Caring is Sharing – Exploiting the Value in Data for Health and Innovation
M. Hägglund et al. (Eds.)

doi:10.3233/SHTI230105

An Architecture for Providing Personalized Digital Health

Jaime DELGADO [1] and Silvia LLORENTE
Departament d'Arquitectura de Computadors (DAC), Universitat Politècnica de Catalunya (UPC), Spain
ORCiD ID: Jaime DELGADO https://orcid.org/0000-0003-1366-663X
Silvia LLORENTE https://orcid.org/0000-0003-2000-6912

Abstract. Patients need mechanisms to integrate health information coming from different sources, including personal devices. This would lead to Personalized Digital Health (PDH). HIPAMS (Health Information Protection And Management System) is a modular and interoperable secure architecture that helps in achieving this objective and building a Framework for PDH. The paper presents HIPAMS and how it supports PDH.

Keywords. Personalized Digital Health, Modular architecture, Security, Privacy

1. Introduction

Integrating different sources of medical information into one system is one step towards achieving personalized health services. For this purpose, we can combine electronic health records coming from different health institutions with information coming from personal health devices, like smart watches or blood pressure monitors.

In order to provide a solution to facilitate this integration, we propose the use of a generic modular architecture called HIPAMS (Health Information Protection And Management System) [1] that is based on REST (REpresentational State Transfer) [2] web services. It is derived from work previously developed by the authors [3][4]. HIPAMS provides new specific modules to support medical information, like provenance and consents, as well as different modules for supporting different health information formats. There are other approaches for integration of different eHealth services, like the Profiles defined by IHE [5], where some of the concepts, like patient privacy consents, have already been defined.

We plan to propose HIPAMS as a way to develop a Personalized Digital Health Framework (PDH-F). In this context, ISO/TC 215/WG 11 (Personalized digital health) [6] has started to specify such a standard [7]. This PDH Framework specification will define how patients may manage their personal medical information in cooperation with health institutions.

In the rest of the paper, we describe HIPAMS and its modules and provide some hints on how such a platform can help in achieving the objectives defined in PDH-F.

[1] Corresponding Author: Jaime Delgado, E-mail: jaime.delgado@upc.edu.

2. Methods

The ideas behind HIPAMS come from existing work already developed for the secure management and protection of different kinds of digital information, like Multimedia content [3] and Genomic information [4]. Some initial ideas on the definition of HIPAMS were already presented in [1].

Figure 1 depicts its structure. The functionality of the most relevant modules is briefly described next. They are ordered alphabetically:

- Authorization Service: Module for access authorization based on privacy and access rules, and for validation of medical consents.
- Certification Authority: Provides digital certificates to secure communications.
- Consent Service: Module in charge of the creation and management of the medical consents.
- Health Content Service: Module in charge of health information management, both in reading and writing operations. This is a critical module covering the formats of the medical information, including Electronic Health Records (EHR) and medical documents, such as those based on HL7's CDA (Clinical Document Architecture) [8], among others.
- Metadata Service: Module in charge of handling metadata of medical documents, which may help in identifying and finding them. Again, very critical for the formats. In addition, FAIR (Findable, Accessible, Interoperable, Reusable) [9] [10] data principles could be considered.
- Policy Service: Module in charge of the creation of the authorization rules, which are organized into policies.
- Protection Service: Module which creates protection information as well as application of the mechanisms defined (i. e. encryption, signature, etc.).
- Provenance Service: Module in charge of adding and managing provenance information for health digital content supported by the platform.
- Report / Track Service: Module in charge of reporting the operations done in the system, especially those not authorized.
- Search Service: Performs searches over medical information, providing extra filtering features.
- User Application: Web application that sends requests to the Workflow Manager based on user actions. The communication between this application and the rest of the architecture is done through a secure channel.
- Workflow Manager: Intermediate module that acts as a unique entry point to the system. It checks operation authorization before interacting with other modules.

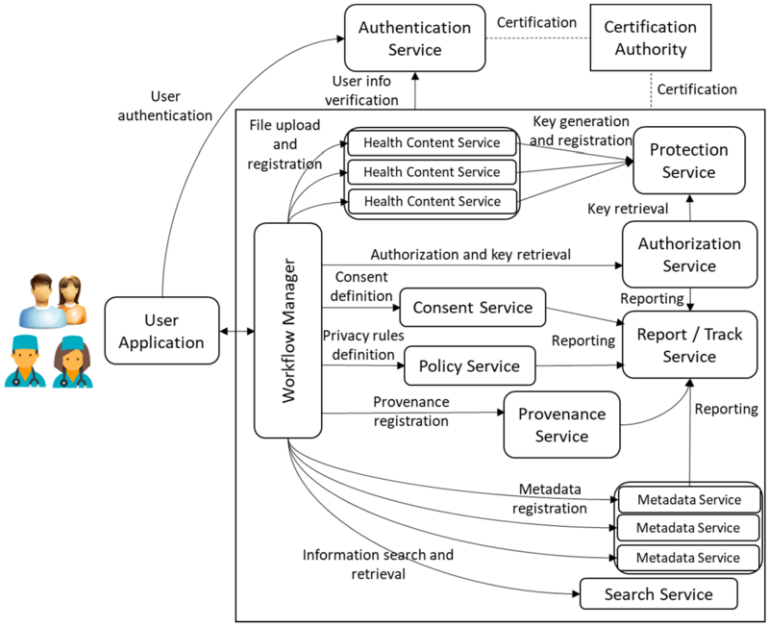

Figure 1. HIPAMS Architecture.

It is worth noting that this architecture allows the use of different formats representing medical information. The services managing these formats are Health Content and Metadata. As it can be seen in Figure 1, we may have several submodules inside Health Content and Metadata to support the different formats supported by the system implementing this architecture. Another approach for HIPAMS modules implementation could be using FHIR resources, such as Consents, or FHIR security aspects [11].

3. Results

We have defined several use cases to illustrate for example how HIPAMS can be used to register and search for medical information in a secure way. Figure 2 shows the workflow diagram for a registration use case, when the medical content requires encryption and privacy protection. The registered medical content may come from different sources (medical records, patient devices, …).

First of all, the user has to authenticate in front of the Authentication Service in order to receive a valid token. This token will be used afterwards when invoking the rest of services through the user application. Four services are used in this use case, Health Content Service (HCS), Metadata Service (MS), Protection Service (PtS) and Policy Service (PS). HCS is in charge of content creation. As protection is required, HCS calls the PtS corresponding operation to encrypt the medical information stored. Then, metadata is registered in MS. In this example, metadata does not need to be protected, but it might happen in other cases, so the PtS would be also called in that case. Afterwards, two privacy policies are created by the PS, to control later access to the protected medical

content. Again, the policies are created to control access to the content, but, if metadata also requires access control, one or more policies could be also created to control it.

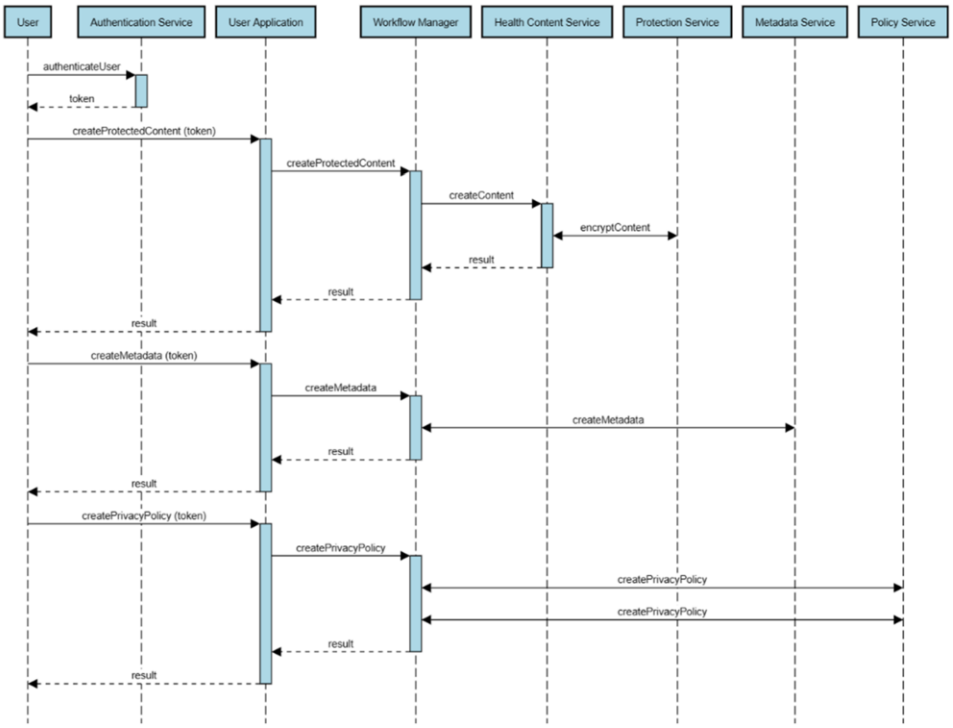

Figure 2. Protected medical content use case.

4. Discussion

HIPAMS is presented here as a possible way of facilitating Personalized Digital Health to patients. The final objective is to give them the opportunity to combine medical information coming from many different sources, like medical records coming from medical institutions and measures taken from their personal medical devices, like smart watches, mobile phones or any other medical device intended for being used at patients' home. This information may be useful for both primary and secondary use.

To do so, different medical information formats should be supported, making use of standardized formats as much as possible. As already shown in Figure 1, HCS and MS may contain submodules to support different formats. Moreover, if new formats appear in the future, they could be supported by implementing / integrating new submodules.

We would like to highlight that the architecture allows the inclusion of externally implemented modules, by defining a REST Application Programming Interface (API) that then calls to the module.

Providing this additional information to healthcare professionals facilitates a better medical decision, but may imply the need of extra work for its processing. However, HIPAMS provides tools, such as advanced search, that reduce this extra burden.

5. Conclusions and Future Work

We have introduced HIPAMS as an architecture to facilitate sharing and integration of health information coming from different sources with a special focus in patients' personal information. This leads to PDH (Personalized Digital Health).

Nevertheless, some specific aspects need further development, such as the idea of dynamic consents, which is implicit in the model, by jointly using Consent and Authorization services. Another example is the Provenance service, which is also very relevant.

On the other hand, HIPAMS could be used for the development of the PDH Framework to be standardized by ISO/TC 215/WG 11 "Personalized digital health". We are currently contributing to this work. With this purpose in mind, APIs should be defined for the different modules and more use cases identified.

Finally, and going further in the issues raised in the Discussion section, the concept of a federation of HIPAMS could be considered in order to support different medical institutions, as it is not realistic to store all this information in only one platform. The definition of standardized interfaces is key to achieve this objective. An advantage of having such a federation is that the communication between equivalent modules could be done through the same operations.

Acknowledgements

The work presented in this paper has been partially supported by the Spanish Government under the project GenClinLab-Sec (Mechanisms for secure and efficient management of genomic information tailored to clinical laboratories: Security Aspects, PID2020-114394RB-C31) funded by MCIN/AEI/10.13039/501100011033 and by the Generalitat de Catalunya (2017 SGR 1749).

References

[1] Delgado, J, Llorente, S. Provenance and dynamic consents for the management of medical data. Studies in Health Technology and Informatics, 2022, Volume 299: 171-176. doi: 10.3233/SHTI220978
[2] Fielding RT. Architectural Styles and the Design of Network-based Software Architectures [PhD. Dissertation]. University of California, Irvine; 2000
[3] Llorente S, Rodriguez E, Delgado J, Torres-Padrosa V. Standards-based architectures for content management. IEEE multimedia. 2013 Oct.-Dec.; 20(4):62-72. doi: 10.1109/MMUL.2012.58
[4] Llorente S, Delgado J. Implementation of Privacy and Security for a Genomic Information System Based on Standards. Journal of Personalized Medicine. 2022; 12(6):915. doi: 10.3390/jpm12060915
[5] IHE International. Integrating the Healthcare Enterprise. Available from: https://www.ihe.net/
[6] ISO/TC 215. Health informatics Information. Available from: https://www.iso.org/committee/54960.html
[7] ISO/TC 215/WG11, ISO/AWI TS 6201, Health Informatics - Personalized Digital Health Framework (PDH-F) (Under development). Information available from: https://www.iso.org/standard/82107.html
[8] HL7. HL7 Clinical Document Architecture (CDA). Available from: http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
[9] Wilkinson MD, Dumontier M, Aalbersberg IJ et al. The FAIR Guiding Principles for scientific data management and stewardship. Sci Data 3. 2016; 160018. doi: 10.1038/sdata.2016.18
[10] Delgado J, Llorente S. FAIR Aspects of a Health Information Protection and Management System. Methods of Information in Medicine. 2022 Dec;61(S 02):e172-e182.
[11] HL7. HL7 Fast Healthcare Interoperability Resource (FHIR). Available from: https://hl7.org/fhir/