Interconnection of Medical Data Acquisition Systems

Lucian Nita
Faculty of Electrical Engineering
"Gheorghe Asachi" Technical University of Iaşi,
RomSoft SRL
Iasi, Romania

***Abstract*—The paper presents a system which interconnects the Hospital Information Systems (HIS) implemented on different medical institutions and makes possible the data transfer between hospitals. The system integrates a middleware cloud component which ensures protection against external and especially, internal data leakage attacks. Also, the system implements a "plug&play" principle which makes it very flexible in the process of adding new data sources.**

Keywords—HIS interconnection, data protection

I. INTRODUCTION

Medical data (X-rays images, CT scans, laboratory analyzes, patient medical history) are very important for a doctor in the diagnosis process. The larger data amounts available for analysis gives possibility for a better diagnosis in complex cases. In the Health Care field there are many actors which provide medical data and actors which need that medical data, but in practice they are not interconnected (Fig.1).

The problem which is common for many medical institutions today is that a doctor from one institution has no access to medical data from another institution for a given patient. And this problem could be very critical during emergency situations.

Even if everybody agrees that a such unified system is better and needed, in practice is difficult to implement, because there are some technical and juridical issues which has to be solved in order to interconnect one medical system to another:

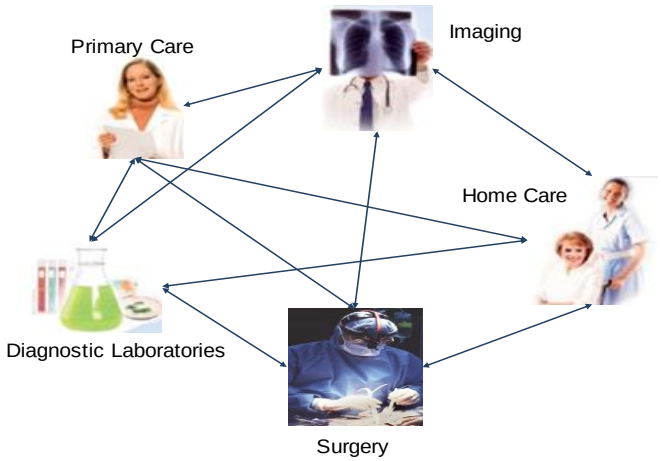


Fig. 1. Medical data sources which need interconnection

- Not all medical institutions have the same Hospital Information System architecture. There are a lot of this kind of systems, with a very different architecture, protocols and facilities. Even in the same hospital it's hard to find a unique system which integrates all medical data available in that institution. Linking together these different medical systems represents a difficult technical task which could be addressed only by a complex team: database administrators, software engineers, system engineers and clinicians.
- Medical data represent a private data which is own by the patient itself. No data access or transfer could be done by doctors without patient permission. Even if the patient grants a doctor or a hospital to access his data, the data could not be sent to another hospital by the granted doctor without patient permission. That's why the interconnection system has to implement a patient application module which allows the patient to communicate with the doctor and to extend when needed the granted access.

The proposed system resolves all these issues by implementing the modern software technologies (web services, ASP.NET Core [1], java scripts libraries) which make possible data source interconnection using the latest HTTP protocol.

II. SYSTEM ARCHITECTURE

A. Central database

The system (Fig.2) is built around a unique database which is stored in the cloud. Each institution added to the system receives a "smart box" software component which links that institution to the central database.

The smart box doesn't store any kind of data, it represents just a communication channel between hospital departments and between hospital and the central database. In fact, the central database neither doesn't store any kind of medical data, all the system is doing is data indexing: the smart box asks periodically each department about the new data produced in

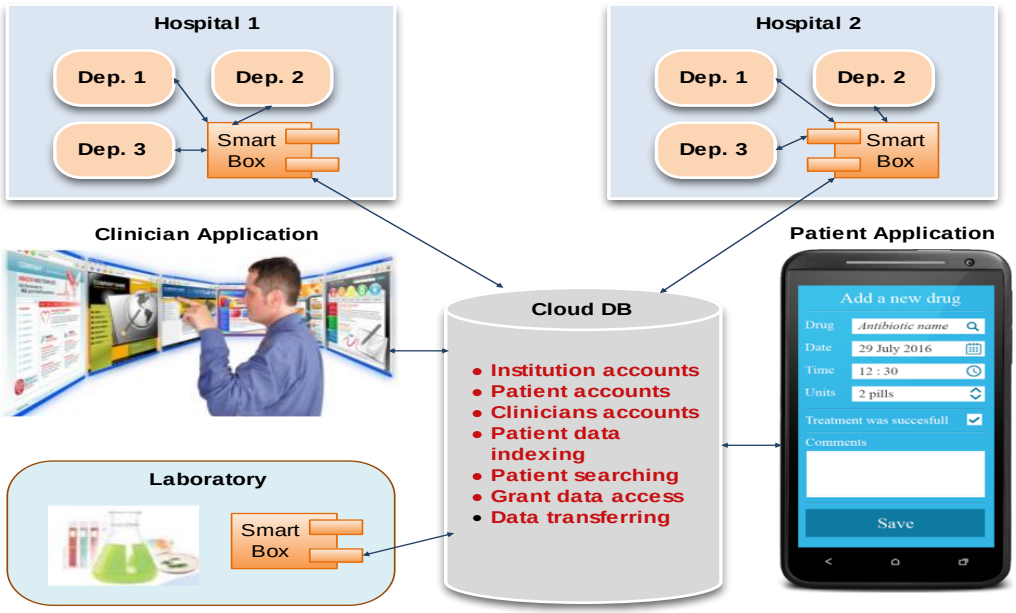


Fig.2. System Architecture

that department and sends this information to the central database. The database only stores this information arrived from each smart box installed on all institutions. This is because, in practice is almost impossible to store into a single database so many information (a medical imaging department from a hospital produces during a year about five terabits of data) and on the other hand, because the data privacy, the data could not be transferred without patient permission. The database only "knows" where the medical data for a given patient is and how to transfer that data between hospitals when needed.

When a patient arrives to a hospital and the doctor from that hospital needs to analyze the patient medical history, in that moment the doctor raises a request into the system to receive medical data for that specific patient. The database responds with a list of medical data files found for that patient and the hospitals which stores that data.

B. Hospital endpoint

Each hospital added to the system receives a smart box component which connects that institution to central database.

This component is configurable in order to adapt to the institution particularities. The smart box talks with each department from that institution using the institution specific protocols. This component which is very flexible and could be adapted to each institution internal protocols resolves the problem given by the incompatibilities between different Hospital Information Systems.

One important component of the smart box is represented by an open source Picture Archiving and Communication System (PACS) [2]. This PACS is connected to all medical imaging source from the hospital and stores the images data produced on that hospital. When a doctor needs other medical images then he/she raises a request and all DICOM [3] files found on other hospitals are downloaded into local PACS. One important aspect is that the smart boxes are smart enough to talk each other and transfer data directly, without using the central database. The central database receives only the metadata which describes the file transferring process: the receiver and the sender, how many files are transferred, data amount, starting and ending time. This feature is needed in order to not load excessively the internet connection of the central database with data which is not valuable for that point.

The files downloaded into local PACS represent redundant data, because they are just a copy of the original files from the sending PACS. These files are deleted automatically after 30 days from the receiving PACS.

The smart box includes also a DICOM viewer (Fig.3) which allows the doctor to search in the local PACS and

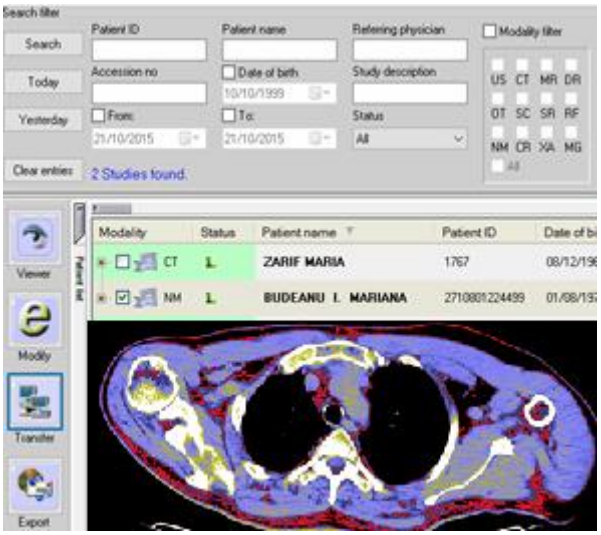


Fig.3. Workstation viewer for DICOM files

visualize the medical images for a given patient. One important rule which must be followed by all images sources is to use the patient numeric personal code (CNP) as unique identifier of the subject from DICOM file. This is the only way for the system to search and identify a patient on all hospitals databases.

C. Patient and Clinician Applications

The system includes a responsive [4] web application which is used by the patient in order to load and view his own medical data and to manage the data access permissions given to doctors from the system.

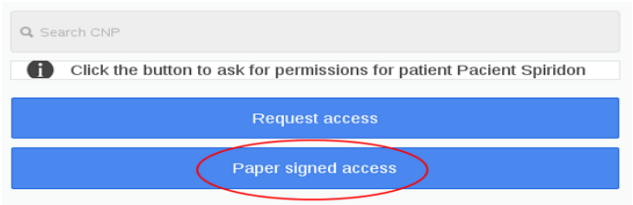
Each patient receives an account and password when he/she arrives to a hospital (no matter which hospital from the system). Using these credentials, the patient logs to the platform and manages his data.

The same application is used by a doctor from the system to ask for permission to access patient data. The workflow for asking-granting data access process is described bellow:

- The doctor searches for a patient with a given CNP:

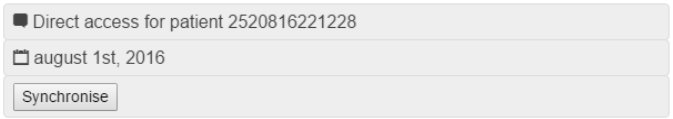
If the system founds medical data for that patient on other medical institutions, then the application displays the files found, if not, displays the message “patient not found”.

- If the system founds data for that patient, then the doctor can raise a request for data access permission



There are two request buttons: the standard one which effectively sends a request to the patient and waits for the response and the second one which is a shortcut for this process. The standard procedure is cumbersome, it requires that the patient has a mobile, runs the application and gives permissions. This is useful for the young patients who know how to use the modern mobile devices. But for old patients, the system implements a simple procedure which supposes that the patient has signed a declaration which states that all medical data from that hospital can be used by other hospitals from the system. Having this declaration signed, the doctor clicks the “Paper signed access” button, which means that the doctor takes responsibility for this action.

- The doctor receives permission for data accessing and clicks the “Synchronize”



- If the doctor asks the patient for permissions, then the patient application displays this message and gives the possibility to accept or reject the request:

III. Data Protection and Privacy Considerations

Data privacy is a very important task when building a such system which gives possibility for many doctors to access patient medical data. Medical data represent private information and nobody can access this data without patient permission. The low particularities differ from country to country, but in general, this interdiction is the same, so the system has to implement effectively these requirements.

There are two important aspects when consider the data privacy:

- The system should prevent data leakage against external attacks.
- The system should be protected too against internal attacks.

A. Protection against external attacks

Protection against external attacks is standard and used by all systems which work with private data. This protection supposes that every user which logs into the system should use a password.

Not all users have the same rights, each user has attached a role which defines very strictly which data that user can access. The patient can view only his/her medical data and history. A doctor from a department can access data only from that department or from the entire hospital, depending on the institution rules. When the system grows by including many medical institutions, this algorithm which establishes the particular rights for a given user increases in complexity. That’s why this logic is implemented by the central database and used by all endpoints. The algorithm uses the concept of access area, resources and predicates [5]. This concept provides a database of parent-son relationships between the resources and the access areas. Mainly, the database establishes which resources can be accessed by users from a given zone. The algorithm is hierarchical, if the parent has a right, then that right is inherited by the suns.

The system should implement all these rules, but on the other hand, the system should be as simple as possible. It is known [6] that the usability of a medical software application depends significantly on the designed user interface. There are medical applications very useful for a given disease, but the patients don’t use them because the bad user interface implemented by those applications. Our system develops a

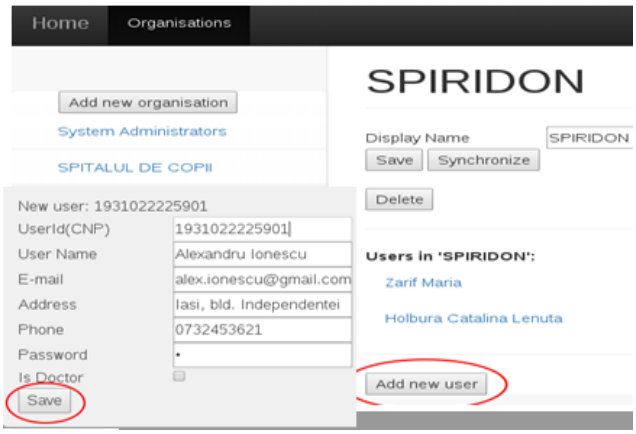


Fig.4. Adding a new institution and a new user to the system

simple user interface (Fig.4) which does not pointless consume the doctor or patient time when is used. The patient accounts are imported automatically from the Hospital Information System database, there is no reason to add patients directly to system database.

B. Protection against internal attacks

We define internal attacks the data leakage attempts made by internal system administrator. A local system administrator or even a doctor, could access a huge amount of medical data collected from all hospitals interconnected by the system. This data can then be stolen and used for fraudulent purposes by that user. There are many Hospital Information Systems which have no protection against internal attacks. If a system administrator who has full rights on HIS database wants to steal that data, nobody can stop him. Stealing data from a single HIS database is critical, but not as critical as in the case of theft from several interconnected HIS databases. That's why our system implements a very powerful logic which stops internal data leakages. This logic is working on the central database and intercepts all data requests made by any user. There are triggers which raise automatically when an unusual request is made into the system. Nobody can request a huge amount of information without to be identified and stopped because, at a given time, there is no reason to request and transfer such amount of data.

On the other hand, the system has the possibility to encrypt the medical data and to store the decrypting keys on several points, so no single user can decrypt the data. They should be two or three users together, each one with his decrypting key in order to decrypt the data. This logic improves substantially the power of the data protection algorithm.

IV. STANDARDS FOR MEDICAL DATA DEFINITION AND TRANSFERRING

Not all clinicians use the same medical terminology for a given drug or disease. This variety of medical terms make it difficult data integration between hospitals.

In this context, one of the future facilities of the smart boxes will be data standardization.

There are two standardization aspects which has to be implemented:

- Clinical terminology standardization: the system will implement the **SNOMED CT** [7] which is the most comprehensive, multilingual clinical healthcare terminology in the world.
- Data exchange, integration, sharing, and retrieval of electronic health information. For data exchange protocols and Clinical Document Architecture, the system will implement the **HL7** [8] standard.

V. CONCLUSIONS

A system which interconnects different Hospital Information System is presented. The proposed system architecture ensures several important advantages for the system:

- Flexibility: due to the smart box component, the system can be easily extended, using a "plug&play" method.
- Data protection: the central database includes algorithms and triggers which protect data against external and internal attacks which represents a new facility for these kind of systems.
- Data privacy: the patient has the possibility to give or remove data access permissions for each doctor or hospital.
- Huge amounts of data transferring:smart boxes talk directly each other during data transferring.

ACKNOWLEDGMENT

This material is based upon the work which is partially supported by the European Union through the H2020 "PEPPER" project: Patient Empowerment through Predictive Personalized decision support, http://www.pepper.eu.com .

REFERENCES

[1] Welcome to ASP.NET Core, Microsoft library, http://www.asp.net/core

[2] Picture archiving and communication system, From Wikipedia, the free encyclopedia,https://en.wikipedia.org/wiki/Picture_archiving_and_communication_system

[3] DICOM – Digital Imaging and Communication in Medicine, http://dicom.nema.org/

[4] Responsive Web Design, Learn to Code Advanced HTML & CSS, http://learn.shayhowe.com/advanced-html-css/responsive-web-design/

[5] Sinica Alboaie, Lenuta Alboaie, Andrei Panu, "Levels of Privacy for e-Health systems in the cloud era", 24th International Conference on Information Systems Development, 2015.

[6] Minshall S, A review of healthcare information system usability & safety, National Center for Biotechnology Information, 2013;183:151-6.

[7] International Health Terminology Standards Development Organisation What is SNOMED CT?, http://www.ihtsdo.org/snomed-ct/what-is-snomed-ct

[8] HL7 standard, http://www.hl7.org/index.cfm?ref=nav