Bundesministerium
Arbeit, Soziales, Gesundheit
und Konsumentenschutz

Mag.ª Beate Hartinger-Klein
Bundesministerin

Stubenring 1, 1010 Wien
Tel: +43 1 711 00 – 0
Fax: +43 1 711 00 – 2156
Beate.Hartinger-Klein@sozialministerium.at
www.sozialministerium.at

Herr
Präsident des Nationalrates
Parlament
1010 Wien

GZ: BMASGK-70500/0003-VIII/A/4/2018

Wien, 27.7.2018

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 977/J der Abgeordneten Stephanie Cox, Kolleginnen und Kollegen** wie folgt:

Fragen 1 bis 3, 6 bis 8 und 9i:

Ich verweise auf die Beantwortung der parlamentarischen Anfrage Nr. 976/J vom 5. Juni 2018 durch die Bundesministerin für Digitalisierung und Wirtschaftsstandort.

Frage 4:

Für ELGA – und damit wegweisend für weitere eHealth-Anwendungen – wurde ein Weg gewählt, der einerseits streng auf bereits bewährte internationale Standards, wie OASIS, W3C, HL7 und IHE setzt, andererseits aber unmittelbar die sichere österreichische eGovernmentarchitektur, insbesondere im Bereich der Identifizierung und Authentifizierung der einzelnen ELGA-Teilnehmer nützt.

Nur durch das eGovernment authentifizierte und bestätigte ELGA-Teilnehmerinnen/ELGA-Teilnehmer (und deren gesetzliche Vertretung) haben Zugang zu ihren eigenen ELGA-Daten. Die österreichische eGovernmentarchitektur (Identitätsmanagement, elektronische Signaturen – insbesondere Handy-Signatur, Portalverbund und vieles mehr) ist die österreichische Lösung bzw. Alternative zur estnischen X-Road-Lösung.

In der ELGA-Architektur wird:

- Die **Interoperabilität** regelmäßig auf dafür jährlich gestalteten internationalen Veranstaltungen *(Connectathon)* getestet und bestätigt.

- Management von **Risiken**: In einer Welt der vernetzten digitalen Lösungen mit Restrisiken zu rechnen ist imperativ. Es müssen daher Maßnahmen ergriffen und Hürden in das System eingebaut werden, die bekannte bzw. erkannte Risiken minimieren, Angriffe und/oder den Missbrauch von Gesundheitsdaten massiv erschweren bzw. im Optimalfall ausschließen. Hierfür werden in Österreich internationale Verfahren verwendet, die auf standardisierten kryptografischen Lösungen aufbauen. Dazu zählen rigorose Zugangskontrolle und Zugangsteuerung, Verschlüsselung, Integritätsschutz, nahtlose Protokollierung sowie Pseudonymisierung. Als Schlüssel dafür verwendet werden die in der eGovernment-Architektur vorgesehenen bereichsspezifischen Personenkennzeichen (bPK). Rückschlüsse auf tatsächliche Personen sind ausschließlich über entsprechend autorisierte Auskunft beim Zentralen Patientenindex möglich. Die technische Art und Weise der Datenspeicherung schließt derzeit eine analytische Auswertung der Daten aus (es existiert keine relationale oder semantische Zerlegung der Daten). Sollte eine analytische Auswertung über zentral oder dezentral gespeicherte Gesundheitsdaten beauftragt werden, müssten zusätzliche architektonische und technische Maßnahmen getroffen werden, um dies zu ermöglichen, da dies derzeit gemäß ELGA-Gesetzgebung *per se* ausgeschlossen ist.

Wie ELGA beruht auch das estnische X-Road auf einem System von Rechts- und Verfahrensvorschriften, technischen Standards und Regeln, Hard- und Software-Komponenten, wie insbesondere dezentrale Datenbanken und vieles mehr, um unbefugte Zugriffe bzw. Manipulationen via Internet zu verhindern. Bürgerinnen und Bürger greifen auf die Daten über Identitätskarten mit Passwort zu. Der wesentliche Unterschied ist jedoch, dass im estnischen System Blockchain-Technologie verwendet wird. Skeptische oder gar kritische Stimmen diesbezüglich werden derzeit noch zu wenig beachtet. Umso mehr müssen Einsatzmöglichkeiten dieser Technologie im Gesundheitswesen umfassend geprüft bzw. evaluiert werden.

Frage 4aa: Die **Integrität** der Gesundheitsdaten sowohl auf Transportebene als auch auf Persistenzebene wird durch international anerkannte kryptografische Verfahren sichergestellt. Es werden elektronische Signaturen auf Basis von qualifizierten Zertifikaten verwendet und verschlüsselte Kommunikationswege entsprechend der jeweils höchsten aktuell verfügbaren TLS Version verlangt.

Frage 4ab: Die **Transparenz** der Zugriffe wird durch nahtlose Protokollierung aller Zugriffe sichergestellt. Die Protokollierung erfolgt mehrfach und entsprechend dem IHE ATNA-Profile (jede/r Akteurin/Akteur ist verpflichtet, Protokoll über die eigene Tätigkeit zu führen) und wird einerseits zentral sicher aufbewahrt und andererseits verteilt in den Rechenzentren der einzelnen ELGA-Bereiche. Für allfällige forensische Recherchen können lokal gespeicherte Kopien und zentral aufbewahrte Versionen der Protokolle abgeglichen werden. Eine erfolgreiche Manipulation der Protokolle ist dadurch ausgeschlossen. Der Zugang zu den Protokollen ist darüber hinaus rigoros überwacht und geschützt.

Frage 4b: Die zur österreichweit einheitlichen Identifikation erforderlichen Daten – sowohl über die Bürgerinnen/Bürger als auch hinsichtlich der Gesundheitsdiensteanbieter – werden in zentral geführten Registern verwaltet. Die in ELGA/eHealth zu verwendenden Terminologien werden über ein zentral geführtes Service zur Verfügung gestellt. Die Willenserklärun-

gen der Bürgerinnen und Bürger, welche Applikationen sie nutzen wollen und welche Applikationen sie nicht nutzen wollen (Widerspruch bzw. opt out), werden zentral geführt und vom Berechtigungssystem, das sowohl zentrale als auch dezentrale Services umfasst, bei jedem Zugriff geprüft.

Frage 4bi: Der Großteil der Gesundheitsdaten wird ausschließlich dezentral gespeichert. Ausnahmen davon sind nur dann vorgesehen, wenn gewichtige Gründe für eine zentrale Speicherung sprechen, beispielsweise im Rahmen der eMedikation: Um Überdosierungen oder tödliche Wechselwirkungen vermeiden zu können ist es erforderlich, dass alle aktuellen Medikationsinformationen im Augenblick der Verschreibung abgerufen werden können. Wenn – im Falle dezentraler Speicherung - nur eines der dezentralen Rechenzentren zum Abfragezeitpunkt nicht erreichbar wäre (z.B. System- oder Netzwerkwartung), wäre das Abfrageergebnis gefährlich und daher wertlos.

Frage 4bii: Die eMedikationsdaten werden in einem hochsicheren Rechenzentrum verschlüsselt gespeichert; damit führt nur ein autorisierter Zugriff innerhalb der definierten Zugangswege zur Lesbarkeit. Darüber hinaus werden diese Daten nur pseudonymisiert gespeichert.

Frage 4biii: Dazu verweise ich auf die Ausführungen zu Frage 5c.

Frage 5:

Die eMedikation in der Steiermark, aber auch in allen anderen Bundesländern, ist entsprechend der internationalen Richtlinien von HL7/IHE *Pharmacy, Community Medication Prescription and Dispense Profile* aufgebaut und mittels sogenannter Implementierungsleitfäden konkretisiert. Die für die eMedikation maßgeblichen Implementierungsleitfäden wurden auf Grundlage von § 16 ELGA-Verordnung 2015 kundgemacht. Die Daten werden zentral in einem hochsicheren Rechenzentrum gespeichert.

Die eMedikation ist eine ELGA-Anwendung, daher folgt sie zwingend nachstehenden Grundregeln:

Die Ärztin/Der Arzt (die Pflegeeinrichtung, die Ambulanz, das Spital) muss sich im Wege eines bekannten Identityproviders (IdP), der dem engen Kreis der von ELGA anerkannten IdPs entstammt, identifizieren und bei ELGA im Wege eines abgesicherten Gesundheitsnetzes verschlüsselt anmelden. Das ELGA-Berechtigungssystem überprüft, ob dieser Arzt aktuell in der Liste der in Österreich für ELGA zugelassenen Ärztinnen/Ärzte aufscheint und somit über eine aufrechte Berufs- und ELGA-Berechtigung verfügt. Wenn diese Überprüfung erfolgreich abgeschlossen ist, überprüft das ELGA-Berechtigungssystem, ob diese Person aktuell im Personenregister (Patientenindex) vorhanden ist. Ist auch diese Prüfung erfolgreich, wird im nächsten Schritt geprüft, ob diese Person bei dieser Ärztin/diesem Arzt aktuell einen Behandlungskontakt hat (im konkreten Beispiel, ob in der Ordination dieses Arztes die eCard dieser Person gesteckt wurde). Ist diese Überprüfung ebenfalls erfolgreich abgeschlossen, dann ruft das ELGA-Berechtigungssystem die allenfalls vorhandene Willenserklärung der

Patientin/des Patienten auf. Nur wenn diese Patientin/dieser Patient nicht aus ELGA oder eMedikation hinausoptiert hat und wenn die zugreifende Ärztin/der zugreifende Arzt von der Bürgerin/vom Bürger nicht gesperrt wurde, dann darf die Ärztin/der Arzt die aktuelle Medikation lesen und/oder neue Verordnungen speichern.

E-Medikation ermöglicht es somit, behandelnden Ärztinnen und Ärzten für Patientinnen und Patienten gespeicherte Medikationsdaten abzufragen und die Verordnung weiterer Medikamente zu speichern (verordnete bzw. von Apotheken abzugebende Arzneien sowie nicht verschreibungspflichtige, von Apotheken abzugebende Arzneien [„OTC-Produkte“ – over the counter-Produkte]).

Die Abfrage („Medikationsliste“) bietet der Ärztin/dem Arzt einen Überblick über die bereits vorhandene Medikation und ermöglicht, dieses Wissen in die weitere Behandlung bzw. Folgemedikation einfließen zu lassen.

Das Rezept wird mit einem 2D-Matrix-Code versehen, der in der Apotheke das Einlesen des Rezeptes und in weiterer Folge die Abgabe von Medikamenten ermöglicht. Voraussetzung ist, dass die Patientin/der Patient an ELGA teilnimmt und von ihren/seinen gesetzlich normierten Widerspruchs-, Einschränkungs- und Löschungsrechten nicht Gebrauch gemacht hat (vgl. insbesondere § 15 Abs. 2, § 16 Abs. 1 und 2 GTelG 2012). Zudem muss ihre/seine Identität bestätigt sein und die Ärztin/der Arzt bzw. die Apotheke zum Zugriff autorisiert sein (vgl. § 18 Abs. 4 und Abs. 6 GTelG 2012). Ebenso müssen die Identität der Ärztin/des Arztes bzw. der Apotheke nachgewiesen sein (§ 19 Abs. 2 GTelG 2012).

Apotheken haben im Fall der bloßen Abgabe eines ärztlich verordneten Medikaments lediglich die Berechtigung zur Eintragung des Abgabevermerks (kein „lesender“ Zugriff). Bei Abgabe bestimmter wechselwirkungsrelevanter OTC-Produkte (Liste der Agentur für Gesundheit und Ernährungssicherheit) muss die Apotheke von der Patientin/vom Patienten für den Zugriff autorisiert werden.

Frage 5a: Es handelt sich um

- Daten der ELGA-Teilnehmerin/des ELGA-Teilnehmers: (Identitätsdaten inkl. bereichsspezifisches Personenkennzeichen Gesundheit - bPK-GH zur verschlüsselten Datenverarbeitung inkl. Unterscheidung von anderen Personen, was bei Wechselwirkungsprüfungen sehr wichtig ist),
- Daten der ELGA-Gesundheitsdiensteanbieter (verordnende/r Ärztin/Arzt, abgebende Apotheke; vgl. § 2 Z 10 lit. a bis lit. c GTelG 2012) und
- Medikationsdaten gemäß § 2 Z 9 lit. b iVm § 13 Abs. 3 Z 4 und 5 GTelG 2012 sowie § 14 ELGA-VO 2015.

Frage 5b: Sicherheitsmaßnahmen, um Angriffe auf die Medikationsdaten in ELGA zu verhindern, sind u.a.:

- das ELGA Berechtigungs-System lässt Zugriffe nur durch Berechtigte zu,
- Netzwerktechnologien befinden sich auf dem aktuellen Stand der Technik (z.B. Web Application Firewalls),

- Transportverschlüsselung (TLS),
- zertifikatsbasierte Authentisierung der beteiligten Systeme,
- Verschlüsselte Speicherung der Gesundheitsdaten.

Frage 5c: Die medizinischen Daten sind durch Verschlüsselung geschützt. Auch Mitarbeiterinnen und Mitarbeiter mit Zugriff auf die produktiven Daten (Datenbank-Administratoren) haben keinen Zugriff auf die Gesundheitsdaten in unverschlüsselter Form. Die Verschlüsselungsalgorithmen und Schlüsselstärken entsprechen dem Stand der Technik.

Auf die Regeln zur Behandlung von Datenbeständen und deren Darstellung (um daraus nicht auf konkrete Personen schließen zu können), wie k-Anonymität, *l*-Diversität und Target Record Swapping darf in Hinblick auf nicht personenbezogene Statistiken aus der Aufbereitung anonymisierter Daten ebenfalls hingewiesen werden.

Damit sind die Daten sowohl gegen Angriffe von außen als auch von innen wirksam geschützt.

Frage 9:

Frage 9ii: Unbeschadet der noch offenen Fragen (z.B. wird die aktuelle eGovernment-Architektur in Richtung Blockchain-Technologie geändert) sind dafür im Gesundheitswesen keine grundlegenden Rechtsänderungen erforderlich. Sollte jedoch eine spezifische eHealth-Applikation – wie beispielsweise der eImpfpass – weitere Rollen für aktive Gesundheitsdienstanbieter erforderlich machen (konkret im Beispiel eImpfpass: Amtsärztinnen/Amtsärzte, Schulärztinnen/Schulärzte), dann ist dies mittels einer gesetzlichen Anpassung zu regeln.

Mit freundlichen Grüßen

Mag.[a] Beate Hartinger-Klein

	Unterzeichner	Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz
	Datum/Zeit	2018-08-01T10:41:36+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.	738854333
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2018-08-01T11:11:03+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.	