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

Alexander Mense
- University of Applied Sciences Vienna
Bernd Blobel
- Medical Faculty, University of Regensburg, Germany
- eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Germany

FH University of Applied Sciences TECHNIKUM WIEN
17th INTERNATIONAL HL7 INTEROPERABILITY CONFERENCE IHIC 2017
Technopolis City of Athens 22-24 October 2017
HL7 AUSTRIA
HL7 Deutschland

Outline

- Objectives
- Context of GDPR
- GDPR Core Aspects
- HL7 Standards and Components to support implementation
- Conclusion & Discussion

Paradigm Change in Health Systems

- For improving safety and quality of healthcare as well as efficiency and efficacy of health services processes under the well-known conditions of demographic changes, demanding attitude regarding health and social services, medical and technological progress, development of human resources and the fundamental right for equal care, health systems undergo organizational, methodological and technological paradigm changes.
- This includes the way security and privacy are guaranteed.

Objective & Methods

- Introducing the fundamental principles and rules of the GDPR as well as providing an overview about relevant HL7 standards for implementing security and privacy and a mapping of HL7 artifacts to GDPR requirements
- Extract technical core aspects from GDPR, identify possibly relevant HL7 standards and frameworks for security & privacy (base standards, CDA R2 based specifications, HL7 V2 and FHIR based resources) and map them

GDPR History

- **2011**: Special Eurobarometer 259 – Report: Attitudes on Data Protection and Electronic Identity in the European Union
  - 74% of the Europeans see disclosing personal information as an increasing part of modern life
  - 70% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected.
  - Even though a majority of European Internet users feel responsible themselves for the safe handling of their personal data, almost all Europeans are in favour of equal protection rights across the EU (90%).
  - …

GDPR History

- **2012**: start of process to develop new data protection regulation 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”
- **2016**, May 24th: the new European General Data Protection Regulation (GDPR) came into force
  - As “regulation” legally binding for the European Union Member States
- It shall apply from May, 25th **2018**

GDPR Context

- Part of key objective “Strengthening trust an security” in European Union’s “Digital Single Market” strategy
  - boost the level of cyber-security by improving security while using digital media and applications, enhancing trust and inclusion and fostering digital privacy in Europe
- NIS-Directive (Directive on security of network and information systems)
  - Main objectives: Member State Preparedness, EU Security Network, Incident Reporting
- ePrivacy Regulation
  - Main objectives: Cover new players (e.g. WhatsApp) and IoT, Guarantee privacy for communication of content and metadata, Simpler rules on cookies, Protection against spam

GDPR Basics

- 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.*" [GDPR]
- 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.
- Also applies to organizations based outside the European Union if they collect or process personal data of EU residents.
- Provides single set of rules and one-stop shop
- Sanctions for violation 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

GDPR Basics

- GDPR defines several obligations for data controllers responsibility to demonstrate compliance and thus, setting up a framework for accountability
  - Requirement for maintaining **documentation**
  - Perform a (continuous) **privacy impact assessment**
  - Designate a **data protection officer** organization of relevant size and specific obligations
  - Implement **data protection measures by design and by default** (data minimization)
  - Notification of the Supervisory Authority on a **data breach** without undue delay

GDPR Technical Core Aspects

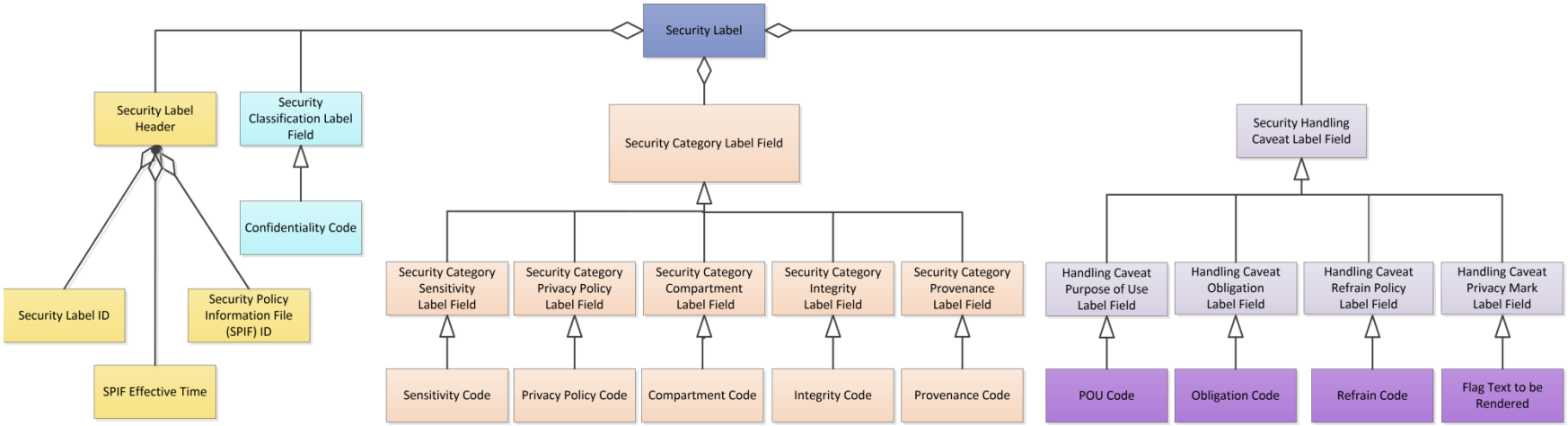
- R1: Data protection by design and by default
- R2: Data portability
- R3: Right to be forgotten–notification requirement
- R4: Unambiguous consent
- R5: “Easy to understand” privacy notices
- R6: Right to Access / Records of processing activities
- R7: Explicit and formally represented policies

GDPR Technical Core Aspects – architectural core requirements

- GDPR requirements can only be met
  - by declaring and managing multiple policies which must be formally represented to enable dynamic and possibly automated policy harmonization
  - 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

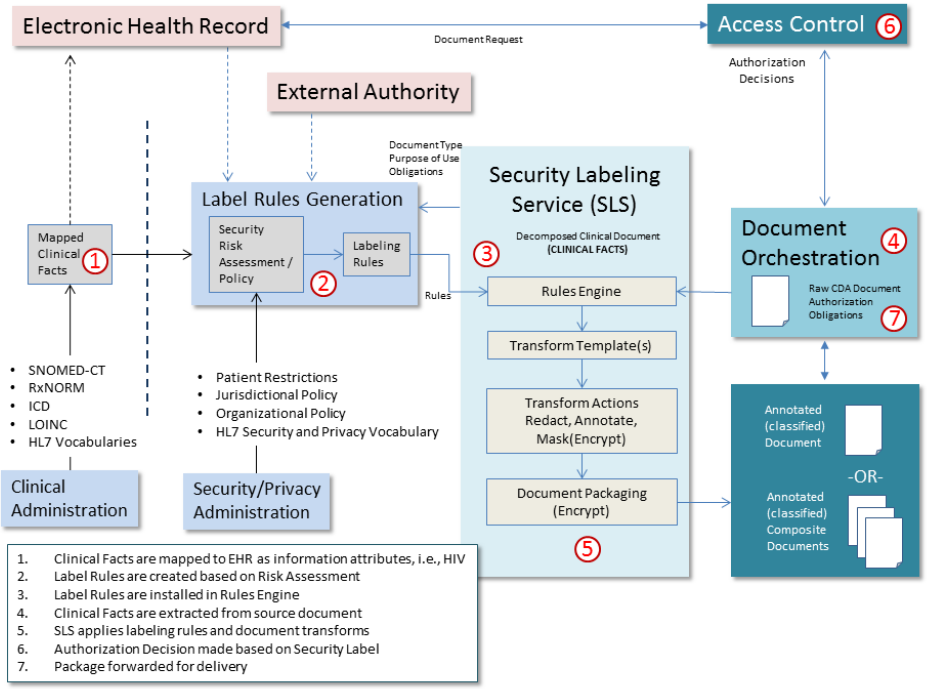
HL7 Security & Privacy Base Standards

- S1: HL7 Version 3 DAM: Composite Security and Privacy Domain Analysis Model – Release 1
  - Based on ISO 22600 policy ontology
- S2: HL7 Healthcare Privacy and Security Classification System (HCS), Release 1



HL7 Security & Privacy Base Standards

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



HL7 Security & Privacy Base Standards

- S4: HL7 Version 3 Standard: Healthcare (Security and Privacy) Access Control Catalog, Release 3
- S5: HL7 Version 3 Standard: Privacy, Access and Security Services (PASS); Access Control, Release 1
- S6: HL7 Version 3 Standard: Privacy and Security Architecture Framework - Trust Framework for Federated Authorization, Release 1

Base Standards to support implemention of GDPR core aspects

	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

HL7 V2 Security & Privacy Artefacts

- V2: CON Segment

	R1 Priv.by Design	R2 portability	R3 right to be forgotten	R4 consent	R5 privacy notices	R6 right to access	R7 explicit policies
V2 (CON)	x						

HL7 CDA R2 Security & Privacy Artefacts

- CDA1: HL7 CDA® R2 Implementation Guide: Privacy Consent Directives, Release 1
- CDA2: HL7 CDA® R2 Implementation Guide: Data Provenance, Release 1 - US Realm
- CDA3: HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1
- CDA4: HL7 CDA® R2 Implementation Guide: Patient-Friendly Language for Consumer User Interfaces, Release 1

HL7 CDA R2 IGs to support implementation of GDPR core aspects

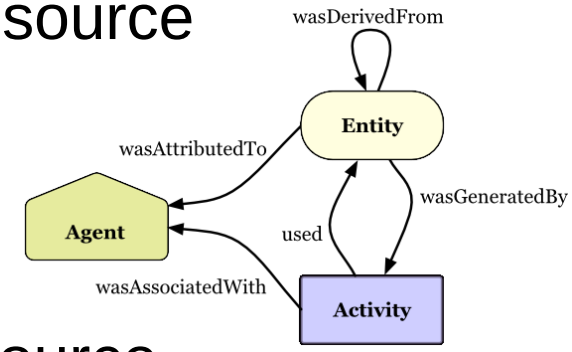
	R1 Priv.by Design	R2 portability	R3 right to be forgotten	R4 consent	R5 privacy notices	R6 right to access	R7 explicit policies
CDA1 (consent)				x	x	x	x
CDA2 (prov.)						x	
CDA3 (segment.)	x					x	
CDA4 (language)					(x)		

HL7 FHIR Security & Privacy Artefacts

- FHIR1: Security Labels

```
<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>
```

- FHIR2: Compartment Resource
- FHIR3: Consent Resource
- FHIR3: Provenance Resource



- FHIR4: AuditEvent Resource

See also: http://hl7.org/implement/standards/fhir/secpriv-module.html

HL7 FHIR components to support implementation of GDPR core aspects

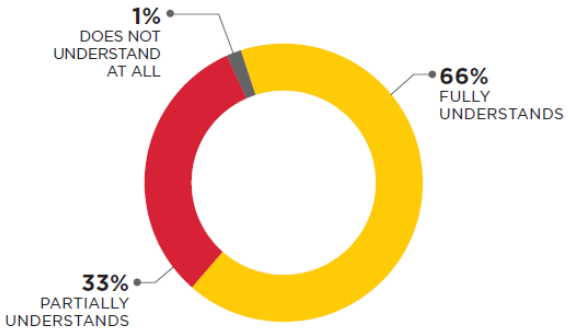
	R1 Priv.by Design	R2 portability	R3 right to be forgotten	R4 consent	R5 privacy notices	R6 right to access	R7 explicit policies
FHIR1 (labels)	x						
FHIR2 (consent)		x		x	x		x
FHIR3 (prov.)		x				x	
FHIR4 (audit)						x	

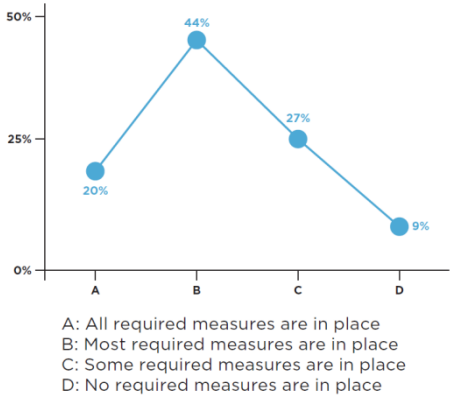
Summary mapping HL7 components to GDPR requirements

	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			

Conclusion

- Using HL7 security and privacy standards and components efficiently helps to implement the technical core requirement of the GDPR
  - Implementation of GDPR needs use of International Standards
- Many companies still do not fully understand requirements or are not prepared





Source: FireEye, June 2017(!!)

Discussion

- Most HL7 specifications still focus on the IT systems interoperability based on ICT ontologies
  - To overcome social, cultural, knowledge and language related requirements of the GDPR, interoperability scope have to be extended beyond the ICT domain
  - Need to include non-ICT domains and specialties and their terminologies and ontologies based on the Interoperability Reference Architecture
    - system-oriented, architecture-centric, ontology-based approach to interoperability as defined at ISO 215 and CEN 251

Thanks for your attention!