HL7 Standards and Components to Support Implementation of the European General Data Protection Regulation (GDPR)

Alexander Mense[1], Bernd Blobel[2,3,4]

[1] University of Applied Sciences Technikum, Wien, Austria
[2] Medical Faculty, University of Regensburg, Germany
[3] eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Germany
[4] First Medical Faculty, Charles University Prague, Czech Republic

Abstract

Objectives: Aiming to strengthen EU citizens' fundamental privacy rights in the digital age the new European General Data Protection Regulation shall apply from May 25th 2018. It will require companies processing personal data to implement a set of organizational and technical controls for ensuring proper handling of these data. Obviously this applies for companies providing eHealth services. As HL7 offers a lot of material to support security and privacy for handling personal healthcare data, this paper aims at showing which HL7 standards and components can be used to support the implementation of GDPR related controls.

Methods: The paper shows some key facts of the European GDPR as well as analyzes HL7 standards and components in the security and privacy domain to provide a basic mapping.
Results: As a result the paper provides a table mapping HL7 artifacts to GDPR requirements.
Conclusion: The paper shows, that consequently using HL7 security and privacy standards and components efficiently helps to implement GDPR requirements.

Keywords

Privacy; Security; HL7; CDA; FHIR

Correspondence to:

Prof. Alexander Mense
University of Applied Sciences Technikum,
Hoechstaedtplatz 6, Wien, Austria.
E-mail: mense@technikum-wien.at

EJBI 2017; 13(1):27-33
received: June 11, 2017
accepted: July 16, 2017
published: October 10, 2017

1 Introduction

On May, 24th 2016, the new European General Data Protection Regulation (GDPR) [1, 2] came into force and shall apply from May, 25th 2018 [3]. It replaces Directive 95/46/EC [4] from 1995 and all related national laws. As regulation (in contrast to a directive) it is in its form legally binding for the European Union Member States. The process of developing this regulation was started in 2012 as "an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market" [5].

The GDPR "*lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*" [2, p.32]. This single set of rules for all countries of the European Union implements a "one-stop shop" for all organizations and companies within the Union.

The regulation will require companies processing personal data and particularly sensitive data to implement a set of organizational and technical controls for ensuring proper handling of these data according to security and privacy requirements. So it protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data without restricting or prohibiting the free movement of personal data within the Union in that context [2]. In consequence this also impacts software companies offering systems for handling personal and sensitive data. Thus, beside the "Directive on security of network and information systems (NIS Directive)" (concerning measures for a high common level of security of network and information systems across the Union) [6] the GDPR will utmost impact the healthcare domain.

"*The regulation applies if the data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU. Furthermore the Regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents.*" [7].

In case of violation of the rule the following sanctions and fees can be imposed [2]:

- a warning in writing in cases of first and non-intentional non-compliance
- regular periodic data protection audits
- a fine up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 4)
- a fine up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater (Article 83, Paragraph 5 & 6)

HL7 International provides "*a comprehensive framework and related International standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services*" [8]. Therefore HL7 International offers several specifications and standards that can be used to support the implementation of the GDPR requirements in EHR and PHR systems as well the health data exchange in an interoperable manner.

This paper aims at introducing the fundamental principles and rules of the GDPR as well as at providing an overview about relevant HL7 standards and a mapping of HL7 artifacts to GDPR requirements.

2 Methods and Materials

In a first step, technical core aspects are extracted from the GDPR (2.1) and possibly relevant HL7 standards and frameworks are identified. They are differentiated into base standards (2.2), CDA R2 based specifications (2.3), FHIR based resources (2.4) and HL7 V2 (2.5).

2.1 Core Aspects of GDPR

The GDPR defines personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*". Thereby, it properly reflects organizational, methodological and technological paradigm changes health systems are facing [9].

The GDPR defines several obligations for data controllers accountable to demonstrate compliance and thus, setting a framework for accountability. This includes the request for maintaining certain documentation, for performing a data protection impact assessment for more risky processing, for designating a data protection officer in some cases and for implementing data protection measures by design and by default, for instance for data minimization. This places the legal obligation on the Data Controller to notify the Supervisory Authority on a data breach without undue delay.

From the text of the regulation the following detailed technical core requirements can be derived [2]:

R1: Data protection by design and by default

Taking into account the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing of their personal data, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures which are designed to implement data-protection principles to meet the requirements of the regulation and protect the rights of data subjects Also the controller shall implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. ([2], Article 25). Besides an appropriate, well documented development cycle this technically requires possibilities to specifically mark (label) information that falls under specific requirements or have to be treated specifically according to a person's privacy policy.

R2: Data portability

"This right allows for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance." [10, p3]. Meaning that any person has a right to take their data elsewhere, and the data controller must provide it machine readable form. This is the requirement for interoperable systems.

R3: Right to be forgotten–notification requirement

Data subjects already have a right to have outdated information removed or updated. Now the data controller must also notify other parties that received the data about the change.

R4: Unambiguous consent

A person's consent for processing and storing your data must be freely given, specific, informed and unambiguous. For sensitive data it must be explicit - implied consent is not accepted. A data subject's consent to processing of their personal data must be as easy to withdraw as to give. The data controller is required to be able to demonstrate that consent was given, which means that detailed consent information has to be maintained on file as well as exchanged with communication partners.

R5: Privacy notices

The GDPR requires that information of how private information is processed has to be presented in an easy to understand, clear and plain language. The same holds true also for the aforementioned consent documents. Data controller's policies have to be transparent and easily accessible.

R6: Right to Access / Records of processing activities

Every data controller must keep records pertaining to all aspects of the data processing operations under its responsibility. Records of processing activities must be maintained, that include purposes of the processing, categories involved and envisaged time limits. These records must be made available to the supervisory authority on request. The GDPR also imposes such record-keeping obligation on data processors and requires data controllers and data processors to cooperate (see also R9). This clearly defines the requirement for maintaining provenance information.

R7: Explicit and formally represented policies

By defining the terms "binding corporate rules" ([2], Article 46) and "joint controllers" ([2], Article 26) implicitly the definition and use of explicit and formally represented policies becomes necessary. An overview how to model a policy-driven system for managing personal health information can be for instance in [11]. For healthcare data exchange this also implies the requirement for setting up a common security and privacy policy domain.

The aforementioned requirements can only be met by declaring and managing multiple policies. Those policies including individual ones must be formally represented to enable dynamic and possibly automated policy harmonization [9]. Requirements R4 and R5, but also some others establish a demand for a system-oriented, architecture-centric, ontology-based approach to interoperability as defined at ISO 215 and CEN 251 with the Interoperability Reference Architecture Model for their interoperability standards and meanwhile approved for ISO 13606 [12].

2.2 HL7 General Concepts for Security and Privacy

HL7 provides some general concepts that can be used as a general basis for implementing a security and privacy framework to cover parts of the GDPR requirements.

S1: HL7 Version 3 DAM: Composite Security and Privacy Domain Analysis Model – Release 1

This DAM [13] contains a harmonized analysis of security and privacy policies required to support the security and privacy needs of healthcare organizations. It is an implementation of the ISO 22600 policy ontology [14] and identifies the information and system behaviors required to implement technological controls enforcing healthcare security and privacy policies, therefore representing the basis for policy based access control systems.

S2: HL7 Healthcare Privacy and Security Classification System (HCS), Release 1

The HCS [15] provides a common syntax and semantics standard for interoperable security labels to bind security labels to (primarily) healthcare data to enable data segmentation, fined grained access control and communication of security information related to a resource. Therefore it defines a normative set of interoperable healthcare security label fields (see Figure 1) to be assigned as a security label to healthcare information passed between systems within a security domain and specifies a conforming standard HL7 security

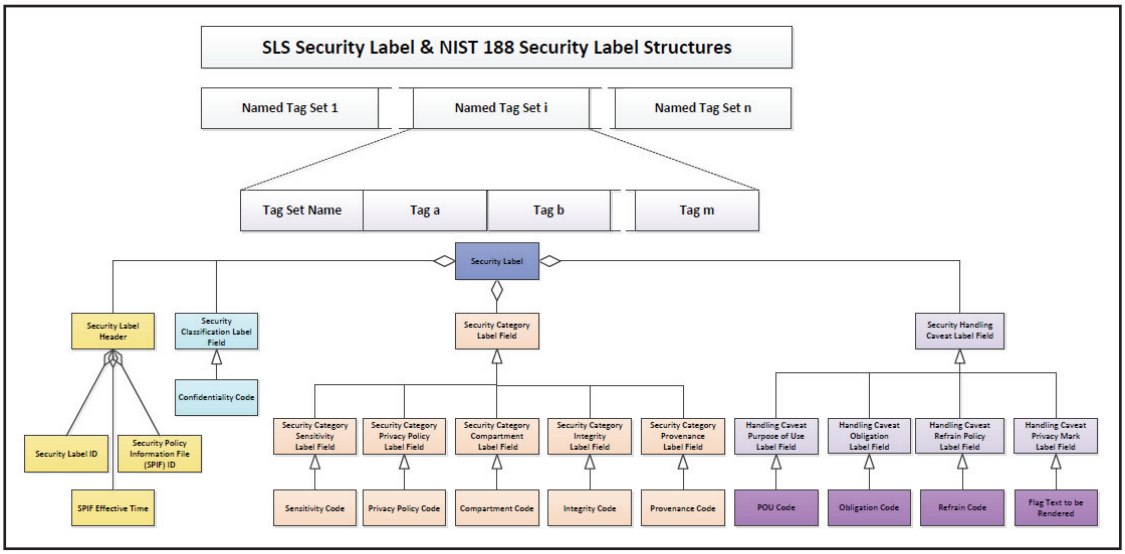


Figure 1: HL7 security and privacy labels [14].

label vocabulary. These definitions have been used as the fundamental basis for CDA R2 implementation guides (see section 2.3) as well as security metadata for FHIR artifacts (see section 2.4). The use of definitions has been show in several projects (e.g. [16]).

S3: HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service, Release 1 (SLS)

This standard specifies interoperable Security Labeling functional capabilities that are exposed through well-defined, technology agnostic service interfaces. Functional capabilities will likely include the following component services and infrastructure: - Security Labeling Manager (SLM) - Security Labeling Service (SLS) - Trust Fabric Services - Security and Privacy Ontology Based Terminology Services - Privacy Protective Services [17]. The definitions have been used for instance in combination with a XAMCL based access control system in the Axle EU project [18] (presented in [19]).

S4: HL7 Version 3 Standard: Healthcare (Security and Privacy) Access Control Catalog, Release 3

Provides HL7 permission vocabulary in constructing permissions {operation, object} pairs supporting Role based Access Control (RBAC) as well as definition additional high-level concepts and vocabulary of Attribute-Based Access Control (ABAC). [20]

S5: HL7 Version 3 Standard: Privacy, Access and Security Services (PASS); Access Control, Release 1

This standard offers a conceptual framework for access control services applicable to Privacy, Access, and Security domains within the healthcare environment and therefore enabling the creation of standard based services and capabilities implementing the policy framework of any domain. [21]

S6: HL7 Version 3 Standard: Privacy and Security Architecture Framework - Trust Framework for Federated Authorization, Release 1

The document defines a trust framework model for federated authorization by presenting a policy driven approach for controlling access to and use of information across security domains. It shows a high-level harmonized view of the trust, security and privacy policy, and information required to support the interoperability needs of healthcare providers. The policies are negotiated (harmonized) in real-time by participating domains through a process called Policy Bridging, and agreed to via a trust contract also established at run time [22].

2.3 HL7 CDA R2 Implementation Guides

HL7 provides several CDA R2 implementation guides that can be taken into account for implementing GDPR compliant systems.

CDA1: HL7 CDA® R2 Implementation Guide: Privacy Consent Directives, Release 1

The implementation guide specifies templates for a CDA document to exchange signed Consent Directives, which can be represented as a narrative, signed document, and computable statements/entries using standard-based terminology. Thus, it can be eventually used to generate enforceable assertions or rules (e.g. SAML, XACML) [23].

CDA2: HL7 CDA® R2 Implementation Guide: Data Provenance, Release 1 - US Realm

This implementation guide is a result of a collaboration of HL7 and the US Health and Human Services Office of National Coordinators Standards and Interoperability Framework Data Provenance Initiative (DPROV) and enables basic provenance information about clinical (and other care related information), who created it, when was it created, where was it created, how it was created, and why it was created, to be integrated into HL7 CDA documents in a consistent and interoperable way [24].

CDA3: HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1

The DS4P implementation guide defines models, concepts and templates to enable segmenting clinical records so that personally identified information (PII) can be appropriately shared as may be permitted by privacy policies or regulations. It introduces reusable privacy building blocks and CDA templates to support the association of information object (e.g. document, section, entry) with security labels, which then can be linked to privacy policies [25].

CDA4: HL7 CDA® R2 Implementation Guide: Patient-Friendly Language for Consumer User Interfaces, Release 1

This standard provides a patient friendly language/ plain language healthcare vocabulary which is targeted specifically toward healthcare consumer user interfaces which create outputs for consumer consumption such as consent directives, reports of disclosures, and notices of privacy practices [26]. It specifies a mapping of the technical/ legal security and privacy language, which patients are often uncomfortable with, to a plain language, which is defined as "communication your audience can understand the first time they read or hear it" (see [27] for complete definition) [26]. The standard provides a mapping to the English language, but can be a template for any other language.

2.4 HL7 FHIR® Artifacts

The HL7 FHIR specification [28] provides a summery page regarding security and privacy principles providing guidance and also an overview on FHIR specific controls [29]. According to the GDPR requirements the following FHIR elements can be considered relevant:

FHIR1: Security Labels

According to the "Healthcare Privacy and Security Classification System (HCS)" [15] the FHIR specification supports the implementation of the security label concept. Security and privacy labels can be attached to a resource or bundle as metadata to provide specific security and privacy attributes and information. Details can be found at [30]. Currently three core Security Labels are defined: **Context of Use** - Purpose Of Use, **Data Sensitivity** - Confidentiality codes, **Control of Flow** - Delete After Use / Do Not Re-use, but supports all categories defined by HCS. Figure 2 shows an example of applying a security label to a FHIR resource [30].

FHIR2: Compartment Resource

The compartment resource was designed to logically group resources which share common properties [31]. Thus, it can be used as the basis for applying access control mechanisms. Currently defined compartments are Patient, Encounter, RelatedPerson, Practitioner and Device. For example a Patient compartment is set of resources associated with a particular patient [32]. For detailed definition and usage of the compartment resource refer to [31].

FHIR3: Consent Resource

The purpose of the consent resource is to enable expressing specific consents regarding healthcare. This can be for instance a Privacy Consent Directive, Medical Treatment Consent Directive, Research Consent Directive or Advance Care Directives [33]. It primarily serves „*as record of a healthcare consumer's policy choices, which permits or denies identified recipient(s) or recipient role(s) to perform one or more actions within a given policy context, for specific purposes and periods of time.*" [33]. But based on different characteristics (e.g. human readability or legal binding) there are several definitions how this resource can be instantiated and used. For detailed descriptions as well as examples see [33].

FHIR3: Provenance Resource

FHIR defines two resources suitable for tracking the origins, authorship, history, status, and access of resources. The Provenance resource enables recording of activities regarding specific resources (entities). This may include consumption, processing, transformation, modification, relocation, usage, or generation of entities. It allows for tracking what has happened to a specific entity in the course of time (i.e. who created it when, who modified or transformed it, etc.). The provenance resource model definition is in alignment with the W3C provenance specification [34] (see Figure 3). The Provenance resource covers "Generation" of "Entity" with respect to FHIR defined resources for creation or updating; whereas AuditEvent (see following section) covers "Usage" of "Entity" and all other "Activity" as defined in W3C Provenance [35].

FHIR4: Audit Event Resource

The Audit event resource is the second resource for tracking activities of specific entities and provides a record of an event made for purposes of maintaining a security log [36].

2.5 HL7 Version 2

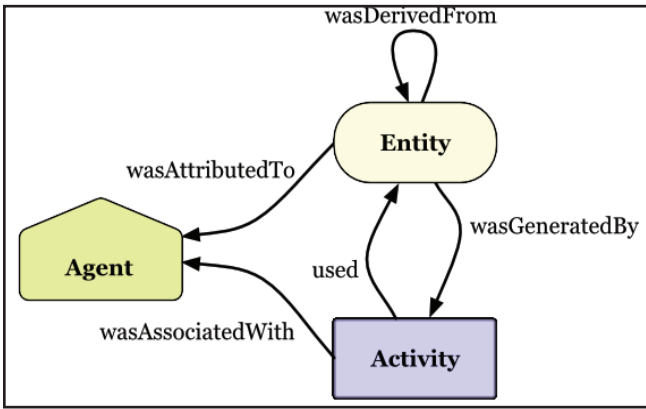
Even though HL7 Version 2 [37] states in its introduction that it does not explicitly provide elements for security and privacy, it offers some elements that can be used to convey information to support also some of the requirements of the GDPR.

V2: CON Segment

The CON segment "*identifies patient consent information relating to a particular message. It can be used as part of existing messages to convey information about patient consent to procedures, admissions, information release/exchange or other events discussed by the message. It may also be used in messages focusing on recording or requesting consent and for*

```
<Patient xmlns="http://hl7.org/fhir">
  <meta>
    <security>
      <system value="http://hl7.org/fhir/v3/Confidentiality"/>
      <code value="R"/>
      <display value="Restricted"/>
    </security>
  </meta>
... [snip] ...
</Patient>
```

Figure 2: Example for security label as meta-data for a FHIR resource.



Target - An entity that is a FHIR resource instance that is created, updated or deleted.
Entity - An entity is a physical, digital, conceptual or other kind of thing with some fixed aspects; entities may be real or imaginary.
Agent - An agent is something that bears some form of responsibility for an activity taking place, for the existence of an entity, or for another agent's activity.
Activity - An activity is something that occurs over a time period and acts upon or with entities. It may include consuming, processing, transforming, modifying, relocating, using, or generating entities.

Figure 3: Provenance model based on W3C provenance specification [35].

Table 1: Mapping HL7 artifacts to GDPR requirements.

	R1 Priv.by Design	R2 portability	R3 right to be forgotten	R4 consent	R5 privacy notices	R6 right to access	R7 explicit policies
S1 (DAM)	x	x		x			x
S2 (HCS)	x	x					
S3 (SLS)	x	x					
S4 (HACC)	x	x					x
S5 (PASS-AC)	x	x					x
S6 (PSAF-AuthZ)		x					x
CDA1 (consent)				x	x	x	x
CDA2 (prov.)						x	
CDA3 (segment.)	x					x	
CDA4 (language)					(x[1])		
FHIR1 (labels)	x						
FHIR2 (consent)		x		x	x		x
FHIR3 (prov.)		x				x	
FHIR4 (audit)						x	
V2 (CON)				x			

[1]As it is provided only in English language it can only serve as template!

consents related to employees or service providers." [37]. While the purpose is mainly for consent to medical treatment it can be also used to express authorization to disclosure protected health information (consent type = 001). [37]

3 Results

There is no doubt, that the GDPR on the one side requires the use of international interoperability standards for systems operating in the healthcare domain and on the other side poses the obligation to implement an well documented appropriate access control system to protect private and especially sensitive data. Table 1 shows the mapping of the aforementioned HL7 standards and definitions to the GDPR core requirements.

4 Discussions

It could be shown, that consequently using HL7 security and privacy standards and components efficiently helps to implement the technical core requirement of the GDPR. Unfortunately many systems in the healthcare domain (EHR as well as PHR systems, especially when it comes to the thousands of applications for mobile devices) are far away from implementing the appropriate controls and even worse many companies have not even realized the absolute necessity to start planning to reach compliance with GDPR in 2018.

However, most HL7 specifications still focus on the IT systems interoperability based on ICT ontologies [38]. For overcoming this limitation and responding to the social, cultural, knowledge and language related requirements of the GDPR, we have to extend the interoperability scope beyond the ICT domain, also directly including non-ICT domains and specialties and their terminologies and ontologies based on the aforementioned Interoperability Reference Architecture Model. Pushed by the crucial impact of multiple non-ICT domains, the HL7 Security Working Group has moved quite early to a system-oriented, architecture-centric, ontology-

based approach to interoperability, also supported by ISO and CEN specs following the same approach. We still hope that other HL7 WGs will adapt that approach quite soon. For deeper reasoning on this, see [39].

References

[1] European Parliament and Council: Regulation (EU) 2016/679 – Summary Page. Online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

[2] European Parliament and Council: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[3] European Commission: Protection of personal data. Online: http://ec.europa.eu/justice/data-protection/

[4] European Parliament and Council: Directive 95/46/EC. 1995, Online: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

[5] European Commission: Reform of EU data protection rules. Online: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[6] European Parliament and Council: Directive (EU) 2016/1148. Online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[7] Wikipedia, General Data Protection Regulation. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[8] Health Level 7 International, Inc., Ann Arbor, USA. www.hl7.org

[9] Bobel B, Lopez DM, Gonzalez C. Patient privacy and security concerns on big data for personalized medicine. Health and Technol. 2016; 6: 75-81.

[10] European Commission – Articel 29 Data Protection Working Party: Guidelines on the right to data portability. Online: ec.europa.eu/newsroom/document.cfm?doc_id=44099

[11] Blobel B, Ruotsalainen P, González C, López D. Policy-driven management of personal health information for enhancing interoperability. Stud Health Technol Inform. 2014; 205:463–467.

[12] International Organization for Standardization. ISO 13606-1 EHR communication – Reference model. Geneva: ISO; 2017.

[13] HL7 International Inc. HL7 V3 DAM: Composite Security and Privacy Domain Analysis Model – Release 1. Ann Arbor: HL7 International; 2014.

[14] International Organization for Standardization. ISO 22600 Health informatics – Privilege management and access control. Geneva: ISO; 2014.

[15] HL7 International Inc. HL7 Healthcare Privacy and Security Classification System (HCS), Release 1. Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/private/standards/v3/PRIV_SEC_CLASS_SYS_R1_2014AUG.zip

[16] Data Segmentation for Privacy VA/SAMHSA RI/Pilot at HIMSS 2013. Online: https://www.healthit.gov/techlab/ipg/node/4/submission/82

[17] HL7 International Inc. HL7 Version 3 Standard: Privacy, Access and Security Services; Security Labeling Service, Release 1 (SLS). Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/private/standards/v3/V3_SECURITY_LABELSRV_R1_2014JUN.ZIP

[18] Axle Project: Advanced Analytics for Extremely Large European Databases. https://axleproject.eu/

[19] Meijer H-J, Gaba A, Havinga Y. Axle Projekt. Privacy-aware analytics on healthcare data. Online: http://nl.portavita.com/sites/default/files/whitepapers/Presentation-Portavita-HL7-Workgroup-Meeting-January-2014.pdf

[20] HL7 International Inc. HL7 Version 3 Standard: Healthcare (Security and Privacy) Access Control Catalog, Release 3. Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/private/standards/v3/HL7_V3_HACC_R3_2016OCT.pdf

[21] HL7 International Inc. HL7 Version 3 Standard: Privacy, Access and Security Services (PASS); Access Control, Release 1. Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/private/standards/v3/V3_PASS_AC_R1_2017JAN.pdf

[22] HL7 International Inc. HL7 Version 3 Standard: Privacy and Security Architecture Framework - Trust Framework for Federated Authorization, Release 1. Ann Arbor: HL7 International, Online: http://www.hl7.org/v3ballotarchive_temp_F8D8D58E-1C23-BA17-0CC585AA2A888F40/v3ballot/html/infrastructure/security/V3_PSAF_R1_I2_2017MAY.zip

[23] HL7 International Inc. HL7 CDA® R2 Implementation Guide: Privacy Consent Directives, Release 1. Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/private/standards/cda/CDAR2_IG_CONSENTDIR_R1_2017JAN.zip

[24] HL7 International Inc. HL7 CDA® R2 Implementation Guide: Data Provenance, Release 1. Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/public/standards/dstu/CDAR2_IG_DATAPROV_R1_DSTU_2016SEP.zip

[25] HL7 International Inc. HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1. Ann Arbor: HL7 International, Online: http://www.hl7.org/documentcenter/private/standards/v3/HL7_V3_IG_DS4P_R1_2014MAY.zip

[26] HL7 International Inc. HL7 CDA® R2 Implementation Guide: Patient-Friendly Language for Consumer User Interfaces, Release 1. Ann Arbor: HL7 International, Online.

[27] The Plain Language Action and Information Network (PLAIN): What is plain language. Online: http://www.plainlanguage.gov/whatisPL/index.cfm

[28] HL7 International Inc. Fast Healthcare Interoperability Resources Release 3(STU). Online: http://fhir.hl7.org

[29] HL7 International Inc. FHIR Release 3 (STU) Security. Online: http://hl7.org/implement/standards/fhir/security.html

[30] HL7 International Inc. FHIR Release 3 (STU) Security Labels. Online: http://hl7.org/implement/standards/fhir/security-labels.html

[31] HL7 International Inc. FHIR Release 3 (STU) Resource Compartment Definition – Content. Online: http://hl7.org/implement/standards/fhir/compartmentdefinition.html

[32] HL7 International Inc. FHIR Release 3 (STU) Compartment Patient. Online: http://hl7.org/implement/standards/fhir/compartmentdefinition-patient.html

[33] HL7 International Inc. FHIR Release 3 (STU) Resource Consent – Content. Online: http://hl7.org/implement/standards/fhir/consent.html

[34] World Wide Web Consortium (W3C). PROV-Overview. Online: https://www.w3.org/TR/2013/NOTE-prov-overview-20130430

[35] HL7 International Inc.: FHIR Release 3 (STU) Resource Provenance – Content. Online: http://hl7.org/implement/standards/fhir/provenance.html

[36] HL7 International Inc.: FHIR Release 3 (STU) Resource AuditEvent – Content. Online: http://hl7.org/implement/standards/fhir/auditevent.html

[37] HL7 International Inc: HL7 Version 2.8.2. Ann Arbor: HL7 International, 2014, Online: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=403

[38] A. Akerman, J. Tyree. Using ontology to support development of software architectures. IBM Systems Journal. 2006; 45:813-825.

[39] B. Blobel, F. Oemig.The Importance of Architectures for Interoperability. Stud Health Technol Inform. 2015; 211:18-56.