MEDINFO 2019: Health and Wellbeing e-Networks for All
L. Ohno-Machado and B. Séroussi (Eds.)

doi:10.3233/SHTI190403

How Does GDPR Support Healthcare Transformation to 5P Medicine?

Bernd Blobel[a,b,c], Pekka Ruotsalainen[d]

[a] *Medical Faculty, University of Regensburg, Regensburg, Germany*
[b] *eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Deggendorf, Germany*
[c] *First Medical Faculty, Charles University Prague, Prague, Czech Republic*
[d] *Tampere University, Tampere, Finland*

Abstract

Health systems advance towards personalized, preventive, predictive, participative precision (5P) medicine, considering the individual's health status, contexts and conditions. This results in fully distributed, highly dynamic, highly complex business systems and processes with multiple, comprehensively cooperating actors from different specialty and policy domains, using their specific methodologies, terminologies, ontologies, knowledge and skills. Rules and regulations governing the business process as well as the organizational, legal and individual conditions, thereby controlling the behavior of the system, are called policies. Trust and confidence needed for running such system are strongly impacted by security and privacy concerns controlled by corresponding policies. The most comprehensive policy dealing with security and privacy requirements and principles in any business collecting, processing and sharing personal identifiable information (PII) is the recently implemented European General Data Protection Regulation (GDPR). This paper investigates how GDPR supports healthcare transformation and how this can be implemented based on international standards and specifications.

Keywords:
European data protection, governing, privacy

Introduction

In the course of methodological paradigm changes, healthcare systems advanced from empirically describing health problems with one solution fits all to dedicated care, stratifying population for specific, clinically relevant conditions resulting in evidence-based medicine. Stratifying population by risk profiles, the current phase of healthcare transformation towards personalized, preventive, predictive and participative precision (5P) medicine considers the individual's health state, conditions and contexts, thereby integrating research and practice. Conditions and contexts include legal, social, environmental, occupational, or any other context. Disciplines or domains engaged in 5P medicine cover medicine, natural sciences, social sciences, engineering, etc., considering the individual from elementary particle to society. The required knowledge sharing and cooperation of multiple stakeholders from different domains using their methodologies, terminologies and ontologies establishes a legal, cultural and language challenge. As individual health state, conditions and contexts are highly dynamic, it is impossible to predefine the business systems, its processes and policies for meeting the business system objectives comprehensively, uniform and legally binding in a static way. Thus, 5P medicine requires the automated management of multiple dynamic domains including multiple dynamic policy domains. [1]

The paper investigates a) how the European General Data Protection Regulation (GDPR) [2] reflects architecture and policies of transformational healthcare systems and b) how GDPR must be implemented to support healthcare transformation. For that purpose, GDPR is structurally and functionally analyzed. For meeting principles and services required by GDPR, standards, specifications and products are recommended and explained in some details.

Methods

For analyzing such complex settings like 5P medicine under dynamically changing perspectives and contexts, a system-theoretical approach is used. According to IEEE 1471-2000, a system is a collection of components organized to accomplish a specific function or a set of functions to realize the business objectives of that business system intended by the involved stakeholders [3]. Systems interact with their environment and can be decomposed to subsystems or composed to super-systems in a recursive way. A system is defined by the system's architecture, i.e., its components, their functions and relations on the one hand, and the system's behavior represented by the system's policy on the other hand. The term policy implies any set of rules for selecting components and functions as well as constraints of the relations according to a business case, thereby controlling the behavior of that system. It represents the perspectives of all domains involved, i.e., process policies, legal constraints, individual preferences, resource management, etc. This behavioral description applies to any of the aforementioned subsystem or super-system.

A security and privacy policy according to ISO 22600 Health informatics – Privilege management and access control [4] is a complex of legal, organizational, functional, social, ethical and technical aspects to be considered in the context of privacy and security. It defines a framework, privileges and obligations, but also consequences and penalties when the regulations are ignored.

Ecosystems are structured systems and communities of living and non-living components, which follow specific rules (policies) and interact as unit among themselves or with their physical environment.

The approach is based on the Generic Component Model (GCM) introduced by the first author in the mid-nineties [5, 6].

How Does GDPR Reflect 5P Medicine?

While the EU Data Protection Directive (Directive 95/46/EC) [7] defined just direct or indirect identifiers as personal data, GDPR extends in Art. 4(1) that definition including "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity" of a natural person [2]. That way, GDPR defines data characterizing an individual's health status, context and conditions in the sense of 5P medicine as personal data. The extended definition of processing in GDPR Art. 4(2) meets contrary to the one in Directive 95/46/EC, the process of 5P medicine as well. GDPR Art. 6(3) requires explicit policies, which have to be represented formally and machine-processable and bound to the information objects or process steps (Art. 4(20) and Art. 26(1)). Those policies must represent the current context, and – because that context is changing – must be managed dynamically (Art. 26(1)). For guaranteeing comprehensive interoperability, policies must be represented using terminologies and ontologies of the addressed audience (Art. 7(2) and Art. 12(1)), that way meeting the requirements of 5P medicine ecosystems. Design and management of that highly complex and highly dynamic ecosystem have to address the security and privacy perspectives according to the ISO 23903 Interoperability Reference Architecture [8], ISO 22600 [4] mentioned before, or ISO 21298 Health informatics – Structural and functional roles [9]. Properly managing the dynamic system in that respect proactively, a permanent risk analysis must be performed, turning the Data Protection Officer from a checkbox marker to a risk manager, directly intervening in the business system and processes throughout the complete system lifecycle presented in the next section.

How to Define a GDPR-Compliant 5P Medicine Ecosystem?

A GDPR-compliant 5P medicine ecosystem must be designed and implemented in an automated process as an architecture-centric, ontology-based, policy-driven multi-domain business system. This has to be done in a formalized and standardized way. Starting point of an appropriate solution is the ISO Interoperability Reference Architecture model and framework developed by the first author. For representing a systems model and framework manageable by engineers, the formal representation of an n-dimensional concept space deploying universal type theory, thereafter refined to a parametrized Barendregt Cube [10, 11], has been transformed in a 3-dimensional system engineering model (Figure 1a). One dimension covers the generic granularity levels or composition/decomposition of any system. The second dimension addresses the system development process following standardized approaches such as ISO 10746 Information technology – Open distributed processing – Reference model [12], SOA (Service-Oriented Architecture) methodology, or the Unified Process (formerly Rational Unified Process). The third dimension concerns the different perspectives on the multi-disciplinary business system in question represented by the variety of domain experts involved in the business process. The concepts have to be represented for each component using the related domain ontologies. The different domains can be properly refined into subsystems with different (sub)ontologies. In the context of GDPR-compliant ecosystems, the policy domain combines different perspectives on ruling the system such as the medical process policy domain, the contextual policy domain, and the administrative/ organizational policy domain managing resources, etc (Figure 1b). The contextual policy domain can be furthermore refined into the legal and regulatory domain, the personal policy domain, and the conditional/contextual domain representing environmental, social, occupational or other contexts.

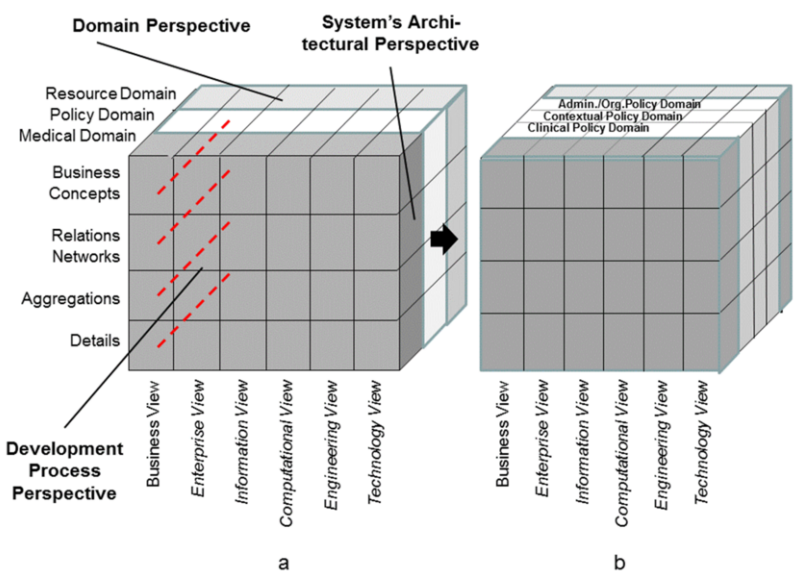

Figure 1. ISO Interoperability Reference Architecture [9]

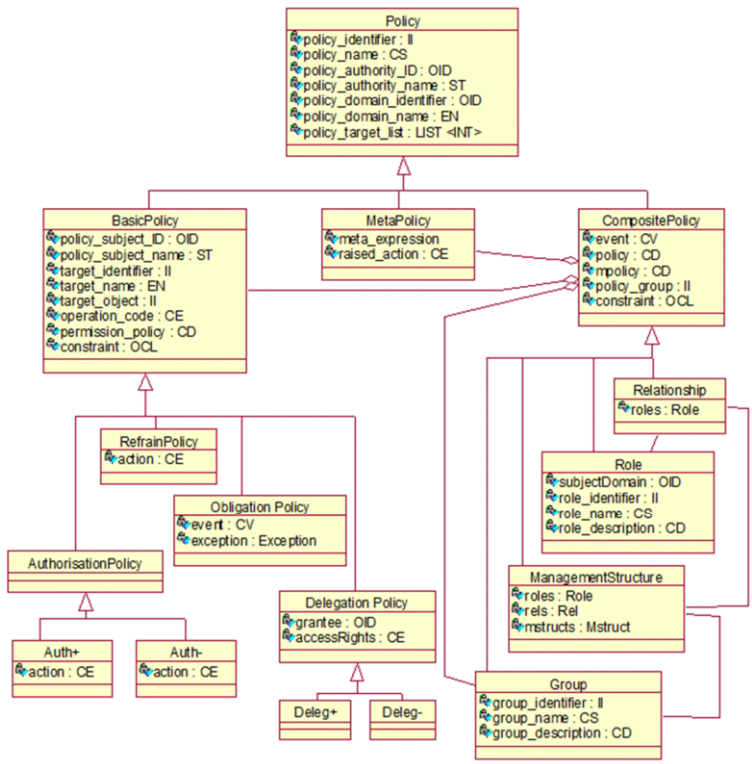

Figure 2. Policy Ontology according to ISO 22600 [4]

For representing policies, the first author has developed a policy ontology based on Damianou's Ponder Policy Specification Language [13]. That policy ontology has been standardized in ISO 22600 Health informatics – Privilege management and access control [4] (Figure 2). The policy ontology defines the entities to be instantiated (left hand side) and the policy management processes (right hand side). Using the presented approach, legally correct policies can be created using specific tooling, e.g., to support the subject of care – usually being a layman in the healthcare domain – to express her will and to understand the policies of other actors using the domain-specific jargon.

The other requirement of GDPR is the binding of policies to information objects and/or activities in the business process to dedicatedly managing them. This mechanism allows for definition and enforcement of data governance, i.e., of constraints on the WHO, HOW, WHEN, WHERE, WHAT FOR and WHY – or in other words, on the actor (which is not necessarily a person) and the context – for accessing and using PII. Such services also address, e.g., the data subject's right of being informed about the processing of personal data as well as rectifying those data if needed. That way, the limitations of that data subject's right offered ín GDPR could be minimized or fully overcome if it proves to be impossible or would involve a disproportionate effort. Alternative to policy binding, binding of labels referring to policies stored in policy repositories can be used. Both ways of binding policies or labels have been standardized in HL7's Healthcare Privacy and Security Classification System (HCS) [14]. As security and privacy labels have been defined: Confidentiality, Sensitivity, Integrity, Compartment and Handling Caveats. The first four are bound to information objects, and the last is bound to activities. The logical architecture to implement the described solution is shown in Figure 3. For enabling an assessment of trustworthiness of the offered service by the service user, a monitoring as well as a trust calculation service have been added to the architecture. Policy binding makes only sense when information is properly structured to enable the assignment of different policies to single, or groups of, information objects on the one hand, or different policies to single actions or related groups of actions on the other hand. Such data segmentation for privacy has been standardized at HL7 [15]. The entire system was demonstrated at HIMSS 2012 [16] and – with further extensions and improvements – also in the following years.

Discussion

Contrary to the Directive 95/46/EC, offering a limited scope and static controls for protection of personal health information, GDPR sets requirements, principles and methodologies to be applied to protect personal identifiable information of EU citizens and to document and demonstrate the compliance with the GDPR independent of the location and the technologies data collection, processing, communication and deployment of that information happen.

Acknowledging the nowadays organizational, methodological and especially also technological paradigm changes leading to highly distributed, complex, highly dynamic settings, turning the data subject to a consumer and changing her role and responsibility, GDPR excellently accommodates healthcare transformation. For that purpose, it has to establish the same

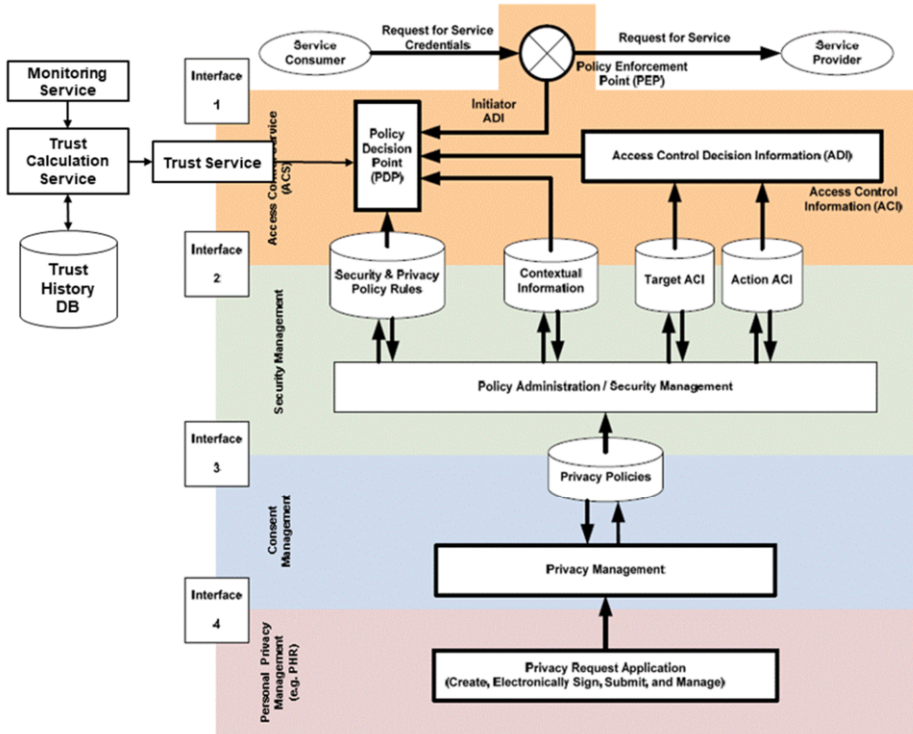

Figure 3. Authorization Reference Model [14]

principles of flexibility, dynamics, complexity, transparency, adaptation, intelligence, automation, etc. Defining principles and methodologies of data governance, GDPR and ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [17] as well as ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls [18] are closely interrelated. While GDPR focuses on the rights of affected persons, ISO addresses the related compliance issues.

Meanwhile, a bunch of standards, specifications and applications for adequately managing GDPR are available, like HL7 Artifacts to support managing GDPR. Here, the HL7 Security Labeling Service has to be mentioned, which contains a Policy Adjudication Engine for policy harmonization, an Ontology Reasoner to check the applicability of security and privacy policies against clinical policies, and the finally the Policy Inference Logic. Furthermore, specific trust services are provided. Most of those services are specified as implementable FHIR resources [19]. Examples are: FHIR consent resource [20]; FHIR AuditEvent or Provenance for storing information about data sources; FHIR AuditEvent enables tracking data communication including the deletion of data; FHIR Security Labels allow tagging data when the purpose of use has changed. For coding the purpose of use, specific vocabulary can be deployed.

Conclusions

Paradigm changes in health and social care lead to highly distributed and dynamic ecosystems, integrating multiple jurisdictional and policy domains, technologies, methodologies, knowledge and concept representation style, languages, cultural background and expectations, education and skills, etc., requiring advanced interoperability solutions. The interoperability challenge is not limited to ICT environment, but includes the entire ecosystem. Appropriate security and privacy solutions provide trust and therefore acceptance of health solutions and their IT support, as shown in Table 1.

Table 1. Relations of GDPR and 5P Medicine

GDPR	Details	Impacts to system architecture	Impacts to 5P medicine
New definitio n to PII	PHI characterizes health status and individual context/ conditions	Multi-domain business system architecture incl. development process	Individually tailored diagnosis and therapy including prediction and prevention
Explicit policies	Machine-processable, dynamically managed, ontology-based know-ledge-driven interopera-bility	Representation and transformation of a real-world business system to implementable artefacts, managing all concept levels from knowledge space to data models	Systems medicine incl. all perspectives from elementary particle to society with active participation of data subject
Business system and business process aware privacy	Permanent risk analysis, business system and process mngt, data governance management	Enterprise model and RM-ODP views for managing the system and selecting and correctly interrelating/ constraining existing resources	Democratizing health and social care, respecting personal wishes and expectations, combined with legal, ethical and fair principles

Thereby, security and privacy are not disabling but enabling new technologies. Security and privacy management will be increasingly model-driven, ontology-based and automated, using system intelligence such as AI and machine learning. Definition, harmonization and enforcement of policies must be automated as well. For that reason, policies must be represented comprehensively and formally. The presented system-theoretical, architecture centered modeling approach does not re-write problematic legislation [21], but supports use case specific analysis, management and design of needed comoonents and relations for 5P systems. That way, it enables intelligent, adaptive systems for advanced 5P medicine.

Acknowledgements

The authors are indebted to thank their colleagues from EFMI WGs "EHR" and "Security, Safety and Ethics" as well as from the IMIA WG "Security in Health Information Systems" for their valuable input. The work would not have been possible without the cooperation with ISO/TC215, CEN/TC251, HL7 International, Inc., but also without the support of the German Data Protection and Data Security Association (GDD).

References

[1] B. Blobel, P. Ruotsalainen, D.M. Lopez, F. Oemig, Requirements and Solutions for Personalized Health Systems. *Stud Health Technol Inform* **237** (2017), 3-21.

[2] European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). EC, Brussels 2016. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] IEEE Standards Association. ANSI/IEEE 1471-2000 - IEEE Recommended Practice for Architectural Description for Software-Intensive Systems. IEEE Computer Society, New York, NY, USA, 2000

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

[5] B. Blobel, Application of the Component Paradigm for Analysis and Design of Advanced Health System Architectures. *Int J Med Inform* **60,3** (2000), 281-301.

[6] B. Blobel, Architectural approach to eHealth for enabling paradigm changes in health. *Methods Inf Med* **49,2** (2010), 123-134.

[7] European Parliament and Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. EC, Brussels 2016. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[8] International Organization for Standardization. ISO 23903 Health informatics - Interoperability Reference Architecture. In preparation.

[9] International Organization for Standardization. ISO 21298:2017 Health informatics – Structural and functional roles. ISO, Geneva, 2014.

[10] F. Kamareddine, T. Laan, R.A. Nederpelt, Modern Perspective on Type Theory. Kluwer Academic Publishers, New York, 2004.

[11] R. Bloe, F. Kamareddine, R. Nederpelt, The Barendregt Cube with Definitions and Generalized Reduction. *Inf Comput* **126,2** (1996), 123-143.

[12] International Organization for Standardization. ISO/IEC 10746-3:2009 Information technology-Open distributed processing-Reference model: Architecture. ISO, Geneva, 2009.

[13] N. Damianou, N. Dulay, E. Lupu, M. Sloman, The Ponder Policy Specification Language. In: M. Sloman, J. Lobo, and E. Lupu (Eds.): *POLICY 2001, LNCS 1995*, 18-38. Springer, Berlin Heidelberg, 2001.

[14] Health Level 7 International, Inc., HL7 Healthcare Privacy and Security Classification System (HCS) – Release 3. HL7 International, Ann Arbor, May 2013.

[15] Health Level 7 International, Inc., HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1. HL7 International, Ann Arbor, September 2013.

[16] Data Segmentation for Privacy HIMSS 2012, Final V2. Available at https://vdocuments.mx/data-segmentation-for-privacy-himss-2012-fina-lv2.html

[17] International Organization for Standardization. ISO/IEC 27001:2017 Information technology – Security techniques – Information security management systems – Requirements. ISO, Geneva, 2017.

[18] International Organization for Standardization. ISO/IEC 27002:2013 Information technology -- Security techniques – Code of practice for information security controls. ISO, Geneva, 2013.

[19] Health Level 7 International, Inc., FHIR Resources. Available at https://www.hl7.org/fhir/

[20] Health Level 7 International, Inc., FHIR consent resource. Available at http://hl7.org/implement/standards/ fhir/consent-examples.html

[21] J.A. Bovenberg, M. Almeida. Patients v. Myriad or the GDPR Access Right v. the EU Database Right. *European J Human Genetics* **27** (2018), 211-215.

Address for correspondence

Bernd Blobel, PhD, FACMI, FACHI, FHL7, FEFMI, FIAHSI, Professor, Medical Faculty, University of Regensburg, Regensburg, Germany; Email: bernd.blobel@klinik.uni-regensburg.de