pHealth 2022
B. Blobel et al. (Eds.)

doi:10.3233/SHTI220978

Provenance and Dynamic Consents for the Management of Medical Data

Jaime DELGADO[1] and Silvia LLORENTE
Information Modeling and Processing (IMP) group – DMAG,
Computer Architecture Dept. (DAC),
Universitat Politècnica de Catalunya (UPC - BarcelonaTECH)

Abstract. Medical data describe patient health information, both in healthy and disease conditions. In any case, health institutions need to ask for patient consent in order to provide their services. Patients usually give consent on a one-time basis, for a specific usage. Afterwards, if medical data usage is research, original patient consent does not apply and further consents should be required. On the other hand, provenance of medical data to verify the origin of health procedures is desirable, as digital health is increasing. We propose HIPAMS modular architecture to provide both provenance and dynamic consents for medical data as described in this paper.

Keywords. Dynamic consents, provenance, modular architecture, HIPAMS

Introduction

Provenance of medical information and dynamic consents from patients are some desirable features for a Health Information System (HIS) that are currently not widely supported.

In this paper, we propose the use of a modular platform, Health Information And Management System (HIPAMS), derived from MIPAMS ("M" for Multimedia) [1] and GIPAMS ("G" for Genomic) [2], [3], to provide support for managing and storing provenance information and also to manage dynamic consents.

It is worth noting that HIPAMS is content agnostic, and it may apply to any health information format. Information for provenance and consents will be independent from the format itself, managed by specific modules, accessed via clear Application Programming Interfaces (API's) in order to provide low coupling between them.

This paper describes the proposed HIPAMS architecture, focusing on how dynamic consents and provenance metadata can be implemented and included in the system. Afterwards, we discuss different issues on provenance, dynamic consents and their integration. Finally, we present conclusions and future work.

[1] Corresponding Author: Jaime Delgado, Universitat Politècnica de Catalunya (UPC), Barcelona, Spain; e-mail: jaime.delgado@upc.edu

1. Methods – HIPAMS Description

The architecture of the developed platform is an evolution of our original Multimedia Information Protection And Management System, MIPAMS [1], [4] and also of the Genomic Information Protection And Management System, GIPAMS [3]. As it now deals with health information, we have called it Health Information Protection And Management System, HIPAMS.

It must be pointed out the modular nature of these architectures, which provides several advantages, like the possibility of reusing modules for different kinds of content and the facility to add more modules with the same foundational principles to support new functionalities.

Figure 1 depicts its structure. Most of the modules were already described in [3], so we only describe the functionality of the new modules and those that have been extended (in alphabetical order):

- Authorization Service: Module for authorization rules *and consents* validation.
- Health Content Service: Module in charge of health information management, both in reading and writing operations.
- Metadata Service: Module in charge of handling metadata of medical documents, which may help in identifying and finding them.
- Policy / *Consent* Service: Module in charge of the creation of the authorization rules, which are organized into policies and consents.
- *Provenance* Service: New module in charge of adding and managing provenance information for health digital content supported by the platform.

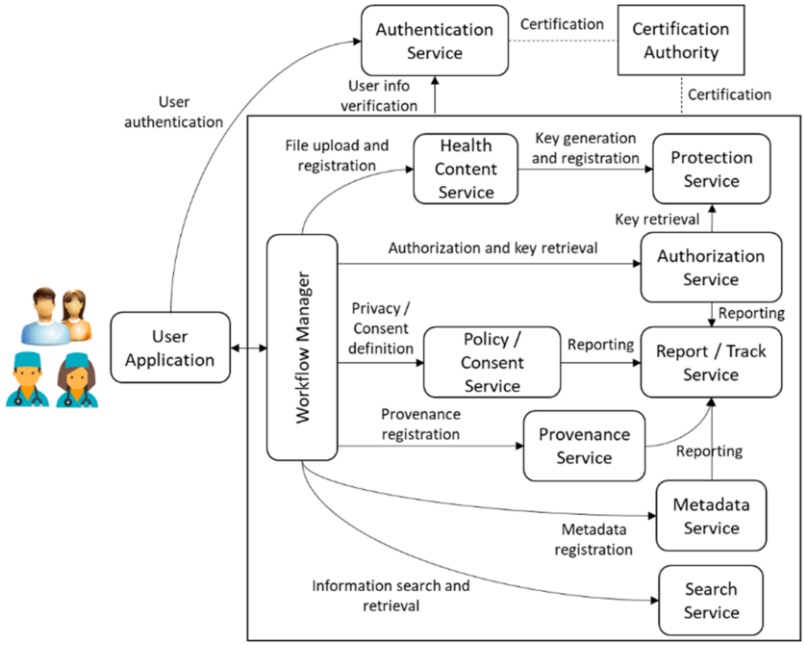

Figure 1. HIPAMS Architecture.

The communication between the modules in HIPAMS architecture is based on Representational State Transfer (REST) [5], which makes use of the HTTP protocol methods to communicate clients and servers.

Each module provides one or more REST operations that can be invoked by the Workflow Manager (WM) or other module(s). The User Application cannot directly invoke any module's operations. User Application requests' can only be done through the WM. Moreover, we make use of JSON Web Tokens (JWT) [6] to guarantee that the user that wants to call an operation is authenticated and has the corresponding permission to do so.

2. Results

The first part of this section on results analyses our approach to, and considerations on, dynamic consents, mainly in relation to static consents and policies and their authorization process. Then, the issue of data provenance is presented, where one of the possible alternative approaches is selected as a starting point.

2.1. Dynamic Consents, Policies and Authorization

Health institutions require patient's consents. They have to request them in order to be able to provide their medical services to patients, who give these consents for specific purposes, usually related to the clinical practice and in a one-time (or a period of time) basis. Therefore, if some medical information can be useful later on, for instance, for research or educational purposes, the initial consent given by the patient may not be enough.

In some cases, consents may change over time (dynamic consents) due to several reasons, but this feature cannot be easily represented and managed in current health systems.

In order to provide a possible solution to the current consent rigidness, we are exploring the dynamic consent concept, using privacy protection policies and its corresponding authorization algorithms. Our proposal is to give the patient, possibly through the Hospital Information System (HIS), the ability to be informed, for example, that her medical information could have a secondary use for research, so a change in the consent is needed. It should be noted that research is not the only possibility. Once the mechanism is established, any use can be informed and requested to the user.

The first step to achieve dynamic consents is to decide the best way of representing the information. Our proposal is to define them as policies and rules for two reasons: 1) there are already expertise and tools available on that, including for example previous work on GIPAMS [3], and 2) authorization mechanisms for policies and rules are in place. Then, dynamic consents could be implemented by creating a new rule (or a policy) with the modified conditions approved by the patient (e.g. usage, timing, health professional, etc.). The system should look for the latest consent when authorization is required.

In any case, to be able to take this approach, we should consider how to integrate it with existing standardized consent formats, like the one currently under development by HL7 FHIR (Health Level 7 Fast Healthcare Interoperability Resources) [7]. This consent format already considers the possibility of computing consents using policies, as it includes a policy element, which may contain a policy expressed in a well-known policy

language, like eXtensible Access Control Markup Language (XACML) [8]. Then, as GIPAMS uses XACML to express policies and rules to authorize access to genomic information, it seems a good starting point to use this language to implement the Policy / Consent Service in HIPAMS (see section 2), including policies into consents following FHIR specifications. Afterwards, when dynamic consent authorization is required, the Authorization Service will be used for this task, as it already supports XACML authorization mechanisms.

2.2. Provenance Information

There are different technical approaches for the digital management of provenance information, or provenance metadata. The approach may vary depending on the kind of information to which provenance metadata is attached. In our case, we are dealing with health information. Provenance requirements for health are not necessarily the same that for multimedia content, such as images, as an example.

In order to obtain the best solution for provenance metadata management, we have analyzed several approaches. These include:

- W3C model [9], which is the basis for several other solutions.
- Specific provenance metadata for images to help controlling fake content, as being considered by the JPEG standardization working group [10].
- The new work in ISO/TC 276 (Biotechnology) for biological samples [11] and its relationship with genomic standards such as ISO/IEC 23092 (Genomic Information Representation, MPEG-G) [12].

Our first solution consists in trying to adapt for health information the work we are doing on a proposal for JPEG provenance metadata [4]. Therefore, a Provenance Service is to be developed for HIPAMS. Although images and health information are different, the structure of the associated provenance metadata and the mechanisms to generate and process that metadada may be rather similar.

3. Discussion

There are many initiatives for the definition and provision of digital consents, like FHIR Consents [5], ONC eConsent Tookit [13] or the electronic Informed Consent concept [14], [15].

They have in common the concern about how informed consent should be managed electronically, facilitating tools and guidelines to do so. Taking some of these initiatives as a base point, they may facilitate dynamic consent, as they already consider electronic means for managing consents.

However, dynamic consent is also already considered in the literature, mainly related to biobanks and other institutions where long term relationship with patients and participants is of utmost importance, as presented in [16].

The initiatives indicated are a small sample of an existing problem, that there is a large number of solutions to address electronic and dynamic consents, as there is not a common universal electronic format to represent and manage consents.

In summary, dynamic consent is a desirable feature when managing consents, but, as briefly stated in this section, there is not a unique way to provide a solution. Our approach is to implement dynamic consents using a modular architecture like HIPAMS. Then, this could be combined with other existing initiatives. Finally, we should always consider the associated legal aspects, restrictions and obligations.

With respect to provenance, the discussion covers different questions, such as: how much detailed provenance metadata is needed, how is these metadata to be expressed and created, which level of protection (security and privacy) is needed? Our first results go in the line of reusing and adapting other existing solutions, many of them still under development.

Finally, we should keep in mind that we are aiming at an integrated approach for handling health information (the HIPAMS architecture described in section 2). Therefore, dynamic consents and provenance are key aspects for this integration since they are usually considered independently.

4. Conclusions and Future Work

The work we have introduced focuses on an integrated and modular architecture for health information management system that is interoperable and secure. HIPAMS is our implementation of such a system. However, there are still a few specific aspects that could be included to improve the system. Two of them have been addressed in this paper, namely the management of dynamic consents and the creation and use of provenance metadata associated to the health information.

For the first aspect, we propose to use privacy rules and associated mechanisms, while for the provenance aspect we want to consider adapting newly defined approaches for other kind of content, such as images or even genomic information.

We would like to stress that we are working on a Spanish Government funded Project (GenClinLab-Sec, PID2020-114394RB-C31), where we are developing the GIPAMS architecture, already mentioned throughout the paper, to support the secure interchange of genomic information applied to the clinical practice in the genomic laboratories. We planned several scenarios to support interchange of information within the same lab and between different labs. We expect that lessons learnt in the implementation of this project could also be applied to health information.

With respect to future work, apart from refining and implementing the 2 new HIPAMS modules, we are considering to contribute these ideas to the just started standardization work on a Personalized Digital Health Framework (PDH-F), taking place in the new working group WG11 of ISO/TC 215 (Health Informatics).

Acknowledgements

This work is partly supported by the Spanish Government (GenClinLab-Sec, PID2020-114394RB-C31) and by the Generalitat de Catalunya (2017 SGR 1749).

References

[1] Llorente, S.; Rodriguez, E.; Delgado, J.; Torres-Padrosa, V. Standards-based architectures for content management, IEEE Multim, 2012. https://doi.org/10.1109/MMUL.2012.58
[2] Delgado, J.; Llorente, S. FAIR aspects of a Genomic Information Protection and Management System, Stud Health Technol Inform, 2021, 287, 50 – 54. https://ebooks.iospress.nl/volumearticle/58254
[3] Llorente, S.; Delgado, J. Implementation of Privacy and Security for a Genomic Information System Based on Standards, J Pers Med, 2022, 12(6):915. https://www.mdpi.com/2075-4426/12/6/915
[4] Fotos, N. Specification and implementation of metadata for secure image provenance information, Master Thesis – ETSETB – UPC, 2022
[5] Fielding, R. T. Architectural Styles and the Design of Network-based Software Architectures. University of California, Irving, 2000. https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm
[6] IETF. JSON Web Token (JWT). 2015. https://datatracker.ietf.org/doc/html/rfc7519
[7] HL7 FHIR (Health Level 7 Fast Healthcare Interoperability Resources), Consent, 2022. http://build.fhir.org/consent.html
[8] OASIS, eXtensible Access Control Markup Language (XACML) v3.0, 2017. http://www.oasis-open.org/specs/index.php#xacmlv3.0
[9] W3C, Provenance Overview, 2013. https://www.w3.org/TR/prov-overview/
[10] JPEG (Joint Pictures Expert Group), JPEG Fake Media, 2022. https://jpeg.org/jpegfakemedia/documentation.html
[11] ISO/TC 276 (Biotechnology), ISO/DTS 23494, Provenance information model for biological material and data, 2022. https://www.iso.org/standard/80715.html
[12] ISO/IEC, ISO/IEC 23092, Genomic Information Representation, 2022. https://www.mpeg.org/standards/MPEG-G/
[13] ONC (Office of the National Coordinator for Health Information Technology), eConsent Tookit, 2022. https://www.healthit.gov/topic/privacy-security-and-hipaa/econsent-toolkit
[14] De Sutter, E. et al. Personalized and long-term electronic informed consent in clinical research: stakeholder views, BMC Medical Ethics 22, 108, 2021. https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-021-00675-7
[15] FDA, Informed Consent, 2014. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/informed-consent
[16] Teare, H. J. A. et al., Reflections on dynamic consent in biomedical research: the story so far, Eur J Hum Genet, 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7695991/