Commentary
Volume 13:5, 2022

Global Journal of Technology and Optimization

ISSN: 2229-8711 Open Access

Electronic Medical Documents Confidentiality and Integrity

Vanessa Addams*

Department of Electrical and Computer Engineering, Carnegie Mellon University, Forbes Ave, Pittsburgh, Pennsylvania, USA

Description

If embraced by healthcare organisations, electronic medical records (EMRs) can offer a number of advantages to physicians, patients, and healthcare services. However, many healthcare organisations may implement EMRs at a relatively low rate because to worries regarding patient data security and privacy [1]. One of the major issues of EMR is the security of a sizable amount of sensitive health data spread across several sites in various formats. The purpose of the review given in this paper is to highlight the privacy and security problems of health organisations and to look at potential solutions. It displays the IT security events that have happened in medical facilities. Researchers will be able to comprehend these security and privacy issues thanks to the review [2,3].

An electronic health record is a digital representation of a patient's medical history that a healthcare provider has kept for a period. It includes all the essential administrative clinical data related to the care that a person receives from a specific provider, including demographics, progress reports, problems, medications, significant signs, medical history, immunization records, laboratory information, and radiology reports. Most healthcare institutions and organisations use paper to record health data, which has resulted in a significant paper trail. As a result, most businesses have developed an interest in switching from paper-based health records to electronic health records. Privacy, security, and confidentiality are major problems that need to be addressed in electronic medical record systems. Although they have a close relationship, security and privacy are actually rather distinct. While security is defined as the level at which access to a person's personal information is limited and permitted for those who are authorized only, privacy refers to the right that someone has to decide for themselves when, how, and the extent to which personal information is transferred or shared by others. When sensitive health information is transferred or shared without authorization, a data breach may result. The unavoidable systemic identification that takes place throughout the whole electronic health infrastructure, as well as by centralized technologies and parties, can also result in numerous scenarios where privacy is violated [4,5].

It is significant to mention that EHR is being utilised more often in a number of developing countries since it not only enhances healthcare quality but is also cost-effective. It is quite difficult to ensure the security of the information that is present in the system since technologies like these have the potential to generate risks. Concerns concerning this system have lately been highlighted due to security breaches. Little thought has been given to the security and privacy concerns that might follow from it, despite the fact that it is becoming more and more helpful and there is rising excitement for its use. As a result, the authors have conducted a thorough examination of all the pertinent problems relating to the privacy and security elements of the EHR system as documented in the scientific literature accessible to the general public. The inherent characteristics of internet of things networks, which make them distinctive in their own ways, are where the internet of things' privacy and security concerns begin. These traits include heterogeneity, an unpredictable environment, limited resources, and a larger requirement for scalability. At the moment, even systems with the smallest number of processors have a very excellent crypto engine and enough programme memory to execute necessary security features. Based on their distinctive qualities, the security needs for Internet of Things systems are divided into the following categories: identity management, network security, resilience and trust, and finally privacy. Even though none of the designs fully addresses all security demands, the critical analysis shows that a number of security needs are taken carefully [3,4].

The third group of topics are technical safeguards, which secure the whole information system of a health organization's network. The majority of security breaches occur via electronic media, through the usage of computers and other portable electronic devices, hence this subject is crucial to guaranteeing the organization's security. This topic includes security procedures for scanning for viruses, using firewalls and encryption, and authenticating information. Lemke came to the conclusion that encryption and firewalls were the most often used security measures. Antivirus software, chief information security officers, and cloud computing are a few other notable security measures that are also in use, though their implementation is budget-dependent. Technical safeguards, which secure a health organization's network's entire information system, make up the third category of subjects. This topic is essential to ensuring the security of the company since the majority of security breaches happen through electronic media, through the use of computers and other portable electronic devices. This subject covers security practices such as virus scanning, employing firewalls and encryption, and information authentication. Encryption and firewalls were found to be the most often deployed security methods, according to Lemke. Other significant security methods include cloud computing, chief information security officers, and antivirus software, albeit their deployment is budget-dependent [1,2].

Acknowledgement

None.

Conflict of Interest

The authors reported no potential conflict of interest.

References

1. Keshta, Ismail and Ammar Odeh. "Security and privacy of electronic health records: Concerns and challenges." *Egypt Info J* 22 (2021): 177-183.
2. Cheng, Long, Fang Liu and Danfeng Yao. "Enterprise data breach: Causes, challenges, prevention, and future directions." *Data Mining Know Dis* 7 (2017): e1211.
3. Bhushan Petlu, Paul Bharath, N.L. Kumar Anantapalli and M. Muralidhara Rao. "Novel Methodologies to Avert Hacker." *Int Conf Comput Sci Eng Info Tech* (2011): 112-120.
4. Barrows Jr, Randolph C. and Paul D. Clayton. "Privacy, confidentiality, and electronic medical records." *J Am Med Info Assoc* 3 (1996): 139-148.
5. Thite, Miss Vrushali and Mininath Nighot. "Honeyword for security: A review." *Int J* 6 (2021).

***Address for Correspondence:** Vanessa Addams, Department of Electrical and Computer Engineering, Carnegie Mellon University, Forbes Ave, Pittsburgh, Pennsylvania, USA; E-mail: addams.vanessa@up.ac.za*

Date of Submission: 09 May, 2022, Manuscript No. GJTO-22-70923; **Editor Assigned:** 11 May, 2022, PreQC No. P-70923; **Reviewed:** 16 May, 2022, QC No. Q-70923; **Revised:** 21 May, 2022, Manuscript No. R-70923; **Published:** 26 May, 2022, DOI: 10.37421/2229-8711.2022.13.295

How to cite this article: Addams, Vanessa. "Electronic Medical Documents Confidentiality and Integrity." Glob J Tech Optim 13 (2022): 295.