*proceedings*

MDPI

*Proceedings*

# FLEXEHR: Proposal of a Platform for Interoperability between Information Systems Based on Electronic Medical Records in Panama †

**Mel Nielsen, Amilkar Saavedra, Vladimir Villarreal *, Lilia Muñoz and Yarisol Castillo**

Grupo de Investigación en Tecnologías Computacionales Emergentes, Universidad Tecnológica de Panamá, Panama City 0819-07289, Panama; mel.nielsen@utp.ac.pa (M.N.); tenzinghang@gmail.com (A.S.); lilia.munoz@utp.ac.pa (L.M.); yarisol.castillo@utp.ac.pa (Y.C.)

* Correspondence: vladimir.villarreal@utp.ac.pa; Tel.: +507-6271-3226

† Presented at the 13th International Conference on Ubiquitous Computing and Ambient Intelligence UCAmI 2019, Toledo, Spain, 2–5 December 2019.

Published: 20 November 2019

**Abstract:** The existing technologies, systems, or models in the hospital system, in certain aspects have, in terms of integrity, difficulties in carrying out an adequate, systematic, and automated record of patient data. To this end, the electronic health records (EHR) have been designed to provide updated information to the entire health system. This document is one of the most important that exists within the hospital system throughout the country, and its main objective is the care, treatment, and monitoring of peoples' health in a simple and conceptualized way. This article proposes the design of a flexible electronic health record system (FLEXEHR), integrating generic systems and totally flexible, based on web services so that different hospital information systems can be interconnected, thus creating a patient data gateway in an orderly and structured way, considering its availability, confidentiality, and integrity. In Panama, existing health systems have the disadvantage that they are not interoperable, which generates duplication of EHR according to the type of health entity visited.

**Keywords:** eHealth; interoperability; electronical medical record; health platform; architectures for health

## 1. Introduction

Information and communication technologies (ICTs) in the health sector are a very important issue within the government and the private sector, since this tool supports management of healthcare in a constant way through the management of information, recording patients' doctors, statistics, etc. The health sector is one of the most important in the social and economic field in different cities. However, even when technology is related to the health sector, certain aspects or barriers that prevent new technologies from being integrated into existing hospital information systems can be appreciated. One of the main barriers is the experience that the doctor has in the health system, since this is one of the main users that updates the electronic patient registration system; they will influence other users such as nurses, technicians, and administrative staff to use the system. Some of the barriers that we could mention within the implementation of a new technology within the hospital system are: The lack of skill in the use of the computer, complexity of the system, communication interface of the system with the user (HCI), and concern of the security of patient data [1]. The latter is a point at which everyone fears that their data is at risk of being exposed; therefore, security must be considered when designing and developing information systems to protect the confidentiality, integrity, and availability of patient data. In addition, a study conducted

by Ochoa [2], established that 93.37% of the users consulted believe that medical records should be digital, while the rest do not, because they believe that digital systems are very unstable.

To offer effective methods of information exchange between hospital systems and to better manage the clinical records of patients, agreements have been defined to establish benefits with electronic health records and to unify said systems. However, the adoption of these technologies seems to be non-existent, or moves too slow.

This article proposes the design of a fully integrated, modular and flexible platform, which allows entities such as pharmacies, clinics, laboratories, and hospitals to integrate into this system with the purpose of sharing patient data with their respective prior authorization. These authorizations focus on the patient, who is the main actor and who will grant the authorization of the data contained in their clinical history. The flexible electronic health record system (FLEXEHR) is called integral because it is intended to incorporate all the necessary characteristics that are kept within a clinical record, modulated by the ability to add new entities within the system. Finally, it is called flexible because the system will have a basic standard of structure and format for the clinical records in such a way that, independently of the standard that a health entity is using, the system will be able to translate the information requested in the format or standard that is used by said requesting entity.

## 2. Problematic

The health sector is a group of numbered and classified entities that attend each of the relevant points in that sector on time. Clinics and hospitals focus on patient care; pharmacies and laboratories are responsible for specific functions, such as the administration of medications and physical or chemical examinations related to healthcare. However, each of these components focuses on patient care and wellbeing, since they are the origin that makes the entire sector work, without forgetting the medical part that combines experience and knowledge in the care and treatment of patients with different conditions.

Currently, in the environment in which health systems operate, the effective management of information is very important. The health sector has accidentally created complex ecosystems where information and data collection adopt regulations that allow information to be related in complex data structures that only make sense in the information systems of each health provider.

To coordinate the operation of all those involved in this sector is the responsibility of the Panamanian state according to Article 109 of Chapter 6 of the Constitution, which states, "that it is an essential function of the state to ensure the health of the population of the Republic." Therefore, Cabinet Decree No. 1 of 15 January 1969, establishes that it comprises the Ministry of Health (MINSA), the formulation and execution of the National Health Plan and the evaluation of all activities carried out in the sector. Under this premise the MINSA since 2010, as part of its strategic plan, sought to improve public health services by opting, as one of the major changes, to implement an information system with the ability to handle electronic clinical records. For the year 2011, the Social Security Fund (CSS), the institution providing health services for the insured in the country, was associated with this movement. By October 2013, the Ministry of Health initiated the electronic clinical file system project. Despite this movement to update the management of clinical records, there is no regular vision of the use or standardization of clinical records in Panama.

The redundancy of clinical records that a patient has in the health sector can, up to a point, cause ignorance and uncertainty about states treated outside each of the electronic clinical records (HCEs). The lack of control of drugs and laboratory supplies caused by the lack of interoperability of the different components of the sector (health provider entities or EPS), with which a patient can interact, truncate and put at risk the administration of drugs and reagents, causing inattention and suspension of treatments, are to a large extent a problem for the country.

The fragmentation caused by each EPS that manages its services offered through different systems based on different standards, customized data structures and adapted to their operational needs [3], makes the HCE in Panama practically non-existent.

The fact that each of the tools that manage this document do it under their own sense of the universe, limits the possibility of knowing the complete clinical history of an individual. Initiatives such as the one chosen by MINSA and CSS are used and known under their own terms and do not consider exchanging information with other EPS.

The reality is that as patients you have the freedom to choose any entity providing public or private health services. That is why it is necessary that MINSA, as the regulatory entity representing the State, take control of the management, regulation, administration, and definition, based on standards that host the country as a sovereign organ, of the electronic medical record [4,5] in order to regulate the information of patients with the necessary characteristics in accordance with the context of the needs of the country to be interoperable. This document is of utmost importance for the understanding of the actions carried out in the doctor–patient relationship.

This proposal is supported by Executive Decree No. 1458 of 6 November 2012, which regulates Law 68 of 20 November 2003 that regulates the rights and obligations of patients, in terms of information and free and informed decision; where Article No. 53 establishes that public and private health centers and services are obliged to organize, maintain, and administer, by conventional or electronic means, the clinical records of patients and ensure the integrity of the documents that comprise it and the confidentiality of the information contained within them [6].

## 3. Proposed Platform

Due to the great segmentation of patient information in various information systems that are currently managed by healthcare providers (EPS), this article proposes a service-oriented platform, managed by the government entity MINSA with the purpose of centralizing and managing the clinical history of patients.

Figure 1 shows the components of the proposed platform. Each of the components present in Figure 1 will independently address each segment of a patient's medical history. The platform system is divided into four important layers, corresponding to the software architecture to be developed.

### *3.1. Application Layer*

The platform is aimed at being a service about that, and needs a way of interacting with other systems or directly with an EPS, so an application layer is established where the applications or services are housed with which they can interact with this system. This layer exposes the services offered by the platform that show two services: Web application and control panel of the governmental system, housed in a server dedicated to the interaction of the users of these services. A dedicated server, API rest, executes the necessary instructions to manage the medical records stored in the data layer. In addition, there will be a mobile extension of the platform, to grant control of access to the patient's medical history.

The web app allows users or EPS to use the platform if they do not have an EHR management system. On the other hand, the Government System Dashboard is aimed at showing demographic information regarding diseases, viruses, and cases strictly defined by the strategic plans of health at the government level, as a tool to support decision-making. The mobile application allows extending health services and managing authorization notifications to the patient's EHR, as well as events such as appointments, laboratory orders, medications, among others. Finally, the API of the platform composes and extends the interoperability layer to facilitate the integration of the platform with other heterogeneous systems.

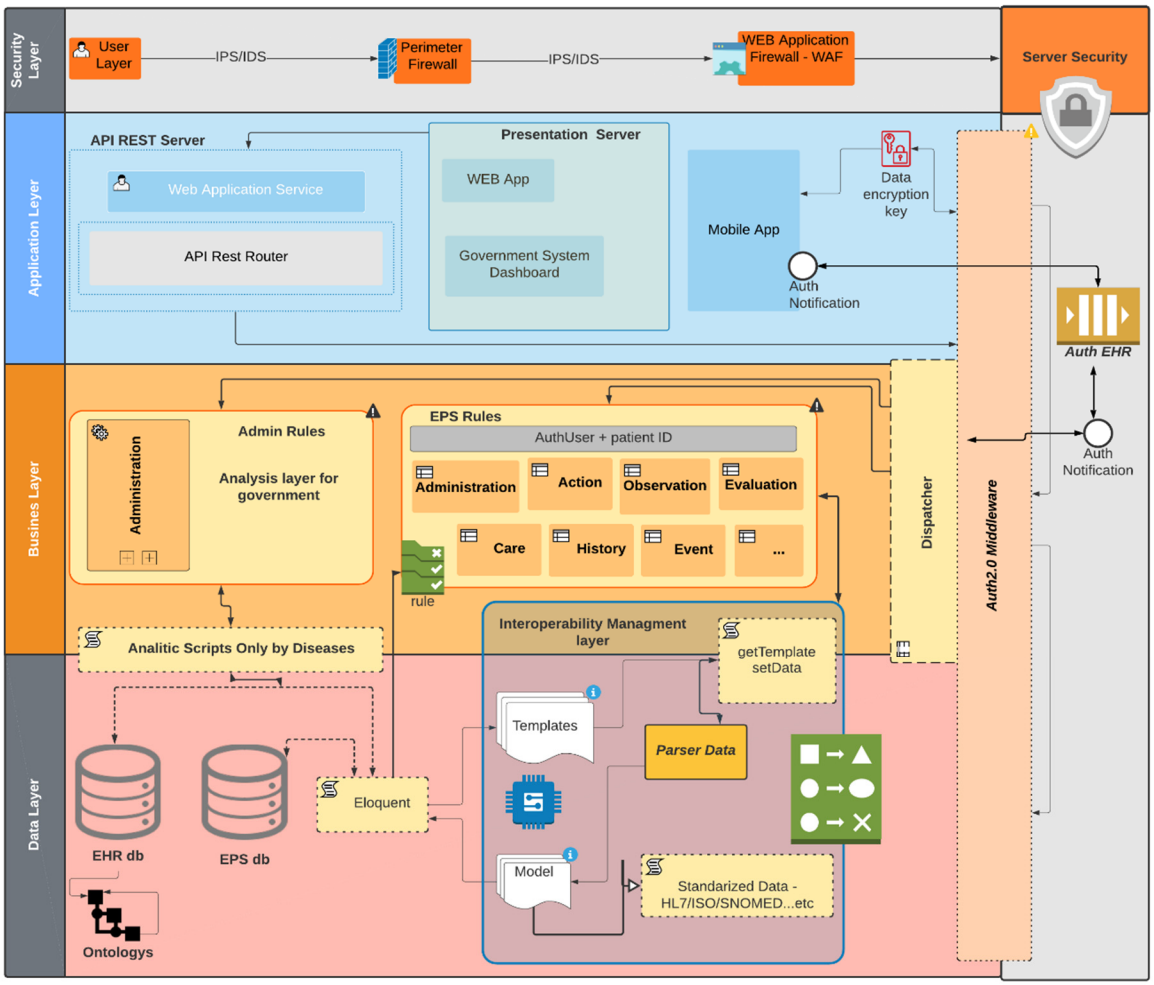


**Figure 1.** Layer diagram of the platform FLEXEHR.

### *3.2. Security Layer*

This layer is subdivided into four other important sublayers to maintain the confidentiality, integrity, and availability of the data, based on the HIPAA (Health Insurance Portability and Accountability Act) recommendations [7]. Therefore, the sublayers that will protect this open and centralized system of clinical histories are schematically described in the security layer. The first sublayer is that of users (see Figure 2). This layer is necessary, since many people tend to leave a risk bias in front of the exposure of their data, consequently they are looking to apply an intrusion prevention system. Then all the requests made advance on the security layer of the perimeter firewall. It filters the requests and mitigates the possible risks using an intrusion prevention system (IPS) and intrusion detection system (IDS) in front of the external network and the internal network. Then the process continues through the third sub-layer: web application firewall (WAF). This layer seeks to mitigate the risks presented by the http protocol and the possible disruptions and intruders that can capture traces of the information and that damage the code or database of the platform. Finally, the process is maintained, but now within the system, where the authentication and authorization protocol OAuth 2.0 [8] is used. This layer will protect the system while descending through the architecture.

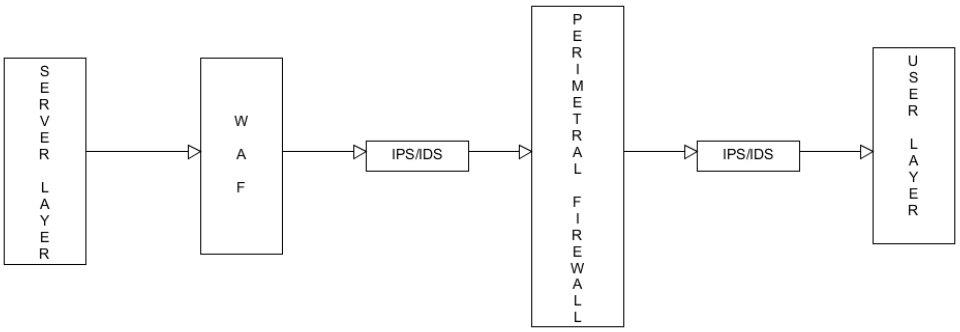


**Figure 2.** Diagram of the structure of the security layer.

### *3.3. Business Layer*

This layer is aimed at serving each type of external request made by each EPS, providing better control of the EPSs that exercise their services in the Panamanian territory, since this proposal must be accompanied by new governmental terms for their access. For example, if an EPS performs its services as a laboratory, it must be registered as a laboratory and comply with the registration requirements for access to the management of a patient's medical history. When descending through the business layer, OAuth 2.0 middleware is activated. To execute the requests in this layer, it is necessary to comply with control rules hosted in this middleware, where the authorization and authentication variables will be evaluated in this process. If an EPS requires consulting or managing the EHR of a patient, the request must be made from an agent (proprietary system) and by a registered IP address, which allows to successfully cross the security layer to the third sublayer, since in the fourth sublayer the middleware will consult the keys of the client_secret and the credentials of the EPS user accessing the system.

IP access*:* It is necessary to know the physical origin of each request to the platform to filter through the security layer, to protect the integrity and confidentiality of the data in the system.

Client_secret*:* The authentication process to access the information must be signed by an access code that defines that the application that makes the request has the right to make this request. This key must be granted in the process of affiliation or registration of the EPS, so that the clinical system of the EPS can make requests to the platform. The registration process will be controlled by MINSA, which, through the dashboard service of the Government System, will perform this task.

The management of the EHR is segmented for each type of EPS, with the necessary restrictions that are defined in the rules of the business layer. In this layer is also the dispatcher middleware, which is responsible for validating the credentials within the request, and then distributing it to the corresponding segment of the EPS that makes the request. On the other hand, the business rules of the Government System Dashboard will have access to information of the EHRs stored in the platform, for the analytical and statistical use of the population, maintaining the confidentiality of the information.

The business layer gives access to the layer that manages interoperability, where it is very important to handle the concept of interfaces and the complications that can add to the execution of a project of this magnitude. It is important to understand that the number of interfaces to be implemented can grow exponentially, based on the following formulation:

$$\text{Interfaces} = (n \times (n - 1))/2 \text{ [8]}$$

where $n$ is the number of systems with which information is exchanged, which can be transformed into a complex implementation problem.

According to the report Review of Interoperability Standards for eHealth in Latin America and the Caribbean of the Pan American Health Organization [9], standardizing information facilitates the timely exchange of information that can be translated into a better quality of care in the health services.

### *3.4. Interoperability Layer*

Each of the EPS manages, in totally heterogeneous systems, its own concept of EHR, whether standardized or not standardized. Forcing each EPS to modify its systems and implement interfaces to operate with this proposal is unattainable in terms of viability and feasibility. That is why the platform bases the concept of interoperability through the use of data templates of each EPS, to reduce the time of transition and implementation. In the EPS register you must present your data dictionary to create a template that subscribes to the standardized EHR of the platform, to your own concept. With the use of templates, the platform offers flexibility in the process of translating data entries and outputs, ensuring that centralized information is in a standardized and homogenous format for future implementations. In addition, the data entries go through an extra process of standardization to format the data that will make sense with the use of ontologies in the data layer, so that an EPS does not have to worry about standardizing its information to do transactions with the platform. The platform will be responsible for this process when translating the requests between the heterogeneous systems, as the centralized nucleus.

### *3.5. Data Layer*

It is composed of the necessary databases for the registration of the EPS and the whole data set of the health records of the users. The EHR database is aimed at the formation of standardized ontologies to give coherent semantic meaning to patient data that help to understand and analyze health status and risk variables.

The confidentiality of the data is a key point of this proposal. Having an authorization mechanism for information management is imperative. HIPAA regulates this fact and defines that the use of patients' clinical records must be duly authorized by the patient. Based on this regulation, the proposal extends this process using mobile technologies. The mobile application, which belongs to the presentation layer of the platform, allows requesting authorization so that EPS can use their EHR. This process is governed by the necessary period of information management by the EPS.

## 4. Discussion and Conclusions

This type of proposal must be accompanied by regulations strictly defined by government laws, to regulate the misuse and segmentation of medical records that may violate the confidentiality and integrity of the data, as well as putting the health of the patients at risk by lack of information about their complete clinical picture.

The health sector, both public and private, has significant advances throughout the world; the proposals for interoperability of clinical histories between countries is one of them. Centralizing and standardizing the clinical information of Panamanians opens the doors to this possibility, where we can share historical clinical information with other countries of the world and guarantee that Panamanians abroad can obtain all the benefits of counting with a ubiquitous EHR.

Safety, at the level of patient data, is essential for interoperability, both between heterogeneous systems and in the same internal systems of an EPS. The establishment of a security layer that monitors incoming and outgoing transactions, makes the platform a more robust and reliable system. It should be noted that, in terms of security, there is no secure system, but if the attacks are mitigated to their maximum expression, it can be specified that the system is reliable for a data gateway. The design and development of this proposal will facilitate the integration of existing EHRs, as well as the integration of new developments, where EPS can interact efficiently for each of the services offered.

**Author Contributions:** Conceptualization, M.N. and A.S.; methodology, L.M. & Y.C.; investigation, V.V.; writing—original draft preparation, M.N. & V.V.; writing—review and editing, M.N. & V.V.; supervision, V.V.

**Acknowledgments:** This research is supported by SNI System in SENACYT. On author is member of Research National System (SNI).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References


1. Ajami, S.; Bagheri-Tadi, B. Barriers for Adopting Electronic Health Records (EHRs) by Physicians. *Acta Inform. Med.* **2013**, *21*, 129.
2. Ochoa Lopez, W.A. Las Tics y su Incidencia en la Calidad de los Servicios de los Centros de Salud del Distrito 12d02, Cantones Urdaneta y Puebloviejo, Provincia de los Rios. Master's Thesis, Quevedo UTEQ, Kwedo, Ecuador, 2016.
3. Cuenca, M.; Oliván, S.; Antonio, J.; Cuenca, G.M.; Oliván, J.A.S. Digital Health Record of the Spanish National Health System. Available online: http://eprints.rclis.org/31486/1/Historia Clínica Interoperable.pdf (accessed on 26 May 2019).
4. Martínez, G.R. Universidad Tecnológica de Pereira. Scientia et technica. Historia Clínica Electrónica Desde Un Dispositivo Móvil. *Sci. Tech.* **2015**, *20*, 370–376. Available online: https://www.redalyc.org/html/849/84946834008/ (accessed on 2 June 2019).
5. Curioso, W.H.; Espinoza-Portilla, E. Framework for the strengthening of health information systems in peru. *Rev. Peru. Med. Exp. Salud Pública* **2002**, *32*, 335–342. Available online: https://www.scielosp.org/scielo.php?pid=S1726-46342015000200019&script=sci_arttext&tlng=pt (accessed on 23 May 2019).
6. Digital, G.O. (n.d.). Decreto Ejecutivo No 1458 No 27160-A Contenido. Available online: https://www.gacetaoficial.gob.pa/pdfTemp/27160_A/GacetaNo_27160 a_20121109.pdf (accessed on 12 June 2019).
7. Secretary of Health and Human Services. Privacy, Security, and Electronic Health Records. Available online: www.hhs.gov/ocr (accessed on 23 May 2019). (In Spanish).
8. OAuth 2.0—OAuth. Available online: https://oauth.net/2/ (accessed on 14 July 2019).
9. Organización Panamericana de la Salud. *Revisión de Estándares de Interoperabilidad Para la eSalud en Latinoamérica y el Caribe*; Organización Panamericana de la Salud: Washington, DC, USA, 2016.