AUTHENTICATION AND ACCESS CONTROL BEST PRACTICES FOR
HEALTHCARE SYSTEMS

Lamaris Davis

ICTN6865

East Carolina University
Abstract

Securing EHR’s continue to be a huge problem for all health care organizations. The security of this highly sensitive information will continue to be a short and long term goal for every organization that deals with healthcare information. Authentication of the systems that holds this information and the proper access controls for this sensitive information are the top concerns for any organization dealing with electronic health records. The United States has made the handling of health information through electronic systems, a very important goal, but completely securing the information is nearly impossible. When dealing with authentication there are usually three methods to provide this, which is to ask the person something they know (Password, pin, etc), or something they are (Fingerprint, retina, face) or something the user has (Key fob, smart card, etc). When it comes down to access to this sensitive information this should directly be tied to the role of the person, and the policy should be based off who need what information to do their job.
Authentication and Access Control best practices for healthcare systems

Authentication and Access control best practices for healthcare systems

**Introduction**

The content in your healthcare records should be kept private according to HIPAA regulations. In order to keep your healthcare records private an organization should implement some type of system that incorporates very good access controls and system authentication. The three components of authentication is something the person knows, something the person is, or it’s something the person has. Most people consider using a single password and username as an adequate level of security when it comes to system authentication, which is totally untrue. Two-factor authentication is the norm these days with so many hacks going on in the world. Along with great authentication access control is also extremely important. Access control is the rules that decide who has access to what. Access control also ensures that individuals can only access the information needed to do one’s job.

Access control is a fundamental method of security for securing data being store in a healthcare information system. Developing the right policies to protect access to private patient information in the healthcare system, and also satisfying the requirements of hospital stakeholders has proven to be difficult for healthcare system administrators to achieve. This paper will take a look at authentication and access controls for the healthcare system to get a better feel for what can be used in these facilities.

**Authentication for healthcare system**

Proper authentication for healthcare is pretty much obtainable if a company follows a certain process. Two-factor authentication would be a great form of proper authentication
Authentication and Access Control best practices for healthcare systems

because it forces the person that’s trying to access sensitive healthcare records to use two types of authentication to access this information. This increases the security of the system overall because when using two forms of authentication hackers will not be able to guess their way through the system so easily. Two-factor authentication should be the standard method used across the board in order to provide proper protection for any EHR. Companies that just use simple passwords are putting their systems at high risk to be breached because these are things that could easily be guessed.

HIPAA has mandated that any company that deals with healthcare information should implement two-factor authentication. This mandate applies to all federal and local information systems and also requires that any information accessed “remotely” should be done so by two-factor authentication. HIPAA also states that if someone chooses to use some type of password that password should be uniquely created.

The overall cost and the ability to add to a two-factor authentication system presents huge issues for any large organization. Even though the cost is somewhat expensive to implement a two-factor authentication system, companies are willing to spend in order to avoid costly data breaches. The type of data being stolen from these healthcare organizations include, but is not limited to SSNs, medical history, medicine prescriptions, and other personal information. Data breaches play a huge role in a company deciding whether or not to go with two-factor authentication.

Protecting electronic health records (EHR) with some type of two-factor authentication method is very important but it’s equally important for healthcare providers to choose a method that will not dramatically impact their overall workflow. Some companies choose to use a strong password and governing policy and also a mobile app that generates a code to be inputted into
Authentication and Access Control best practices for healthcare systems

the system. We need to keep in mind that only about 16% of healthcare organizations choose to use two-factor authentication with the majority only using a simple password and username.

Carolinas Healthcare System (CHS) is a very big healthcare system with at least 15 hospitals located in North and South Carolina and they have well over 30,000 employees. CHS has had problems with deciding on the best methods to secure their facilities and the organization was using tokens from one of the top security vendors in the country. CHS discovered that the tokens were actually a problem for CHS because even though the tokens improved the security of their systems, the improvement came with very high costs. So when we think about more than 30,000 employees and over 25,000 pc, across the system. The tokens created problems because if you think about every time someone quits their profile has to be deactivated, and every time someone is hired an IT person has to create the token for that person.

Every time someone lost a token or one was stolen someone from the IT Dept. has to react. The CHS administration said that the tokens were a great addition to the overall security of the system, but employees had a hard time keeping up with them. CHS decided that they needed something that would not reduce the security level by putting in place something cheap. CHS also decided that they needed some form of authentication that would ensure the integrity of their healthcare systems and electronic health records inside.

CHS decided to go with something called SecureAuth, which uses two-factor authentication to help secure healthcare systems. SecureAuth also gave CHS the ability to customize the interface. SecureAuth also provides outstanding support to ensure that CHS gets up and running. In order to implement a secure solution within a healthcare system, the solution has to follow HIPAA regulations. SecureAuth doesn’t use any tokens and it’s also non-phishable, and it’s also two-factor based. The software also includes a VPN and a suite of mobile
Authentication and Access Control best practices for healthcare systems

resources for a customer. CHS has decided to stick with a two-factor authentication procedure because it provides protection against likes like a man-in-the-middle attack and also phishing as mention before.

SecureAuth incorporates a x509 digital certificate (credential) which is the second factor with the first factor being a username and password. A username and password will give the system admin full control over enterprise level systems.

Bio-Key is software that’s being deployed into hospitals, private practices, and clinics across the country. Organizations use the fingerprint biometric technology to increase the facility’s overall security. Bio-Key is used to allow the individual to access EHR records, and it’s also used to provide two-factor authentication for some of the healthcare systems. In healthcare today organizations are getting very frustrated with typing to come up with passwords that meet the administrator’s password requirements. This also includes tokens, cards, or other forms of authentication for their electronic health records. Bio-Key can be integrated directly into EMR/EHR systems or if the organization decides to use the single sign on solution Bio-Key can be integrated into that also.

Bio-Key software also gives the organization the ability to authenticate on multiple devices within an organization with just one single enrollment. Bio-Key software has the ability to extract over 1,600 individual data point from each fingerprint. West Tennessee Converted over the Bio-Key software and the main reason listed for this conversion was to increase the overall security of the healthcare system and also as a way to quickly identify the hospital staff. The hospital staff was having a hard time keeping up with their password and Bio-Key is a good idea if the organization wants to create a single sign on solution, which is what west Tennessee was looking for.
Authentication and Access Control best practices for healthcare systems

Smart cards are another way to authenticate into healthcare systems and along with biometrics would make for a very good method of authentication. Smart cards have an embedded chip in them and also include a gold-plated contact plate. Smarts with biometrics will provide hospitals, clinics, and other healthcare facilities with a way to verify the identities across the whole organization. Smart cards can provide two-factor authentication for any healthcare system and the smart cards can also provide a way for staff to access patient electronic records. Smart cards can be easily combined with a fingerprint scanner to allow staff into a system.

Hospitals and clinics could decide to use a solid solution like Entrust. Entrust is probably one of the best identity authentication solutions available on the market. Entrust is a turn-key system and that mean it’s built to be ready to use out of the box. The amazing thing about this solution is that it assigns and authenticates the credentials it passes out. Entrust is an easy deployable solution for any healthcare system and should make authenticating hospital staff easier. I also think that Entrust will cut down on overall IT costs, because this solution will allow the user to reset their own self assigned credentials and you can also change your pin if you have one when they need to.

It’s probably a good idea to install Entrust wherever the hospital has their physical access card system setup. This will definitely make things easier for the system admin to add and remove people to and from the system. Another feature of Entrust that healthcare systems could benefit from will be Entrust’s ability to setup an embedded digital certificate that basically turns your mobile device into a smart card device. If the smart card is setup through your mobile device, the administrator will not have to replace a physical card every time one is lost or stolen. Entrust will offer any healthcare system, a bunch of benefits when compared to a system that only uses simple authentication, which most hospital still currently use.
Access Control for healthcare systems

Access control is definitely needed when you consider how many patients a hospital or clinic or private practice sees every single year. Access control basically consists of rules that only authorize certain people to access certain information. Access is usually given to an individual based off their job role and what they actually need to do their jobs. The overall goal of access control is to provide the best care to the patient and also to protect patient data.

Physical access to a healthcare facility the security has to consider every entrance to the healthcare facility.

Most of the entrances to these healthcare facilities are controlled by some form of security such as the smart card reader, security key pad that link to a security fob. Additional security is also added to the healthcare facilities to fully service the entrances. When it comes to ED their entrance is very important and must be free of obstruction when the emergency vehicle comes, but as we now know most entrances to the ED are in hard to see areas of the facilities. Most facilities chose to address this problem by adding some kind of call system for the personnel that’s trying to access the facility to contact someone. Most facilities also decided to add a card reading system to the doors to allow access into the hospital or other healthcare facilities.

If the hospital can’t afford card reader technology for their entrances or the call system for the doors, the hospital could try to bring in a security guard or the concierge to guard the entrances to the hospital, especially the ED entrance. The concierge or security guard would be able to control access to different parts of the healthcare facility depending on where the person needs to go and if they have permission to go to that area.
Along with the security guard or concierge the hospital should decide on some type of policy that would help any person in charge of managing the entrances to the hospital specifically when they encounter someone suspicious in the hospital or encounter a difficult situation involving a suspicious person. Any person chosen to guard the entrances must take into account that the main reason is to protect the patient’s information within the healthcare system. Access control should definitely be based off the role of the person.

Role-based access control includes the users and their roles and their individual permissions’. A system administrator will usually work with management to decide which permissions’ a person will have assigned to them. Permissions’ are always a good thing to have because they will let a person know where their responsibility starts and ends within the healthcare system. Role-based access control identifies users to roles as many to many and this pretty much the same when you think about roles to resources, or system objects (Stallings, Brown, computer security: principles and practice, p.121). Most roles are individually assigned to an individual by someone in their management chain of command. Each usually will have access rights to multiple resources.

Role-based access control is based off a hierarchy system where the person with the greater responsibility has more access to more resources throughout the healthcare system. It is possible for someone under the top managing person to have some access to resources only given to the top managing person in the healthcare system. This could happen if the subordinate job function includes a subset of the access rights given to their immediate manager. When using a hierarchy system within an organization like a healthcare system it uses some type of tradition to enable one role to include access rights associate with a role that’s above their role. So just for
Authentication and Access Control best practices for healthcare systems

e.g., a nurse in a hospital could have some of the same rights as the director of nursing (DON).

A healthcare system could decide to use discretionary access control (DAC) by itself or along with Role-based access control (RBAC). Discretionary access control involves access control being given to an individual based on their identity and what the individuals are able to view or what they are not able to view. Another unique thing about DAC is that this policy gives an individual the right to allow another individual access rights to resources they would otherwise not have access to. In dealing with DAC there should be some type of matrix in place, especially if the healthcare system is a large system.

Placing a matrix into a large system will be a very tiresome task and putting it down as a matrix will take up a lot of resources. The best way to represent this matrix in any big system is by implementing an access control list (ACL) and maybe a capability list (CL). An access control list deals with assigning certain objects to the users that can use it to complete their jobs within the healthcare system. On the other hand a Capability List (CL) deals with the access permissions’ of the objects being assigned to individuals throughout the healthcare system, so together with ACL makes for a pretty tight system overall.

Mandatory access control (MAC) is also an access control used within some healthcare systems if not all of them. MAC does not look at individuals and assign them rights to the resources within a system. Access to resources is primarily controlled by the security level given to the particular resource trying to be accessed. Now how this all work is in order for someone to access any resource when MAC is applied the individual has to possess a high enough clearance to access the resources. In a healthcare environment, it’s probably not a good idea to assign
Authentication and Access Control best practices for healthcare systems

security level to the resources to control access to these resources. It’s not a good idea because the same type of files may have different sensitivity levels for different patients.

When dealing with MAC it’s very hard to define a clear hierarchy structure because of how sensitive some patient’s information is. For example, anything sex related and mental health related could be highly sensitive but that same information could not be all that sensitive to other individuals. If an organization like a healthcare organization try to implement some form of hierarchy it would be very difficult to keep all patient’s information private within the hierarchy.

If a healthcare facility decide to go with a hierarchy within their MAC controlled system most of them will use sensitivity labeling of their EHR information.

When a healthcare system decides to use sensitivity labeling they allow sensitivity labels to be set by the patients and the medical staff also defined sensitivity labeling. The good about this setup is the fact that the patient’s sensitivity labeling will come before the labeling defined by healthcare personnel. By the healthcare system using sensitivity labeling this ensures that only the relevant information is available to the right person in order for them to complete their jobs.

Conclusion

I conclude this research paper by agreeing that smart cards combined with some sort of biometric technology would make for a very tight and secure healthcare system. By using the biometric technology you leave little room for manipulation of the authentication system put in place to provide the best possible protection of the patient’s information throughout the healthcare system. I also believe that by assigning a smart card to an individual you put some of the responsibility back into the hands of the individual in case of a data breach or some other security breach. Access control is equally as important as authentication because the healthcare
Authentication and Access Control best practices for healthcare systems

system should make sure that only the individuals that need certain information have access to the information.

Most healthcare system implement multiple methods of access control to secure there patient’s records. Role-based access control and along with mandatory access control seem to work the best when it comes to complete access control over the system. MAC will ensure that a security level is assigned to specific resources within the system and that only certain individuals will have access to these resources. Role-base access control will ensure the permissions and rights assigned to the specific roles within the healthcare system is granted or denied access to patient’s records.

My belief is that access control will continue to be the proper way to secure information systems for healthcare facilities and any other organization out there. DAC, MAC, RBAC will remain the most popular methods of access control, and it’s very important for organizations to careful define what they would like within their DAC, MAC, RBAC based systems because there are so many different variations available. There are certain requirements that have to be met in order to achieve proper access control through the system, and for any healthcare system, it’s vital to build a complete set of purposes and maintain them accordingly.
Authentication and Access Control best practices for healthcare systems

References


Authentication and Access Control best practices for healthcare systems