BUNDESMINISTERIUM
FÜR GESUNDHEIT

Alois Stöger
Bundesminister

XXIV. GP.-NR
9309 /AB
05. Dez. 2011

zu 9408 /J

Frau
Präsidentin des Nationalrates
Mag.ª Barbara Prammer
Parlament
1017 Wien

GZ: BMG-11001/0286-I/A/15/2011

Wien, am 5. Dezember 2011

Sehr geehrte Frau Präsidentin!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 9408/J des Abgeordneten Dr. Karlsböck, Dr. Belakowitsch-Jenewein und weiterer Abgeordneter** nach den mir vorliegenden Informationen wie folgt:

Einleitend wird festgehalten, dass zur vorliegenden parlamentarischen Anfrage Stellungnahmen des Hauptverbandes der österreichischen Sozialversicherungsträger sowie der Tiroler Gebietskrankenkasse (TGKK) eingeholt wurden, die in die nachstehenden Ausführungen eingeflossen sind.

Frage 1:
Von der TGKK wurde meinem Ressort mitgeteilt, dass die in den Medienberichterstattungen angegebenen Äußerungen, wonach sensible Patient/inn/endaten über sechs Monate ungesichert auf einem Onlinespeicherdienst abrufbar gewesen wären, bisher nicht verifiziert und objektiviert werden konnten. Dazu ist anzumerken, dass Anonymous Austria behauptet, im Besitz von 600.000 Datensätzen der TGKK zu sein, diese aber jedenfalls nicht veröffentlicht hat.

Interne und externe Firmen haben die IT-Sicherheitsstandards bei der TGKK geprüft und feststellen können, dass sie dem derzeitigen neuesten Stand entsprechen würden. Nach der erst später erfolgten Bekanntgabe von Anonymous Austria, dass es sich nicht um einen erfolgreichen Einbruch in die gesicherten Netze der Sozialversicherung gehandelt habe, sondern offenbar um öffentlich zugängliche Daten (im Sinne von ungesicherten Daten auf einem Onlinespeicherdienst), wurde auch intensiv im Internet nach etwaig frei zugänglichen Sozialversicherungsdaten gesucht. Auch diese Nachforschungen konnten die Angaben von Anonymous Austria nicht bestätigen.

Radetzkystraße 2, 1031 Wien Telefon **+43 1 71100-4300** Fax **+43 1 71100-14300**
Internet **www.bmg.gv.at** E-Mail **alois.stoeger@bmg.gv.at**

Fragen 2 und 3:
Der Vorfall bei der TGKK verlangt nach einer grundsätzlichen Überprüfung dahingehend, wie weit die einschlägigen gesetzlichen Bestimmungen zur Datensicherheit und die faktischen Gegebenheiten des Datenaustausches übereinstimmen. Gemäß § 31a ASVG sind unter anderem die Bestandteile des Elektronischen Verwaltungssystems der gesetzlichen Sozialversicherungsträger (ELSY) verbindlich im Rahmen der jeweils vorgesehenen Aufgaben zu verwenden, was meiner Auffassung nach nicht nur den Hauptverband und die Versicherungsträger, sondern auch deren Systempartner/innen einschließt. Ich habe daher in einem Schreiben an den Hauptverband der österreichischen Sozialversicherungsträger unter Hinweis auf § 31a ASVG um die Durchführung einer Erhebung bei allen Versicherungsträgern hinsichtlich der Anbindung von Vertragspartner/inne/n an ELSY bzw. der allenfalls sonstigen Art des Datentransfers ersucht. Das Ergebnis dieser Untersuchung bleibt zunächst abzuwarten.

Unter Hinweis auf die Beantwortung der Frage 1 ist festzuhalten, dass die ungesicherte Verfügbarkeit von sensiblen Patientendaten bei einem Onlinespeicherdienst nicht verifiziert und objektiviert werden konnte.

Frage 4:
Es werden permanent Anstrengungen unternommen, auch durch wirtschaftliche Anreize die Teilnehmer/innenzahl am e-card-Netz und damit am Elektronischen Verwaltungssystem der Sozialversicherung auszuweiten. Durch die Entwicklung und Bereitstellung von (dem aktuellen technischen Sicherheitsniveau entsprechenden) Systemen kann den Vertragspartner/inne/n z.B. ein Teil der für eine sichere Infrastruktur aufzubringenden Aufwendungen abgenommen werden.

Frage 5:
Ich verweise dazu auf die Beantwortung der Fragen 2 und 3. Unabhängig davon wurden bereits bisher die Sicherheitsmaßnahmen regelmäßig durch unabhängige externe Fachkräfte geprüft.

Frage 6:
Im Unterschied zum gegenständlichen Fall der TGKK würden im Rahmen der elektronischen Gesundheitsakte - ELGA keine großen oder zusammenhängenden Datenmengen physisch zwischen zwei Kommunikationspartner/inne/n bewegt. ELGA ist vielmehr so konzipiert, dass Zugriffe auf verteilte, nämlich bei den verschiedenen Gesundheitsdiensteanbieter/inne/n (GDA) erzeugte und gespeicherte Daten ermöglicht werden würden.

Die Zugriffe im Rahmen von ELGA sollen höchsten Sicherheitsvorkehrungen unterliegen. Gesetzlich wäre eine entscheidende technisch-organisatorische Sicherheitsschranke – insbesondere e-card beim GDA oder Bürgerkarte durch Privatperson - für jeden Zugriff auf personenbezogene ELGA-Gesundheitsdaten vorgesehen. Darüber hinaus wird vom ELGA-Berechtigungssystem geprüft, ob und gegebenenfalls inwieweit Zugriffe auf Daten zulässig sind. Diese Prüfungen umfassen in jedem Fall die Au-

thentifizierung der/des Zugreifenden und bei Zugriffen von Gesundheitsdiensteanbieter/inne/n auf Patient/inn/endaten die Autorisierung der/des Zugreifenden anhand von rollenabhängigen (allgemeinen bzw. gesetzlich festgelegten) Berechtigungen, sowie anhand der von den Betroffenen selbst festgelegten oder modifizierten allgemeinen Zugriffsrechte. Eine weitere Sicherheitsschranke besteht darin, dass nur definierte Dokumente (Daten), somit ein selektiver Ausschnitt der potenziell zu einer Person verarbeiteten Gesundheitsdaten, und nicht etwa ihre gesamte Krankengeschichte eingesehen werden kann. Massenabfragen, etwa Gesundheitsdaten über eine Mehrzahl von Personen oder den Gesamtdatenbestand einer Person sind somit schon technisch nicht möglich. Durch die Verwendung von Technologien entsprechend dem Stand der (Sicherheits-)Technik und die Vermeidung sicherheitstechnisch kaum kontrollierbarer Services von Drittanbieter/inne/n (z.B. Onlinespeicherdienste) ist ein dem genannten Vorfall vergleichbares Bedrohungspotenzial nicht gegeben.

Frage 7:
Seitens des Hauptverbandes der österreichischen Sozialversicherungsträger wurde dazu im Wesentlichen Folgendes mitgeteilt:

„Das Intrusion Detection System (IDS) wird regelmäßig evaluiert und laufend an den jeweiligen Stand der Technik angepasst. In diesem Zusammenhang werden auch regelmäßig externe Sicherheitschecks durchgeführt. Maßnahmen zur langfristigen Sicherung der Datenwege werden evaluiert. Ziel ist, die Zahl der Datenübertragungswege zu minimieren und Zugriffe über das gesicherte e-card-Netz weiter zu fördern. Trägerübergreifende Eskalationspfade bzw. abgestimmte Kommunikation im Krisenfall soll verbessert werden.

Die Datenübertragung der Sozialversicherung findet bereits jetzt in zielgruppenorientiert gesicherten Netzen statt (z.B. nach außen abgeschottetes CNSV-Netz für Sozialversicherungsträger [Corporate Network der Sozialversicherung]; Netz für Gesundheitsdiensteanbieter/innen: das e-card-Netz); die Netzwerksicherheit wird regelmäßig evaluiert und laufend an den jeweiligen Stand der Technik angepasst."

Um die Sicherheit der ELGA-Gesundheitsdaten weiter zu erhöhen, werden neben den zu Frage 6 ausgeführten Zugriffsschutzmechanismen zusätzliche Maßnahmen getroffen (proaktiver Datenschutz). Exemplarisch wird in diesem Zusammenhang auf das ELGA-eigene Sicherheitsframework, das Informationssicherheitsmanagement, verwiesen, in dem eine Reihe weiterer technischer und organisatorischer Anforderungen festgelegt werden und deren Einhaltung im Rahmen der vorgesehenen Audits auch überprüfbar ist.

Für den Nicht-ELGA-Bereich bzw. für die Weitergabe von Gesundheitsdaten außerhalb von ELGA wurde mit den spezifischen Datensicherheitsbestimmungen im Gesundheitstelematikgesetz dem besonderen Schutzbedürfnis von sensiblen Daten bereits sehr früh Rechnung getragen. Auch beim Aufbau und beim Betrieb von Netz-

werken, etwa für die e-card oder für Healix, wurde auf die besonderen Schutzanforderungen von Gesundheitsdaten geachtet. Dass bei den einzelnen Gesundheitsdiensteanbieter/inne/n vor Ort eine dem Stand der Technik entsprechende Absicherung bei der Verarbeitung oder bei der Weitergabe erfolgt, kann schon allein in Bezug auf die verfügbare Infrastruktur und das vorhandene Know-how bei den Krankenanstaltenverbünden vorausgesetzt werden. Auch im extramuralen Bereich sind in den letzten Jahren keine gravierenden oder unmittelbaren Handlungsbedarf erfordernden Vorfälle bekannt geworden. Trotzdem werden in das neugefasste Gesundheitstelematikgesetz spezielle Dokumentations- und Nachweispflichten im Rahmen eines intern zu führenden IT-Sicherheitskonzepts aufgenommen.

Bekannt ist aber, dass technische Maßnahmen zum Schutz sensibler Daten allein nicht ausreichen, sondern begleitend dazu auch ergänzende innerorganisatorische Vorkehrungen und Schulungen des Personals erfolgen müssen. Schon im Hinblick auf ein nicht ausschließbares Fehlverhalten von Mitarbeiter/inne/n und das unzweifelhaft extern vorhandene kriminelle Potenzial muss aber bewusst sein, dass Maßnahmen der IT-Sicherheit einer ständigen Anpassung an sich verändernde Rahmenbedingungen bedürfen.