A Privacy Management Analysis (PMA) of Exchanging International Patient Summary

Gokce B. Laleci ERTURKMEN[a,1], Ezelsu SIMSEK[a], Giorgio Cangioli[b] and Catherine Chronaki[b]
[a] *SRDC Software Research & Development and Consultancy Corp., Ankara, Turkey*
[b] *Health Level Seven (HL7) International Foundation, Brussels, Belgium*

Abstract. This paper provides a summary of the Privacy Management Analysis method followed for the analysis of the International Patient Summary exchange use cases of Trillium II Project. The objective is to recommend the required security and privacy measures by providing traceability from Regulations/Principles/Preferences to the recommended Security & Privacy Measures that needs to be implemented in pilots.

Keywords. Security and Privacy Controls, Privacy by Design, International Patient Summary

Introduction

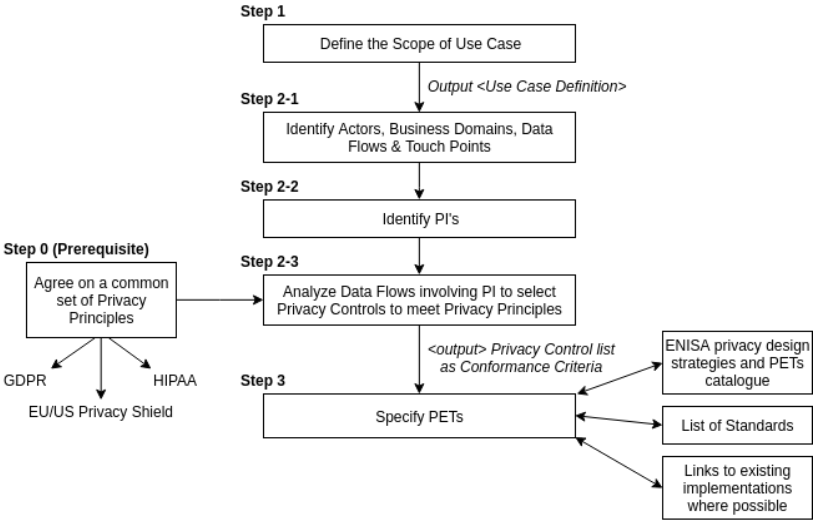
The mission of the Trillium II project is to advance an International Patient Summary (IPS) standard [1] in order to ease accessing and sharing health information of people in case of emergency or unplanned care anywhere and as needed. Trillium II gives priority to immunizations, allergies, medications, clinical problems, past operations and implants in such cases. Thanks to IPS offering a window to a person's health, citizens gain health-awareness, while health professionals are better informed which causes fewer errors and better decisions. This paper summarizes the analysis of the selected IPS exchange use cases in order to recommend the required security and privacy measures that can be employed during pilot implementations. In this respect, it examines the regulatory challenges/barriers (introduced by EU GDPR, US Health Information Portability and Accountability Act (HIPAA)); identifies the information security and privacy risks concerning Personal Information (PI); identifies the needs for security and privacy controls and provides a 'catalogue' of security and privacy services and methods as a guidance to implementers of these selected use cases.

1. Methodology

We have carried out a Privacy Management Analysis (PMA) for the IPS exchange use cases which provides traceability from Regulations/Principles/Preferences to the recommended Security & Privacy Measures that needs to be implemented in pilots. As

1 Corresponding Author: Gökce B. Laleci Ertürkmen, SRDC Software Research & Development and Consultancy Corp., Ankara, Turkey; E-malil: gokce@srdc.com.tr

mandated by The General Data Protection Regulation (GDPR) [2], it is aimed to follow a Privacy by Design (PbD) approach for a standard based methodology utilizing the best practices established in the domain. For this purpose, we have conducted an analysis of a number of key studies in this field [3,4,5] providing guidance about how PbD approach can be successfully employed for analysing a use case at hand to identify the required security and privacy architecture that meets the expectations of the legal landscape and the security and privacy principles of all of the affected parties in the selected use case. Consequently, we have decided to follow a hybrid approach by



exploiting the strengths of each of the mentioned references. Step by step demonstration of our methodology can be seen in Figure 1.

Figure 1. Trillium PMA Methodology

1.1. Selected Privacy Principle Set

Trillium II project aims the cross-border exchange of patient summaries between U.S. and EU countries. Within U.S., the processing and exchange of health information is subject to compliance to the Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules [6]. On the other hand, in EU regulation for the protection of natural persons with regard to the processing of personal data and on the free movement of such data depend on the EU General Data Protection Regulation (GDPR). ENISA Report in PbD, has thoroughly examined the new GDPR clauses and mapped these to nine Privacy and Security Principles, that can be used during Privacy and Security by Design procedures [5]. Those principals are; *Lawfulness, Consent, Purpose Binding, Necessity and Data Minimisation, Transparency and Openness, Rights of the Individual, Information Security, Accountability, Data Protection by design and by default.*

In the project, we carry out our PMA based on the ENISA principles, which has already been mapped to the EU GDPR clauses. On top of this, we have carefully analysed HIPAA Security and Privacy Rules to extract the security and privacy principles to be addressed and mapped these to the nine principles identified by ENISA [7].

2. Analysis of the Selected Use Cases and Results

In this paper we will focus on the analysis of the 'Cross-border Unplanned Care', which has been defined by epSOS project and will be operationalized via the eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) enabling cross-border health data exchange under the Connecting Europe Facility (CEF). Each country is represented by a "National Contact Point for eHealth (NCPeH)" creating a Circle of Trust" (CoT) that enables inbound and outbound communication cross borders. It is assumed that within each country, through the agreements between point of cares (PoC) and NCPeH a national CoT is created, which leads up to building cascaded circles of trust. For the interactions between the NCPeHs of corresponding countries, either EU-US Privacy Shield (when cross border exchange between an EU member state and U.S. is targeted) or directly GDPR (when cross border exchange between an EU member states) would apply.

Patient Summary used for the medical treatment of a patient and metadata needed to control the exchange of healthcare related data between NCPeHs and between NCPeHs and PoCs, respectively) are the Personally Identifying (PI) that have been identified for this use case. Among these, Patient Consent and Identity Claims can be categorized as Incoming PIs, the log data and administrative data as Internally Generated PIs, while Patient Summary can be categorized as both Incoming and Outgoing PIs.

Having examined the system and identifying PIs, we identified a total of 53 different privacy controls as set of selected privacy conformance criteria that would apply to this use case to fulfill the aforementioned privacy principles. Afterwards, we presented pointers to the recommended security and privacy enhancing technologies in order to address the needs of the security controls identified (as exemplified in Table 2). The full list of recommended PETs can be found in our report available at [7].

Table 2. Example Security and Privacy controls and recommended PETs

Security and Privacy Controls	**Recommended security and privacy enhancing technologies to address these requirements**
Principle: Information Security *Privacy Controls: Identification (C.20) & Authentication (C.21, C.22, C.23, C24)*	* eHDSI Identity Management Service Specification description [8] * CEF eID building block (the eIDAS Regulation (EU 910/2014, 2014)) * HL7 FHIR security guidelines recommends OAuth and OpenID Connect to be used to authenticate and/or authorize the users.
Principle: Transparency and Openness *Privacy Controls:* C.9-C.14	The following transparency enhancing techniques can be implemented as recommended by ENISA Report [5]: * Privacy dashboards that presents the type of personal data collected, how they are used, to what parties they are made visible * Tools that extract by themselves the privacy information rather than depending on the declarations of the service providers, such as browser add-ons that analyses the events occurring when a user visits a website and continuously updates a graph showing the tracking sites and their interactions * Tools that rely on the effort of communities of peers (or experts) to evaluate privacy policies and track their evolution *Formal languages such as P3P, Privacy Bird, CI (Contextual Integrity), S4P and SIMPL can be utilized to make it easier for service providers and users to express their privacy policies and privacy requirements
Principle: Data Protection by design	Implement Minimize", "Hide", "Separate", "Enforce" and "Demonstrate" design strategies pointed out by ENISA Report. Guidance about the Privacy Enhancing

and by default *Privacy Controls:* C.52-C.53	Technologies (PETs) implementing these strategies can be found in ENISA Report [5].

3. Conclusions

In this analysis we have greatly benefited from the eHealth Digital Service Infrastructure (DSI) Security Service Specifications [8] as one of the analysed use cases is cross border "unplanned care". The eHDSI Security Policy specifications, and the accompanying Security Services Specifications very well addresses the requirements of *Information Security* principle (including identification, authentication, digital signatures, access control, confidentiality, system and data integrity, non-repudiation) and *Accountability* principle. On the other hand, the new requirements introduced by GDPR such as *Transparency and Openness*, and *Rights of Individuals (*online access to personal data and possibilities to exercise data subject rights such as withdrawing consent or requesting rectification, blocking and erasure of personal data) are not directly addressed eHealth DSI Security Services Specifications. Here we have utilized the guidance provided by ENISA report to point the implementers to the possible Privacy Enhancing Technologies (PETs) suggested by ENISA (e.g. implementing formal languages such as P3P, Privacy Bird, CI (Contextual Integrity), S4P and SIMPL for transparently sharing privacy policies). In addition to these, different from the eHDSI (exchanging Patient Summaries represented as HL7 CDA documents over an IHE XC*-based infrastructure), Trillium II intends to use HL7 FHIR resources to better reflect the new needs of the International Patient Summary [9]. In our analysis we have taken in to account these differences and provided references to security and privacy measures that is also applicable to RESTful HL7 FHIR resource exchange paradigm (e.g OAuth and OpenID Connect).

References

[1] International Patient Summary Standard for Trial Use, http://international-patient-summary.net/mediawiki/index.php?title=IPS_implementationguide_1

[2] European Parliament & Council, Regulation 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). *L119*, 1-88

[3] OASIS PMRM TC, OASIS Privacy Management Reference Model (PMRM) Version 1.0, 2016.

[4] PRIPARE Consortium, PRIPARE Privacy- and Security-by-design Methodology Handbook, 2016.

[5] ENISA, Privacy and Data Protection by Design- from Policy to Engineering, 2015. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

[6] HHS, Health Insurance Portability and Accountability Act of 1996.

[7] Trillium II Consortium, Deliverable D3.6 Catalogue of Security and Privacy Controls and Methods for mitigating the security and privacy risks associated with use cases, https://trillium2.eu/deliverables/

[8] eHDSI, eHealth DSI Security Services Specification, 2017. Retrieved from https://ec.europa.eu/cefdigital/wiki/download/attachments/37752830/Security%20Services%20Specification_v2.1.0.doc?version=1&modificationDate=1496299722709&api=v2

[9] International Patient Summary Implementation Guide, http://hl7.org/fhir/uv/ips/2018May/index.html