- **ISSN-p:** 2791-0237 - **ISSN-e:** 2791-0202 - **DOI:** 10.55737/qjss.883465001
- **Pages:** 34 – 40 - **Vol.** 1, **No.** 1 (2020)

Data Security Challenges in Healthcare System

QLANTIC JOURNAL OF SOCIAL SCIENCES

Rabbiya Zaheer [1] Maida Arif[2] Amina Bibi[3]

Abstract: *This research paper assesses the challenges faced by the modern health care system and its adverse effects. Present literature on the challenges of data security in modern healthcare sector, user error in technology adoption, email scams with malware and other such challenges in the data security impeachment are being reviewed. This research article reviews different literatures and attempts to better explain and analyze the use of better data security in the modern healthcare system.*

Key Words: Data Security Impeachment, Email Scams, Data Backup and Recovery, System Monitoring Apps

Introduction

What is data Security

Data security is the process throughout its life cycle that protects digital information from unwanted access, corruption or theft. This notion covers everything from the physical security of hardware and storage devices to administrative and access controls and the logical security of software applications. It also covers corporate policies and processes. Strong data security plans, when correctly implemented, safeguard information resources of the company from cybercriminal operations but also defend against insider threats and human mistake, which remain one of the major reasons for data breaches today. Data security includes the use of tools and technology to increase the visibility of an organization to the location and usage of vital data. Ideally, the protection of sensitive files should be applied by the instruments, such as encryption, data masking and editing, and reporting should be automated to simplify checks and adhere to regulatory standards.

Data Security and its Importance in Healthcare

Health institutions such as Veterans Affairs (VA) hospitals are particularly vulnerable to hacker cyber assaults in order to gather personal information and fraud. It is essential for healthcare organizations, both internally and externally, to thoroughly evaluate the probable reasons of data failures and to design efficient safety solutions. The type of information gathered and kept is one of the primary reasons why the health care business has a larger risk of attacks than other industries. Health organizations have very detailed patient records which include their name, date of birth,

[1] Research Scholar, Department of Social and Behavioural Sciences, NUMS, Rawalpindi, Pakistan.

[2] Research Scholar, Department of Social and Behavioural Sciences, NUMS, Rawalpindi, Pakistan.

[3] Research Scholar, Department of Social and Behavioural Sciences, NUMS, Rawalpindi, Pakistan.

address, social security number, payment accounts, etc. With the collection of these information by healthcare institutions, the danger of data assaults is increased. In addition, the amount of health data in the black markets is higher compared to other types of stolen information. Health records contain both data and views about the physical and/or mental health of a patient. The medical records contain consultation notes and scan results, films, audio graphics, pictures, tissue samples, and correspondence (in other words) between specialists. These documents include an abundance of information that is sensitive and secret and are thus safeguarded. It is essential that all your personnel are equipped with adequate data protection training while processing a big quantity of sensitive health data. Data infringements of the healthcare environment can have disastrous effects for both organizations and people: organizations may face crushing fines, and patients' rights, freedoms and privacy are affected. To safeguard your organization and patients, the training of all your personnel in best practices in data protection is important. For these reasons, the deployment of appropriate data security solutions is highly vital for companies like VA hospitals. Health records have an 8-year minimum hospital record retention duration, 10 years for GP records and extended periods for the medical, obstetrical and psychiatric records. The documents must be duly disposed of in confidential trash after these timeframes.

Chalenges

Health Information Exchanges and Electronic Health Records

A network that stores large quantities of medical data shared between multiple providers creates a tempting opportunity for data thieves. Where once, you might have had to break into a doctor’s office and flip through physical files to access a person’s medical history, now all you need is a lack of moral compunction and some hacking know-how. This creates a new burden for providers to maintain compliance and healthcare data security. For example, providers are required to notify patients any time there is a as healthcare data makes its rapid migration into the digital realm, encryption is becoming the law of the land.

User Error in Technology Adoption

In the 21st century, especially in last decade there has been a jump in the advancement in technology. Most of the Users which are normally people who don’t have a lot of experience with technology have not been able to keep up with the pace and so don’t fully understand the risks. Once accessing your lab work from your provider’s portal, your medical privacy is in your hands. If you store your data in unencrypted folders in the cloud, or if you send your results to your mom via email, you pave a simple pathway for a hacker to access your most personal data. Users should be taught to be more cautious. That health data or any other personal data for that matter should be sent around causally without proper encryptions.

Hackers

Earlier this year there was an infamous accident, the CHS Heartbleed attack, proving that in the age of data nothing is saved. Even though the Community Health System, Inc. (CHS) is one of the largest hospital groups in the United States hackers were able to get past their security checks and have access to their patient's personal data which even included social security numbers of over a million people. Hackers from Internet vigilante group Anonymous also targeted the Boston Children's Hospital, launching a DDoS attack on the hospital website as an act of "hacktivism. It shows just how vulnerable healthcare data security can be to a group of determined hackers.

Outdated Technology in Hospitals

There is a constant budgetary constraint on the healthcare system. Lifecare is often prioritized in comparison to IT demands. In a country like Pakistan where the healthcare system receives very little budget from the government, the condition is worsened. There is dire need to upgrade the system with new efficient technology that only makes work for the health providers easier and efficient but at the same time protects the system from breaching. The importance of new IT technology is yet to recognized by higher officials but on the contrary, one could argue that is a third world country like ours, where the residents are battles different life-threatening problems at the same time, IT doesn't top the priority list.

Health Care Data Risk Factors

We should be aware of some common risk factors in health care operation in developing health care data security solutions but they are not limited.

Use of Legacy System

It is possible for hackers to access health care system through outdated operating systems. Outdated system and applications lack proper security because the company that created the software or hardware no longer supported that. It is better to upgrade the system.

Malware Email Scams

Utilizing the same techniques as email phishing, this attack encourages targets to click a link or download and attachment so malware can be installed on the device. It is currently the most pervasive form of phishing attack.

Risk by Internal Employees

Health care data could be stolen and share by internal employee, contractors and vendors or obtained by disgruntled employees.

Most breaches are caused by employee negligence and healthcare is no exception.

Risk by Poor Wireless Security Network

The increasingly popular wireless network devices used in healthcare facilities, though convenient and time-saving, exacerbates the administration difficulty of network security. Wireless networks should be protected with heavy passwords.

Lacking Strong Passwords

Many data breaches are due to poor password security. Employees use the same password across multiple work and home applications which are also weak and do not protect healthcare information. It is important to keep strong password.

Untrained data Security Practices

When data is handled by untrained employees which don't know the security protocols and issues than data can be stolen easily. It is important to train new staff. It also important to check on the staff whether they are following latest security practices or not.

Failure of Data Security

Safeguarding a huge quantity of health data that is sensitive at separate locations in different forms is one of the big challenges. Sometimes healthcare workers leave workstations unlock and anyone can use and steal data. They should be aware of locking workstations and also installed features of auto locking in order to keep the data safe and secure.

Solutions

There are different types of Data security solutions. The solutions suitable for a Healthcare organization depend upon the needs of that particular organization. These needs are based on the data storage methods, the amount of data to be stored, how long that data must be stored etc. Every organization should have some precautionary measure in place to protect their data.

It is important in a Healthcare system that the patient data not be accessible to everyone. Only relevant professionals should have access to data. For example, knowledge about the patient's history, diagnosis, medication should only be accessible to the doctors and nurses handling that particular case. Same is the case with billing and patient insurance. Patient information is strictly confidential and should be protected at all costs.

Some Solutions are as Follows

Data Backup and Recovery

It should be ensured that your data is backed up on secure servers such as a portable NAS server every day. Portable servers are the ideal place to store your security in a secure and secure location if you have multiple locations.

The Necessity of Data Encryption

Encryption is now the highest available level and should be used absolutely. Data encryption plays a vital role when it comes to transfer the data from workstations to servers or the internet or the cloud-based systems.

Increase the use of Anti-virus/Malware/spyware Apps

The systems must be protected from any kind of viruses, malware, spyware so proper and updated app that meets the requirements should be used.

System Monitoring Apps

These are apps that are used to keep a check on who is accessing, updating and deleting files. They can also be used to monitor infringement of data privacy. Some of these apps also are used to keep an eye on unauthorized access to the system.

Multifactor Authentication

A healthcare system is usually accessed by a multitude of people including employees, supplies, vendors, contractors etc. So, it is not feasible to trust on all of them to use secure passwords. Another way around this is to enable multi-factor authentication. Most systems can be accessed with only one password. However, multi-factor authentication system requires more than one piece of information for successful authentication. For example, the system maybe asks for employee's name, password and one-time passcode sent on their phones for access.

Protection against Ransomware

Ransomware is a software that blocks a person's access to his or her computer until a payment is made to the hacker. It basically holds a computer hostage and demands a "ransom". These costs an individual or an organization a lot of money and there is still no guarantee that all the data will be restored. Healthcare system requires an app that will protect its servers against ransomware.

Employee Training

Healthcare Organizations must hold periodic training sessions with their old and new employees to make sure that they are properly storing, organizing and protecting patient data.

Some Additional Challenges and Solutions

Some other challenges in data security can also be that when a doctor is given an app to use and enter the data in that app can be downloaded on and accessed from any device hence making it very easy for the hacker to access the files. We have to look at different aspects while analyzing a breach in data security for example if there is any tunneling taking place, or is there a one patch to the data center. You have to see where the data base is being exposed; is it a hard line, is it being picked wirelessly and the list goes on. To better protected the data some software's, exist that are also being used by the US military, such as the RSA algorithm. These algorithms mainly use prime numbers and when we talk about prime numbers we mean prime numbers in millions, and so one prime number is picked but the catch is that the next prime number also has to choose to run the algorithm hence the use of big numbers. Prime numbers keep your encrypted data safe. Hash stored passwords are also a safer option.

Conclusion

Data security is very crucial in every field but specially in the field of medicines as the data at stake is very sensitive and very personal. If things go into the wrong hand's lives can destroyed. So hence in conclusion in order to prevent dangers and ensure optimum information security, IT solutions must be created and utilized in the health business in accordance with all requirements. The use of appropriate data protection policies and solutions will ensure that healthcare institutions comply with and exchange data securely with monitoring and reporting laws.

References

Systems, S. O. (2020). *Managed IT Services, Copiers, Telephony | Standard Office Systems of Atlanta*. Soscanhelp. https://www.soscanhelp.com/

Cprime Studios | Custom Software Development Company | You can build it all. (2020). Cprime Studios. https://archer-soft.com

Offshore Software Development Company | Outsourcing Team - ONIX. (2019). ONIX. https://onix-systems.com

Moved. (2015). Oracle. Data Security Challenges - Oracle Help Center https://docs.oracle.com M. (2020, March 15). *Master programs to help professionals upskill*. Top 10 Challenges of Cyber Security Faced in 2021. Jigsaw Academy. https://www.jigsawacademy.com

Online veiligheid- en privacyproducten | F-Secure. (2018). Big Data security – challenges and solutions. F-Secure. https://www.f-secure.com/nl