Ehealth-Anwendungen: Jetzt wird die Datenproduktion erst richtig angeheizt

| ePA, KIM, Notfalldatensatz, elektronischer Medikationsplan, Arztbriefe |
| Versichertenindividuelle Zugriffe mit Rollen- und Rechteverwaltung |
| Wer liefert den Überblick über die produzierten Metadaten? |

In einem der unzähligen Artikel zur elektronischen Patientenakte wurde berichtet, dass der Notfalldatensatz, der elektronische Medikationsplan, sowie elektronische Arztbriefe, auf der ePA gesichert werden können. Und es wurde versichert, dass der Arzt die Datenspeicherung auf der ePA vornimmt und Daten niemals automatisch ohne Wissen des Arztes übertragen werden. Das Mantra der Freiwilligkeit der Nutzung der ePA, auch intoniert in diesem Artikel, begleitet die Umsetzung der Telematikinfrastuktur seit langem, aber wie sieht die Wirklichkeit aus?

Die Formulierung: -Datenspeicherung auf der ePA- suggeriert eine zusammenhängende Akte, in die Nähe gestellt zu analogen Akten, bzw. zu kompakten elektronischen Dokumenten, wie wir sie heute in der Regel nutzen. Es handelt sich aber bei der ePA , der elektronische Patientenakte, eher um eine mächtige Client-Server Software als ein singuläres Datenobjekt, die einen Einstiegspunkt in eine Datensammlung ohne Begrenzung darstellt. Eine Datensammlung, die alle Arten an Arztdokumenten und medizinischen Informationen enthalten kann und über eine große Datenbank und ein DMS-Dokumenten-Management-System des ePA-Providers an die Telematikinfrastruktur angebunden wird.

Mit dem Einsatz eines DokumentenManagementSystem kommen typische Komponenten zum Einsatz, wie z.B. ein DMS-Repository, ein Zugriffsspeicher mit erweiterten Möglichkeiten und Funktionen für die bessere Handhabung riesiger Dokumentenmengen.

siehe allgemeine Informationen zu einem Dokumentenmanagementsystem (DMS):

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

Die ePA ist nach Aussen ein Stück Software, der grafisch und funktional aufbereitete Endpunkt für die Datensammlung in einem DokumentenManagementSystem, mit einem Inhaltsverzeichnis.

Der Zusammenhalt der gesammelten Dokumente und Daten wird dabei über lesbare und nicht verschlüsselte Metadaten realisiert, das existierende versichertenindividuelle Inhaltsverzeichnis in der grafischen Oberfläche der ePA, im Hintergrund mit den Metadaten verknüpft, ermöglicht die Übersicht und Durchsuchung der Dokumenten- und Informationsansammlung.

Die ePA ist somit der referentielle Endpunkt eines weiteren großen IT-Systems und reproduziert -just in time- aus den Einträgen der DMS-Datenbank und den DMS-Speichern einen Zugriff auf die Datenkopien der Primärsysteme (Ärzte, Apotheken, Krankenhäuser, usw.).

Wenn man nun berechtigterweise nicht mehr zufrieden ist mit der Aussage, das Dokumente -auf der ePA- abgespeichert werden, kann im Internet der Frage nachgehen: Wo werden die Daten in der ePA gespeichert? und erhält dann allmählich die notwendigen Antworten, die eine bessere Vorstellung ermöglichen was die ePA-Anwendung eigentlich ist.

Hier beantwortet ein Mitarbeiter der gematik die Frage:

https://www.serapion.de/interview-mit-holm-diening-gematik-wo-werden-die-daten-der-epa-gespeichert/

Antworten aus dem Interview, ich zitiere:

*HD: Gemäß unserer Spezifikation **erfolgt die Datenspeicherung** pro teilnehmendem Versicherten **zentral bei einem der zugelassenen Anbieter.** // Wir rechnen mit einer kleineren zweistelligen Zahl von durch die gematik zugelassenen Aktenbetreibern.*

In der deutschen ePA ***wird es zwar eine zentrale Datenspeicherung beim Anbieter des jeweiligen Versicherten geben, allerdings haben wir Rollen, die Zugriff auf alle Daten haben, gänzlich ausgeschlossen****. Die gespeicherten Dokumente sind ohnehin Ende-zu-Ende verschlüsselt und werden erst beim Arzt bzw. Versicherten lesbar gemacht.* ***Die Metadaten sind versichertenindividuell durchsuchbar, der Zugriff des Aktenbetreibers, auch über privilegierte Systemprozesse, ist aber durch die Ausführungsumgebung technisch ausgeschlossen.***

Die ePA bedeutet also eine zentrale Datenspeicherung mit einem für die Versicherten lesbaren Inhaltsverzeichnis, was über Rollenprofile ausgeschlossen, bzw. geschützt wird. Die Umsetzung einer Rechteverwaltung und die Zuordnung von Rollen ist eine seit langem gängige Methode gezielt Zugriffe auf bestimmte Ordner und Dateien zu erlauben oder zu verhindern. Eines der bekanntesten und weit verbreitesten Rechteverwaltungen ist das von Linux und das von Microsoft, das Active-Directory. Rechteverwaltungen sind generell immer eine Fehlerquelle und es Bedarf ständiger und aufmerksamer administrativer Arbeit, damit hier möglichst keine Fehler entstehen, das bedeutet aber nicht das Fehler hier ausgeschlossen werden können.

Weitere Punkte sind die zugegebene Zentralität der Dokumenten- und Datensammlungen und das bisher wenig beachtetete Problem, dass die begleitenden Metadaten lesbar und durchsuchbar sein müssen, damit der Versicherter -versichertenindividuell- über ein Inhaltsverzeichnis nachvollziehen kann welche Dokumente und Informationen existieren. Dies bedeutet auch, die Metadaten, mit denen die Übersicht realisiert wird bei einem zentralen ePA-Provider für das ePA-Dokumenten-Management-System, werden für viele Versicherte aufaddiert. Dies ist eine weitere ernstzunehmende Gefahrenquelle weil über Metadaten ermittelt werden kann welche verschlüsselten Dokumente zu einem Versicherten existieren. Man muss hier berücksichtigen, dass über die Nutzung der ePA auch ein Klassifikationssystem greift welches die in das DMS hochgeladenen Dokumente klassifiziert und strukturiert einordnet. Es entstehen also neben den simplen Informationen zu dem Dokument, wie z.B. der Name des Dokumentes oder dem Titel, samt der referentiellen Zuordnung der Dokumente zur Versicherten-ID des Versicherten, eine schematische Einordnung, die eine Klassifikation z.B. nach Medizinbereichen ermöglicht.

Diese Klassifikationen und die daraus resultierende Strukturierung können Sie hier über diesen Artikel ansatzweise nachvollziehen:

https://www.it-zoom.de/it-director/e/schneller-zugriff-auf-die-elektronische-patientenakte-10063/

Die Verschlüsselung der Daten ist in Bezug auf die vollständige Systematik und Funktionsumfang der vernetzten ePA-DMS Anwendung vollkommen unzureichend. Wir müssen stets immer den Anfangs- und Endpunkt, vor der Verschlüsselung und nach der Entschlüsselung der Dokumente und Daten, betrachten und immer paralell aufklären welche Metadaten und lesbare Informationen entstehen und wie sie verknüpft sind .

Alleine der Titel eines medizinischen Dokumentes in einem lesbaren Inhaltsverzeichnis kann sehr aufschlussreich sein!

Meine Hinweise auf die Systematik der ePA-Anwendung ersetzen nicht die fehlende detaillierte Beschreibung und erst recht nicht die fehlende Schwachstellen-Analyse. Und einfach so in dieser Situation auszuschließen dass keine unbeabsichtigte Datenübertragung in die ePA erfolgen kann ist eine reine Schutzbehauptung deren gründliche Überprüfung aussteht. So ist es mehr als wahrscheinlich dass durch die fehlenden Systemanalysen und die hohe Komplexität der Technologien es jederzeit zu neuartigen Software- und Systemfehlern kommen kann, die eine unbeabsichtigte Datenübertragung in die ePA auslösen können.

Neben der Nennung der Schwachpunkte der Rollen- und Rechteverwaltung und der lesbaren und durchsuchbaren Inhaltsverzeichnisse sollten wir uns die Metadatenverarbeitung der medizinischen und klinischen Dokumente noch etwas genauer anschauen.

Im Rahmen der Arztbriefe gelten die Grundlagen der Clinical Documentl Architecture (CDA) und für die Umsetzung der Arztbriefe innerhalb der TI und ePA soll der neue Standard SNOMED-CT angewendet werden.

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

*Zitat: Die **Clinical Document Architecture (CDA)** ist ein von HL7 erarbeiteter, auf XML basierender Standard für den Austausch und die Speicherung klinischer Inhalte. Dabei entspricht ein CDA-Dokument einem klinischen Dokument (z. B. Arztbrief, Befundbericht). Es erfolgt keine Zusammenfassung mehrerer Dokumente wie in einer Patientenakte.*

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

*Zitat: Die **Systematisierte Nomenklatur der Medizin (SNOMED)** (englisch Systematized Nomenclature of Medicine) ist eine Familie medizinischer Terminologiesysteme.*

Jetzt in diesem Moment der Systembeschreibungen liegen bereits mehrere Metadatensysteme vor die Metadaten produzieren und in unterschiedlichen IT-Systemen abspeichern:

- eGK und HBA mit Konnektor
- PVS/AVS (Praxisverwaltungssoftware, Apotheker-Software)
- ePA-Dokumenten-Management-System und DMS-Datenbanken
- das ePA-Frontend, eine graphische Software als Einstiegsmaske für die Nutzung der Funktionen, wie dem versichertenindividuellen Inhaltsverzeichnis
- Arztbriefe auf SNOMED-CT Basis

Betrachten wir nur die Arztbriefe, hierbei geht es um die Kernstücke der klinisch-medizinischen Dokumentenverarbeitung, es geht wieder um neue Begriffe und Standards, wie dem IHE ITI XDS Standard. Und es bedeutet hinsichtlich der Metadatenverarbeitung ein weitere massive Steigerung der Metainformationselemente, deren Anzahl sich **im 5-7-stelligen Bereich** bewegen können. Ohne jetzt näher darauf einzugehen bedeutet also jeder neue Einstiegspunkt in beteiligte Technologien und Standards eine exponentielle Steigerung des Anspruchs an Wissen und Informationen.

Siehe Links:

https://wiki.hl7.de/index.php?title=cdaab2:Umsetzungsstufen

http://wiki.hl7.de/index.php?title=IG:Arztbrief_2014

https://www.vesta-gematik.de/standard/formhandler/324/gemSpec_DM_ePA_V1_0_0.pdf

Zu berücksichtigen ist, dass die Vorverarbeitung mit SNOMED-CT den Inhalt der Arztbriefe semantisch und ontologisch erweitert und danach über den Upload in das ePA-System eine weitere Metadatenverarbeitung stattfindet. Hieraus ergeben sich interessante Fragen wenn SNOMED-CT Metadaten in dem einem Datenpool **prinzipiell** mit den Metadaten aus dem anderen Pool des ePA-Systems kombiniert ausgewertet werden. Diese potentiellen Möglichkeiten, die im Moment eine naheliegende aber theoretische Option darstellen, können nur dann nachgewiesen werden wenn die komplette Systematik der ineinander verschachtelten Systeme offen gelegt ist. Es gibt aber leider höhere Wahrscheinlichkeiten für Cross Over Auswertungen von unterschiedlichen Metadatenpools, die an allen möglichen Stellen in der Telematikinfrastruktur entstehen. Dies ist ein Thema moderner Informationswissenschaft in der die semantische und ontologische und KI-basierende Datenverarbeitung vollkommen neue Möglichkeiten schafft. Auch dürfen wir nicht vergessen, der Ausbau der Telematikinfrastruktur ist sehr sehr offen und grenzenlos was die geschaffenen Datenverarbeitungs-Optionen und die Weiterentwicklung generell angeht. Hier wird sehr viel umgesetzt was im Moment nicht überblickt werden kann hinsichtlich dann weiterer gesteigerter Möglichkeiten, die womöglich erst dann entdeckt werden.

Siehe hier mein Artikel:

http://www.rdlenkewitz.eu/html/pdf/snomedct.pdf

Ein Arzt hat während der Vorarbeit zu diesem Artikel z.B. folgende naheliegenden Fragen gestellt:

Wichtig wäre tatsächlich eine kompakte, für (uns) Laien verständliche Erläuterung,

1. *ob etwa das e-Rezept oder ein Arztbrief vor dem elektronischen Versand schon "abgezogen" bzw. ausgewertet werden können, und.*

2. *inwiefern bei/vor der Verschlüsselung eben auch Metadaten entstehen (z. B. welche?), die wo dann abgreifbar bzw. auswertbar wären, und.*

3. *ob dann von einem Versand von Arztbriefen über KIM abgesehen werden sollte (angeblich Versand ähnlich wie Mail. Aber wie verschlüsselte Mail?).*

Zu 1.

Ein Hackerangriff von Aussen oder ein Zugriff von Innentätern, die Zugriff auf ein Arztverwaltungssystem haben und dadurch auch offene VPN-Verbindungen sehen können sind wahrscheinliche Szenarien. Auch sind Szenarien denkbar wo ein Versicherter sein lesbares Inhaltsverzeichnis der ePA anschaut und ein Angreifer dies mitliest oder über einen Keylogger die Tastatureingaben erfasst. Eine Auswertung ist dann in unterschiedlichen Formen möglich.

Zu 2.

Vor der Verschlüsselung entstehen Software- und Hardware-seitig sehr viele Metadaten, dies ist nachgewiesen worden aber welche Metadaten entstehen und verknüpft werden können, darüber können nur die Hersteller der Software und die Betreiber der IT-Systeme erschöpfende Antworten geben.

Und damit sind wir bei einem der wichtigsten Punkte und Herausforderungen in der schönen neuen Welt des neuen Gesundheitssystems, der Telematikinfrastruktur und der semantischen Datenverarbeitung mit Metadaten:

Die Hersteller dieser gesellschaftlich bedeutenden IT-Systeme, die unsere sensibelsten und schützenswertesten Daten verwalten wollen, müssen uns Bürgern die fehlende Übersicht über die Metadaten in einer verständlichen und nachvollziehbaren Form liefern!

Natürlich können wir Kritiker von Aussen über die frei zugänglichen technischen Dokumentationen eine Ermittlung der Metadaten durchführen, soweit wir kommen, dies wird aber immer unzureichend sein und dafür gibt es mehrere gravierende Gründe:

1. Es existieren noch keine Lösungen und Konzepte die in der Läge wären die integrierte Metadatenverarbeitung und die Verkettungen über die eHealth-Anwendungen und kombinierten IT-Systeme hinweg in für Laien verständlicher Form zu beschreiben und zu visualisieren

2. Es gibt keine eindeutige gesetzliche Anordnung die Metadatenverarbeitung **vollständig** in der interaktiven Systematik eines IT-Systems, wie der Telematikinfrastruktur, aufzuschlüsseln oder gar auf Basis der DSGVO und einer Datenfolgeabschätzung über ein rudimentäres Maß hinaus zu bearbeiten.

3. Die Metadatenverarbeitung wird von den System- und Softwareentwicklern als teilweise fertige Komponentenwelt mit fertigen Funktionen integriert und wird nicht vollständig nach aussen kommuniziert, als Teil der sensiblen Bereiche der Anwendung, insbesondere im Bereich der Datenbank-Systematik und der Auswertung und Weiterverarbeitung der Metadaten an dieser Stelle!

4. Die vernetzten ineinandergreifenden Systeme wie z.B. die PVS/AVS-Software auf der einen Seite und die ePA-Systeme der ePA-Provider auf der anderen Seite werden keiner system-übergreifenden Analyse und Darstellung der Metadatenverarbeitung unterzogen

5. Die entstehenden Metadaten-Pools werden erst nachträglich weiter ausgewertet und verknüpft, wie dies für die Umsetzung der KI-Prozesse auf die Telematikinfrastruktur angekündigt ist

6. Der zeitliche und personelle Aufwand die Metadatenverarbeitung des größten IT-Projektes der Welt aufzuschlüsseln ist unvorstellbar hoch.

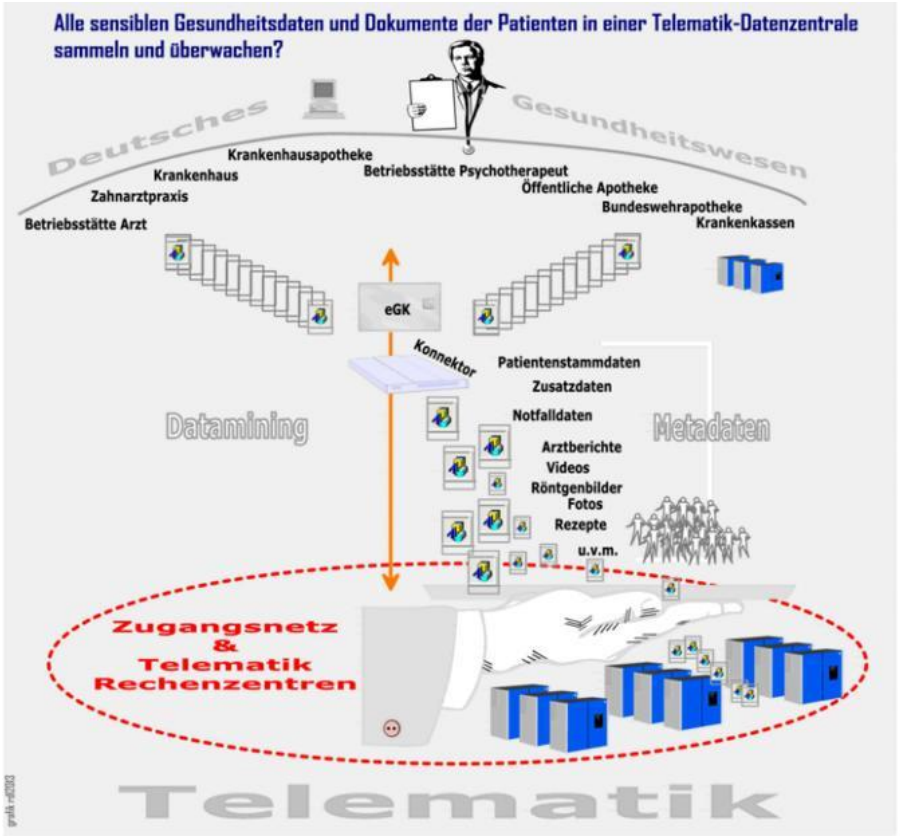
Zu 3.

Der Versand von Arztbriefen über KIM unterliegt der Tatsache einer proprietären Software innerhalb eines zentralistischen Mastersystems der Telematikinfrastruktur. Auch hier gilt, es fehlen die Informationen über den erhobenen Umfang der begleitenden Datenproduktion, inkl. der Metadaten.

Die Frage nach Alternativen für die Verschlüsselung von Daten und dem Versand ergeben sich aus den Angeboten freier Software die für diese Anforderungen zur Verfügung steht.

Wir müssen uns auf das Konzentrieren was machbar ist im Engagement gegen ein IT-Zwangssystem und wir können soweit aufklären wie dies im ehrenamtlichen Engagement neben Job und Familie möglich ist, daher liegt der besondere Wert in der reinen Erkenntnis der Bedeutung und Gefährlichkeit der Metadaten, der Benennung der ungeheuren großen Anzahl der Metadaten und dem Umstand, dass die Datenproduktion jetzt erst richtig anheizt wird!

rdl



Oberrieden, 29.10.2020 Rolf D. Lenkewitz 87769 Oberrieden 0163170 68 09 www.rdlenkewitz.eu http://www.rdlenkewitz.eu/DSGVO/dsgvo.html