Advanced Security Policies towards Healthcare Information Systems

Charupalli Sunil Kumar and Nalathati Hari Babu
1. Faculty of Electronics and Computer Engineering, Sreenidhi Institute of Science and Technology, Jawaharlal Nehru Technological University Hyderabad, Hyderabad 501301, Andhra Pradesh, India
2. Faculty of Computer Science and Engineering, Jyothishmathi Institute of Technology and Science, Jawaharlal Nehru Technological University Hyderabad, Karimnagar 505 481, Andhra Pradesh, India

Corresponding author: Charupalli Sunil Kumar (ccharupalli@gmail.com)

Abstract: Now it is a high time to reform the advanced security policies in the world health care sector instead of revival. Health sector is one of the most important sectors playing the vital role in the country’s GDP (gross domestic product) after the agriculture and manufacturing sectors. Healthcare assures efficiency, accuracy and availability of medical treatment; however it also introduces the potential for serious mistreatments including major privacy violations, staff unfairness and even life-threatening attacks. In this paper, we discussed some potential threats and opened the discussion about the security requirements of this new scenario. It takes a few initial steps towards a Healthcare security policy and proposes system architecture designed to enforce security policies with a high confidential data security system.

Key words: PDA (personal digital assistant), HL7, interoperability, HL7 CDA (clinical document architecture), sensor.

1. Introduction

The healthcare secretarial structure in all countries is naturally distributed, being a geographical spread of centres’ at different levels of difficulties: from the general hospitals down to individual physicians. The crucial objective of such a structure is to build a network of corresponding [10] centres (e.g., hospitals, laboratories, ambulatories, coordination canters) spread over the country, to meet effectively the social needs in the area.

This necessary distribution makes it very hard for physicians to capture a complete clinical history of the patient because the patient’s health information may be spread out over a number of different organizations or different departments within the same healthcare institute. As a matter of fact, the medical and economic blow of not knowing a patient’s complete medical history is thoughtful. Medical practice today still involves sorting through a stack of laboratory reports, trying to find specific patient information. But thousands of people die each year due to lack of patient information. As per investigations, poor information is the primary killer in the world.

The challenge of E-Health is to allow health care experts’ to interact in time with heterogeneous and distributed medical relational databases. So, the vital problem to address is exchanging patient medical records between healthcare institutions or between different units within the same organization: radiology, cardiology, neurology, etc. The mechanism is that to provide healthcare institutions with a complete collection of patient information.

It should firstly recognize a patient and then it should locate the patient’s information, including clinical and laboratory results. The access and the availability of this information have to be
authenticated, according to rules strong-minded by the
data owner through data access security policies.

The fact that the inappropriate disclosure of private
medical information can harm the patient has been
clear since at least the 4th Century BC. But what
exactly are the security requirements in this age of
increasing computerization. Ten years ago, security
policy [1] described the protection goals of clinical
information systems: its motivation was that storing
patient medical records on a nationwide distributed
computer system endangered the principle of patient
consent and increased the possibility of data
aggregation. Healthcare, in turn, brings new threats
and vulnerabilities.

2. Terminology

Electronic healthcare systems are the existing
healthcare information systems that use networked
computing systems for recording and accessing
medical records. Ever-present healthcare systems,
instead, adopt computing as an enabling technology,
with sensors monitoring the patient continuously, and
include disease care systems and independent living
systems. There are several Healthcare Providers,
including but not limited to clinicians and GPs
(general practitioners): for all of them, provider term
may also be used. The more general terms are
preferable if the clinics can be replaced by other
healthcare services such as gyms and healthcare web
services shall be considered.

As for sensor devices, there are body sensors and
infrastructure sensors. Examples of the latter include
scales and sensors of ambient temperature, light or
movement. These sensor devices transfer data to base
stations such as PDAs (personal digital assistant),
Smart phones and PCs (personal computers). The
union of these sensors and base stations form a
personal healthcare system, which is used and
controlled by an individual patient, or by some trustee
on behalf of the patient. The sensor data is then
transferred to a clinical system for further analysis if
needed.

3. Existing Methodologies

A dominant integration technology, which allows
immediate access to distributed information, is needed
in order to provide healthcare institutions with a
complete collection of patient information. A number
of standardization proposals are progressing to
address these interoperability problems such as HL7
(Health Level Seven) [2], a non-profit, ANSI
accredited standards developing organization, founded
in 1987 that provides standards for the exchange,
management and integration of data to support patient
clinical care and the management, delivery and
evaluation of health care services. GEHR/openEHR
[3], an initiative that fosters EHR interoperability
started in 1992 as the “Good European Health Record”
EU research project that is currently maintained by the
openEHR Foundation CEN/TC 251 [4], the technical
committee on Health Informatics of the European
Committee for Standardization, that, since 1998, is
standardizing CEN EN 13606/EHRcom [5, 6] and
IHE (Integrating the Healthcare Enterprise), a
not-for-profit initiative founded in 1998 that does not
develop standards as such, but selects and
recommends appropriate standards for specific use
cases [7].

Most of those initiatives have been active for more
than a decade and, after a first attempt in specifying
the format of each of the message that can be
exchanged among any couple of systems (e.g., HL7
v2.x), they realized that they need to derive messages
and interaction patterns from a common shared
conceptual model.

A substitute is offered by HL7 RIM (reference
information model) which is the ultimate source from
which all HL7 v3 protocol specification standards
draw their information related content [8, 9]. The RIM
model is an unambiguous data semantics model by
which the messages can be implemented locally and
top-down, highlighting reuse across multiple
situations. Furthermore, RIM offers formalism for vocabulary support that permits to get domain concepts from the most excellent terminologies (SNOMED, LOINC, etc.).

4. Towards Security Policies

4.1 Monitoring

Traditionally, health status was measured either directly by the provider or the patient; more recently such measurement may have received some form of technological assistance. Such collected data is usually analyzed in real-time and is summarized and discussed before being recorded. In contrast, when a ubiquitous monitoring environment is used, computing devices may create a permanent record in much greater detail. To protect the privacy of the patient:

Principle of self-care is proposed: Data collected in a ubiquitous monitoring environment must be processed and stored on a personal healthcare system under the sole control of the patient. No sensor data shall leave the personal healthcare system without the patient’s permission. This principle reflects our current concept of healthcare: A patient will contact a provider only after a medical problem is discovered, and providers only receive medical facts from the patient or perform an examination with the informed consent of the patient.

In some cases, the ubiquitous monitoring environment is analyzed, reported and automatically executed actions based on the sensor data. For example, a diabetes patient may use a body sensor network to keep him informed of his current glucose level and perhaps even automatically trigger the delivery of insulin. In this case, the principle of self-care means that glucose level readings and insulin delivery must operate within the personal healthcare system and run independently of all clinical systems under the control of the provider. It is a value noting that this type of independent operation may be sensible from a safety and reliability perspective, too.

4.2 Consultation

There will be times when a patient will seek the advice of a provider. This might happen at pre-defined intervals, whenever the personal healthcare system reports a potentially life-threatening reading, or during an emergency. In these cases, the patient will require understanding the data recorded by the personal healthcare system. Since the patient cannot know what facts the sensor data contains, he cannot give his informed permission to the release of all sensor data directly into his medical record. Therefore, to protect the privacy of the patient: Principle of non-disclosure is proposed: The patient may transfer sensor data from his personal healthcare system into a temporary repository which is also accessible by a provider. Only data useful in assessing the state of health of the patient is transferred.

By default, data may not be transferred out of the repository, which shall exist for a limited time. In practice, it is impossible to delete all traces of the analysis since the provider and patient may mentally recall some of the information. This principle means that at the end of any consultation between a patient and the provider, there should be no electronic record of either the raw sensor data or any derived data.

Some forms of analysis may require several providers to collaborate, and this might make it difficult to arrange for all the specialists and the patient to meet at once. In this case, the principle of non-disclosure means that as the data is analyzed, the patient is kept informed of what data is collected from his personal healthcare system. It is important to limit both the amount of time data can be kept, and the number of providers who may access the repository. If this is not the case, the lifetime of the repository may last as long as the lifetime of the patient, and it becomes a medical record in all but name. The length of time data can be held in a repository will depend on the medical condition under analysis; for complex situations this is something that needs to be reviewed by provider and patient at regular intervals.
5. Architecture

Security policy is derived to provide the patient with a method to control access to any sensor data recorded by a personal healthcare system. From a computer science perspective at least, that it is practical to build a system that conforms to this security policy is believed. In order to support a temporary repository, a software mediator is predicted which logically sits between a personal healthcare system used by the patient and any clinical system used by the provider. The concept of an intermediate component exists already in many diverse research areas of computer science and includes proxies, agents, guardians, Trusted Computing Bases, etc.

The mediator as shown in Fig. 1 should provide an interactive environment in which a patient and a provider can explore the data recorded by the body sensor network, extract the relevant medical facts from the collected data and, with the patient’s informed [14] permission, append those facts to the medical record. In order to meet the criteria set in the security policy, it is important that the patient be in control and be able to limit: (1) the raw sensor data sent to the mediator and (2) the derived facts transferred from the mediator to the medical record. Obviously it is paramount that all data stored by the mediator be deleted at the end of any period of consultation [13].

6. Sharing Health Care Data

The existing methodologies in sharing health care data is achieved by standard application protocols (For e.g., HL7, openEHR, EHRcom and IHE), which define meaningful components of the messages to be exchanged, and domain vocabularies (e.g., SNOMED, LOINC, etc.), which define the meaning of the data transported by each message. On the converse, TRSC enables communication via persistent magazine of the information.

Such message-based communication has confirmed efficient and effective for certain activities in this area (i.e., hospital management), but has shown some difficulties to effectively and flawlessly collecting and integrate data from EHRs. When addressing such a need, at least two are the possible solutions. On the one hand, a possible solution is to build centralized databases that would contain all the medical records on every patient. It would also incorporate all of the different access rules and policies regarding different users and different levels of access. But this kind of efforts has four weak points:

- The cost of constructing the infrastructure and collecting the data is massive;
- The centralized repository method creates competitive and security issues about who controls and has access to the information on an unambiguous patient;
- The complexity in maintaining up-to-date a repository originating from a large number of independently evolving systems; and
- Last but not least a message once sent gives the owner a sense of rescue instead of strengthening the sense of ownership.

On the other hand, a possible solution is to exchange messages only when required. In this way no central repository is required and the ownership of the data seems respected, but this solution has several weak points too [12].

Each receiver must know in advance where to look for the information. Each receiver must know in advance the terminology (e.g., SNOMED, LOINC) to
use when asking for a specific record. Each receiver ends up maintaining a specific interface for each system it has to interact with, and data mining (for disease prevention, early diagnosis, pharmaceutical research, improvement of patient safety) becomes almost impossible due to the large amount of messages to be exchanged.

The principle of self-care is a realistic solution for the data ownership problem because healthcare organizations will not lose their control over resources and they will be able to share information only with those that are authorized. It provides a simple way to guarantee reliability because health data won’t be neither transmitted or copied but simply used. It supplies a straightforward way to deal with integrity because data won’t be transmitted and it should be impossible for anybody, but the owner, to modify the data. Finally, it is a cost-effective solution because additional storage resources [11] related to the management cost are radically reduced.

7. Conclusions

Healthcare introduces great convenience but at the same time equally great hazard. The shift to 24/7 patient monitoring via body sensors is not just an incremental improvement over the existing practice: it is a qualitative step change. So is the shift to remotely-activated drug dispensers implanted in the patient’s body. The main message of this paper is that such major paradigm shifts demand a rethinking of the security and privacy aspects and solutions. The desire is to engage all parties, including the clinicians and patients, and understand what is acceptable and desirable before the coming generation of Healthcare systems is deployed. There will certainly be tension between security and usability, between patient privacy and the clinician convenience. In this context, security policy is first of all an instrument of communication. By writing down, at least as a working draft, the protection goals of future Healthcare systems, we allow the community of stakeholders to think, agree, disagree and debate. So that it can never be misused to cause harm to their patients. It will be enhanced in the future with the advanced cryptographic techniques.

References