**Info & Knowledge Management**

**NURS: 6412  
   
Walden university  
   
Ritu Adhikari   
   
Date: 01/28/2024**

**Introduction**

Database security is the process of protecting a database from any intentional and accidental

threats. Sensitive data security and maintaining confidentiality, integrity, and availability of the database are the main objectives of database security. Along with data protection, the entire database management system, its applications, and servers both physical and virtual is protected under database security.

**Items to include**

Including both software engineering and database perspectives can help in designing and developing a security project. EHR is a computer-based patient record (CPR) system therefore bringing a software engineering approach while developing a database will incorporate aspects of database design, web development, and security. (Cankaya & Kywe, 2015)

When a user logs in to EHR the system should first check the username and password in the database, when it is found, the encrypted password should be retrieved and decrypted from the database, following this the entered password should match the decrypted password, if there is a match then only the user will grant the assets. This type of system needs to be included in the new organization to maintain safety and security.

Patient privacy requirements enforced by HIPPA need to be followed when developing the design. Health care is a complicated system as it involves aspects from management to staff tracking, so we need to focus on the manipulation of patient records.

Our network is surrounded by a network firewall which is the device in our network’s main router to the internet. The firewall blocks and allows traffic and is based on a set of rules that are loaded in its configuration. There is already a loaded software package in some routers whereas some do not have. In this case, we can use an Access Control List (ACL) to control what is allowed and what is not. (Chhery, 2015)

**Policies expected**

It is not only the responsibility of an institution to maintain the security of confidential information but also every individual should be responsible for this. The main item that should be included in an organization for maintaining security is the development of an appropriate and effective policy.

Policies must be based on risk assessment results, whose findings will provide policymakers with an accurate picture of the security needs specific to the organization.  According to NCES, this is very important as proper policy development requires decision-makers to ensure that mechanisms to achieve the goals are in place, the security goals of an organization are defined, and local, state, and federal laws along with ethical standards are incorporated. Doing this organizational characteristics, legal and regulatory concerns, user inputs and environmental issues can be included in policy making. Policymakers who are experienced in this field can bring skill to security policy development. The person in charge should be concerned with protecting sensitive information that can be accessed from within that site. There should be revision of policies frequently due to the rapid technological innovations. Considering writing separate security regulations that support broader policy, for each user group can increase the involvement and acceptance of having staff contributing towards developing their guidelines and policies.

Meeting staff frequently to learn about significant issues that affect their work can be beneficial as these can be incorporated into policy making. *Assigning a committed administrator to be accountable for security can be* done and the designated staff member must be authorized to both reprimand and reward employees, if necessary. Breaking down recommended security practices into pieces that are manageable and tailored to meet individual job duties.  A short message every week can work better than receiving a large volume every month. Outsiders who have access to the system should sign an agreement about respecting and maintaining the confidentiality of the information.

**Security Challenges**

Databases are the main target for cyberattacks as they store valuable and sensitive information. Various security challenges can occur during this process such as Data theft that will lead to business damage and a negative brand reputation, Patient hesitate to come to a healthcare organization with such a reputation that will cause revenue loss. Data theft can slow the business until the security challenges are resolved.

There can be breaches of data that will cost millions of dollars to repair which will include assisting victims, legal fees, and extra expenses to restore the system. Organizations may have to compensate patients and families as they fail to protect their patient data.

**Strategies**

To secure data and networks any organization can install a firewall that serves as a first line of protection. A firewall increases security by providing a chokepoint where security measures can be focused. Access management can be another option where comes Authentication, Authorization, and Access control.

**According to Microsoft Azure, Authentication** is proving the identity of the user by entering the correct user ID and password. Administrators can also manage this centrally which will minimize password storage and bring centralized password rotation policies. **Authorization** will allow every user to access and perform certain data objects like read but not edit or modify data, modify but not delete data, or delete data. **Access control** can be performed by the system administrator who gives permissions to a user within a database. Permissions are managed by adding user accounts to database roles and assigning database-level permissions to those roles.

**Auditing** can be another strategy that helps us track database activities and assist in maintaining compliance with security standards. This can be done via recording database events to an audit log which allows us to monitor ongoing database activities and analyze as well as investigate historical activity to find out potential threats and security violations.

### To protect information, data encryption can be done that secures sensitive data by converting it into an alternative format so that only intended parties can decipher it back to its original form and access it. Data backup and physical security can also be some strategies for securing data and the network.

**Best practices for securing data and healthcare institutions.**

Best practice plays the number one role in data security because no matter how many policies we make, or how much advanced technology we bring if we don’t follow best practices, it is useless, therefore there is a relationship between best practices for data security and health care. It protects data from unauthorized access, modification, use, disruption, or destruction. Data security can be achieved by using the following best practices.

Data Classification: This approach can divide data into many categories according to their sensitivity and apply the proper measure to store data according to the value of the organization and the sensitivity of the data.

Data Backup and Recovery: This approach creates copies of data that ensure data availability in case of data loss due to any means.

Data Encryption: This approach prevents unauthorized access to data by converting data into a code.

Access Control: This approach protects data by providing access to data according to the user's role and need-to-know basis.

Security awareness training:

This approach ensures proper education to employees on how to identify and respond to security threats.

**Conclusion**

Database security should protect against human error, hackers, malware, media exposure, and physical damage to database servers. To conclude, this paper discussed the scenario, items that need to be included in the assessment, network security challenges, strategies for securing data and networks, and the relationship between best practices for safeguarding data and the network.

**References:**

Cankaya, E. C., & Kywe, T. (2015). [A secure healthcare system: From design to implementationLinks to an external site.](https://go.openathens.net/redirector/waldenu.edu?url=https://www.sciencedirect.com/science/article/pii/S1877050915025764?via%3Dihub). *Procedia Computer Science, 62*, 203–212.

Cherry, D. (2015). [*Securing SQL server: Protecting your database from attackersLinks to an external site.*](https://ebookcentral.proquest.com/lib/waldenu/detail.action?docID=2037826)*.* Waltham, MA: Syngress.

Chapter 3-Security Policy: Development and implementation, from safeguarding your technology, NCES publication 98-297 (National Center for Education Statistics). (n.d.).

<https://nces.ed.gov/pubs98/safetech/chapter3.asp>

*Database security best practices and solutions: Microsoft Azure*. Database Security Best Practices and Solutions | Microsoft Azure. (n.d.).

<https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-database-security/?ef_id=_k_EAIaIQobChMIg4uxtr33gwMVFlRHAR0FtAACEAAYAiAAEgL6HfD_BwE_k_&OCID=AIDcmme9zx2qiz_SEM__k_EAIaIQobChMIg4uxtr33gwMVFlRHAR0FtAACEAAYAiAAEgL6HfD_BwE_k_&gclid=EAIaIQobChMIg4uxtr33gwMVFlRHAR0FtAACEAAYAiAAEgL6HfD_BwE>