A Study of Access Control for Electronic Health Records

Sergio V. Senese
Graduate Student
Governors State University
Overview

- Introduction
- Electronic Health Record
- Access Control
- Access Control Configuration
- SQL Server Label Security Toolkit 5.1
- Example Application
- Future Research
- Conclusion
Introduction

- Healthcare has become increasingly advanced in scientific breakthroughs, in part due to the use of Information Technology and Computer Science.

- The Electronic Health Record (EHR) was created to use across the healthcare field to digitize the massive amounts of paper-based records that are taking up space and contributing to medical errors.

- An EHR can contain important personal information and there are great advantages to using electronic records more extensively.

- Concerns about Privacy and Security.

- Access Control using Row and Cell Level Security through use of Labels to create a secure database for EHR patient information.
Summary

- Security is a need when dealing with privileged information, but more so when that information is people’s confidential medical records.

- Electronic medical records are exposed to possible misuses and risks. The process in which these parcels of information are stored and accessed currently has to be questioned and scrutinized.

- Medical data is also susceptible to misuse by those seeking to profit from it.

- In deploying access control to Electronic Health Records, overall security can be increased and patient care and quality will improve as well as overall healthcare costs.
Electronic Health Record (EHR)

*Definition* - Electronic Health Record (EHR) is a compilation of medical records of an individual patient or population group transformed into a digital format.

Records can include data in various forms including personal information. An EHR will also include medical information.

EHR’s sharing could be widespread with the eventual goal being that a patient's overall medical record is available anytime, anywhere, to any healthcare provider or location.

EHRs and the capability to exchange health information electronically can help healthcare organizations provide higher quality and safer care for patients.
EHR Medical Record Schema
EHR Standards

- **ISO** - ISO TC 215 provides international technical specifications for EHRs. ISO 18308 describes EHR architectures.

- **HL7** - a standardized messaging and text communications protocol between hospital and physician record systems, and between practice management systems.

- **DICOM** - an international communications protocol standard for representing and transmitting radiology (and other) image-based data, sponsored by NEMA. (National Electrical Manufacturers Association)

- **Continuity of Care Record** - ASTM International Continuity of Care Record standard.

- **HISA** (EN 12967), a services standard for inter-system communication in a clinical information environment.

- **CONTSYS** (EN 13940), supports continuity of care record standardization.

- **EN 13606** - communication standards for EHR information.

- **ANSI X12 (EDI)** - transaction protocols used for transmitting patient data.
EHR Architecture

- Must have homogeneous framework fundamentals in order to facilitate auto processing and interchangeable operations.

- Basic architecture begins with a database to store information for the EHR. This patient information can be shared through a network with firewalls provided to ensure security.

- Basic architecture can be implemented for a single entity such as a hospital, doctor’s office, or clinic to produce an Electronic Health Record that could be then shared in a national/regional Public Health System.
EHR Network

Electronic Health Record

Single Sign-On

Clinics/Community Health Workers
Primary Healthcare
Laboratory
Hospitals
Pharmacies
Patients

Government
Universities
Patient Index
Provider Index
Regional/National Systems
**Database Type**

- The ideal database type for securing electronic health records must have some sort of principle behind it. The database must respect the disclosure of data it manages.

- A Hippocratic Database is a set of technologies that manages disclosure of electronic health records in compliance with data protection laws without impeding the legitimate flow of information.

**EHR Software**

- EHR systems currently are in a median phase of development, with small companies trying to grab a niche, while larger ones vying for an untapped business model.

- Currently the most successful execution of an EHR system is the U.S. Department of Veterans Affairs (VA) system known as VistA. Australia, the United Kingdom, and Canada have also begun EHR system.
Access Control

Access Control has been described as “The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner”

Access control comes in three major flavors – Administrative, Logical, and Physical.

Access Control has three major areas – Subject, which is the entity that is given permission to the data. Objects, which is the actual items being protected. Access Rights, which is the way that the level of control is established.

The architectures and schemas for Access Control define the rule-based logic behind the definition of entry for the user. Access Control can be a basic concept or it can become very detailed down to the smallest granularity.
Discretionary Access Control (DAC)

- Right of entry is normally based on the authentication approved to the user based on the classifications they presented at the time of validation and the identity of the control to elect whether to authorize or decline an request for access.

- In the centralized version, a single or group of authorization entities grants access. In a distributed version the most qualified persons give access.

- Demonstrates one or more of the following characteristics: Administrators can transfer rites of information to other users. Administrators can choose the kind of permissions given.
Mandatory Access Control (MAC)

- Guarantees that the implementation of a security regulation is not based on voluntary application user fulfillment.

- Assigns a security label to all data, and a security level to each user to ensure that all users will only have permission to information for which they have access.

- One or more of the following characteristics: Only administrators, not information providers, make changes to a user’s security label. All information is granted a security level that imitates its code value. Users can access a lower classification than the one they are permitted. All users can modify a higher classification.
Role-Based Access Control (RBAC)

- Is based on a user’s roles and position within an organization or company.

- Has five major elements. The user or the person trying to gain access, role that configures what permissions the user has, the permissions themselves, operations, and the objects which are the needed to be accessed.

The following attributes can be found:

1. Roles are given based on organizational arrangement.

2. Each role is given profiles that consist of all authorized commands, transactions, and object access.

3. Roles are created with a separation of tasks. Roles are overseen centrally.
Security Labeling

Can be a piece of data that represents the privacy of an object. It is a sequence containing markings from one or more categories. Users (subjects) have permissions described with the same markings.

Each subject has a label of their own. The subject’s label is compared against the label on the object to determine access to that object. For example, the following table fragment has rows annotated with security labels in the Classification column.
Security Label example

<table>
<thead>
<tr>
<th>Name</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sergio Senese</td>
<td>RESTRICTED</td>
</tr>
<tr>
<td>Linda Napoli</td>
<td>CONFIDENTIAL</td>
</tr>
<tr>
<td>Steve Duignan</td>
<td>PUBLIC</td>
</tr>
</tbody>
</table>

Applications containing this data could have operator accounts as follows:

Example operator accounts

<table>
<thead>
<tr>
<th>Operator</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anthony</td>
<td>CONFIDENTIAL</td>
</tr>
<tr>
<td>Spike</td>
<td>PUBLIC</td>
</tr>
<tr>
<td>John</td>
<td>RESTRICTED</td>
</tr>
</tbody>
</table>

Each operator’s security label defines which rows in a table they can retrieve. If Anthony delivered a TSQL `SELECT * FROM <name of table>` against this table, he should get the subsequent results.

Query Result

<table>
<thead>
<tr>
<th>Operator</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anthony</td>
<td>CONFIDENTIAL</td>
</tr>
<tr>
<td>Spike</td>
<td>PUBLIC</td>
</tr>
</tbody>
</table>
Row Level Security

For each marking in the categories defined, a corresponding database role is created. Roles allow users to be granted permissions that exactly match the security labels to which they should have access.

A view is used to display the data and prevent users from actually accessing the base table.

Cell Level Security

Most of a row could be visible to one set of users, while certain additional confidential cells might require additional permissions to view.

SQL Server offers internal functions to effortlessly encrypt and decrypt data using a certificate, asymmetric key, or symmetric key.
Encryption Hierarchy

Windows Operating System Level Data Protection API (DPAPI) protects the SMK.

DMK is protected by the Service Master Key which is created by SQL Server setup.

PW PW PW PW PW PW PW

Database Master Key

Certificate Asymmetric Key

Symmetric Key

Symmetric Key

Encrypted Data
Label Policy Designer Application

The SQL Server Label Policy Designer can be implemented to outline a label policy and then apply the label policy by creating objects and code in a database.

It is a group of metadata tables, functions and stored procedures, database roles, and other objects inside of the database.

Needs full database owner rights on the home database. Ideally this tool should be used only by administrators with authorization to data stored inside these databases.

To provide for cell-level security, a database master key must be present in the home database.

The Key Broker Username is the name of a database element that will be created to regulate access to symmetric keys in the label policy.
SQL Server Label Security Toolkit 5.1 Example
Log In

Please enter your username and password.

Account Information

Username

Password

Login
Future Research

- The electronic health record (EHR) is becoming more of an accepted practice among health care providers. There are still many concerns about the security and confidentiality of how and even where patients data is kept.

- With the creation of Cloud Computing and Mobile Applications, a whole new set of concerns about EHR information has arrived.

New Frameworks

- Some frameworks are actually taking into account the requirements for EHR’s or health networks.

- Proposing greater access, sharing, and mobility for the record.
Patient-Centric Privacy

- Envision that each patient specifies their own privacy policy and rules
- An attribute-based system, where the patient agrees to authorization policies based on specific attributes (with specific values) that the requester must possess in order to gain permission to access the records

Broker Based Framework

- Ideas of letting healthcare providers register their credentials in a Universal Description, Discovery and Integration structure. This will allow these Healthcare entities to add patient information, services, and data to a broker Patient metadata store.
- They can reside in a single cloud or multiple clouds (public cloud, private cloud, or hybrid cloud) depending on their deployment needs.
- Another proposal has healthcare using Case-Based Reasoning (CBR) combined with other technology like intelligent agents.
Outlook and Vision

- The future of EHR data can be valuable to many different parties. Currently some government agencies are creating EHRSS systems also known as Electronic Health Record Surveillance.

- This data is extracted from EHR’s where traditionally these systems would rely on census, medical studies, and population surveys.

- Future of Security Labels and Access Control has grown into a multi-purpose security feature and the limits for design are growing in numbers.

- Security Labels are at a juncture where more implementation is needed, especially at the database level. The potential for their use is far from being utilized and the solutions they offer are not always being considered.

- Multilevel security (MLS) is a field that needs to be explored further considering the vast changes undergoing the Internet with Cloud computing and mobile devices.
Conclusion

- Access Control provides a solution for securing Electronic Health Records and systems. Coupled with row and cell level security while instituting encryption, this combination provides a security policy for safeguarding sensitive health information.

- Presented a vision of using this type of security to enact a type of solution for a progressive issue challenging the IT Healthcare frontier.

- Developed a prototype example to demonstrate the possible solution and preformed actual tests to produce results.

- The example and results exhibit that by using the principle of Security Labels as an Access Control method that data can and is secured to a level that gives health records a more reliable option.