ePA, DMS, SNOMED-CT und ePA-DMS

1. Unsicherheitsfaktoren durch die Anmeldung am ePA-System mit mobilen Geräten (Smartphone, Tablet) auf Basis der im Gerät gebildeten Device-ID (IMEI)?

2. Die Rolle der Device-ID (IMEI) Auswertung in neueren Verfahren zur Identifizierung eines mobilen Endgerätes in einem digitalen-zellulären Mobilfunknetz

3. Aspekte der ePA als datenbank-basierendes Dokumenten-Management-System (DMS) in Beziehung zur semantischen Datenverarbeitung und SNOMED-CT

1./2.

Die Grundlagen der semantischen Datenverarbeitung und technischen Prozesse sind eine lohnende Quelle für die Analyse aller eHealth-Projekte in Deutschland.

Im dem öffentlich zugänglichen Dokument, mit dem Titel "Spezifikation Autorisierung ePA", dass sich an, ich zitiere:

...Hersteller und Anbieter der Komponente "Autorisierung" für die Nutzung in einem ePA-Aktensystem sowie an Hersteller und Anbieter von Produkttypen ePA, die Schnittstellen der Komponente "Autorisierung" umsetzen wollen

richtet, siehe

https://www.vesta-gematik.de/standard/formhandler/324/gemSpec_Autorisierung_V1_0_0.pdf

in dem die Anmeldeprozesse von mobilen Endgeräten beschrieben werden, wird ein Faktor der Verschlüsselung genannt, der aus der einmaligen Hardware-ID (IMEI) des mobilen Endgerätes gebildet wird.

Zitat Wikipedia:

Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät weltweit eindeutig identifiziert werden kann

https://de.wikipedia.org/wiki/International_Mobile_Equipment_Identity

Siehe im Dokument

https://www.vesta-gematik.de/standard/formhandler/324/gemSpec_Autorisierung_V1_0_0.pdf

Kapitel 6.4 und 6.5 ab Seite 54 von 67

mit den Titeln:

"Hardware-Merkmal der Komponente Autorisierung"

In dem Dokument gemSpec_Autorisierung_V1_0_0.pdf wird die IMEI als DeviceID bezeichnet, die die Gerätekennung eines vom Nutzer verwendeten Gerätes enthält .

Hieraus ergeben sich drei Gesichtspunkte, die einmal die kryptografische Schlüsselbildung (a.) betrifft, zweitens die Möglichkeiten zur globalen Identifizierung (b.) der mobilen Endgeräte und der Nachverfolgbarkeit der Bewegungen des Menschen und drittens der Rolle der Metaelemente und Metainformationen (c.) in den Verflechtungen der semantischen Datenverarbeitung.

a.
Bei der Bildung von Schlüsseln ist es schon lange üblich vorhandene Hardwareinformationen der Geräte mitzunutzen, damit eine eindeutige Zuordnung und Absicherung der Berechtigungen, für die Nutzung einer Software oder wie im vorliegenden Fall des Zugangs zum ePA-System, ermöglicht wird. So wird z.B. bei der Lizenzierung von Microsoftprodukten, neben vielen anderen Faktoren, die eindeutige MAC-Adresse des Computers genutzt.

Die Nutzung der IMEI als ein Faktor für die Anmeldung an der ePA folgt also beliebten Methoden und betrifft eine leicht zugängliche und im Prinzip auch veränderbare Information in der Hardware, siehe

https://www.giga.de/ratgeber/specials/imei-aendern-wie-geht-das-und-ist-das-wechseln-der-seriennummer-bei-smartphones-und-tablets-legal/

Allgemeine Information /Zitat:

Bei der Anmeldung ins Mobilfunknetz wird die IMEI-Seriennummer an den Mobilfunkbetreiber übermittelt. Dieser gleicht sie mit dem Equipment ID Register (EIR) ab, darin befinden sich gesperrte Nummern, beispielsweise aufgrund von Diebstählen.

Auch wenn es strafbar ist prinzipiell kann die IMEI mit einem Hex Editor wie dem Hex Editor Free für Android auf dem Smartphone geändert werden.

Normalerweise sollten die Hardwareinformationen versteckt werden, so gibt es schon lange Maßnahmen um die Mac-Adresse in Netzwerken zu verschleiern, siehe z.B.

https://tails.boum.org/doc/first_steps/welcome_screen/mac_spoofing/index.de.html

Im Falle der IMEI bei mobilen Endgeräten liegt nun eine andere Situation vor, die mit der schönen neuen Welt zutun hat in der wir leben und in der es zum Normalzustand werden soll permanent lokalisiert zu werden und in der es normal ist, dass alle anfallenden Daten – meta-informationalisiert - an zentrale Mastersysteme weitergegeben werden, die IMEI kann somit nicht versteckt werden, weil sie ein Bestandteil der Kommunikations- und Datenverarbeitungsprozesse darstellt.

Es stellt sich also mehrere Fragen, welche zukünftigen Gefahren und Mißbrauchsmöglichkeiten sich für das ePA-System aus der offen einsehbaren IMEI ergeben. Fragen sind:

Wie stark ist ein Verschlüsselung- und Zugriffsverfahren, was die IMEI nutzt?

Welche evolutionären technischen Analysen dieser Aspekte wurden hier für das ePA-System durchgeführt?

b)
Besonders wichtig ist sich hier an dieser Stelle klar zu machen wohin die Reise der Nachverfolgbarkeit mit mobilen Endgeräten geht. Bisher wurden bei der sogenannten Funkzellenortung bisher immer nur die SIM-Karten über die Telefonnummer geortet. In neueren Verfahren ist das Ziel eine Identifizierung für Endgeräte in Mobilfunknetzen zu ermöglichen, die nach anderen Standards als GSM arbeiten, in der das zu identifizierende Endgerät nach seiner IMSI (International Mobile Subscriber Identity) oder seiner IMEI (International Mobile Equipment Identity) gefragt wird

Siehe neuere Möglichkeiten des IMEI-Trackings im Patentstreit der Thales Group, Anbieter von Sicherheitstechnologien:

https://www.epo.org/law-practice/case-law-appeals/recent/t132032du1.html

und dort über den Link zum Text:

https://www.epo.org/law-practice/case-law-appeals/pdf/t132032du1.pdf

Eine **global** eindeutige Nummer des Smartphone, ein Verfahren zur Identifizierung des Smartphones mit Hilfe der IMEI, die gleichzeitig als Metatdateninformation im ePA-System abgespeichert wird muss sehr tief untersucht werden, in Bezug auf mögliche Gefährdungen durch Data- und Textmining-Verfahren mit Hilfe von Querweisen in Datenquellen aller Art.

Zitat Wikipedia:

Unter Data-Mining [ˈdeɪtə ˈmaɪnɪŋ] (von englisch data mining, aus englisch data ‚Daten' und englisch mine ‚graben', ‚abbauen', ‚fördern')[1] versteht man die systematische Anwendung statistischer Methoden auf große Datenbestände (insbesondere „Big Data" bzw. Massendaten) mit dem Ziel, neue Querverbindungen und Trends zu erkennen

https://de.wikipedia.org/wiki/Data-Mining
https://de.wikipedia.org/wiki/Text_Mining

c.
Alle beschriebenen Vorgängen basieren heute auf Metadaten und Metainformationslementen, wie dem Element -DeviceID- in der "Spezifikation Autorisierung ePA". Somit muss das Vorkommen des Informationselementes auch in den möglichen Verkettungen der Metadatenpools und Klassifikationssysteme in der Telematikinfrastruktur untersucht werden.

3. Aspekte der ePA als datenbank-basierendes Dokumenten-Management-System (DMS) in Beziehung zur semantischen Datenverarbeitung und SNOMED-CT

Was ist Snomed-CT, siehe

https://www.healthcare-computing.de/was-ist-snomed-ct-a-912647/

Siehe hier, ich zitiere:

Doch nicht nur zum „Lückenschließen" zwischen bestehenden Codiersystemen (Katalogen) und zur automatisierten „Übersetzung" bereits strukturiert vorliegender Information benötigt man SNOMED CT. Möchte man Freitexte wie z.B. Arztbriefe automatisiert analysieren, ist die treffende „Übersetzung" in computerlesbare Einheiten durch SNOMED CT gewährleistet.

Denn die Aufbereitung natürlichsprachlicher (freitextlicher) Information zur Datenanalyse erfordert zwingend ein Terminologiesystem mit starker Fähigkeit

zur sog. Postkoordination: D.h. freitextlich formulierte Informationseinheiten können, in ihre terminologischen Bausteine zerlegt, in einzelne Codes überführt werden, die in ihrer Gesamtheit genau den freitextlichen formulierten Begriff repräsentieren – ohne dass diese Information bereits „vorgedacht" in einem Katalog existieren muss. Gerade diesbezüglich ist SNOMED CT weitgehend konkurrenzlos und daher als grundlegende Referenzterminologie für die Digitalisierung in der medizinischen Forschung wie in der Patientenversorgung sehr geeignet.

(Der Einsatz von SNOMED-CT, also die Anwendung der Nomenklatur, ermöglicht Freitexte in losgelöste Informationseinheiten zu zerlegen)

Eine weitere übersichtliche Beschreibung findet sich in dem Dokument TMF_B.6_SNOMED_CT_Dewenter_Thun.pdf (bitte den Namen und das Dokument über google suchen).

Wir haben auf der einen Seite ein ePA-Dokumentenmanagement-System, in der ausschließlich verschlüsselte Dokumente gespeichert werden sollen und auf der anderen Seite die Tatsache die ePA auf Basis von SNOMED-CT umzusetzen. Siehe

https://www.bvitg.de/elektronische-patientenakte-weiter/

Elektronische Patientenakte - Wie geht's weiter - BViTG
www.bvitg.de › elektronische-patientenakte-weiter
vom 20.11.2019 -

Wie passt das zusammen? Welche Folgen hat dies für die Systematik eigentlich nicht zugänglicher Daten? Welche Informationen und Metadaten bleiben dabei unverschlüsselt?

Um ein Verständnis für diese Fragen und Sachverhalte zu erlangen muss man berücksichtigen, dass wir es mit einem vielschichtigen IT-System zutun haben, in der es verschiedene gestufte Öffnungs- und Zugriffmöglichkeiten auf die Daten geben soll, wie z.B. die Freigabe zu Forschungszwecken. Auch ist zu berücksichtigen, dass nach der Durchführung einer Pseudonymisierung und Anonymisierung von Daten, bestimmte Anteile von Daten, wie auch Metadaten, situationsabhängig verarbeitet werden dürfen.

Das heißt es entstehen sehr viele nutzbare Daten, die unabhängig vom Nutzer erhoben werden. Die Klassifikation der ePA-Daten mit der medizinischen Terminologie SNOMED-CT wird auf internationaler Ebene als semantische Komponente für den interoperablen Austausch von Gesundheitsdaten favorisiert.

Die hervorgehobene Interoperabilät der anfallenden Daten in der Telematikinfrastruktur soll mit SNOMED-CT weiter verbessert werden und führt zu einer weiter gesteigerten Menge nutzbarer Daten.

Die Abspeicherung der ePA-Daten erfolgt in datenbankbasierten DMS-Speichern der DMS-Provider und damit ist derzeit nicht ausreichend transparent nachvollziehbar welche Daten in welchen Verflechtungen produziert werden und welche dadurch in welchen Schichten zugänglich, also verkettbar und auswertbar sind.

Dabei ist zu berücksichtigen, dass eine Vorstrukturierung und Klassifikation der Datenelemente in den ePA-Dokumenten erforderlich ist, da eine logische Beziehung zwischen der Datenbankstruktur und der Metadatenverarbeitung bestehen muss. Es gibt verschiedene Wege dies zu bewerkstelligen, wenn z.B. Word oder PDF-Dokumente vorliegen können diese als Objekte abgepeichert werden (Repository des DMS) und parallel die darin enthalten Textinformationen in eine erweiterte Struktur, auf Basis der Erweiterungssprache XML gebracht und/ oder mit SNOMED-CT klassifiziert werden, was letztlich auch wiederum bedeutet das Textinformationen extrahiert werden und in SNOMED-CT Container gepackt und referentiell verknüpft werden über Marker oder Codesysteme, siehe z.B.

https://wiki.hl7.de/index.php?title=1.3.6.1.4.1.19376.1.3.11.8

Die Kombination von Datenbanksystemen mit den semantischen Verarbeitungsmethoden und Klassifikationssystemen hat bereits einen gigantischen Informationspool in der Telematikinfrastruktur eröffnet, der immer noch nicht ausreichend erforscht worden ist.

Das heißt es entstehen riesige Mengen an Datenbank- und Metadateninformationen zu jeder elektronischen Akte der Patienten/innen, alleine durch die Nutzung der an die Telematikinfrastruktur angepassten Software-Systeme im Gesundheitswesen und den damit wirksamen eingesetzten Erweiterungstechologien.

Die tieferen Informationen des ePA-Systems sind in Wirklichkeit öffentlich nicht verfügbar und würden eine sehr aufwendige Systemanalyse, sowie Beschreibung und Visualisierung des in die Telematikinfrastuktur eingebetteten ePA-Systems voraussetzen.

Wir folgen hinsichtlich der Umsetzung der IT-Systeme, wie der Telematikinfrastuktur und der ePA, der Automation der Software, ohne uns einen kompletten Überblick verschaffen zu können und nehmen damit in Kauf die sensibelsten Daten, die einen Mensch ausmachen, zu verkaufen.

Abschließend will ich erneut auf einen wenig untersuchten Punkt der ePA eingehen, den der Freiwilligkeit. Geplant ist ja erst, wenn der/die Patient/in einwilligt einen Datensatz in einem ePA-Dokumenten-Management-System eines ePA-Prodividers anzulegen um dann die elektronischen Patentienakten, die in unterschiedlichen Formaten, wie Word, PDF, u.v.m. vorliegen, im ePA-Pool abzuspeichern. Hier ist es erforderlich zu untersuchen welche Metadaten-

Vorverarbeitung der Patientendaten bereits nach semantischen Standards erfolgt und wo diese Daten abgespeichert werden. Sollte bereits einer Vorverarbeitung, z.B. nach SNOMED-CT, über die Arztsoftware und ein cloud-basiertes Produkt stattfinden, dann existieren bereits Daten in der Form, die es eigentlich gilt abzulehnen, da auch die ePA abgelehnt wird. Weiterhin bedeutet die Produktion von Daten nach gleichen Standards, auch dass sie prinzipiell über die verschiedenen Datenpools hinweg verkettet ausgewertet werden können.

Es muss immer wieder betont werden wie wenig wir uns vorstellen können welche Möglichkeiten mit den hochmodernen und im Grunde genommen innovativen Datenverarbeitungstechnologien entstehen. Auch erfahren wir keine Unterstützung von Seiten der Projektleiter, denn eine vollständige Sicht auf die Datenverarbeitung in der Telematikinfrastruktur ist nicht erwünscht. Im Gegenteil, es wird integriert und installiert um möglichst viele Optionen schaffen und möglichst viele verwertbare Informationen zu produzieren.

Hier gilt wieder, die Nutzung der Telematikinfrastuktur und ihrer Anwendungen bedeutet sich der Verarbeitung der Daten nicht entziehen zu können (Stichworte: Opt In versus Opt Out).

23.8.2020

Rolf D. Lenkewitz
87769 Oberrieden
0163170 68 09

www.rdlenkewitz.eu

http://www.rdlenkewitz.eu/DSGVO/dsgvo.html