenverarbeitung beim Übermittler kann als gegeben angesehen werden, da ihr Zweck und Inhalt von den rechtlichen Befugnissen von Ärzten, Krankenanstalten und Labors gedeckt sind (§ 7 Abs 1 DSGVO):

- In der Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 werden ausdrücklich Datenanwendungen genannt, welche nicht meldepflichtig sind. Es ist daher davon auszugehen, dass der Gesetzgeber Standardanwendungen, für die er eine Meldefreiheit normiert als zulässige Formen der Datenanwendung vorsieht.
- In Anlage 1 der StMV 2004 wird unter SA024 Patientenverwaltung und Honorarabrechnung detailliert aufgezählt, welche Daten ein Arzt von seinen Patienten speichern darf.
- Das Ärztegesetz, sowie die Landeskrankenanstaltengesetze bilden ebenfalls eine Rechtsgrundlage für die Verarbeitung von Befunddaten.

Auf jeden Fall ist also das Speichern von Befunden durch Ärzte, Krankenanstalten und Labors eine zulässige Verarbeitung von Daten iSd § 7 Abs 1 DSGVO.

3.1.5.2 Befugnis des Empfängers

Für die Übermittlung ist es notwendig, dass auch der Empfänger eine rechtliche Befugnis zur Datenverarbeitung hat und diese dem Übermittelnden glaubhaft macht – soweit sie nicht außer Zweifel steht (§ 7 Abs 2 Z 2 DSGVO).

In Anlage 1 der StMV 2004 werden unter SA024 Patientenverwaltung und Honorarabrechnung in Nr. 22 Fremddiagnosen explizit erwähnt. Wirklich bestimmend hierfür sind aber wohl die Regelungen des Gesundheitsrechts (s. unten).

Aus diesen Regelungen folgt: Als behandelnder Arzt/Krankenanstalt hat der Empfänger idR eine ausreichende rechtliche Befugnis, die Befunddaten eines anderen Arztes/einer anderen Krankenanstalt übermittelt zu bekommen.

3.1.5.3 Schutzwürdige Geheimhaltungsinteressen

In § 9 DSGVO ist geregelt, unter welchen ausschließlichen Voraussetzungen die **Verwendung sensibler Daten** schutzwürdige Geheimhaltungsinteressen nicht verletzt und Verarbeitung und Übermittlung dieser Daten daher zulässig sind:

Im vorliegenden Fall kommen folgende Möglichkeiten in Frage:

- Die Ermächtigung und Verpflichtung zur Verwendung ergibt sich aus gesetzlichen Vorschriften, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen (Z 3). In den Erläuternden Bemerkungen zur Regierungsvorlage findet sich zur Z 3 keine für das Gesundheitswesen einschlägige Anmerkung. Es ist jedoch davon auszugehen, dass gesetzliche Vorschriften für Ärzte, Krankenanstalten und Labors dem wichtigen öffentlichen Interesse der Gesundheitsversorgung dienen. Wie unten noch ausgeführt wird, finden sich in diesen Ermächtigungen zur Datenübermittlung. Erfolgt eine Datenübermittlung aufgrund dieser gesetzlichen Vorschriften, so ist die Ausnahmeregelung der Z 3 erfüllt und die Verwendung zulässig.
- Der Betroffene hat seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt (Z 6).
- Die Verarbeitung oder Übermittlung erfolgt zur Wahrung lebenswichtiger Interessen des Betroffenen und seine Zustimmung kann – zB im Falle einer schweren Verletzung mit Schock – nicht rechtzeitig eingeholt werden (Z 7).
- Die Daten sind zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder –behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich und die Verwendung dieser Daten erfolgt durch ärztliches Personal oder sonstige Personen, die einer entsprechenden Geheimhaltungsverpflichtung unterliegen (Z 12).

Abgesehen von diesen Voraussetzungen besteht ein grundsätzliches Verarbeitungsverbot für sensible Daten, da schutzwürdige Interessen nach § 1 Abs 1 DSGVO verletzt würden.

3.1.6 Freigeben von Befunden

Es gelten die soeben genannten Bestimmungen über die Zulässigkeit der Datenübermittlung zwischen Ärzten und Krankenanstalten.

Allerdings handelt es sich in diesem Bereich bei Praxisnetzwerk um ein Informationsverbundsystem (§ 4 Z 13 DSGVO).

Sinn und Zweck ist die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden.

Das DSGVO sieht besondere Regelungen für Informationsverbundsysteme vor:

§ 50. (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, dass kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Die Unterstützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne dass eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten auf den Betreiber übertragen werden. Soweit dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang gegenüber den Betroffenen und den für die Vollziehung dieses Bundesgesetzes zuständigen Behörden nur wirksam, wenn er - auf Grund einer entsprechenden Meldung an die Datenschutzkommission - aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(3) Die Bestimmungen der Abs. 1 und 2 gelten nicht, soweit infolge der besonderen, insbesondere internationalen Struktur eines bestimmten Informationsverbundsystems gesetzlich ausdrücklich anderes vorgesehen ist.

3.1.7 Datensicherheit

Nach § 14 DSGVO sind für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, **Maßnahmen zur Gewährleistung der Datensicherheit** zu treffen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Gemäß § 15 DSGVO haben Auftraggeber, Dienstleister und ihre Mitarbeiter die Daten aus den Datenanwendungen **geheim zu halten**, soweit kein rechtlich zulässiger

Grund für die Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht.

3.2 Gesundheitstelematikgesetz (GTelG)

Dieses Gesetz enthält zwingende Bestimmungen zum elektronischen Gesundheitsdatenaustausch.

Allerdings normiert § 19 Abs 2 GTelG:

„Der elektronische Gesundheitsdatenaustausch darf auch dann bis zum 31.12.2007 durchgeführt werden, wenn er den Bestimmungen des 2. Abschnitts dieses Bundesgesetzes nicht entspricht.“

Bei dem Dienst „Praxisnetzwerk“ handelt es sich um einen Gesundheitsdiensteanbieter iS des § 2 Z 2 GTelG, da die regelmäßige Verwendung von Gesundheitsdaten (iS § 2 Z 1 GTelG) Bestandteil des Dienstleistungsangebotes ist.

Das GTelG sieht bei Weitergabe von Gesundheitsdaten oder Einräumung von Zugriffsrechten auf solche Daten eine Identifikationspflicht der Empfänger und der Gesundheitsdiensteanbieter, die ein Zugriffsrecht in Anspruch nehmen wollen, vor.

Der Identitätsnachweis ist gemäß § 3 GTelG in elektronischer Form zu erbringen und zu prüfen. Nach § 4 Abs 1 GTelG ist der Nachweis der Identität durch Vorlage eines qualifizierten Zertifikats (§§ 3 bis 6 E-Government-Gesetz; Bürgerkarte) zu erbringen. Außerdem hat der Bundesminister für Gesundheit und Frauen qualitative Mindestanforderungen für die Zertifikate und elektronischen Signaturen mit Verordnung festzulegen (§ 7 Abs 5 GTelG).

Außerdem ist bis 1. Juli 2006 die Einführung eines eHealth-Verzeichnisdienstes geplant. Für Gesundheitsdiensteanbieter, die in diesem Verzeichnis eingetragen sind, kann ein Nachweis nach § 4 Abs 1 GTelG unterbleiben, wenn die Eintragung vom Gesundheitsdaten weitergebenden oder den Zugriff darauf einräumenden Gesundheitsdiensteanbieter durch Einsichtnahme in den eHealth-Verzeichnisdienst überprüft wird (§ 4 Abs 2 GTelG). Die Aufnahme in den eHealth-Verzeichnisdienst erfolgt ausschließlich auf Antrag eines Gesundheitsdiensteanbieters und ist kostenlos (§ 11 Abs 1 GTelG).

Bei ausschließlich programmgesteuerter Abwicklung des Datenaustausches genügt die Identifizierung durch Serverzertifikate (§ 4 Abs 3 GTelG).

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

Bei direkter Bedienung aus der Ferne kann die Identifikation aus technischen oder wirtschaftlichen Gründen auch nur im Zuge der Implementierung der Zugangsberechtigung erfolgen. Die Identität ist mindestens einmal im Monat vom Gesundheitsdiensteanbieter zu prüfen (§ 4 Abs 4+5 GTelG).

Bei Versendung von Gesundheitsdaten über ein öffentlich zugängliches Netz müssen kryptographische Verfahren zur Anwendung kommen, die nach dem jeweiligen Stand der Technik mit wirtschaftlich vernünftigem Aufwand nicht kompromittiert werden können (§ 6 Abs 1 GTelG).

Die Verschlüsselung muss auf den Anlagen des Absenders erfolgen, die Entschlüsselung auf den Anlagen des Empfängers der Gesundheitsdaten (§ 6 Abs 2 GTelG).

Die Integrität bei der Übertragung von Gesundheitsdaten ist ebenfalls durch elektronische Signaturen nachzuweisen und zu prüfen (§ 7 Abs 1 GTelG).

Elektronische Signaturen müssen jedoch nicht verwendet werden, wenn der elektronische Gesundheitsdatenaustausch ausschließlich programmgesteuert oder durch direkte Bedienung einer Datenanwendung aus der Entfernung erfolgt (§ 7 Abs 2 GTelG).

Das Anbringen elektronischer Signaturen kann automationsunterstützt erfolgen. Im Fall einer fehlgeschlagenen Signaturprüfung dürfen die empfangenen Gesundheitsdaten nicht verwendet werden.

Die Datensicherheitsmaßnahmen sind in den innerorganisatorischen Datenschutz- bzw. Datensicherheitsvorschriften zu dokumentieren (§ 8 Abs 1 GTelG, vgl. § 14 DSG 2000).

Die Gesundheitsdiensteanbieter werden in Rollen eingeteilt, dh nach der Art ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebotes (§ 2 Z 4 GTelG). Der Bundesminister für Gesundheit und Frauen legt die für den elektronischen Gesundheitsdatenaustausch in Betracht kommenden Rollen sowie jene Stellen, die die Zuordnung von Rollen zu einem Gesundheitsdiensteanbieter authentisch bestätigen, mit Verordnung fest (§ 5 Abs 1 GTelG). Der Nachweis der Rolle erfolgt durch Zertifikat und kann wiederum unterbleiben, wenn der Gesundheitsdiensteanbieter in den eHealth-Verzeichnisdienst eingetragen ist und die Eintragung vom weitergebenden Gesundheitsdiensteanbieter überprüft wird (§ 5 Abs 2+3 GTelG).

Bei ausschließlich programmgesteuerter Abwicklung des Datenaustausches, bzw direkter Bedienung aus der Ferne kann die Prüfung der Rolle aus technischen oder wirtschaftlichen Gründen auch nur vor der erstmaligen Datenübertragung, bzw im Zuge der Implementierung der Zugangsberechtigung erfolgen. Die Rolle ist mindestens einmal im Monat vom Gesundheitsdiensteanbieter zu prüfen (§ 5 Abs 4 bis 6 GTelG).

3.3 Ärztegesetz

§ 51 Ärztegesetz:

- (1) Der Arzt ist verpflichtet, Aufzeichnungen über jede zur Beratung oder Behandlung übernommene Person, insbesondere über den Zustand der Person bei Übernahme der Beratung oder Behandlung, die Vorgeschichte einer Erkrankung, die Diagnose, den Krankheitsverlauf sowie über Art und Umfang der beratenden, diagnostischen oder therapeutischen Leistungen einschließlich der Anwendung von Arzneyspezialitäten und der zur Identifizierung dieser Arzneyspezialitäten und der jeweiligen Chargen im Sinne des § 26 Abs. 8 des Arzneimittelgesetzes, BGBl. Nr. 185/1983, erforderlichen Daten zu führen und hierüber der beratenden oder behandelnden oder zu ihrer gesetzlichen Vertretung befugten Person alle Auskünfte zu erteilen.(...)
- (2) Ärzte sind zur automationsunterstützten Ermittlung und Verarbeitung personenbezogener Daten gemäß Abs. 1 sowie zur Übermittlung dieser Daten
 1. an die Sozialversicherungsträger und Krankenfürsorgeanstalten in dem Umfang, als er für den Empfänger zur Wahrnehmung der ihm übertragenen Aufgaben eine wesentliche Voraussetzung bildet, sowie
 2. an andere Ärzte oder medizinische Einrichtungen, in deren Behandlung der Kranke steht, mit Zustimmung des Kranken berechtigt. Die zur Beratung oder Behandlung übernommene Person hat das Recht auf Einsicht, Richtigstellung unrichtiger und Löschung unzulässigerweise verarbeiteter Daten.

Für Ärzte besteht also eine Übermittlungsermächtigung ohne Zustimmung des Patienten, wenn der Empfänger eine Krankenanstalt ist. Die Übermittlung an andere Ärzte oder medizinische Einrichtungen (Labors) setzt die Zustimmung des Patienten voraus.

3.4 Bundesgesetz über Krankenanstalten und Kuranstalten (KAKuG)

Im KAKuG sind folgende, für Praxisnetzwerk bedeutende Grundsatzbestimmungen für die Landesgesetzgeber hinsichtlich Umgang mit Patientendaten geregelt (In diesem Gesetz finden sich für dieses Thema keine unmittelbar geltenden Bestimmungen):
(Hervorhebungen durch den Autor):

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

„§ 9. (1) Für die bei Trägern von Krankenanstalten und in Krankenanstalten beschäftigten Personen sowie für die Mitglieder von Ausbildungskommissionen (§ 8 Abs. 4) und für die Mitglieder von Kommissionen gemäß § 8c besteht Verschwiegenheitspflicht, sofern ihnen nicht schon nach anderen gesetzlichen oder dienstrechtlichen Vorschriften eine solche Verschwiegenheitspflicht auferlegt ist. Die Verpflichtung zur Verschwiegenheit erstreckt sich auf alle den Gesundheitszustand betreffenden Umstände sowie auf die persönlichen, wirtschaftlichen und sonstigen Verhältnisse der Pfleglinge, die ihnen in Ausübung ihres Berufes bekannt geworden sind, bei Eingriffen gemäß § 62a auch auf die Person des Spenders und des Empfängers.“

„§ 10. (1) Durch die Landesgesetzgebung sind die Krankenanstalten zu verpflichten:

1. über die Aufnahme und die Entlassung der Pfleglinge Vormerke zu führen, sowie im Fall der Ablehnung der Aufnahme und bei der Aufnahme nach § 22 Abs. 1 letzter Satz die jeweils dafür maßgebenden Gründe zu dokumentieren;

2. Krankengeschichten anzulegen, in denen

a) die Vorgeschichte der Erkrankung (Anamnese), der Zustand des Pfleglings zur Zeit der Aufnahme (status praesens), der Krankheitsverlauf (decursus morbi), die angeordneten Maßnahmen sowie die erbrachten ärztlichen Leistungen einschließlich Medikation (insbesondere hinsichtlich Name, Dosis und Darreichungsform) und Aufklärung des Pfleglings und

b) sonstige angeordnete sowie erbrachte wesentliche Leistungen, insbesondere der pflegerischen, einer allfälligen psychologischen bzw. psychotherapeutischen Betreuung sowie Leistungen der medizinisch-technischen Dienste, darzustellen sind;

3. (...)

4. den Gerichten und Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, ferner den Sozialversicherungsträgern und Organen von Landesgesundheitsfonds im Sinne der Vereinbarung gemäß Art. 15a B-VG über die Organisation und Finanzierung des Gesundheitswesens bzw. von diesen beauftragten Sachverständigen, soweit dies zur Wahrnehmung der diesen obliegenden Aufgaben erforderlich ist, sowie einweisenden oder weiterbehandelnden Ärzten oder Krankenanstalten kostenlos Kopien von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Pfleglingen zu übermitteln;

(...)

(5) Die Landesgesetzgebung kann die Rechtsträger von Krankenanstalten ermächtigen, die Speicherung, Verarbeitung und Aufbewahrung von Krankengeschichten anderen Rechtsträgern zu übertragen, wenn für diese Rechtsträger und die in ihnen beschäftigten Personen eine gesetzliche

Verschwiegenheitspflicht besteht oder durch die Landesgesetzgebung auferlegt wird. Die Ermächtigung kann auch die Speicherung, Verarbeitung und Aufbewahrung mittels automationsunterstützter Datenverarbeitung beinhalten. Weitergaben von personenbezogenen Daten durch Rechtsträger, denen die Speicherung, Verarbeitung und Aufbewahrung übertragen wurde, sind nur an Ärzte oder Krankenanstalten zulässig, in deren Behandlung der Betroffene steht.“

3.5 Oö Krankenanstaltengesetz 1997 (Oö KAG)¹

Gemäß § 20 Abs 1 OöKAG sind „alle beim Träger einer Krankenanstalt und in einer Krankenanstalt beschäftigten Personen (...) zur Verschwiegenheit über alle Umstände, die ihnen in Ausübung ihrer Tätigkeit oder mit Beziehung auf ihre Tätigkeit über den Gesundheitszustand von Patienten und über deren persönliche, wirtschaftliche und sonstige Verhältnisse bekannt geworden sind, verpflichtet.(...) Die Verschwiegenheitspflicht ist zeitlich unbegrenzt, sie endet also insbesondere nicht mit dem Ende der Beschäftigung oder der Tätigkeit in der Krankenanstalt.“

§ 21 Oö KAG (Hervorhebungen durch den Autor)::

(5) „Die Verwahrung der Krankengeschichten und sonstigen Vormerke hat derart zu erfolgen, dass eine missbräuchliche Kenntnisnahme ihres Inhaltes verlässlich ausgeschlossen ist. Nach ihrem Abschluss sind Vormerke gemäß Abs. 1 Z. 2, 3 und 4 mindestens 30 Jahre, allenfalls in Form von Mikrofilmen oder auf einem zur Speicherung geeigneten Medium der elektronischen Datenverarbeitung (Magnetband, Diskette, Bildplatte usw.) in doppelter Ausfertigung, getrennt aufzubewahren; Hilfsmittel zur Erstellung von Befunden (wie Röntgenbilder, Präparate, EEG- und EKG-Aufzeichnungen und dgl.) sowie Vormerke gemäß Abs. 1 Z. 2 und 3 bei ambulanter Untersuchung oder Behandlung sind mindestens zehn Jahre aufzubewahren, falls nicht der jeweilige Abteilungsleiter (Leiter der Krankenanstalt) eine längere Aufbewahrung anordnet. Wird eine Krankenanstalt aufgelassen, so sind Vormerke gemäß Abs. 1 Z. 2, 3 und 4, deren Verwahrungsdauer noch nicht abgelaufen ist, der Landesregierung zu übermitteln. Nach Ablauf der Verwahrungsdauer können solche Vormerke vernichtet werden. Verwahrung und Vernichtung haben so zu erfolgen, dass eine missbräuchliche Kenntnisnahme des Inhalts verlässlich ausgeschlossen ist.

(6) Kopien von Krankengeschichten und von ärztlichen Äußerungen über den Gesundheitszustand von Patienten sind von den Krankenanstalten

1. (...)

2. den Sozialversicherungsträgern, den Kranken- und Unfallfürsorgeeinrichtungen öffentlichen Rechts, den Organen des Oö. Krankenanstaltenfonds sowie von diesen beauftragten Sachverständigen, der Patientenvertretung (§ 12) und dem Oö. Patientenentschädigungsfonds (§ 86a), soweit dies zur Wahrnehmung der ihnen obliegenden Aufgaben eine wesentliche Voraussetzung bildet, und

¹ Grundsatzgesetz: Bundesgesetz über Krankenanstalten und Kuranstalten (KAKuG).

3. den einweisenden oder behandelnden Ärzten und den Krankenanstalten, in deren Behandlung der Betroffene steht, auf Grund eines entsprechenden Ersuchens ohne Verzug kostenlos auszufolgen. Anderen Versicherungsträgern sind Kopien der Krankengeschichten ihrer Versicherten gegen Kostenersatz auszufolgen, wenn der Versicherte dem Rechtsträger gegenüber ausdrücklich schriftlich zugestimmt hat oder soweit dies zur Wahrung überwiegender berechtigter Interessen des Versicherungsträgers notwendig ist.

(7) (...)

(8) (...)

(9) (...)

- (10) Die Rechtsträger der Krankenanstalten dürfen die Speicherung, Verarbeitung und Aufbewahrung von Krankengeschichten, auch mittels automationsunterstützter Datenverarbeitung, durch Vertrag solchen Rechtsträgern übertragen, die den Kriterien des Abs. 5 entsprechen. Für die bei diesen Rechtsträgern beschäftigten Personen besteht die Verschwiegenheitspflicht gemäß § 20 sinngemäß. Diese Personen sind vom Rechtsträger, bei dem sie beschäftigt sind, auf die Einhaltung dieser Verpflichtung vor Aufnahme dieser Tätigkeit ausdrücklich hinzuweisen. Weitergaben von personenbezogenen Daten durch Rechtsträger, denen die Speicherung, Verarbeitung und Aufbewahrung übertragen wurde, sind nur an Ärzte oder Krankenanstalten, in deren Behandlung der Betroffene steht, und nur, sofern ein Auftrag jener Krankenanstalt vorliegt, die die Krankengeschichte angelegt hat, zulässig.“

„§ 48 OÖ KAG

Entlassung von Patienten

- (1) Patienten, die auf Grund des durch anstaltsärztliche Untersuchung festgestellten Behandlungserfolges der Anstaltspflege nicht mehr bedürfen, sind aus der Anstaltspflege ohne Verzug zu entlassen. Anstaltsbedürftige Patienten sind zu entlassen, wenn ihre Überstellung in eine andere Krankenanstalt notwendig und sichergestellt ist. Die von der Anstaltsleitung bestimmten Anstaltsärzte haben vor jeder Entlassung durch Untersuchung festzustellen, ob der Patient geheilt, gebessert oder ungeheilt entlassen wird.
- (2) Bei der Entlassung eines Patienten ist neben dem Entlassungsschein unverzüglich ein Arztbrief anzufertigen, der die für eine allfällige weitere medizinische Betreuung maßgebenden Angaben und Empfehlungen sowie allfällige Anordnungen für die Angehörigen der Gesundheits- und Krankenpflegeberufe im mitverantwortlichen Tätigkeitsbereich zu enthalten hat. Dieser Arztbrief ist nach Entscheidung des Patienten
1. diesem, oder
 2. dem einweisenden oder weiterbehandelnden Arzt und
 3. bei Bedarf der für die weitere Pflege und Betreuung in Aussicht genommenen Einrichtung oder dem entsprechenden Angehörigen der Gesundheits- und Krankenpflegeberufe zu übermitteln. Bei Bedarf sind dem Arztbrief auch Angaben zu Maßnahmen im eigenverantwortlichen Tätigkeitsbereich anzufügen. Konnte
-

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

bei der Entlassung des Patienten nur eine medizinische Kurzinformation angefertigt werden, so muß ein ergänzender ausführlicher Arztbrief so rasch wie möglich nachgesandt werden.“

§ 94 Oö KAG (Berechtigung zur Datenverarbeitung):

„Die Rechtsträger der Krankenanstalten sind insoweit zur Ermittlung, Verarbeitung und Übermittlung bzw. Weitergabe von personenbezogenen Daten im Sinn des Datenschutzgesetzes 2000 ermächtigt, als dies in Art und Umfang auf den berechtigten Zweck der Krankenanstalten beschränkt oder zur Erfüllung der den Krankenanstalten gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung ist.“

Das oö KAG kennt also zwei einschlägige Datenübermittlungen: Die Übermittlung einer Kopie der Krankengeschichte an andere Krankenanstalten und den einweisenden Arzt (offenbar ohne Zustimmung des Patienten) gemäß § 21 OÖ KAG und die Übermittlung des Arztbriefes gemäß § 48 OÖ KAG nach Wahl des Patienten (also mit dessen Zustimmung) an diesen selbst, den behandelnden Arzt oder andere Einrichtungen.

3.6 NÖ Krankenanstaltengesetz (NÖ KAG)

Auch das NÖ KAG kennt die Übermittlung einer Kopie der Krankengeschichte uU ohne Zustimmung des Patienten:

§ 21 Abs 3 NÖ KAG

„Die Krankenanstalten sind verpflichtet, den Gerichten und Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, ferner den Sozialversicherungsträgern und von Sozialversicherungsträgern beauftragten Sachverständigen sowie den Geschäftsführern des NÖ Gesundheits- und Sozialfonds und von diesen beauftragten Sachverständigen oder Bediensteten des NÖ Gesundheits- und Sozialfonds, soweit dies zur Wahrnehmung der diesen obliegenden Aufgaben erforderlich ist, sowie einweisenden oder weiterbehandelnden Ärzten oder Krankenanstalten über Anforderung kostenlos Kopien von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln. Ferner sind sonstigen Gesundheits- und Sozialeinrichtungen (Sozialdienste, Sozialstationen) über deren Anforderung Abschriften jener Teile der Krankengeschichte kostenlos zu übermitteln, deren Kenntnisse für die weitere medizinische Betreuung der Patienten unbedingt erforderlich ist. Ferner sind den privaten Versicherungsträgern über deren Anforderung Abschriften von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand des Patienten gegen Ersatz der damit verbundenen Aufwendungen zu übermitteln, soweit dies für die Erfüllung ihrer vertraglichen Pflicht

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

notwendig ist und dies mit dem Versicherten bei Abschluß des Versicherungsvertrages ausdrücklich schriftlich mit einer Widerrufsmöglichkeit vereinbart wurde. Außerdem ist dem Patienten, seiner Vertrauensperson oder der NÖ Patienten- und Pflegeanwaltschaft (§ 91), über Wunsch des Patienten, Einsicht in die Krankengeschichte zu gewähren oder ihnen kostenlos eine Abschrift derselben zu übermitteln, wobei die Ausfolgung vom ärztlichen Leiter der Krankenanstalt an die Erläuterung durch den behandelnden Arzt geknüpft werden kann, wenn dies zur Wahrung des Patientenwohls geboten ist.“

Auch die Übermittlung des Arztbriefes mit Zustimmung des Patienten ist im NÖ KAG normiert:

§ 21 Abs 4 NÖ KAG

„Bei der Entlassung eines Patienten ist neben dem Entlassungsschein unverzüglich ein Arztbrief anzufertigen, der die für eine allfällige weitere medizinische Betreuung maßgebenden Angaben und Empfehlungen, die Entlassungsdiagnose sowie allfällige Anordnungen für die Angehörigen des gehobenen Dienstes für Gesundheits- und Krankenpflege im mitverantwortlichen Tätigkeitsbereich zu enthalten hat. In die Therapievorschläge sind vorzugsweise Arzneimittel nach dem jeweils gültigen Heilmittelverzeichnis des Hauptverbandes der österreichischen Sozialversicherungsträger, die keiner chefärztlichen bzw. kontrollärztlichen Bewilligung bedürfen, aufzunehmen. Dieser Arztbrief ist nach Entscheidung des Patienten

1. diesem, oder

2. dem einweisenden oder weiterbehandelnden Arzt und

3. bei Bedarf der für die weitere Pflege und Betreuung in Aussicht genommenen Einrichtung oder den entsprechenden Angehörigen des gehobenen Dienstes für Gesundheits- und Krankenpflege zu übermitteln.

Bei Bedarf sind dem Arztbrief auch Angaben zu Maßnahmen im eigenverantwortlichen Tätigkeitsbereich anzufügen.“

3.7 Wiener Krankenanstaltengesetz 1987 (Wr. KAG)

Ähnliche Bestimmungen sind auch im Wiener KAG zu finden:

§ 17 Abs 4 Wr. KAG

„Abschriften von Krankengeschichten und von ärztlichen Äußerungen über den Gesundheitszustand von Patienten sind von den Krankenanstalten den Gerichten sowie den Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, kostenlos zu übermitteln. Das Vorliegen des öffentlichen Interesses ist bei Anforderung einer Krankengeschichte anzuführen.“

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

Ferner sind den Sozialversicherungsträgern und den Organen des Wiener Krankenanstaltenfinanzierungsfonds bzw. den von diesem beauftragten Sachverständigen, soweit dies zur Wahrnehmung ihrer Aufgaben erforderlich ist, sowie den einweisenden oder behandelnden Ärzten über Anforderung kostenlos Abschriften von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Anstaltspatienten zu übermitteln. Soweit dies für die Erfüllung ihrer vertraglichen Pflichten und zur Antragsprüfung notwendig ist, sind sonstigen Versicherungsunternehmen Abschriften von Krankengeschichten ihrer Versicherten gegen Kostenersatz zu übermitteln, wenn und soweit dies mit dem Rechtsträger der Krankenanstalt vereinbart ist und der Versicherte im Versicherungsvertrag oder gesondert zugestimmt hat; Krankengeschichten oder Teile von Krankengeschichten, die Daten über Gentherapien enthalten und außerhalb der Krankengeschichte zu führende Daten über Genanalysen dürfen jedoch nicht übermittelt werden.“

Im Wr KAG gibt es einen Patientenbrief bei Entlassung des Patienten, der inhaltlich dem Arztbrief entspricht und dessen Übermittlung ebenfalls an die Zustimmung des Patienten gebunden ist:

§ 38 Abs 2 Wr. KAG

„Bei der Entlassung eines Patienten ist neben dem Entlassungsschein unverzüglich ein Patientenbrief anzufertigen, der die für eine allfällige weitere medizinische Betreuung maßgebenden Angaben und Empfehlungen sowie allfällige Anordnungen für die Angehörigen der Gesundheits- und Krankenpflegeberufe im mitverantwortlichen Tätigkeitsbereich zu enthalten hat. Dieser Patientenbrief ist nach Entscheidung des Patienten diesem oder dem einweisenden oder weiterbehandelnden Arzt und bei Bedarf der für die weitere Pflege und Betreuung in Aussicht genommenen Einrichtung oder dem entsprechenden Angehörigen der Gesundheits- und Krankenpflegeberufe zu übermitteln. Bei Bedarf sind dem Patientenbrief auch Angaben zu Maßnahmen im eigenverantwortlichen Tätigkeitsbereich anzufügen.“

3.8 Steiermärkisches Krankenanstaltengesetz 1999 (KALG)

Im KALG ist die Übermittlung von Krankengeschichten an die Zustimmung des Patienten gebunden:

§ 72 KALG

„Übermittlung von Krankengeschichten und Arztbriefen

Den Gerichten und Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im

öffentlichen Interesse von Bedeutung ist, ferner den Sozialversicherungsträgern und SKAFF-Organen bzw. von diesen beauftragten Sachverständigen sind, soweit dies zur Wahrnehmung der diesen obliegenden Aufgaben erforderlich ist, sowie vorbehaltlich der Zustimmung des Patienten einweisenden oder weiterbehandelnden Ärzten oder Krankenanstalten kostenlos Kopien von Krankengeschichten (§ 13 Abs.1 Z. 2 und 4) und ärztlichen Äußerungen (Arztbrief gemäß § 31 Abs. 2) über den Gesundheitszustand von Patienten zu übermitteln.“

Auch das KALG kennt den Arztbrief und macht die Übermittlung desselben von der Zustimmung des Patienten abhängig:

§ 31 Abs 2 KALG

„Bei der Entlassung eines Patienten ist neben dem Entlassungsschein unverzüglich ein Arztbrief anzufertigen, der die für eine allfällige weitere medizinische Betreuung maßgebenden Angaben und Empfehlungen sowie allfällige Anordnungen für die Angehörigen der Gesundheits- und Krankenpflegeberufe im mitverantwortlichen Tätigkeitsbereich zu enthalten hat. Dieser Arztbrief ist nach Entscheidung des Patienten diesem oder dem einweisenden oder weiterbehandelnden Arzt und bei Bedarf der für die weitere Pflege und Betreuung in Aussicht genommenen Einrichtung oder dem entsprechenden Angehörigen der Gesundheits- und Krankenpflegeberufe zu übermitteln. Bei Bedarf sind dem Arztbrief auch Angaben zu Maßnahmen im eigenverantwortlichen Tätigkeitsbereich anzufügen. Konnte bei der Entlassung des Patienten für den behandelnden Arzt nur eine medizinische Kurzinformation ausgefertigt werden, so muss ein ergänzender ausführlicher Arztbrief so rasch wie möglich nachgesandt werden. Sowohl die Unterfertigung des Arztbriefes als auch der medizinischen Kurzinformation hat unter sinngemäßer Anwendung der Bestimmungen im § 13 Abs. 2 zu erfolgen.“

3.9 Kärntner Krankenanstaltenordnung

Die Kärntner Krankenanstaltenordnung normiert bei der Übermittlung von Gesundheitsdaten ein Weitergabeverbot:

§ 34 Abs 6 Kärntner Krankenanstaltenordnung

„Abschriften (Kopien) von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten sind auf Verlangen den Gerichten und den Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, ferner mit der Aufnahmezahl den von den Sozialversicherungsträgern oder dem Kärntner Krankenanstaltenfonds beauftragten Ärzten oder derselben Verschwiegenheit unterstellten Personen, soweit dies zur Wahrnehmung der diesen obliegenden Aufgaben erforderlich ist, sowie den

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

einweisenden oder weiterbehandelnden Ärzten oder Krankenanstalten unverzüglich und kostenlos sowie mit dem Auftrag des Weitergabeverbotes zur Verfügung zu stellen. Mit Zustimmung des Patienten sind Abschriften (Kopien) von Krankengeschichten auch dem Patientenanwalt kostenlos zur Verfügung zu stellen.“

Die Übermittlung des Arztbriefes ist wiederum an die Zustimmung des Patienten gebunden:

§ 54 Abs 5 Kärntner Krankenanstaltenordnung

„Bei der Entlassung eines Patienten ist neben dem Entlassungsschein unverzüglich ein Arztbrief auszufertigen, der die für eine allfällige weitere medizinische Betreuung maßgeblichen Angaben und Empfehlungen sowie allfällige Anordnungen für die Angehörigen der Gesundheits- und Krankenpflegeberufe im mitverantwortlichen Tätigkeitsbereich zu enthalten hat. Dieser Arztbrief ist nach Entscheidung des Patienten

a) diesem, oder

b) dem einweisenden oder weiterbehandelnden Arzt und

c) bei Bedarf der für die weitere Pflege und Betreuung in Aussicht genommenen Einrichtungen oder dem entsprechenden Angehörigen der Gesundheits- und Krankenpflegeberufe zu übermitteln. Bei Bedarf sind dem Arztbrief auch Angaben zu Maßnahmen im eigenverantwortlichen Tätigkeitsbereich anzufügen.“

3.10 Salzburger Krankenanstaltengesetz 2000 (SKAG)

Auch das SKAG regelt die Übermittlung von Krankengeschichten:

§ 35 Abs 9 SKAG

„Folgenden Personen oder Institutionen sind auf Ersuchen unentgeltlich Kopien von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Patienten zu übermitteln:

1. den Gerichten und den Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist;

2. den Sozialversicherungsträgern und den ärztlichen Kontrollorganen des Salzburger Krankenanstalten- Finanzierungsfonds (SAKRAF) sowie den von diesen beauftragten Sachverständigen, soweit dies zur Wahrnehmung der diesen obliegenden Aufgaben erforderlich ist;

3. den einweisenden oder weiterbehandelnden Ärzten oder Krankenanstalten.

An den SAKRAF bzw die von diesem beauftragten Sachverständigen sind Krankengeschichten grundsätzlich nur unter der Aufnahmeummer (ohne Angabe des Namens des Patienten) zu übermitteln. Der Versicherungsträger bzw der

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

SAKRAF hat sicherzustellen, dass gemäß Z 2 übermittelte personenbezogene Gesundheitsdaten ausschließlich von Personen eingesehen werden, die Ärzte sind.“

Zum Arztbrief enthält das SKAG folgendes:

§ 56 Abs 2 SKAG

„Bei der Entlassung eines Patienten ist neben dem Entlassungsschein unverzüglich ein Arztbrief anzufertigen, der die für eine allfällige weitere medizinische Betreuung maßgebenden Angaben und Empfehlungen zu enthalten hat. Dieser Arztbrief ist nach Entscheidung des Patienten diesem, dem einweisenden oder dem weiterbehandelnden Arzt zu übermitteln. Bei Patienten, die nach der Entlassung weiterer Pflege bedürfen, soll weiters ein Pflegebrief mit den erforderlichen Angaben über die erforderlichen bzw empfohlenen pflegerischen Maßnahmen ausgefertigt werden, der nach der Entscheidung des Patienten für ihn selbst oder die die Pflege durchführende Person oder Einrichtung bestimmt ist.“

3.11 Tiroler Krankenanstaltengesetz (Tir KAG)

Das Tir KAG beinhaltet ebenfalls Bestimmungen zur Übermittlung von Krankengeschichten ohne Zustimmung des Patienten:

§ 15 Abs Tir KAG

„(1) Die Träger der Krankenanstalten haben

(...)

e) den Gerichten und Verwaltungsbehörden in Angelegenheiten, in denen die Feststellung des Gesundheitszustandes für eine Entscheidung oder Verfügung im öffentlichen Interesse von Bedeutung ist, weiters den Versicherungsträgern im Sinne des § 52 und den Organen des Tiroler Krankenanstaltenfinanzierungsfonds oder den von ihnen beauftragten Sachverständigen, soweit dies zur Wahrnehmung der ihnen obliegenden Aufgaben erforderlich ist, sowie den einweisenden oder weiterbehandelnden Ärzten oder Krankenanstalten auf Verlangen kostenlos Abschriften oder Ablichtungen von Krankengeschichten und ärztlichen Äußerungen über den Gesundheitszustand von Pflinglingen zu übermitteln. Den privatrechtlichen Versicherungsträgern sind auf Verlangen Abschriften oder Ablichtungen von Krankengeschichten ihrer Versicherten gegen Kostenersatz auszufolgen, wenn der Versicherte dem schriftlich zugestimmt hat;“

Der Arztbrief ist auch im Tir KAG nur mit Zustimmung des Patienten zu übermitteln:

§ 35 Abs 6 Tir KAG

„Bei der Entlassung eines Pflinglings ist neben dem Entlassungsschein unverzüglich ein Arztbrief anzufertigen, der die für eine allfällige weitere medizinische Betreuung

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

maßgebenden Angaben und Empfehlungen sowie allfällige Anordnungen für die Angehörigen der Gesundheits- und Krankenpflegeberufe im mitverantwortlichen Tätigkeitsbereich zu enthalten hat. Dieser Arztbrief ist nach Entscheidung des Pfléglings diesem oder dem einweisenden oder weiterbehandelnden Arzt und bei Bedarf der für die weitere Pflege und Betreuung in Aussicht genommenen Einrichtung oder dem entsprechenden Angehörigen der Gesundheits- und Krankenpflegeberufe zu übermitteln. Bei Bedarf sind dem Arztbrief auch Angaben zu den von Angehörigen der Gesundheits- und Krankenpflegeberufe im eigenverantwortlichen Tätigkeitsbereich zu treffenden Maßnahmen anzufügen.“

3.12 Zusammenfassung

Sämtliche Landeskrankenanstaltengesetze verpflichten also die Krankenanstalten zur Führung einer Krankengeschichte und Aufbewahrung von ärztlichen Äußerungen.

Die Übermittlung der Krankengeschichten und ärztlichen Äußerungen an einweisende oder weiterbehandelnde Ärzte und weiterbetreuende Einrichtungen wird ausdrücklich vorgeschrieben und ist nicht an die Zustimmung des Patienten gebunden. Einzige Ausnahme stellt das Steiermärkische Krankenanstaltengesetz 1999 dar, in dem eine Zustimmung des Patienten vorgesehen ist.

Eine weitere Besonderheit beinhaltet die Kärntner Krankenanstaltenordnung, indem sie für die Empfänger ein Weitergabeverbot normiert.

Der Arztbrief/Patientenbrief darf jeweils nur nach Zustimmung des Patienten an einweisende oder weiterbehandelnde Ärzte und weiterbetreuende Einrichtungen übermittelt werden. Dies gilt ausnahmslos für alle geprüften Landeskrankenanstaltengesetze.

4 Gutachten

4.1 Einhaltung des DSG

4.1.1 Zulässigkeit der Nutzung des Systems gemäß DSG

Die Verarbeitung und Übermittlung von Daten muss laut § 7 DSG von rechtlichen Befugnissen gedeckt sein. Diese Befugnisse liegen in Form des Ärztegesetzes und der Landeskrankenanstaltengesetze jedenfalls vor.

Die Speicherung und Übermittlung von Befunddaten im System Praxisnetzwerk ist aufgrund § 9 Z 12 DSG dann zulässig, wenn sichergestellt ist, dass die Daten nur Personen zu Gesicht kommen, die entweder „ärztliches Personal“ darstellen oder sonstigen Geheimhaltungspflichten unterliegen. Zusätzlich können gesetzliche Vorschriften dazu ermächtigen und natürlich auch der Betroffene selbst.

Wird die Möglichkeit der „Freigabe“ eines Befundes für eine größere Benutzergruppe eingerichtet, so liegt ein Informationsverbundsystem vor, da jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden.

4.1.2 Registrierungspflicht, Vorabkontrolle gemäß DSG

Das System Praxisnetzwerk verarbeitet sensible Daten und stellt uU ein Informationsverbundsystem dar.

Sowohl Datenanwendungen, die sensible Daten enthalten, als auch Informationsverbundsysteme unterliegen der Vorabkontrolle (§ 18 Abs 2 DSG). Dies gilt allerdings nur, sofern überhaupt eine Meldepflicht besteht, also insbesondere nicht für Standardanwendungen nach § 17 Abs 2 Z 6.

Man muss nun 2 Möglichkeiten unterscheiden:

a) nur Ärzte und Labors nehmen an Praxisnetzwerk teil

Es handelt sich um eine Standardanwendung nach § 17 Abs 2 Z 6, die meldefrei ist da sie durch die Standardanwendung SA024 „Patientenverwaltung und Honorarabrechnung“ inklusive der nötigen Übermittlungen der Befunddaten definiert ist. Auch wenn die Möglichkeit genutzt wird, Befunde freizugeben ist keine Vorabkontrolle nötig, obwohl ein

Informationsverbundsystem vorliegt. Dies deshalb, weil § 18 Abs 2 nur von meldepflichtigen Datenanwendungen spricht.

b) auch Krankenanstalten nehmen an Praxisnetzwerk teil

In diesem Fall ist eine Individualmeldung der Krankenanstalten an die Datenschutzkommission nötig, da keine Standardanwendung vorliegt. Diese Anmeldung sollte allerdings ohnehin schon passiert sein, da sie Voraussetzung auch für die bisherige Befundspeicherung und -übermittlung bildet.

Wenn die Möglichkeit der Befundfreigabe genutzt wird, handelt es sich um ein Informationsverbundsystem, das laut § 18 Abs 2 Z 4 einer Vorabkontrolle unterliegt und erst nach Prüfung durch die Datenschutzkommission den Betrieb aufnehmen darf.

Die Vorabkontrolle entfällt jedoch, wenn die Datenanwendung vor dem 1.1.2000 bereits im Datenverarbeitungsregister registriert war.

4.1.3 Datensicherheitsmaßnahmen

Zu den Datensicherheitsmaßnahmen nach § 14 DSGVO liegen bisher Informationen vor, die uns Hr Eduard Schebesta, Geschäftsführer der HCS Health Communication Service GmbH per E-Mail mitgeteilt hat:

- Nur Mitarbeiter der Technik und der Entwicklung haben Zugang zu den Anwendungen (§ 14 Abs 2 Z 1 DSGVO).
- Für jeden Mitarbeiter gelten Datenschutzrichtlinien, die dieser durch Unterschrift zur Kenntnis nimmt (§ 14 Abs 2 Z 2 und 3 DSGVO).
- Der Zutritt zum Büro ist mittels Alarmanlage gesichert, jeder Mitarbeiter verfügt über einen eigenen Zutrittscode. Der Zugang zum Rechenzentrum ist mittels eines elektronischen Zutrittssystems geregelt, welches mit einer Chipkarte arbeitet (§ 14 Abs 2 Z 4 DSGVO).
- Programmzugriffe und Datenzugriffe sind durch ein Firewallsystem auf Mitarbeiterebene geregelt (§ 14 Abs 2 Z 5 DSGVO).
- Die Berechtigung zum Betrieb der Datenverarbeitungsgeräte wird durch das erwähnte Zugangskontrollsystem zu Büro und Rechenzentrum erreicht (§ 14 Abs 2 Z 6 DSGVO).

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

- Die eingesetzten Programme, Firewalls und Router führen jeweils Protokolldateien, damit tatsächlich durchgeführte Verwendungsvorgänge nachvollzogen werden können (§ 14 Abs 2 Z 7 DSGVO).
- Ein Entwurf der Dokumentation all dieser Maßnahmen ist bereits fertig, die endgültige Version wird gerade erstellt (§ 14 Abs 2 Z 8 DSGVO).

Damit scheinen die Anforderungen aus § 14 DSGVO erfüllt, wenn die schriftliche Dokumentation nachgereicht wird.

4.2 Einhaltung der Vorgaben des GTelG

4.2.1 Nachweis von Identität und Rolle

Die Gesundheitsdaten liegen auf einem System von Praxisnetzwerk, den Benutzern wird ein Zugang über eine Webmaske angeboten. Der Zugriff auf die medizinischen Daten erfolgt also durch direkte Bedienung aus der Ferne. In diesem Fall kann die Identifikation der Benutzer des Systems aus technischen oder wirtschaftlichen Gründen im Zuge der Implementierung der Zugangsberechtigung erfolgen. Allerdings ist die Identität mindestens einmal im Monat vom Gesundheitsdiensteanbieter zu prüfen (§ 4 Abs 4f GTelG).

Nach Aussage von Eduard Schebesta, Geschäftsführer der HCS Health Communication Service GmbH erfolgt die Identifikation bei Praxisnetzwerk wie folgt:

Bei der erstmaligen Vergabe von Zertifikaten wird eine Kopie des Arztausweises oder des Führerscheines eingefordert und intern abgelegt. Die Daten des Anwenders werden dann mit der Standesmeldung der Ärztekammer über den Evga - Server verglichen um sicherzustellen, dass der Anwender als aktiver Arzt geführt wird.

Bei der Vergabe von Zugangsinformationen und Zugangsschlüsseln erfolgt ebenfalls eine Prüfung der Arztdaten gegen die Standesmeldung der Ärztekammer. Die Versendung der Zugangsinformation erfolgt per Einschreiben an die angegebene Adresse des Benutzers.

Diese Art der Identifikation genügt den Anforderungen des § 4 Abs 4 GTelG. Gemäß Abs 5 muss diese Identifikation jedoch monatlich wiederholt werden.

Eine Eintragung der Teilnehmer in den eHealth - Verzeichnisdienst die Identifikation wesentlich erleichtern. Diese Möglichkeit sollte also in Betracht gezogen werden, sobald dieser Verzeichnisdienst in Betrieb ist.

Für die Festlegung von Rollen gemäß § 5 GTelG wurde bisher noch keine Verordnung des BMGF erlassen, sodass der Nachweis der Rolle außerhalb der Kategorisierung Arzt oder nicht Arzt momentan nicht möglich ist.

4.2.2 Benutzeridentifikation bei Nutzung des Systems

Die Identifikation bei Anmeldung am System ist durch Eingabe von Username, PIN-Code, sowie eines nur ca 1 min gültigen Kennworts, generiert mit einem Cryptomodul von RSA Inc gesichert.

4.2.3 Vertraulichkeit - Verschlüsselung

Die versendeten Daten müssen laut § 6 GTelG ausreichend verschlüsselt werden, sodass sie mit wirtschaftlich vertretbarem Aufwand nicht entschlüsselt werden können. Die Verschlüsselung muss auf den Anlagen des Absenders erfolgen, die Entschlüsselung auf den Anlagen des Empfängers der Gesundheitsdaten.

Die Verschlüsselung erfolgt im Praxisnetzwerk durch ein starkes kryptographisches Verfahren (3DES). Die Verschlüsselung zwischen Benutzer und Praxisnetzwerk bei Benutzung der Webmail-Oberfläche erfolgt mittels SSL. Es wird also die Verschlüsselung mit SSL auf dem Computer des Benutzers vorgenommen. Im Praxisnetzwerk erfolgt sodann eine Umschlüsselung auf 3DES, wie es in den Erläuterungen zum Gesundheitstelematikgesetz ausdrücklich vorgesehen ist.

Es ist daher ausgeschlossen, dass Gesundheitsdaten im Klartext über das Internet an den Dienstleister übermittelt werden. Den Anforderungen des § 6 GTelG ist damit Genüge getan.

4.2.4 Sicherstellung der Integrität (Unverfälschbarkeit) der Befunddaten

Die Integrität bei der Übertragung von Gesundheitsdaten ist durch elektronische Signaturen nachzuweisen und zu prüfen (§ 7 GTelG).

Die Integrität der Gesundheitsdaten wird im Praxisnetzwerk durch elektronische Signaturen realisiert (RSA 1024 Bit). Im Fall einer fehlgeschlagenen Signaturprüfung werden die empfangenen Gesundheitsdaten nicht verwendet. Dies entspricht § 7 Abs 4 GTelG.

4.2.5 Dokumentation

Eine Dokumentation der getroffenen Datensicherheitsmaßnahmen einschließlich wirksamer Mechanismen zur Kontrolle und Sicherstellung ihrer Einhaltung wird zur Zeit ausgearbeitet. Unter der Voraussetzung, dass diese Ausarbeitung fertig gestellt

Dipl.-Ing. Dr. iur. Dr. techn. Walter J. Jaburek

Allgemein beeideter und gerichtlich zertifizierter Sachverständiger für Informationstechnik und Telekommunikation

IT-Projektcontrolling, EDV-Vertragsberatung, Streitschlichtung

Universitätslektor im Fach EDV- und Fernmelderecht

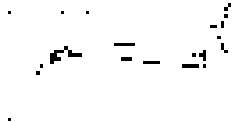
Steigenteschg. 13/3/2, A-1220 Wien

Telefon: 203 53 81-0, Fax: 203 53 81-5

E-Mail: walter.jaburek@edv-concept.at

wird, entspricht das System dem GTelG. Es darf allerdings gemäß § 19 Abs 2 GTelG bis Ende 2007 auch ohne diese Dokumentation betrieben werden.

Wien, am 18.05.2005



Dipl.-Ing. DDr. Walter J. Jaburek