MINISTERIUM FRAUEN GESUNDHEIT

Dr.in Pamela Rendi-Wagner, MSc
Bundesministerin

Frau
Präsidentin des Nationalrates
Doris Bures
Parlament
1017 Wien

GZ: BMGF-11001/0029-I/A/5/2017

Wien, am 31. März 2017

Sehr geehrte Frau Präsidentin!

Ich beantworte die an meine Amtsvorgängerin gerichtete schriftliche parlamentarische **Anfrage Nr. 11724/J der Abgeordneten Dr. Dagmar Belakowitsch-Jenewein und weiterer Abgeordneter** nach den mir vorliegenden Informationen wie folgt:

Frage 1:

- *Wie sehen Sie die Kritikpunkte der Wiener Ärztekammer bezüglich der Gefährdung sensibler Patientendaten durch den Einsatz von ELGA, wie sie in der OTS vom 24.01.2017 formuliert wurden?*

Zu den wichtigsten Zielen bei der Errichtung und dem Betrieb der elektronischen Gesundheitsakte ELGA zählt die bestmögliche Erreichung von Datenschutz und Datensicherheit. Bereits in der Entwicklung der ELGA-Architektur wurde mit dem Einsatz von State-of-the-Art-Standards besonderer Wert auf Sicherheit gelegt. Umfangreiche Tests schon während der Entwicklung sowie spezielle Sicherheitstests, sogenannte Penetrationstests, gewährleisten die bestmögliche Ausgangsbasis für einen funktionierenden und sicheren Start von ELGA.

Die ELGA-Befunde entstehen bei den ELGA-Gesundheitsdiensteanbieter/inne/n und werden in deren Verantwortungsbereich entweder in eigenen Hochsicherheitsrechenzentren oder in jenen ihrer Dienstleister gespeichert. Der Zugriff auf Daten im technischen Bereich ist nur im 4-Augen-Prinzip oder mit vergleichbaren technischen Sicherheitsmaßnahmen gestattet. Zur Gewährleistung von Datenschutz und Datensicherheit bei ELGA wird für eine enge Zusammenarbeit und Abstimmung der Sicherheitsexpert/inn/en der beteiligten Organisationen gesorgt.

Das ELGA-Berechtigungssystem steuert und protokolliert alle ELGA-Transaktionen. Der Zugriff für eine/n ELGA-Gesundheitsdiensteanbieter/in ist grundsätzlich nur bei einem aufrechten Behandlungs- bzw. Betreuungsverhältnis möglich, welches technisch nachgewiesen werden muss, z. B. durch das Stecken der e-card im niedergelassenen Bereich. Wenn Bürger/innen selbst auf ihre eigene ELGA zugreifen wollen, müssen sie sich mit dem technisch derzeit sichersten Identitätsnachweis im Internet, nämlich via Bürgerkartenfunktion (Karte oder Handysignatur) am ELGA-Portal anmelden.

Der Datentransport erfolgt bei ELGA ausschließlich verschlüsselt. Die Kommunikation zwischen den ELGA-Gesundheitsdiensteanbieter/inne/n und im gesamten ELGA-System muss über speziell abgesicherte Gesundheitsnetze erfolgen. Über diese technischen Sicherheitsmaßnahmen hinaus verpflichten sich alle an ELGA beteiligten Organisationen zur Einhaltung der Leitlinien des ELGA-Informationssicherheits-Managementsystems (ISMS), das sich an internationalen Sicherheitsstandards orientiert (Normserie ISO 27000, BSI Grundschutz) und bereits 2011 von den ELGA-Systempartner/inne/n beschlossen wurde.

Die in der genannten Presseaussendung geäußerte Kritik der Wiener Ärztekammer an der Gefährdung der Patient/inn/endaten richtet sich an die ordnungsgemäße und sichere Verwendung der „Peripheriegeräte“ in Ambulatorien, Spitälern und Arztpraxen. Der Autor ist in der zitierten und von der Ärztekammer in Auftrag gegebenen Studie zu dem Ergebnis gekommen, dass die elektronische Gesundheitsakte ELGA von der Gesamtarchitektur her sicher aufgestellt ist und sehr überlegt konzipiert wurde. Als potenziell gefährdenden Angriffspunkt hat er die Peripherie herausgearbeitet und Maßnahmen zur Verbesserung der Sicherheit an dieser Stelle vorgeschlagen. Es wurde aufgezeigt, dass Sicherheitsverletzungen durch „ausgespähte“ Passwörter geschehen können, festgehalten werden muss in diesem Zusammenhang jedoch auch, dass damit alleine noch kein Zugriff auf die ELGA möglich wäre, weil zusätzlich beispielsweise das jeweilige gesicherte Netz „aufgebrochen“ und sämtliche dort eingerichteten Sicherheitssysteme ausgeschaltet werden müssten.

Zusammenfassend hat somit die zitierte Studie nicht nur der ELGA ein dem Stand der Technik entsprechendes Datenschutz- und Sicherheitsniveau bescheinigt, sondern auch auf den diesbezüglichen Handlungsbedarf bei den „Endusern“ (Leistungserbringer/inne/n) aufmerksam gemacht. Die Umsetzung muss allerdings vor Ort erfolgen und durch die Verantwortlichen veranlasst werden.

Frage 2:

- *Wie beurteilen Sie die von der Wiener Ärztekammer geforderte zentrale Benutzerverwaltung für alle ELGA-berechtigten Anwender?*

Das ELGA-Berechtigungssystem ist ein zentraler Baustein von ELGA. Jeglicher Zugriff auf ELGA kann nur nach Prüfung im ELGA-Berechtigungssystem erfolgen. Hierbei erfolgt auch ein Abgleich der verwendeten Identität mit dem zentralen Gesundheitsdiensteanbieterindex (§ 19 Gesundheitstelematikgesetz - GTelG). Die Organisation der konkreten Benutzerverwaltung setzt aus Gründen der Zweckmäßigkeit und Wirtschaftlichkeit auf bereits bestehenden Strukturen auf (§ 10 GTelG). Die in § 22 GTelG festgelegte Pflicht zur Protokollierung des Namens der natürlichen Person, die die ELGA-Gesundheitsdaten tatsächlich verwendet hat, ist zudem als wesentliche Maßnahme der Datensicherheit zu betrachten, da sie eine inhärent präventiv-abschreckende Wirkung hat. Die Nachvollziehbarkeit von Zugriffen und Zugriffsversuchen auf ELGA ist somit gegeben.

Fragen 3 und 4:

- *Wie beurteilen Sie die von der Wiener Ärztekammer geforderte Einführung einer verpflichtenden separaten Authentifizierung beim Einstieg in ELGA durch jeden ELGA-User?*
- *Wie beurteilen Sie die von der Wiener Ärztekammer geforderte Verwendung einer starken Zweifaktor-Authentifizierung?*

Laut Gesundheitstelematikgesetz muss jeder Zugriff auf ELGA-Gesundheitsdaten personenbezogen, zuordenbar und nachvollziehbar erfolgen. Bereits dieses Faktum erhöht die Datensicherheit in Spitälern massiv: Bisher vereinzelt verwendete „Sammeluser“, wie etwa „Chirurgie“ für das gesamte chirurgische Team, sind in ELGA nicht mehr zulässig. Eine Zwei-Faktor-Authentifizierung – analog zur Authentifizierung der Bürgerin bzw. des Bürgers am ELGA-Portal mittels Bürgerkarte/Handysignatur – wäre prinzipiell auch seitens der ELGA-Gesundheitsdiensteanbieter/innen möglich, ist jedoch mit beachtlichen Aufwänden und Eingriffen in die etablierten Prozesse verbunden. Die Verantwortung für die Einführung einer Zwei-Faktor-Authentifizierung obliegt daher dem/der betreffenden ELGA-Gesundheitsdiensteanbieter/in bzw. dessen/deren Rechtsträger (z. B. Spitalsbetreiber). Zur Gewährleistung des geforderten Sicherheitsniveaus wurde demzufolge entschieden, zumindest durch entsprechende Vorgaben beim Passwort-Login die Sicherheit weiter zu erhöhen: Mindestlänge von Passwörtern, zwingende Verwendung von Buchstaben, Zahlen und Sonderzeichen, Beschränkung der zeitlichen Gültigkeit von Passwörtern.

Frage 5:

- *Wie beurteilen Sie die von der Wiener Ärztekammer geforderte Einführung einer flächendeckenden digitalen Signatur von Gesundheitsdokumenten?*

Durch die Einführung von ELGA wurden die Voraussetzungen für das digitale Signieren von Gesundheitsdokumenten wesentlich vorangetrieben.
Es dürfen nur ärztlich vidierte/validierte Befunde in ELGA registriert werden. Für ein korrektes ELGA-Gesundheitsdokument, das die Anforderungen der Clinical Document Architecture (CDA) erfüllt, ist die Angabe einer/eines inhaltlich Verantwortlichen

zwingend erforderlich, diese Informationen sind auch in ELGA enthalten. Die Umsetzung der konkreten Berechtigung für das Vidieren liegt – wie schon bisher – in der Verantwortung der einzelnen Krankenanstalt bzw. des einzelnen Labor- und Röntgeninstitutes.

Frage 6:

- *Wie beurteilen Sie die von der Wiener Ärztekammer geforderte regelmäßige Informationen an Patienten über sie gespeicherte Daten und deren Abrufe, zum Beispiel über E-Mail oder SMS ("Push Service")?*

ELGA bietet jeder Patientin/jedem Patienten jederzeit die Möglichkeit im Wege des ELGA-Portals einfach und sicher Kenntnis davon zu erlangen, welche ELGA-Gesundheitsdaten (z. B. ärztlicher Entlassungsbrief) in ELGA zur Verfügung gestellt wurden und wer wann auf diese Dokumente zugegriffen hat. Ersatzweise werden diese Informationen jenen Betroffenen, die über keine entsprechende technische Ausstattung und/oder Bürgerkarteninfrastruktur verfügen, durch die ELGA-Ombudsstelle erteilt.

Die Errichtung eines „Push-Services“ wäre technisch möglich, wenngleich finanziell und organisatorisch aufwendig (z.B. Pflege der Kontaktdaten). Es wurde daher vorerst davon Abstand genommen.

Dr.in Pamela Rendi-Wagner, MSc

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR GESUNDHEIT UND FRAUEN @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Gesundheit und Frauen
	Datum/Zeit	2017-03-31T11:50:26+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1610631462
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2017-03-31T12:27:03+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	