Die miteinander verzahnten Paradigmenwechsel im Gesundheitswesen hin zu pervasiver sowie personalisierter Versorgung erfordern möglichst umfassende Interoperabilität zwischen verschiedenen Organisationen und Domänen bei Verknüpfung unterschiedlicher Prozesse und Datenverwendungszwecke (z.B. klinische Versorgung und Forschung als Secondary Use). Akteure können Personen, Organisationen, aber auch Geräte, Anwendungen oder Komponenten sein. Die resultierenden diversifizierten, hochdynamischen, hochkomplexen und verteilten Geschäftsprozesse erfordern eine massive Unterstützung durch Informations- und Kommunikationstechnologien und stellen besondere Anforderungen an die Gewährleistung von Datenschutz und Datensicherheit. Mittlerweile betreffen 50% der Aufwendungen für nationale Programme und Projekte zu eHealth und personalisierter Versorgung die Implementierung von Datenschutz- und Datensicherheitsdiensten und mechanismen. Diese müssen ebenso dynamisch, verteilt und intelligent sein. In diesem Zusammenhang kommt dem Privilegmanagement sowie der Zugriffskontrolle eine besondere Bedeutung zu.

In vielen Gesundheitseinrichtungen und Versorgungsprozessen gibt es trotz der rechtlichen und ethischen Erfordernisse keine Lösungen für das Privilegmanagement und die Zugriffskontrolle. Bestenfalls sind rollenbasierte Dienste und Mechanismen wie Role Based Access Control (RBAC) – ein NIST Standard – implementiert. Diese können unter Berücksichtigung funktioneller Rollen zusätzlich zu den üblichen strukturellen Rollen entsprechend dem HL7 RBAC Healthcare Permission Catalog verfeinert werden.

Dabei ist die die genannten Paradigmenwechsel am besten unterstützende Lösung bereits seit Jahren als internationaler Standard ISO 22600 "Health Informatics - Privilege management and access control" spezifiziert. Diese Lösung definiert die zur Sicherung von Datenschutz und Datensicherheit erforderlichen Regeln als ontologiebasierte, explizite Policies, die kontextuelle und Umgebungsbedingungen ebenso wie individuelle Präferenzen flexibel auf jedem Granularitätsniveau berücksichtigen und so umfassende Interoperabilität unterstützen.

Als Interimslösung wird in jüngster Zeit eine Initiative der US-Administration vorangetrieben, die von HL7 International standardisiert wird. Diese besteht aus zwei Teilen:

a) der kontextsensitiven Segmentierung medizinischer Daten entsprechend den Anforderungen verschiedener Verwendungszwecke und
b) dem Security and Privacy Labeling dieser Datensegmente in einer maschinenverarbeitbaren Weise.

Security and Privacy Labels sind an eine Ressource gebundene Markierungen, die ein Informationsobjekt mit einem Set von Datensicherheits- bzw. Datenschutzattributen verbinden. Im neuesten HL7-Standard wurden folgende Security und Privacy Labels definiert: Vertraulichkeit, Sensitivität, Integrität, und Handlungsinstruktionen.

- Vertraulichkeits-Labels werden verwendet, um das erforderliche Schutzniveau der geschützten Information, zu der das spezifische Informationsobjekt gehört, zu identifizieren.
- Sensitivitäts-Labels erlauben, die Sensitivität von Informationen, d.h. ihren Wert und die Bedeutung für das Informationssubjekt, oder auch dessen Verwundbarkeit zu identifizieren.
- Integritäts-Labels werden verwendet, um die Vollständigkeit, Glaubwürdigkeit, Zuverlässigkeit, Vertrauenswürdigkeit, Ursprung von Informationen zu bestimmen.

- Handlungsinstruktions-Labels dienen der Identifikation von Verbreitungskontrollen, Verwendungszweck, Unterlassungs-Policies und Verpflichtungen, die der Verwalter einer IT-Ressource befolgen muss.

Durch die Definition von

a) Befugnissen, die von einer Entität für den Zugriff auf eine geschützte Ressource verlangt wird
b) Privilegien für einen Akteur, auf Daten oder Informationen auf oder unter einem bestimmten Security/Privacy Level zuzugreifen,
c) Security and Privacy Labels und
d) Security and Privacy Information Files, die definieren, welche Security und Privacy Labels gültig sind und wie sie gegen die Privilegien geprüft werden können

kann das Privileg- und Zugriffkontrollmanagement in Gesundheitsinformationssystemen automatisiert werden.

In einer grob strukturierten Variante realisiert diese Lösung ein kontextsensitives RBAC, während eine Segmentierung bis auf ein atomares Niveau der expliziten Policy-Definition nach ISO 22600 nahekommt. Somit präsentiert der Beitrag eine Roadmap, die Anwendern erlaubt, mit Minimallösungen für Privilegmanagement und Zugriffskontrolle zu starten und diese konsistent zu skalieren und qualitativ weiterzuentwickeln. Die Lösung unterstützt die Nutzung klinischer Informationen in der Forschung.