AUCTORES
Globalize your Research

International Journal of Clinical Case Reports and Reviews
Cheryl Ann Alexander *

Open Access

Review Article

The Development of An Identity and Access Management Plan for A Medical Center

Cheryl Ann Alexander [1]*, Lidong Wang [2]

[1] Institute for IT innovation and Smart Health, Mississippi, USA.

[2] Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA.

***Corresponding Author:** Cheryl Ann Alexander, Institute for IT innovation and Smart Health, Mississippi, USA.

Received Date: November 17, 2023 | **Accepted Date:** December 22, 2023 | **Published Date:** January 02, 2024

Citation: Cheryl A. Alexander, Wang L., (2024), The Development of an Identity and Access Management Plan for a Medical Center, *International Journal of Clinical Case Reports and Reviews*, 16(1); **DOI:10.31579/2690-4861/353**

Abstract:

Over the last decade many changes have occurred to Healthcare Information Technology (HIT). IT professionals must find new ways to manage the massive amounts of healthcare data. The correct information to the right patient is the most critical factor in identity and access management. IT professionals can set Authenticator traps for preventing cyberattacks and mitigating cybercrimes. Preventing attacks is an enormous undertaking for IT professionals. Access review determines what IT professionals need to do to prevent cyberattacks in the enterprise. This could include many activities. Labeling and identification are essential to preventing attacks. This paper explores access management and review, authenticator, attacks, mitigation, and access review and implementation in healthcare. All this is essential to a successful endeavor at preventing attacks on healthcare information.

Key words: identity and access management; authenticator; attacks; mitigation; access review; healthcare; public health

1. Introduction

Health Information Technology (HIT) has rapidly developed over the last decade and has contributed to many advances in the confidentiality of patient data and the management of patient health records. Health Information workers are members of the allied health team and have greatly impacted the protection of health data to secure the privacy, confidentiality, and integrity of the patient's electronic health record (EHR) and electronic medical record (EMR). When the EMR went digital, many new responsibilities fell to the IT professionals. Once digital records accumulated over the last few years, IT professionals began to look for ways to manage the massive amounts of patient data and the means to keep them safe. New laws were passed and blockchain and big data analytics became popular methods of repelling cybercriminals. Advancements in data storage and data analytics enabled IT professionals to utilize advanced algorithms such as Artificial Intelligence (AI) and machine learning (Stanfill & Marc, 2019). The most popular AI algorithms are currently being used in the Picturing and Communications System (PACS) and other radiological applications. However, many factors are driving the use and development of AI in healthcare including financial pressures and keeping up with competitors the most common. The growing elderly population is putting a strain on healthcare as well as simply the huge amounts of healthcare data. Data that requires ever more sophisticated interpretation is continually driving data for the provider. The right information to the right individual is a major concern for the IT professional. The increased use of AI and ever more sophisticated practices of access point care such as practical entry point testing, medical coding appropriately, and the ability for Health Information Management (HIM) to manage Health Information and Management (Stanfill & Marc, 2019).

2. Maintaining Confidentiality in Health Data

With the modernization of healthcare imaging data, the amount of data is expanding exponentially. Most HIM and IT professionals are using advanced tools to manage the privacy and confidentiality issues associated with the use of medical imaging tools. Patient imaging data contains sensitive information, and most programs contain large amounts of patient data such as computer imaging technology (CT), magnetic resonance imaging (MRI), ultrasound, etc. Transmission of patient imaging data is highly at risk for cybercriminals and interception of the transmission of any imaging data is a security challenge. A catastrophic event can occur when there is an interception of imaging by any malicious actors or there is tampering with the images or privacy disclosures. Effective services, then, can only be provided when medical data is secure (Zhang et al., 2020). The responsibility for medical data security lies with medical personnel. Medical data is susceptible to hackers looking to make money on the information related to the patient (Madhusudhan & Sakthivel, 2021). Patient data is more valuable to hackers than a person's

social security number because third-party businesses can use medical data to deny or modify insurance. For example, with a person's medical data in possession, an insurance company has access to all of their history. The patient may then be flagged, and their insurance claims or application denied.

With telemedicine becoming widely available in multiple care areas, data security becomes an issue for maintaining confidentiality, integrity, and availability. Some medical images need to be transmitted over an insecure public network so that treating hospitals and medical providers can interact. Maintaining confidentiality then becomes the problem. Studies have been published but are not widely available. There are no systematic literature reviews related to patient data security for telemedicine. Therefore, the available options for data transmission need to be studied (Zhang et al., 2020). Big data analytics can store vast amounts of data and can provide patient data with a secure and private access model. To branch off this cloud networking plays an integral part in saving data. Traditional EMRs pose a real challenge to the access of patient data. Despite the ease of medical records programs, they still present some challenges, both for integrity and confidentiality. Because the EMR contains many sensitive and confidential information about the patient, it is a very likely target of malicious actors (Mani et al., 2021). A centralized database of patient data can expose the data to cyberattacks and malicious actors. However, stakeholders and providers can have further challenges when trying to access patient data and the EMR. Patient data can be permanently lost when it is deleted from the hospital database, thereby making it more difficult for stakeholders and providers to access patient data in the mobile setting. Patients also have limitations when accessing mobile apps that give them a wide variety of their patient data including labs, imaging, provider notes, and scheduling doctors' appointments (Mani et al., 2021).

3. Maintenance of Integrity and Confidentiality

Hospitals and other healthcare facilities still maintain stewardship over patient data despite patients having the increased freedom to modify their patient data, view their data, and share their data with other stakeholders and providers. By sharing patient data, the healthcare data management system becomes more secure and effective (Ismail & Materwala, 2020). The qualities of healthcare data have a propitious future for protecting data characteristics such as confidentiality, integrity, and availability. With issues such as integrity taking the spotlight in protecting patient data, the need for solutions is increasing. There is an increasing need for the healthcare industry to work on such critical issues and produce a proposed model for protecting healthcare data. The introduction of smart controls such as cybernetics for the protection of data against cyberattacks should produce a model with strong performance against malicious actors (Ismail & Materwala, 2020).

4. Integrity and Availability

The unprecedented number of cyberattacks has led to a challenging task for protecting health data. Healthcare data has been targeted more often and by cyber-invasions. The management and direction of smart healthcare facilities have become directly dependent upon digital cyberstructure. Hence, there is a need for healthcare workers to define their facilities and the digital interactions that are currently being used from a new perspective. In addition, the COVID-19 pandemic defined fault lines across the smart healthcare infrastructure that need to be defined and protected maintaining a new perspective (Alhakami et al., 2020). Healthcare data management must be improved while ensuring trust within the healthcare community. The exponential growth of healthcare data and the overall improved healthy living situations of seniors, the disabled, etc., at home, in residency, and in hospitals, demand a stronger, more propitious healthcare data protection program. Currently, healthcare data is protected in a secure centralized data management plan. However, a decentralized program could provide a more secure and improved plan. Blockchain has been examined by scholars for protecting healthcare data (Naresh et al., 2021).

Nurses, providers, staff, etc. providing patient care and responsible for documenting patient care may be responsible for transporting a tablet or cell phone outside of patient care areas although it has patient data on it. These cell phones and tablets must have cybersecurity protection. The vulnerability of patient data is the highest priority for all staff and providers of patient care. All smart devices have made healthcare data transmissible, portable, and more likely for a cyberattack. Confidentiality is typically a passcode known only to the user or biometrics, barcodes, or other biometric entries to protect healthcare data. Confidentiality is preserving authorized restrictions on information access.

Integrity means guarding against unsuitable information destruction or modification. Availability means guaranteeing reliable and timely access to and utilization of information by authorized users. If data have not been adequately backed up, an integrity problem due to attacks can happen (Warsinske et al., 2019). Other actors who play a role in the security of healthcare data may be external stakeholders or services such as dining servers who provide food for the patient or patient and family. There also may be Durable Medical Equipment suppliers and other suppliers of equipment, medications, or dialysis machines. The security of healthcare data must be vigorous and detailed.

5. Security and Resilience of Systems and Assets

It is vital to improve the resilience of information systems in the Medical Center to ensure the security and resilience of systems and assets. Multi-factor authentication (MFA) is performed. Only authorized employees have access to sensitive resources and employees' online activities are properly monitored and audited. Important assets are tracked, and asset data are captured and reported in time. Annual training regarding identity and access management as well as data security protection is offered to all employees in the Medical Center.

6. People, Devices, and Services in Identity and Access Provisioning

Access control and identity settings should be maintained up to date (Warsinske et al., 2019). It is necessary to update the identity and access status of people who leave the Medical Center or change departments or jobs within the center. An internal employee's tasks, access, and trustworthiness are evaluated frequently to decide if his/her access matches the tasks. An employee has the minimum access right needed for assigned tasks (Warsinske et al., 2019).

There are many devices (such as computers, laptops, tablets, and biometric devices) in the Medical Center. If an employee does not work in the center anymore, the employee will be asked to return devices that had been issued to him/her for work. Authentication services such as biometric services are constantly advancing. A service or server with a centralized credentials aggregation is a major attacking target (Warsinske et al., 2019). In the Medical Center, only authorized professionals have access to important resources to provide medical services.

External people including providers from other hospitals may be seeking a high level of care for patients. They use a higher level of resources such as trauma care (including access to expert providers) and specialized testing devices and services. They are only authorized a short lime of access depending upon their requirements.

7. Authenticator Threats/Attacks Threat Mitigations

Table 1 lists authenticator threats/attack mitigations (Grassi et al., 2020) in the Medical Center.

Authenticator Threats/Attacks	Description	Examples	Mitigation Strategies
Duplication	Subscribers' authenticators have been copied with or without their knowledge.	Passwords (stored in an electronic file or written on paper), biometrics (such as fingerprint), and passcodes to rooms (such as medication rooms) with patient data are copied without owners' knowledge.	Using an authenticator with long-term authentication secrets (difficult to extract and duplicate), and changing passcodes on a staggered timeline (every week, once a month, or every three months).
Theft	An authenticator is stolen.	A cellphone (with patient data), badge (allowing access to protected health data), or tablet (including medical charting) is stolen.	Using multi-factor authenticators (activated through a biometric or memorized secret) or two-step authenticators.
Social engineering	An attacker creates trust with a subscriber by convincing the subscriber to expose the authenticator output/secret.	A password is exposed by a subscriber during a telephone inquiry from an attacker who masquerades as a coworker or the administrator of the system.	Avoid using an authenticator with a risk of social engineering of a third party (e.g., a customer service agent).
Phishing	An authenticator output is obtained by fooling a subscriber into believing an attacker is a verifier or reliable party.	An online attacker acts like a verifier, steals a password, and receives entry to patient data.	Using an authenticator that provides verifier impersonation resistance.
Online guessing	An attacker connects to a verifier online and tries to guess a valid authenticator output in the context of the verifier.	An online dictionary attacker tries to guess a memorized secret.	Using an authenticator that locks up after a few repeated failures in activation attempts or generates high entropy output.
Eavesdropping	An authenticator secret or authenticator output is exposed to an attacker as a subscriber is authenticating.	An attacker listens for codes to enter patient care areas or overhears an authenticator's secret and patient information in the medical ward near the nurses' station or in a patient's room.	Avoiding non-trusted wireless networks as unencrypted secondary out-of-band authentication channels; ensuring the security of the endpoint, especially regarding freedom from malware.

Table 1: Authenticator Threats/Attacks and Mitigations in the Medical Center

8. An Access Review Schedule with Provisioning and De-provisioning, Auditing, and Enforcement.

For user access review, access privileges must be periodically reviewed (once a year in the Medical Center) according to each user. The review process includes all the accounts, databases, computers, applications, data that a user can see or change, and websites controlled by the Medical Center. As for system account access review, the process is fulfilled (once a year) system by system, for every security device and computer on the network, every database, and every technical entity—to see which systems and software can do any of the things such as connection, reading or changing access settings, and performing privileged actions, or acting as a system administrator (Warsinske et al., 2019).

Provisioning is the act by which an identity is made available for use. It is what the Information Security Department of the Medical Center does when creating an account on the center's computer for an employee. De-provisioning is the act of deactivating an identity and associated access. If a person is not an employee in the Medical Center anymore, his/her account will be deactivated. Additional aspects of de-provisioning include removing the employee from the list of authorized computer users and any role-related access control lists, disabling his/her email, etc. (Warsinske et al., 2019).

It is necessary to perform auditing and enforcement to avoid or reduce mistakes and oversights in identity and access management. Internal auditing is conducted once a year in the Medical Center. The center makes rules as appropriate, provides training, measures performance (auditing is part of this), and then enforces consequences for failure. The failure can be problems in policies or actions of human resources, the poor execution of technical steps by the Information Security Department, oversight by a manager or team member, etc. (Warsinske et al., 2019). Auditing and enforcement work together in the Medical Center.

9. Conclusion

Medical centers are highly vulnerable to malicious actors. These attacks can disable medical care and resources. The medical center must be protected against these types of attacks. By identifying these malicious acts, IT professionals can intercept the attacks and mitigate damage. Identity and access management is a key issue in mitigating many risks. Access review, auditing, and enforcement are necessary steps to protect security and make the medical center safer.

Conflict of Interest

The author declares no competing financial interests.

References

1. Alhakami, W., Baz, A., Alhakami, H., Pandey, A. K., & Khan, R. A. (2020). Symmetrical model of smart healthcare data management: A cybernetics perspective. *Symmetry*, 12(12), 2089.
2. Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R., Regenscheid, A., et al. (2020). Digital identity guidelines: Authentication and lifecycle management. *NIST special publication*, 800-63B.
3. Ismail, L., & Materwala, H. (2020). Blockchain paradigm for healthcare: Performance evaluation. *Symmetry*, 12(8), 1200.
4. Madhusudhan, K. N., & Sakthivel, P. (2021). A secure medical image transmission algorithm based on binary bits and Arnold map. *Journal of Ambient Intelligence and Humanized Computing*, 12, 5413-5420.
5. Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S., & Khalaf, O. I. (2021). Hyperledger healthchain: patient-centric IPFS-based storage of health records. *Electronics*, 10(23), 3003.
6. Naresh, V. S., Reddi, S., & Allavarpu, V. D. (2021). Blockchain-based patient-centric health care communication system. *International Journal of Communication Systems*, 34(7), e4749.
7. Stanfill, M. H., & Marc, D. T. (2019). Health information management: implications of artificial intelligence on healthcare data and information management. *Yearbook of medical informatics*, 28(01), 056-064.
8. Warsinske, J., Henry, K., Graff, M., Hoover, C., Malisow, B., et al. (2019). The Official (ISC) 2 Guide to the CISSP CBK Reference. *John Wiley & Sons*.
9. Zhang, Bin, Bahbibi Rahmatullah, Shir Li Wang, A. A. Zaidan, B. B. Zaidan, et al. (2020). A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges, and recommendations. *Multimedia Tools and Applications*, 1-40.

DOI:10.31579/2690-4861/353