Stellungnahme der ARGE DATEN zum Entwurf:
Verordnung zur Dokumentation im ambulanten Bereich

INHALT:

1. EINLEITUNG

Ziel des vorliegenden Entwurfs ist die Wahrnehmung der Verpflichtungen, die sich aufgrund des Gesetzes zur Dokumentation im Gesundheitswesen (DokuG) für das Bundesministerium für Gesundheit (BMG) ergeben.

Die DokuVO soll dabei

1. die Erstkonfiguration der Pseudonymerstellungseinheit,
2. die Aufbewahrung der Konfiguration sowie
3. den technisch/organisatorischen Schutz der Pseudonyme regeln.

Diese Punkte werden im vorliegenden Entwurf jedoch nicht gesetzeskonform umgesetzt. Insbesondere wiederspricht der Entwurf § 5a DokuG und wird deshalb abgelehnt.

1.1 Erstkonfiguration der technischen Einheit zur Pseudonymerstellung

Das DokuG hält in § 5a Abs 2 unmissverständlich fest, dass weder dem BMG noch dem Hauptverband der österreichischen Sozialversicherungsträger (Hauptverband) bekannt sein darf, wie Pseudonyme von Leistungsempfängern gebildet werden. Dennoch lässt es die DokuVO in § 6 Abs 4 offen, durch welche Stelle die Erstkonfiguration des Hardware Security Modul (HSM), in welchem die Pseudonyme generiert werden sollen, erfolgen soll. Darüber hinaus soll die Konfiguration des HSM in den Räumlichkeiten des Hauptverbandes unter Anwesenheit eines Vertreters des BMG vorgenommen werden. In Anbetracht der Bestimmungen des DokuG erscheint die Anwesenheit von Vertretern des BMG, bei der Erstkonfiguration des HSM, jedoch gesetzwidrig.

Es wird dringend empfohlen vorzusehen, dass die Erstkonfiguration des HSM von einer unabhängigen Dritten Stelle unter Ausschluss von Vertretern des Hauptverbandes und des BMG durchgeführt wird.

1.2 Aufbewahrung der Erstkonfiguration des HSM

Die in § 5a Abs 2 DokuG vorgesehene Aufgabe der Aufbewahrung des Algorithmus (bzw. Schlüssels), mit welchem die Pseudonyme von Leistungsempfängern generiert werden, soll gem. § 6 Abs 4 DokuVO das Zentrum für sichere Informationstechnologie – Austria (A-SIT) übernehmen. Neben dem A-SIT kommen jedoch zahlreiche andere Unternehmen bzw. Organisationen, darunter insbesondere Zertifizierungsdiensteanbieter, in Frage, die diese Aufgabe übernehmen könnten.

Zur Förderung eines fairen Wettbewerbs wird empfohlen die Aufgabe der sicheren Verwahrung der HSM-Konfiguration öffentlich auszuschreiben.

1.3 Fehlende Verschlüsselung von Pseudonymen

Die in § 6c Abs 1 Z 2 lit b bzw. § 5a Abs 1 Z 1 DokuG vorgesehene Verschlüsselung von generierten Pseudonymen findet sich nicht in der DokuVO wieder.

Es wird empfohlen in der DokuVO festzuhalten, dass Pseudonyme nach deren Generierung zu verschlüsseln sind.

2. VERORDNUNG ZUR DOKUMENTATION IM AMBULANTEN BEREICH IM DETAIL

2.1 § 2 DokuVO – Verschlüsselte Datenübermittlung

Diese Bestimmung sieht vor, dass sämtliche Datenübermittlungen verschlüsselt zu erfolgen haben.

Die durchgängige Verschlüsselung von Daten bei deren Übertragung wird begrüßt.

2.2 § 6 Abs 1 und Abs 2 DokuVO – Generierung der Pseudonyme

§ 6 Abs 1 und Abs 2 DokuVO bestimmen, dass die Generierung von Pseudonymen von Leistungserbringern und Leistungsempfängern innerhalb eines HSM zu erfolgen hat. Die § 6c Abs 1 Z 2 lit b bzw. § 5a Abs 1 Z 1 DokuG bestimmen dabei, dass die im HSM generierten Pseudonyme von Leistungserbringern bzw. Leistungsempfängern zu deren Schutz zusätzlich zu verschlüsseln sind.

In der DokuVO selbst befinden sich diesbezüglich lediglich in den Erläuterungen, die die Datenflüsse im extra- bzw. intramuralen ambulanten Bereich schematisch darstellen, Hinweise auf eine, der Generierung der Pseudonyme folgende - nicht näher beschriebene - „Transportsicherung". Die gesetzlich geforderte Pflicht zur Verschlüsselung der Pseudonyme lässt der Verordnungsentwurf jedoch vermissen.

In § 6 Abs 1 und Abs 2 DokuVO ist festzuhalten, dass Pseudonyme nach deren Generierung verschlüsselt werden müssen.

Bei der Verschlüsselung von Pseudonymen ist zu deren Schutz darauf zu achten, dass die Verschlüsselung gleicher Pseudonyme zu unterschiedlichen Zeitpunkten unterschiedliche Ergebnisse liefert. Dies kann beispielsweise dadurch erreicht werden, dass wie bei der Verschlüsselung von bereichsspezifischen Personenkennzeichen (bPK) als Eingangswert für die Verschlüsselung das generierte Pseudonym, das aktuelle Datum und die aktuelle Uhrzeit dienen. Nach Entschlüsselung können Datum und Uhrzeit entfernt werden und das Pseudonym steht wieder zur Verfügung. Dadurch ist sichergestellt, dass Dritten, die nicht im Besitzt des Schlüssels sind, nicht ausschließlich nur das Pseudonym einer Person nicht bekannt wird, sondern diese auch nicht feststellen können, dass unterschiedliche Leistungsfälle den selben Leistungsempfänger bzw. dieselbe Leistungsempfängerin betreffen. Eine Verschlüsselung ohne sich ändernde Parameter würde lediglich dazu führen, dass ein Pseudonym durch ein anderes ersetzt wird, der Forderung des Gesetzgebers nach dem Schutz der Pseudonyme würde so nicht nachgekommen.

Die Pflicht zur Verschlüsselung von Datenübermittlungen in § 2 DokuVO ist dabei nicht ausreichend um die gesetzliche Pflicht zur Verschlüsselung der Pseudonyme zu erfüllen, da hierbei die Gefahr besteht, dass Pseudonyme dem Hauptverband bekannt werden.

2.3 § 6 Abs 3 DokuVO – Erstkonfiguration des HSM

Vorgesehen ist, dass die erstmalige Konfiguration des HSM in den Räumlichkeiten der beim Hauptverband eingerichteten Pseudonymisierungsstelle unter Anwesenheit einer Vertreterin bzw. eines Vertreters des BMG und lediglich unter der Aufsicht des A-SIT zu erfolgen hat. Welche Stelle

(Hauptverband, BMG, A-SIT oder ein unabhängiger Dritter) die tatsächliche Konfiguration des HSM durchführt geht nicht aus dem Verordnungstext hervor.

§ 5a Abs 2 DokuG schreibt jedoch vor, dass der für die Generierung der Pseudonyme verwendete Algorithmus dem BMG und dem Hauptverband nicht bekannt sein darf. Weiters muss der Algorithmus von einer unabhängigen dritten Stelle sicher verwahrt werden. Sowohl das BMG als auch der Hauptverband kommen somit nicht als geeignete Stelle zur Konfiguration des HSM in Frage.

Aus der DokuVO muss klar hervorgehen, dass eine dritte unabhängige Stelle die Erstkonfiguration des HSM durchführen muss.

Geeignete Stellen für die Konfiguration des HSM stellen beispielsweise Zertifizierungsdiensteanbieter iSd Signaturgesetzes dar.

Aufgrund von § 5a Abs 2 DokuG, wonach sowohl dem BMG als auch dem Hauptverband der Algorithmus zur Generierung der Pseudonyme nicht bekannt sein darf, erscheint die Anwesenheit einer Vertreterin bzw. eines Vertreters des BMG als gesetzwidrig.

§ 6 Abs 3 DokuVO hat festzuhalten, dass bei der Erstkonfiguration des HSM keine Vertreter des BMG oder des Hauptverbandes anwesend sein dürfen.

Alternativ muss aus der DokuVO klar hervorgehen, durch welche Maßnahmen sichergestellt wird, dass anwesenden Vertretern des BMG bzw. des Hauptverbandes der Algorithmus zur Generierung der Pseudonyme nicht bekannt wird.

2.4 § 6 Abs 4 DokuVO – Sichere Verwahrung der HSM Konfiguration

Gemäß § 5a Abs 2 DokuG ist der Algorithmus zur Generierung von Pseudonymen von einer unabhängigen dritten Stelle sicher zu verwahren. Gemäß § 6 Abs 4 DokuVO soll es sich dabei um das A-SIT handeln.

Zur Verwahrung der HSM-Konfiguration kommen grundsätzlich viele Organisationen in Frage, neben Zertifizierungsdiensteanbietern könnten beispielsweise auch Notare die Verwahrung übernehmen. Zur Förderung eines fairen Wettbewerbs sollten daher sämtliche Unternehmen, die in der Lage sind eine sichere und unabhängige Verwahrung der HSM-Konfiguration zu garantieren, bei der Vergabe der gesetzlich vorgesehenen Aufgabe bedacht werden.

§ 6 Abs 4 DokuVO hat, zur Förderung des fairen Wettbewerbs, die öffentliche Ausschreibung der sicheren Verwahrung der HSM-Konfiguration vorzusehen.

ARGE DATEN

VO Dokumentation im ambulanten Bereich
E-Mail: thomas.worel@bmg.gv.at

An das
Bundesministerium für Gesundheit

Radetzkystraße 2
1031 Wien

Wien, 8. August 2013

Betreff: Zeichen: BMG-71100/0008-I/B/12/2013
Stellungnahme der ARGE DATEN zum
Entwurf einer Verordnung zur Dokumentation im ambulanten Bereich (DokuVO).

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

elektronisch erstellt
Dr. Hans G. Zeger (Obmann)

Anlage:
Stellungnahme

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/privacy/gesetze veröffentlicht.