BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2008 Ausgegeben am 9. Dezember 2008 Teil II

451. Verordnung: Gesundheitstelematikverordnung (GTelV)

451. Verordnung der Bundesministerin für Gesundheit, Familie und Jugend, mit der die für den elektronischen Gesundheitsdatenaustausch in Betracht kommenden Rollen sowie die qualitativen Mindestanforderungen für Verschlüsselung und elektronische Signaturen festgelegt werden – Gesundheitstelematikverordnung (GTelV)

Auf Grund der §§ 5 Abs. 1, 7 Abs. 5 und 9 Abs. 6 des Gesundheitstelematikgesetzes (GTelG), BGBl. I Nr. 179/2004, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 23/2008, wird verordnet:

1. Abschnitt
Datensicherheit

Identität

§ 1. (1) Nachweis und Prüfung der Identität von Gesundheitsdiensteanbietern haben

1. durch Verwendung elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen sowie bereichsspezifischer Personenkennzeichen (§ 9 E-Government-Gesetz, BGBl. I Nr. 10/2004 in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008) oder
2. durch Einsichtnahme in den eHealth-Verzeichnisdienst (§§ 9 ff GTelG)

zu erfolgen.

(2) Nachweis und Prüfung der Identität von Gesundheitsdiensteanbietern dürfen abweichend von Abs. 1 auch auf andere Art und Weise erfolgen, wenn

1. der elektronische Gesundheitsdatenaustausch gemäß § 3 Abs. 1 stattfindet,
2. die Verbindung der Gesundheitsdaten, die im Rahmen des elektronischen Gesundheitsdatenaustausches übermittelt werden und der Identitätsdaten nicht oder nicht spurlos verändert werden kann und
3. eine Verwechslung von Gesundheitsdiensteanbietern ausgeschlossen werden kann.

Rollen

§ 2. (1) Im Rahmen des elektronischen Gesundheitsdatenaustausches haben Gesundheitsdienste-anbieter ausschließlich die Rollen gemäß **Anlage 1** zu verwenden.

(2) Bei der Aufnahme eines Gesundheitsdiensteanbieters in den eHealth-Verzeichnisdienst hat die Zuordnung einer Rolle zu einem Gesundheitsdiensteanbieter für

1. die in den Z 1 bis 3 der Anlage 1 genannten Rollen durch die Österreichische Ärztekammer,
2. die in den Z 4 und 5 der Anlage 1 genannten Rollen durch die Österreichische Zahnärztekammer,
3. die in der Z 10 der Anlage 1 genannte Rolle durch das Österreichische Hebammengremium,
4. die in der Z 26 der Anlage 1 genannte Rolle durch die Österreichische Apothekerkammer,
5. die in der Z 38 der Anlage 1 genannte Rolle durch den Hauptverband der österreichischen Sozialversicherungsträger sowie
6. in allen anderen Fällen durch den Bundesminister für Gesundheit, Familie und Jugend

zu erfolgen.

(3) Die in Abs. 2 Z 1 bis 5 genannten Stellen haben dem Bundesminister für Gesundheit, Familie und Jugend alle verfügbaren Daten gemäß § 10 Abs. 1 GTelG

1. sowie das Geburtsdatum der Gesundheitsdiensteanbieter,
2. nicht jedoch

a. die eindeutige elektronische Identifikation gemäß § 10 Abs. 1 Z 1 GTelG und

b. die Angaben des § 10 Abs. 1 Z 3 und 7 GTelG

über eine elektronische Schnittstelle laufend aktualisiert zur Verfügung zu stellen.

(4) Der Bundesminister für Gesundheit, Familie und Jugend hat auf Grund der gemäß Abs. 3 zur Verfügung gestellten Daten die bereichsspezifischen Personenkennzeichen (bPK) für den eHealth-Verzeichnisdienst von der Stammzahlenregisterbehörde errechnen zu lassen. Soweit die gemäß Abs. 3 zur Verfügung gestellten Daten nicht zur Errechnung der bPK ausreichen, sind dem Bundesminister für Gesundheit, Familie und Jugend zusätzlich

1. der Geburtsort,
2. das Geschlecht und
3. die Staatsangehörigkeit

des betreffenenden Gesundheitsdiensteanbieters zur Verfügung zu stellen.

(5) Nachweis und Prüfung der Rollen von Gesundheitsdiensteanbietern haben durch Abfrage des eHealth-Verzeichnisdienstes (§§ 9 ff GTelG) zu erfolgen.

Vertraulichkeit

§ 3. (1) Die Vertraulichkeit beim elektronischen Gesundheitsdatenaustausch ist dadurch sicherzustellen, dass

1. der elektronische Gesundheitsdatenaustausch über Netzwerke durchgeführt wird, die entsprechend dem Stand der Netzwerksicherheit hinreichend gegenüber unbefugten Zugriffen abgesichert sind, indem sie zumindest
   a. die kryptographische Absicherung des Datenverkehrs,
   b. den Netzzugang ausschließlich für eine geschlossene oder abgrenzbare Benutzergruppe sowie
   c. die Authentifizierung der Benutzer

   vorsehen, oder
2. Protokolle und Verfahren verwendet werden, die
   a. die vollständige Verschlüsselung der Gesundheitsdaten ermöglichen und
   b. deren kryptographische Algorithmen in der **Anlage 2** angeführt sind.

(2) Beim elektronischen Gesundheitsdatenaustausch gemäß Abs. 1 Z 2 dürfen die allenfalls von der Verschlüsselung ausgenommenen Informationen weder Hinweise auf die Betroffenen (§ 4 Z 3 Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 in der Fassung des Bundesgesetzes BGBl. I Nr. 2/2008), deren Gesundheitsdaten verwendet werden, noch auf allfällige Authentifizierungsdaten enthalten.

Integrität

§ 4. (1) Nachweis und Prüfung der Integrität von Gesundheitsdaten, die im Rahmen des elektronischen Gesundheitsdatenaustausches übermittelt werden, haben durch die Verwendung elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen, zu erfolgen.

(2) Nachweis und Prüfung der Integrität von Gesundheitsdaten, die im Rahmen des elektronischen Gesundheitsdatenaustausches übermittelt werden, dürfen abweichend von Abs. 1 auch auf andere Art und Weise erfolgen, wenn

1. der elektronische Gesundheitsdatenaustausch gemäß § 3 Abs. 1 stattfindet und
2. die Gesundheitsdaten nicht oder nicht spurlos verändert werden können.

Dokumentationspflichten

§ 5. (1) Gesundheitsdiensteanbieter haben

1. alle Maßnahmen, mit denen die Anforderungen der §§ 1 Abs. 2, 3 Abs. 1 Z 2 oder 4 Abs. 2 erfüllt werden,
2. die Kontaktaufnahme und Änderung der Kontaktdaten gemäß § 6 Abs. 2 und 3 sowie
3. die Prüfung der Rufnummern gemäß § 7 Z 2

zu dokumentieren.

(2) Die Dokumentation gemäß Abs. 1 Z 1 und 3 ist auf Verlangen dem Bundesminister für Gesundheit, Familie und Jugend zu übermitteln.

2. Abschnitt
Übergangs- und Schlussbestimmungen

Erleichterte Voraussetzungen des Identitäts-, Rollen- und Integritätsnachweises

§ 6. (1) Sind Nachweis oder Prüfung von Identität, Rollen oder Integrität nach den Bestimmungen des 1. Abschnitts nicht möglich, darf ein elektronischer Gesundheitsdatenaustausch nur erfolgen, wenn zumindest die Identitäten und maßgeblichen Rollen der am elektronischen Gesundheitsdatenaustausch beteiligten Gesundheitsdiensteanbieter gegenseitig durch

1. persönlichen Kontakt oder
2. telephonischen Kontakt oder
3. Vertragsbestimmungen zur elektronischen Erreichbarkeit oder
4. Abfrage elektronischer Verzeichnisse der Stellen gemäß § 2 Abs. 2 Z 1 bis 5

bestätigt sind.

(2) In den Fällen des Abs. 1 Z 1 und 2 sind vor dem erstmaligen elektronischen Gesundheitsdatenaustausch zwischen den beteiligten Gesundheitsdiensteanbietern

1. Datum und Art der Kontaktaufnahme,
2. die vollständigen Namen und maßgeblichen Rollen der am elektronischen Gesundheitsdatenaustausch beteiligten Gesundheitsdiensteanbieter,
3. die Angaben zur elektronischen Erreichbarkeit der Gesundheitsdiensteanbieter sowie
4. die an der Kontaktaufnahme beteiligten natürlichen Personen

zu dokumentieren.

(3) Änderungen der Daten gemäß Abs. 2 Z 2 und 3 sind zu dokumentieren.

Erleichterte Voraussetzungen der Vertraulichkeit

§ 7. Abweichend von § 3 darf der elektronische Gesundheitsdatenaustausch auch per Fax erfolgen, wenn

1. die Faxgeräte vor unbefugtem Zugang und Gebrauch geschützt sind,
2. die Rufnummern, insbesondere die verspeicherten Rufnummern, mindestens alle zwei Monate nachweislich auf ihre Aktualität geprüft werden,
3. automatische Weiterleitungen, außer an den Gesundheitsdiensteanbieter selbst, deaktiviert sind,
4. alle vom Gerät unterstützten Sicherheitsmaßnahmen genützt werden und
5. allenfalls verfügbare Fernwartungsfunktionen nur für die vereinbarte Dauer der Fernwartung aktiviert sind.

Schlussbestimmungen

§ 8. (1) Personenbezogene Bezeichnungen beziehen sich auf Frauen und Männer in gleicher Weise.

(2) Diese Verordnung tritt mit Ausnahme des § 2 Abs. 3 mit 1. Jänner 2009 in Kraft.

(3) Der Bundesminister für Gesundheit, Familie und Jugend hat die technische Spezifikation der Schnittstelle gemäß § 2 Abs. 3 unter der Adresse http://www.ehvd.at im Internet zu veröffentlichen. § 2 Abs. 3 tritt sechs Monate nach Veröffentlichung dieser Schnittstellenspezifikation in Kraft.

(4) Bis zum Ablauf des 31. Dezember 2010 darf der elektronische Gesundheitsdatenaustausch unter den erleichterten Bedingungen der §§ 6 und 7 erfolgen, wobei die Abfrage elektronischer Verzeichnisse gemäß § 6 Abs. 1 Z 4 nur bis zum In-Kraft-Treten des § 2 Abs. 3 zulässig ist. Bis zum Ablauf des 31. Dezember 2010 dürfen Gesundheitsdiensteanbieter,

1. die Gesundheitsdaten in Übereinstimmung mit dieser Verordnung verwenden oder
2. deren Rollen nicht in der Anlage 1 angeführt sind,

nicht gemäß § 17 Abs. 1 GTelG bestraft werden.

Kdolsky

Anlage 1: Rollen

1. Approbierte Ärztin/Approbierter Arzt
2. Ärztin/Arzt für Allgemeinmedizin
3. Fachärztin/Facharzt, unter Beifügung des Wortes „für“ und des folgenden, jeweils zutreffenden Sonderfachs
   – Anästhesiologie und Intensivmedizin
   – Anatomie
   – Arbeitsmedizin
   – Augenheilkunde und Optometrie
   – Blutgruppenserologie und Transfusionsmedizin
   – Chirurgie
   – Frauenheilkunde und Geburtshilfe
   – Gerichtsmedizin
   – Hals-, Nasen- und Ohrenkrankheiten
   – Haut- und Geschlechtskrankheiten
   – Herzchirurgie
   – Histologie und Embryologie
   – Hygiene und Mikrobiologie
   – Immunologie
   – Innere Medizin
   – Kinder- und Jugendchirurgie
   – Kinder- und Jugendheilkunde
   – Kinder- und Jugendpsychiatrie
   – Lungenkrankheiten
   – Medizinische Biophysik
   – Medizinische Genetik
   – Medizinische und Chemische Labordiagnostik
   – Medizinische Leistungsphysiologie
   – Mund-, Kiefer- und Gesichtschirurgie
   – Neurobiologie
   – Neurochirurgie
   – Neurologie
   – Neuropathologie
   – Nuklearmedizin
   – Orthopädie und Orthopädische Chirurgie
   – Pathologie
   – Pathophysiologie
   – Pharmakologie und Toxikologie
   – Physikalische Medizin und Allgemeine Rehabilitation
   – Physiologie
   – Plastische, Ästhetische und Rekonstruktive Chirurgie
   – Psychiatrie
   – Psychiatrie und Psychotherapeutische Medizin
   – Radiologie
   – Sozialmedizin
   – Spezifische Prophylaxe und Tropenmedizin
   – Strahlentherapie-Radioonkologie
   – Thoraxchirurgie
   – Unfallchirurgie
   – Urologie
   – Virologie

4. Zahnärztin/Zahnarzt
5. Dentistin/Dentist
6. Psychotherapeutin/Psychotherapeut
7. Klinischer Psychologe/Klinische Psychologin
8. Gesundheitspsychologin/Gesundheitspsychologe
9. Musiktherapeutin/Musiktherapeut
10. Hebamme
11. Physiotherapeutin/Physiotherapeut
12. Biomedizinische Analytikerin/Biomedizinischer Analytiker
13. Radiologietechnologin/Radiologietechnologe
14. Diätologin/Diätologe
15. Ergotherapeutin/Ergotherapeut
16. Logopädin/Logopäde
17. Orthoptistin/Orthoptist
18. Diplomierte Gesundheits- und Krankenschwester/Diplomierter Gesundheits- und Krankenpfleger
19. Diplomierte Kinderkrankenschwester/Diplomierter Kinderkrankenpfleger
20. Diplomierte psychiatrische Gesundheits- und Krankenschwester/Diplomierter psychiatrischer Gesundheits- und Krankenpfleger
21. Heilmasseurin/Heilmasseur
22. Krankenanstalt (§ 2 Abs. 1 Z 1 bis 6 KAKuG)
23. Selbständiges Ambulatorium (§ 2 Abs. 1 Z 7 KAKuG)
24. Einrichtung des Strafvollzugs
25. Kuranstalt (§ 42a KAKuG)
26. Öffentliche Apotheke
27. Gewebebank
28. Blutspendeeinrichtung
29. Untersuchungsanstalt
30. Augenoptik
31. Kontaktlinsenoptik
32. Bandagist
33. Hörgeräteakustik
34. Orthopädietechnik
35. Rettung
36. Patiententransport
37. Hauptverband der österreichischen Sozialversicherungsträger
38. Versicherungsträger
39. Krankenfürsorgeeinrichtung
40. Privatkrankenanstaltenfinanzierungsfonds
41. Personenversicherung Gesundheitsrisiken
42. Krankenanstaltenträger
43. Kuranstaltenträger
44. Gesundheitsverwaltung
45. Patientenvertretung (§ 11e KAKuG)
46. Dienstleister Gesundheitswesen

Anlage 2: Zulässige Algorithmen

1. Alle Verfahren, die im Anhang der Signaturverordnung 2008 (SigV 2008), BGBl. II Nr. 3/2008 angeführt sind, sind zulässig.
2. Als symmetrische Verfahren sind geeignet, wobei eine effektive Schlüssellänge von mindestens 100 Bit gegeben sein muss:
   - Advanced Encryption Standard (AES) [FIPS197]
   - TripleDES [ANSI X9.52]

   jeweils in CBC oder CTR Modus [NIST 800-38A].

Abkürzungen (zitierte Referenzen):

[ANSI X9.52]	„Triple Data Encryption Algorithm Modes of Operation“, American National Standards Institute, ANSI X9.52, 1998.
[FIPS197]	„Advanced Encryption Standard (AES)“, National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication, FIPS 197, November 2001.
[NIST 800-38A]	M. Dworkin: „Recommendation for Block Cipher Modes of Operation“, National Institute of Standards and Technology, NIST Special Publication 800-38A, 2001.

Erläuterungen (Auszug)

Allgemeiner Teil

1. Umsetzung des Konzepts der rollenbasierten Identität

Das Gesundheitstelematikgesetz (GTelG) verfolgt die Intention, das Vertrauen und die Sicherheit im elektronischen Verkehr mit Gesundheitsdaten zu verbessern. Die Kernelemente dazu sind im Wesentlichen der Nachweis von Identität und Rolle sowie die Sicherstellung der Vertraulichkeit und der Unverfälschtheit (Integrität) von Gesundheitsdaten. Für eine inhaltlich und ökonomisch zweckmäßige Umsetzung wird bei den Regelungen weitgehend auf die in der Praxis bereits eingeführten Lösungen Bedacht genommen.

Für den elektronischen Verkehr mit Gesundheitsdaten wird entsprechend dem Konzept der rollenbasierten Identität gefordert, dass für die Kommunikationspartner die Funktion (Rolle), in der sie Gesundheitsdaten anfordern oder erhalten, in Verbindung mit der Identität überprüfbar ist. Für den qualitätsvollen Nachweis bzw. die Überprüfung der Rolle sieht das GTelG im Wesentlichen zwei Möglichkeiten vor: Einerseits eine elektronische Bescheinigung gemäß den §§ 4 Abs. 1 und 5 Abs. 2 GTelG, andererseits die Überprüfung, ob ein Gesundheitsdiensteanbieter in den eHealth-Verzeichnisdienst (eHVD) eingetragen ist (§§ 4 Abs. 2 und 5 Abs. 3 GTelG). Von einer speziellen elektronischen Bescheinigung der Rollen wurde insbesondere auf Grund der eingeleiten Bestrebungen auf europäischer Ebene zur Harmonisierung der elektronischen Identifikation Abstand genommen. Für den Nachweis bzw. die Prüfung der Identität ist grundsätzlich das eingeführte Instrumentarium der elektronischen Signaturen zu verwenden, wobei lösungsbedingte Ausnahmen zulässig sein sollen.

Die sich speziell an der sogenannten gerichteten Kommunikation orientierenden Regelungen werden für die künftigen Anforderungen der ungerichteten Kommunikation im Gesundheitswesen, aber auch im Hinblick auf neue elektronische Gesundheitsdienste, dynamisch weiterzuentwickeln sein.

2. Rollen im elektronischen Gesundheitsdatenaustausch

Es wird ein Set jener Rollen festgelegt, die bereits derzeit für den elektronischen Gesundheitsdatenaustausch von hoher Relevanz sind. Dieses Basisset an Rollen wird entsprechend dem in der Praxis vorzufindenden Bedarf dynamisch zu ergänzen sein. In diesem Zusammenhang beispielhaft zu nennen ist insbesondere die Aufnahme weiterer Rollen für den elektronischen Gesundheitsdatenaustausch an den Nahtstellen zum Sozialwesen. Weiters werden die Stellen festgelegt, die die Zuordnung der Rollen zu einem Gesundheitsdiensteanbieter authentisch bestätigen.

3. Vertraulichkeit und Integrität

Der gleichsam professionelle Umgang mit sensiblen Daten durch die Rolleninhaber bedingt hohe Anforderungen an die Vertraulichkeit und die Erkennbarkeit von Veränderungen während des Transports. Bei der Konkretisierung dieser Anforderungen musste jedoch einerseits den bereits eingeführten Praktiken und andererseits den - auch wirtschaftlich verkraftbaren - technischen Möglichkeiten Rechnung getragen werden, damit die Erreichung des Ziels einer verbesserten Datensicherheit nicht konterkariert wird. Eine differenzierte Vorgangsweise erschien aber auch deshalb geboten, weil „Sicherheit“, nämlich die Sicherheit konkreter Daten, die Netzwerksicherheit oder die Informationssicherheit ganz allgemein, kein statisch definierbarer Zustand ist, sondern den Kontext und seine potenziellen Veränderungen durch die (technische) Weiterentwicklung berücksichtigen muss. Ausgehend davon und unter Bedachtnahme auf die vorzufindende Praxis werden zwar grundsätzlich einzuhaltende Maßnahmen festgelegt, jedoch auch alternative Methoden und Verfahren, mit denen ein ausreichendes Sicherheitsniveau erzielbar erscheint, zugelassen.

Entsprechend der Zielsetzung, für den Gesundheitsdatenaustausch ein möglichst hohes Qualitäts- und Sicherheitsniveau zu erreichen, wird besonders darauf hingewiesen, dass die getroffenen Regelungen Mindestanforderungen darstellen und es den GDA (bzw. den Dienstleistern) unbenommen bleibt, diese zu überschreiten oder – im Hinblick auf die Übergangsbestimmungen – in kürzerer Zeit umzusetzen .

Bewusst sein muss jedoch, dass Vertraulichkeit und Integrität von Gesundheitsdaten zwar als besondere, jedoch die Datensicherheit nicht vollständig charakterisierende Aspekte nicht allein durch den präventiven Einsatz technischer Werkzeuge, sondern insbesondere auch durch zusätzliche organisatorische Maßnahmen, die auch den Faktor Mensch als Nutzer der Technologien einbeziehen, zu verbessern sein werden.

Besonderer Teil

Zu § 1:

Beim elektronischen Gesundheitsdatenaustausch müssen Rolle und Identität der beteiligten Gesundheitsdiensteanbieter (GDA) anhand der übermittelten Daten festgestellt werden. Dies ist grundsätzlich ein zweiteiliger Prozess, da vor der Rolle die zugehörige Identität festgestellt werden muss (vgl. §§ 1 Abs. 1 und 2 Abs. 5):

1. Es muss die Identität des Absenders festgestellt werden, dies geschieht durch elektronische Signaturen, die Daten mit bestimmten Zertifikaten (= Identitäten) verknüpfen.

2. Nach der Identitätsfeststellung muss überprüft werden in welchen Rollen diese Identität tätig werden darf. Dies erfordert die Verknüpfung von Rolle und Identität, die nach Abs. 1 grundsätzlich mittels des im eHealth-Verzeichnisdienst (eHVD) gespeicherten bereichsspezifischen Personenkennzeichens (§ 9 E-Government-Gesetz, BGBl. I Nr. 10/2004 in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008) zu erfolgen hat.

Statt „*qualifizierter Signaturen*“ wird in dieser Verordnung die Wendung „*elektronische Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen*“ verwendet. Damit sollen praxisnahe Lösungen, bei denen etwa ein Zustellungsdienst als Aussteller „normaler“ Zertifikate, die einfach in bestehende Softwarelösungen importiert werden können, fungiert, ermöglicht werden. Es ist also zulässig – vor allem wenn dies aus Gründen der Praxistauglichkeit erforderlich ist – von einem qualifizierten Zertifikat abgeleitete Zertifikate zu verwenden.

Mit der Verwendung elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sind, kommen die Bestimmungen des Signaturgesetzes (SigG), BGBl. I Nr. 190/1999 in der Fassung des Bundesgesetzes BGBl. I Nr. 59/2008, zur Anwendung. Es ist daher nicht erforderlich zusätzliche Bestimmungen etwa über Verzeichnisdienste oder die Geheimhaltung von Schlüsseln zu normieren, da über die Regelungen für qualifizierte Signaturen im SigG auf dessen bewährtes System zurückgegriffen werden kann.

Beim Gesundheitsdatenaustausch unter gesicherten Bedingungen kann gemäß **Abs. 2** vom Identitätsnachweis bzw. der Identitätsprüfung mittels elektronischer Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen, abgesehen werden, wenn qualitativ vergleichbare Vorgänge Bestandteil dieser Lösungen sind. Vergleichbar sind jedenfalls alle Verfahren, die eindeutige Identitäten – etwa durch Prüfung gegen das ZMR – ermöglichen, sich auf die Identifikation mit Hilfe eines amtlichen Lichtbildausweises stützen und die Geheimhaltung der privaten Schlüssel, etc… vorsehen, mit denen die Verbindung zwischen Daten und Identität gewährleistet wird.

Zu § 2:

Die in der Anlage definierten Rollen stellen das Basisset dar; die Art und Anzahl der Rollen wird bei entsprechendem Bedarf zu erweitern sein. Ebenso wird die Granularität der Rollen anhand der Anforderungen der Praxis zu evaluieren sein. Die Bestimmung des **Abs. 1** verbietet es andere als die in Anlage 1 aufgezählten Rollen zu verwenden. Für Rollen, die nicht in der Anlage 1 genannt sind, gilt § 8 Abs. 4.

Die in **Abs. 2** genannten Stellen verfügen bereits über qualitätsvolle Daten für die Zuordnung von Rollen. Der Vollständigkeit halber soll erwähnt werden, dass die in Abs. 2 genannten Stellen nur innerhalb ihrer eigenen Zuständigkeit Rollen bestätigen dürfen. Dies ergibt sich eigentlich sowieso aus dem Berufsrecht, soll hier aber noch einmal ausdrücklich betont werden, um Missverständnisse zu vermeiden. Es soll – mit Blick auf die in Abs. 2 genannten Selbstverwaltungskörper – eben nicht zur Erweiterung des übertragenen Wirkungsbereichs kommen.

Durch den in **Abs. 3** vorgesehenen Datenaustausch ist ein ökonomisch zweckmäßiger Prozess zur Wartung bzw. Aktualisierung der in den eHVD zu übernehmenden Daten sicherzustellen. Dazu trägt u.a. die vom Bundesminister für Gesundheit, Familie und Jugend zu spezifizierende Schnittstelle bei.

Laufend aktualisiert bedeutet nicht unbedingt mehrmals täglich. Es ist bloß zu gewährleisten, dass beispielsweise Berechtigungslöschungen – d.h. der Entzug von Rollen – auch in annehmbarer Zeit an den eHVD weitergeleitet werden. Jedenfalls nicht überschritten werden darf die zweiwöchige Frist des § 9 Abs. 5 GTelG.

Nach **Abs. 4** ist der Bundesminister für Gesundheit, Familie und Jugend verpflichtet, den eHVD mit bPK auszustatten. Dies hat im Wege der Stammzahlenregisterbehörde (§ 7 E-GovG) zu erfolgen. Die Ausstattung einer Datenanwendung mit bPK erfolgt nach den Bestimmungen der Stammzahlenregisterverordnung (StZRegV), BGBl. II Nr. 57/2005, insbesondere deren §§ 15 ff. Die weiteren Daten, die der Bundesminister für Gesundheit, Familie und Jugend im Bedarfsfall zusätzlich erheben darf, stellen das

maximale Set an Identifikationsdaten von Stammzahlen- und Ergänzungsregister für natürliche Personen dar.

Nachweis und Prüfung von Rollen haben gemäß **Abs. 5** durch Abfrage des eHVD zu erfolgen. Unbeschadet dessen, dass diese Vorgänge in gesicherten Umgebungen auch auf andere Art und Weise zulässig sind (vgl. § 6), wird im Hinblick auf die Festlegungen betreffend die Zuordnung von Rollen zur einfacheren technischen Umsetzung mittelfristig der eHVD als Quelle zu etablieren sein.

Zu § 3:

Anders als Identität, Rolle und Integrität ist Vertraulichkeit kaum nachzuweisen, da Verletzungen im Geheimen erfolgen. Alleine aus der Tatsache, dass die Daten nicht verändert wurden und auch sonst keine Hinweise auf unbefugte Zugriffe vorliegen, kann nicht mit Sicherheit geschlossen werden, dass es tatsächlich keine Verletzung der Vertraulichkeit gegeben hat. Deshalb spricht **Abs. 1** auch bloß von Maßnahmen zur Sicherstellung der Vertraulichkeit. Z 1 behandelt die als sicher zu bewertenden Netze. Diese Netze sind insofern wichtiger Anknüpfungspunkt in dieser Verordnung, als mehrere Ausnahmen (vgl. §§ 1 Abs. 2, 2 Abs. 6 und 4 Abs. 2) auf ihre Verwendung abstellen.

Obwohl der Begriffsinhalt der „hinreichenden" Absicherung auf Grund der Dynamik der technologischen Entwicklung nicht abschließend beschrieben werden kann, wurden in den lit. a) bis c) wesentliche Elemente für seine Eingrenzung detektiert. Darüber hinausgehende Schutzmechanismen können sowohl aus technischen als auch aus organisatorischen Vorkehrungen bestehen. In technischer Hinsicht zu nennen wären etwa die Vorhaltung von speziellen Intrusion-Detection- und/oder Intrusion-Prevention-Systemen, (konfigurierbare) Firewall-Systeme, und Maßnahmen im Kontext sogenannter kritischer Infrastruktur. Organisatorische Vorkehrungen regeln u.a. auch besondere Betriebsbedingungen (z.B. redundante Systeme, Datensicherung, Protokollierung) sowie die Überprüfung (Audits) der Maßnahmen zur Risikominimierung. Weiters zu nennen wären Sicherheitszertifizierungen nach anerkannten Standards, wie insbesondere der BS 7799, die ITIL oder der Common Criteria-Standard. Ausgehend davon, kann mit guten Gründen angenommen werden, dass insbesondere der Gesundheitsdatenaustausch über das Gesundheitsinformationsnetz (GIN) oder das HEALIX-Netz oder die speziellen Netze der Sozialversicherung die festgelegten Anforderungen bereits heute erfüllen.

Z 2 referenziert weitere Möglichkeiten des elektronischen Gesundheitsdatenaustausches, bei denen zwar nicht alle Anforderungen der Z 1 erfüllt werden, jedoch durch entsprechende technische Vorkehrungen Vertraulichkeit und Integrität sichergestellt werden können. Sie betreffen insbesondere die Verwendung marktüblicher Kommunikations- bzw. Netzwerkprotokolle, die überwiegend auf den unteren Schichten des OSI-Referenzmodells aufsetzen (z.B. IPsec, SSL) und/oder darauf aufbauende Tunneltechniken (z.B. VPN) verwenden. Manche davon sehen auch eine gegenseitige Authentifizierung vor. Aus der Sicht der geforderten Datensicherheit erscheinen zusätzliche Maßnahmen im Sinne der §§ 6 und 7 GTelG nicht zwingend erforderlich. Nach Z 2 ist somit etwa auch der Versand von Gesundheitsdaten per E-Mail zulässig, wenn die Gesundheitsdaten vollständig verschlüsselt sind und die dabei verwendeten Algorithmen den Anforderungen der Signaturverordnung 2008 entsprechen. Die Versendung bloß kennwortgeschützter, aber ansonsten unverschlüsselter Dokumente per Mail ist hingegen unzulässig.

Von manchen Protokollen und Verfahren werden sogenannte Header-Informationen oder Authentifizierungsprozeduren von der Verschlüsselung nicht umfasst. **Abs. 2** stellt daher klar, dass unverschlüsselte Daten keinen Personenbezug enthalten dürfen. Umgekehrt ergibt sich aus Abs. 2 somit auch, dass beispielsweise im E-Mail-Verkehr nicht die gesamte E-Mail verschlüsselt werden muss, sondern nur jene Bereiche, die Gesundheitsdaten enthalten.

Zu § 4:

Abs. 1 bestimmt, dass grundsätzlich *elektronische Signaturen, die auf qualifizierte Zertifikate rückführbar sein müssen* – vgl. zu dieser Wendung bereits die Erläuterungen zu § 1 Abs. 1 – zum Nachweis und zur Prüfung der Integrität zu verwenden sind.

Alternativ dürfen gemäß **Abs. 2** auch andere Verfahren eingesetzt werden, wenn sie in sicherer Umgebung (§ 3 Abs. 1) eingesetzt werden und mit ihnen der Nachweis und die Prüfung der Gesundheitsdatenintegrität erbracht bzw. durchgeführt werden kann.

Zu § 5:

Die Dokumentationspflichten gelten lediglich für jene Fälle, in denen der elektronische Gesundheitsdatenaustausch auf der Grundlage von Ausnahme- bzw. Übergangsregelungen durchgeführt wird. Ausnahmebestimmungen sind die in **Abs. 1** Z 1 genannten Bestimmungen und Übergangsbestimmungen die in den Z 2 und 3 genannten.

Die Dokumentation hat so zu erfolgen, dass sie zu Beweiszwecken herangezogen werden kann, d.h. in der Regel schriftlich. Neben der Beweiserleichterung ist vor allem auch ihre Warnfunktion Grund für die Einführung von Dokumentationspflichten.

Die Dokumentationsverpflichtung der Ziffer 1 wird grundsätzlich nur für neu eingerichtete Systeme relevant. Eine gewichtige Ausnahme stellt das In-Kraft-Treten des gegenständlichen Entwurfs dar: Hier ist für alle in Ziffer 1 genannten Systeme, kurz festzuhalten, auf Grund welcher technischer, organisatorischer oder baulicher Maßnahmen, die Gesundheitsdiensteanbieter vom Erfüllen der Ausnahmetatbestände ausgehen.

Die Ziffern 2 und 3 hingegen verpflichten im Endeffekt zu einer laufenden Dokumentation, wenn auch mit größeren, zeitlichen Intervallen, wie etwa der Zwei-Monatsfrist gemäß § 7 Z 2.

Zum 2. Abschnitt:

Bis ein dem 1. Abschnitt der Verordnung entsprechend qualitätsvoller elektronischer Gesundheitsdaten-austausch in technischer und ökonomischer Hinsicht flächendeckend umgesetzt werden kann, sind als Übergangsregelung (vgl. § 8 Abs. 4) Erleichterungen der Datensicherheitsanforderungen zulässig. Durch die Formulierung der §§ 6 und 7 als Mindestanforderungen (vgl. „zumindest“ in § 6 Abs. 1 sowie die ausdrückliche Bezugnahme des § 7 nur auf Fax) dürfen bestehende Systeme, die zwar nicht die Anforderungen des 1. Abschnitts erfüllen, aber über die erleichterten Voraussetzungen der §§ 6 und 7 hinausgehen, weiterhin betrieben werden. Es besteht zwar keine Pflicht zur Beibehaltung bereits vorhandener höherer Sicherheitsstandards nach dieser Verordnung, allerdings sind die höheren Sicherheitsstandards des 1. Abschnitts im Auge zu behalten, die ab 1. Jänner 2012 uneingeschränkt gelten. Eine temporäre Rücknahme des Sicherheitsstandards wäre wohl sehr unökonomisch.

Wie bereits erwähnt, besteht keine Pflicht zur Beibehaltung bereits vorhandener höherer Sicherheitsstandards nach *dieser* Verordnung – sehr wohl kann sich eine derartige Pflicht aber aus dem Datenschutzgesetz 2000 ergeben. Nach dem klaren Wortlaut des § 1 Abs. 1 GTelG handelt es sich beim GTelG um „ergänzende“ Datensicherheitsbestimmungen. Deshalb kann auch die auf Grund des GTelG erlassene Verordnung auch nicht mehr als „ergänzende“ Datensicherheitsbestimmungen umfassen. Es ist somit jedenfalls rechtlich möglich, dass nach den Bestimmungen des § 14 DSG 2000 strengere Datensicherheitsmaßnahmen – wie etwa ein durchgängiges Faxverbot – erforderlich sind.

Zu § 6:

Nachweis oder Prüfung von Identität, Rollen oder Integrität nach den Bestimmungen des 1. Abschnitts sind im Sinne des **Abs. 1** insbesondere solange nicht möglich, als die Spezifikation gemäß § 2 Abs. 3 noch nicht veröffentlicht worden ist. Auch die nicht bloß temporäre – etwa in der Anlaufphase – Verzögerung der Arbeitsabläufe um mindestens 50 Prozent wird als Unmöglichkeit im Sinne des Abs. 1 anzusehen sein. Für den Fall, dass eine Unmöglichkeit im Sinne des Abs. 1 vorliegt, können Nachweis und Prüfung von Identität und Rollen entsprechend den Z 1 bis 4 vorgenommen werden. Auch wenn hier auf das Wort „ausschließlich“ verzichtet wurde, so ist diese Liste dennoch taxativ zu verstehen. Die in Ziffer 3 angesprochenen Vertragsbestimmungen können beliebige sein: es kommt einzig und allein darauf an, ob beispielsweise die E-Mail-Adressen der beiden Gesundheitsdiensteanbieter, die elektronischen Gesundheitsdatenaustausch betreiben wollen, im Vertrag angeführt sind. Klarerweise muss es sich bei der elektronischen Erreichbarkeit nicht um E-Mail-Adressen handeln, auch andere Arten der exakten, zweifelsfreien Adressierung wie etwa über URL und Port-Angaben sind zulässig. Bei der Ziffer 4 sei auf das frühere Außer-Kraft-Treten gemäß § 8 Abs. 4 hingewiesen. Es handelt sich hierbei um Verzeichnisse, die von den Stellen gemäß § 2 Abs. 2 des Entwurfs betrieben werden, wie etwa das elektronische Verzeichnis der Gesundheitsdiensteanbieter (vgl. http://www.evga.at [17.11.2008]).

§ 6 bietet auch die Rechtsgrundlage für die Kommunikation mittels Serverzertifikaten, wenn die Identitäten und Rollen gemäß Abs. 1 gegenseitig bestätigt sind.

Die Übergangsbestimmung des Abs. 1 stellt ein wesentliches Entgegenkommen an die Praxis dar, da insbesondere das Erfordernis der Integritätsgewährleistung entfällt. Es erscheint daher nur gerechtfertigt in den Fällen des Abs. 1 Z 1 und 2 – wenn per se also keine schriftliche Bestätigung vorliegt – eine kurze Notiz der Gesundheitsdiensteanbieter, die ihre Identität entweder mittels persönlichem oder telephonischem Kontakt bestätigt haben, über diese „Ersatzidentifizierung“ gemäß **Abs. 2** zu verlangen. *Erstmalig* stellt auf den überhaupt ersten Gesundheitsdatenaustausch zwischen bestimmten Gesundheits-diensteanbietern ab. Davon nicht umfasst sein soll jeder erstmalige Gesundheitsdatenaustausch nach In-Kraft-Treten dieses Entwurfes.

Zu § 7:

Die Verwendung von Telefax-Geräten und im Wesentlichen auch der in die IT-Umgebung integrierten Software-Faxlösungen für die Übermittlung von Gesundheitsdaten ist als ein rechtlich und technisch unzuverlässiges Verfahren einzustufen, weil

- Informationen in den überwiegenden Fällen unverschlüsselt übertragen werden („Postkarte“) und damit die Vertraulichkeit von Gesundheitsdaten leicht verletzt werden kann.
- die Adressierung nur anhand von Ziffern erfolgt, damit Bedienungsfehler wahrscheinlicher werden und Übermittlungen an den falschen Empfänger nicht oder zu spät bemerkt werden.
- Fernwartungen durchgeführt und dabei Speicherinhalte ausgelesen oder manipuliert werden können, ohne dass der Benutzer diesen Zugriff merkt.
- ein „OK-Sendebericht“ keinerlei Gewähr für die tatsächliche, richtige und vollständige Übermittlung bietet.
- auch ohne Bedienungsfehler oder unbefugte Zugriffe Dritter eine nicht zu vernachlässigende Anzahl von Rufnummernfehlschaltungen festzustellen ist.
- gekündigte Faxrufnummern von Diensteanbietern bereits nach kurzer Zeit neu vergeben werden können.

Tatsache ist allerdings auch, dass Telefax ein einfach handhabbares, kostengünstiges und in der Praxis weit verbreitetes Kommunikationshilfsmittel ist. Die anzustrebende Ablöse muss daher sowohl dem Gesichtspunkt des Investitionsschutzes als auch den zeitlichen Anforderungen für die Implementierung technischer Alternativen Rechnung tragen. Dem gegenüber stehen jedoch auch kurzfristig umsetzbare Vorkehrungen, die zwar keine generelle Lösung der damit verbundenen Problemstellungen bewirken können, jedoch zu Verbesserungen im Umgang mit diesem Medium führen können. Die vorgesehenen Maßnahmen stellen solche kurzfristig mögliche Vorkehrungen dar, ohne das mittelfristige Ziel, wie es auch in § 8 Abs. 4 dokumentiert ist, zu ändern.

Ergänzend zu den vorgesehenen Maßnahmen sollte daher auch geprüft werden, ob nicht eine getrennte Übermittlung von medizinischen Daten und personenbezogenen Angaben möglich ist. Zweifel hinsichtlich der Vollständigkeit (Integrität) können im Wege von Rückfragen ausgeräumt werden. Die dafür benötigten Angaben (z.B. Absenderangaben, Seitenanzahl) können etwa durch die Verwendung eines Deckblattes zur Verfügung gestellt werden. Für Nachweiszwecke erscheint es empfehlenswert, die Sendeprotokolle aufzubewahren. Bei Weitergabe eines Faxgeräts sollten jedenfalls gespeicherte Daten gelöscht werden.

Da sich § 7 als Übergangsbestimmung zur Vertraulichkeit ausschließlich auf den Faxverkehr bezieht, ist im Umkehrschluss die Übermittlung unverschlüsselter Gesundheitsdaten via E-Mail oder jeder anderen Art des elektronischen Gesundheitsdatenaustausches unzulässig.

Zu § 8:

Die Schnittstellenspezifikation für den Datenaustausch gemäß § 2 Abs. 3 bedarf der Akkordierung mit den genannten Stellen, bei der insbesondere allfällige technische Anforderungen der Partner abgeklärt werden müssen. Zudem bedarf es für deren Umsetzung eines angemessenen Zeitrahmens, wofür **Abs. 3** die notwendige Festlegung trifft.

Wie bereits ausgeführt, bedarf es zur Umsetzung der durch in dieser Verordnung festgelegten Maßnahmen eines ausreichenden Zeitraums, um die technische und ökonomische Machbarkeit sicherzustellen. Ausgehend von abschätzbaren Produktlebensdauern und der Durchdringungsgeschwindigkeit technischer Neuerungen sieht **Abs. 4** eine dreijährige Übergangsphase vor, mit der der elektronische Gesundheitsdatenaustausch einerseits unter den erleichterten Bedingung zulässig ist und mit dem andererseits technische Umstellungen im Zuge anstehender Reinvestitionsvorhaben kostenminimierend erfolgen können. Konsequenter Weise kann ein unter diesen Voraussetzungen konformes Verhalten der Gesundheitsdiensteanbieter nicht den Strafbestimmungen des GTelG unterliegen. Im Umkehrschluss bedeutet dies, allerdings, dass Verstöße gegen diese Verordnung, die zugleich auch Verstöße gegen das GTelG darstellen, jedenfalls nach § 17 GTelG strafbar sind.

Die in der Anlage enthaltenen Rollen können derzeit noch nicht abschließend definiert werden und sind daher laufend zu ergänzen. Bis zur Verfügbarkeit der diesbezüglichen Festlegungen sind daher die nicht in der Anlage aufgezählten Gesundheitsdiensteanbieter jedenfalls von der Strafbarkeit gemäß § 17 GTelG ausgenommen. Dies bedeutet jedoch keinesfalls die Suspendierung der Datensicherheitsmaßnahmen in § 14 DSG 2000 oder des Verwaltungsstraftatbestands in § 52 DSG 2000, da die Bestimmungen des DSG 2000 – wie bereits erwähnt – unabhängig vom GTelG gelten.

Zu Anlage 1:

Die in den **Z 1** bis **21** genannten Rollen stellen auf Gesundheitsdiensteanbieter ab, die auf Grund der für sie jeweils geltenden berufsrechtlichen Vorschriften die Rollen freiberuflich ausüben dürfen. Die in den **Z 22** bis **45** genannten Rollen beziehen sich auf Gesundheitsdiensteanbieter, die im Gesundheitsdaten-austausch als Organisationen auftreten. Wesentliches Kriterium dabei ist nicht, dass diese Organisationen über eigene Rechtspersönlichkeit verfügen, sondern dass sie tatsächlich und in ihrem Namen den elektronischen Gesundheitsdatenaustausch durchführen. Diese Organisationsrollen sind jeweils auch von organisatorischen Gliederungen im Sinne des § 10 Abs. 3 GTelG zu verwenden, wenn sie auf Grund einer diesbezüglichen Berechtigung der übergeordneten Organisation am elektronischen Gesundheitsdaten-austausch teilnehmen. Die Rollen sind zum Einen nicht hierarchisch aufgebaut und zum Anderen exklusiv. Demzufolge kann etwa die Rolle Krankenanstaltenträger nicht von einer Krankenanstalt wahrgenommen werden. Nimmt beispielsweise eine natürliche Person oder eine Organisation mehrere Rollen wahr (Arzt für Allgemeinmedizin und Psychotherapeut), sind diese auch dementsprechend zuzuordnen.

Hinsichtlich der Rolle Krankenanstalt wurde auf eine weitergehende Differenzierung verzichtet; der **Z 22** werden somit alle gemäß KAKuG referenzierten Krankenanstalten zugeordnet. Der **Z 35** sind ausschließlich auf gesundheitsbezogene Notfälle spezialisierte Einrichtungen, die auch eine medizinische Erstversorgung durchführen, zuzuordnen. Nicht darunter fallen andere im allgemeinen Sprachgebrauch als solche bezeichnete Rettungsorganisationen, wie etwa die Feuerwehr. Der **Z 38** sind alle im Hauptverband zusammengeschlossenen Versicherungsträger zugeordnet. Die mit unterschiedlicher Bezeichnung eingerichteten Krankenfürsorgeeinrichtungen (einschließlich der Unfallfürsorge) sind der in **Z 39** zusammengefasst. Für die Rolle gemäß **Z 41** kommen jene Einrichtungen in Betracht, die private Versicherungen für gesundheitsbezogene Risiken anbieten. Die **Z 42** und **43** sind für Betriebsgesellschaften, Verbünde oder Holdings, aber auch für konfessionelle und private Betreiberorganisationen sowie Gebietskörperschaften und Selbstverwaltungseinrichtungen als Träger heranzuziehen. Die **Z 44** ist für die Verwaltungseinrichtungen (Geschäftsapparate) und Behörden (z.B. Bezirksverwaltungsbehörden, Magistrate) der Gebietskörperschaften, aber auch für die im Eigentum oder einem vergleichbaren Beherrschungsverhältnis stehenden Planungseinrichtungen der Gesundheits-verwaltung, vorgesehen. Die Rolle Patientenvertretung (**Z 45**) bezieht sich ausschließlich auf die im KAKuG vorgesehenen Einrichtungen. In Bezug auf die Dienstleister (gemäß Definition des DSG 2000) wurde zunächst auf eine Differenzierung verzichtet, eine granularere Festlegung von Dienstleisterrollen erfolgt gegebenenfalls auf Grund der Evaluierung eines diesbezüglichen Bedarfs.