ejpmr, 2023, 10(9), 764-771

SJIF Impact Factor 6.222

EUROPEAN JOURNAL OF PHARMACEUTICAL AND MEDICAL RESEARCH

www.ejpmr.com

Review Article

ISSN 2394-3211

EJPMR

ENSURING MEDICAL DATA SECURITY AND INTEGRITY IN THE AGE OF DIGITAL HEALTH

[1]*Namana Tejasri, [2]Buchigari S. Haripriya and [3]Seelam Manju Lakshmi

[1]Pharm D., Student at Clinosol Research, Hyderabad, India.
[2]B. Pharmacy, Student at Clinosol Research, Hyderabad, India.
[3]M. Pharmacy, Student at Clinosol Research, Hyderabad, India.

***Corresponding Author: Namana Tejasri**

Pharm D., Student at Clinosol Research, Hyderabad, India.

Article Received on 21/07/2023 **Article Revised on 11/08/2023** **Article Accepted on 01/09/2023**

ABSTRACT

Maintaining data integrity & security continues to be a persistent problem in the current healthcare sector. They can become significant health threats for patients & big responsibility for clinicians, resulting in problems such as scam, misconduct, inadequate treatment & data theft. Healthcare data no matter how useful for the advancement of medical science & vital to the success of all healthcare organizations, can only be used if data integrity & security issues are addressed. The healthcare sector also embraced digital technology to facilitate technological change from mechanical and analogue electronic devices to the digital technology that is available today. The article presents the impact of technology in healthcare along with the integrity and security concerns related to technology use in healthcare and discussed ways in which they may be addressed. We mainly focused on the recently proposed technological methods based on anonymization and encryption.

KEYWORDS: Data Security, Data Integrity, Digitization, Electronic Health Records, HIPAA compliance, Encryption.

INTRODUCTION

In today's world we can recognize huge growth in the development of security and integration of apparent technologies, in practically each and every part of our existence and community tends to create extraordinary chances; however, it also procreates specific challenges.[1] In reality, digitization of health and medical data is undergoing into a dramatic and fundamental shift in the clinical, medical, operating and generally in the world of economy to act in advance to the future. This shift is being encouraged by aging population and lifestyle alters.

The increase in the number of software applications and mobile devices; new methods of treatments; intense focus on care quality and value; and proof -based medicines as defers to subjective clinical decisions -- all of which are most important to offer these opportunities for holding up clinical decisions, improving medical and healthcare delivery, management and policy making, monitoring diseases, surveilling adverse events (AE), optimal treatment for diseases affecting various organ systems.[2,3]

Data security and data integrity are the two different and major processes for healthcare sector to give improved patient outcomes by keeping them secure and consistence.

Data security is the process or typically defined as the protection against unauthorized access to digital data, such as electronic health records (EHR's). Data security in the healthcare and medical industry resists from cyberattacks or threats, data breaches, and other security challenges. As data security is one of the healthcare industries top most priority.[4]

Whereas, data integrity is defined as the complete, consistent, and accurate data. It should be attribute, legible, contemporarily recorded, original and accurate (ALCOA). Data integrity is not only involved in processes of computer systems, devices, tools but it is also concerns about the medical health. It maintains the accuracy of patient's personal data, briefing of health, clinical investigations, test results, and also family information. This is the process for keeping digital health more meaningful, accurate and complete. It helps easily accessible so, that clinical routes can be improved, optimized to help with good clinical management.[5] Data integrity is the one which drives (EHR) systems and is important in providing functions at all extents.

These two data security and integrity are connected with each other closely. Data security guarantees preventing access to unauthorized users to digital health but providing easy access to authorized management and healthcare professionals.[6]

Successful related works

From the recent reports Healthcare law of Kingdom of Saudi Arabia which also focuses on emerging problem for debate of digitization now it is the most absolutely necessary area for (KSA). Vision 2030 mission intends to guide the Kingdom as a Middle East Asian Leader of technological innovations in healthcare and a successful economical country. KSA 's goal and vision would find a need for a safe and protected data system for healthcare in the country.[7]

Apart from this enabling data integrity is another serious issue in KSA according to a recent report. Meddling with medical and health records and data can cause an endangering circumstance for patients.[8]

Here we came to known that security and integrity are interrelated. Violation of security can influence data integrity. An unauthorized person or an attacker could change related data or can corrupt health records, making them irrelevant and perilous for deciding.

Perfectly consistent security and integrity to an extraordinary extent of various big healthcare data technologies can not only make it possible for us to opt deeper insights into the medical and organizational processes but also provides faster and safer amount of data of patients and create high efficiencies and help improve patient flow, safety, quality of care and the overall patient experience no matter how costly it is.

Such has the case with South Tyneside NHS Foundation Trust, a person who provides acute and community health services in Northeast England came to understanding about the priority of providing high quality, safe and concern care for the patients at all the times, but needs a good comprehension of how its hospitals works to improve source, supply and support allocation and time to ensure that any problems are recognized early and to take an action upon.[9]

Another example of Kaiser permanent medical network based in California. It has more than 9 million persons, approximately to control wide range of data which is ranging from 26.5 petabytes to 44 petabytes.[10]

In meanwhile the techniques have led to improve patient care processes and reduce costs, it is on rising of healthcare factual information to an increased extent of security and integrity unauthorized access. In 2016, Cynergis Tek has released the Reds pin's 7th annual breach report: Protection of Health Information (PHI)[11] in which it was reported that hacking of healthcare data was increased by 81 % in 2016 resulted from hacking attacks specifically. In addition, ransomware defined as a type of malware that encrypts data and holds it hostage until a ransom demand was not met, which has identified as the most particularly noticeable threats to hospitals.[12]

In January 2014, The White House, led by the President Obama's counselor John Podesta, took the responsibility of a 90-day review of big data and its privacy. This review brought particular proposal to maximize benefits and minimize risks of large data.[13]

The OECD Health Care Quality Indicators (HCQI) project is responsible for a plan in 2013/2014 was set forth tools to aid countries in equalizing data privacy risks and risks from not developing and using health data. This plan includes developing risk categorization of several types and uses of information and the promising practices that countries can bring into action to decrease or reduce issues that directly affect patient daily life and enable data use.[14]

HEALTHCARE DATA & ITS DIGITIZATION

Healthcare data security and integrity are the most delicate concern for the current reports, diagnostic reports, laboratory tests reports, and also other records. Ensuring management of medical data security and integrity is not an easy process for health professionals and research scientists. Attackers specifically target healthcare and medical data domains and sub-domains to manipulate valuable information. Hence protecting the medical data is the most existing issue in this era. Healthcare data examples include:

1. Patients' test outcomes
2. Doctor's notes
3. Information about products and medications
4. Patient results
5. Clinical research[15]

For better experience and fewer infrastructure facilities, each country is following to be digitized healthcare sector. However, the process of digitization towards the health and medical care sector poses many intricate challenges for security experts. Attacks on confidentiality, privacy violations, quality of data breach and other various risks are the continuously increasing problems for procedures and experts in digitization.

Medical data security and integrity is a critical component of healthcare, but it also includes various challenges:

1. **PRIVACY AND SECURITY:** Protecting patient data is more important than anything in the healthcare sector. Unauthorized access can lead to severe consequences. So, regulations like HIPPA in the U.S. and GDPR in Europe aim to address these problems.
2. **DATA VOLUME:** Medical data is the vast factual information which includes electronic health records (EHR's), imaging and genomics etc., management and analysis of such large datasets can be daunting.

3. **INTEROPERABILITY:** Healthcare systems often use different formats and standards, which makes data incompatible, difficult to share and integrate for patient care.
4. **DATA QUALITY:** Inaccurate and inconsistency in medical data can lead to incorrect diagnosis and treatment decisions.
5. **ETHICAL ISSUES:** There will be many ethical confusions related to the use of medical data, such as consent for data sharing and potential biases in AI algorithms.
6. **DATA STORAGE AND INFRASTRUCTURE:** Managing the storage and processing demands of vast amounts of digital health requires robust infrastructure and investment.
7. **REGULATORY COMPLIANCE:** Staying compliant with evolving healthcare regulations and standards can be complex and resource-intensive.
8. **RESOURCE CONSTRAINTS:** Many healthcare institutions lack the resources and expertise needed to effectively manage and utilize medical data.
9. **PATIENT EMPOWERMENT:** Ensuring patients have access to and control over their own medical data is a growing concern in today's time.
10. **DATA INTEGRATION:** Integration of various sources of medical data, such as clinical, genetic and wearable data, is essential for holistic patient care but can be technically challenging.[16]

HEALTHCARE DATA SECURITY

Security is defined as the protection against unauthorized access, with some including explicit mention of integrity & availability. It focuses on protecting data from pernicious attacks and stealing data for profit.

While healthcare organizations store, maintain, and transmit huge amounts of data to support the delivery of efficient & proper care, the downsides are lack of technical support & minimal security. It is critical that organizations implement healthcare security solutions that will protect important assets while also satisfying health care compliance mandates.[13]

Objectives

Few of the security objectives for the healthcare sector and the techniques to achieve those objectives

- **CONFIDENTIALITY**

Only authorized individuals such as healthcare providers and medical staff can get the access to the patient medical and health data. Private network such as encryption techniques were used.

- **PRIVACY**

Unauthorized access as well as protection against personal information breaches. Some of the techniques used are anonymization, pseudonymization and encryption of data.

- **AUTHENTICATION**

In this verification of identity of users is done and access to the healthcare staff is given to prevent unauthorized access to patient information. Techniques used are password-based authentication, two-factor authentication, biometric authentication, smart card authentication, token based and certification-based authentication etc.

- **NON-REPUDIATION**

Non-repudiation prevents individuals from denying actions which are taken within the healthcare organization, such as changes to patient data or permission to sensitive data. Here technologies used are digital signatures and block-chain.[17]

Significance of Data Security in Healthcare

Unquestionably, one of the top objectives for the healthcare sector is data security. Cyberattacks and data breaches have substantially escalated in recent years across all sectors of industry. Recovery after a breach can be time-consuming and perhaps expensive. Widespread healthcare breaches can have detrimental effects. Healthcare organisations may fight against attacks and breaches by putting data security measures in place.

1. **Protection Against Cyber Attacks**

Because PHI is so valuable, cybercriminals are increasingly targeting healthcare organisations. An extremely serious consequence of a data breach is the compromise of patient privacy, which has serious financial and reputational repercussions.

2. **Compliance with Regulations**

To protect patient privacy and data security, the healthcare sector is heavily regulated. A federal legislation known as the Health Insurance Portability and Accountability Act establishes guidelines for the security and privacy of PHI. HIPAA violations can lead to hefty fines, legal action, and other consequences.

3. **Trust and Confidence**

Establishing trust and confidence between patients and healthcare professionals requires data security in EHRs. Patients need to feel in control of who can access their personal information and that it is safe and secure.

4. **Improved Patient Outcomes**

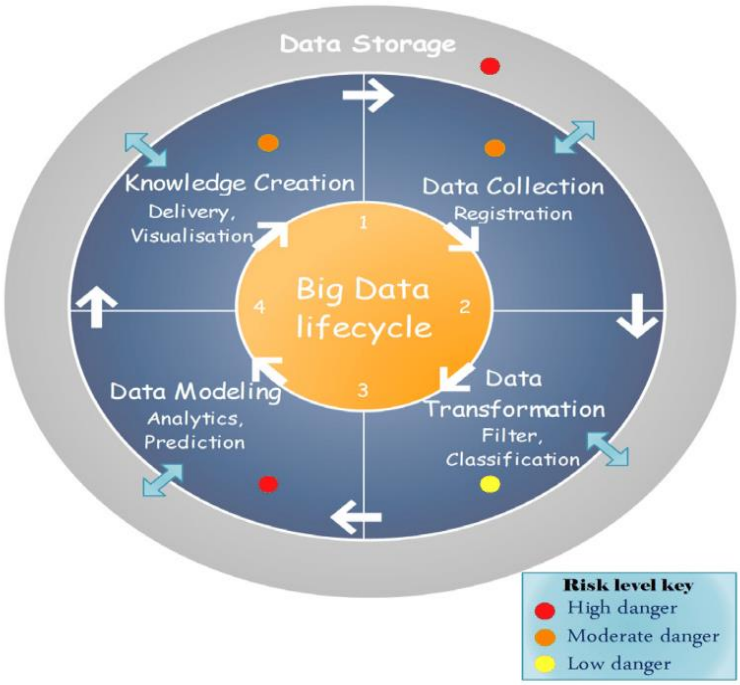
EHR data security can also result in better patient outcomes. Healthcare providers can develop more informed treatment plans and deliver better overall care if they have access to complete and accurate patient data. Patients might be reluctant to give their information if they are worried about its security, which could result in incomplete or erroneous medical records and potentially jeopardise patient treatment.[4]

Data security Life cycle

Various models were proposed to secure the healthcare data. Among them, one method is designed to address

the phases of data life cycle & correlate threats & attacks that face data environment within these phases while address big data life cycle from user role perspective: data provider, data collector, data miner & decision maker.

The model proposed in comprised of 4 interconnected phases:



- Data Collection Phase: It is the first step which involves collecting data from different trusted sources, preserve patient's privacy & make sure that this phase is secured and protected from unauthorized access, disclosure, modification, duplication, diversion, destruction, loss, misuse or theft.
- Data transformation phase: Once the data is available the next step is data filtering, enrichment & transformation to improve the quality of data. During transformation & storing the collected data containing sensitive information should remain isolated & protected by maintaining access level security & defining some security measures like data anonymization approach, permutation & data partitioning.
- Data modelling: After the data has been collected, transformed, stored in secured storage solutions, data mining techniques such as clustering, classification & association can be employed for feature selection & predictive modelling. This process helps eliminate some vulnerabilities & mitigates others to a lower risk level
- Knowledge creation phase: It comes up with new information & valued knowledges to be used by decision makers.[13]

Challenges of Healthcare Data Security

- **Health information exchanges**

Data must be sent and received between health information exchanges and physicians, patients, and insurance providers. It can be challenging to secure these communications and ensure that people transferring data use the right digital channels.

- **User error in technology adoption**

There may be instances when healthcare workers are so busy that they lack the time to adequately study how their technology functions. Others might merely lack computer literacy. Whatever the reason, people frequently make mistakes when learning new technology.

- **Hackers and the rise of "Hacktivism"**

Because they are either after the company's revenue or the sensitive data flowing via its networks, hackers frequently target healthcare organisations.

- **Adoption of cloud and mobile technology**

While cloud and mobile technology might make managing healthcare IT systems more convenient, they can also pose security threats. For instance, if a hacker were to take control of a doctor's mobile device or password, they might have access to a sizable payload of private data.

- **Outdated technology**

Hackers have previously gained access to a lot of older technologies. For instance, there are several hospitals that still use expensively outmoded technology. Outdated technology may be easier for an attacker to breach since it may have flaws that haven't been fixed by the most recent security updates.[18]

HEALTHCARE DATA INTEGRITY

Data must accurately reflect the source from which it was derived. It should be reliable, should have internal consistency, adhere to rules. The accuracy, internal quality, and reliability of data are frequently referred as data integrity. This means the enforcement of data integrity ensures the quality of data

Information that is reliable, relevant, and secure makes up data integrity. Security breaches and incorrect patient care might result from poor data integrity. Healthcare organizations can achieve high data integrity by enforcing data entry policies and a high level of accuracy.[19]

Necessity to maintain data Integrity in health care

Worldwide, the provision of high-quality healthcare depends on the accuracy and completeness of healthcare data.[20] Your biotech study will benefit from better data since you will have more resources at your disposal. However, it may have detrimental effects if the data you get is incomplete, inaccurately modified, or shared.[21] For instance, some adverse effects of data with poor integrity include:

1. Scams
2. Suspension of a product
3. Bans on imports or forced recalls
4. legal ramifications
5. decline in reputation
6. theft of data
7. faulty prescriptions

You can preserve data integrity with the aid of EHRs and blockchain technologies. While a primary goal of HER implementation is the reduction of medical errors, reports of new errors directly related to HER implementation that can compromise quality of care & patient safety have emerged.

Potential EHR risk	Impacting data integrity example
Data can be jumbled, deleted, changed, or placed in the wrong place by software defects.	An extra character may have been accidentally added to a laboratory value.
Software default settings	A patient's treatment for cancer was delayed by several years because a setting in her physician's EHR system defaulted to an old normal Pap test result instead of the more recent abnormal results[3]
Software internal programming error	Calculations like pounds to kilograms or Celsius to Fahrenheit
Transcription error	A baby died from a massive drug overdose as a result of a transcription error that occurred when a handwritten order was entered into the computer system. However, this medical error could have been prevented if automated alerts had been activated[4]
Inconsistencies between data fields	A structured data field may indicate that one pill should be taken twice a day, while the free-text filed says to take two pills in the morning and one pill in the evening
Copying and pasting information	Copying and pasting the same note accidentally for several rows may result in the same medication or condition repeated unnecessarily
Templates default values	Templates automatically fill in data elements based on other data entries before clinicians complete the actual data
Clinical environment may contribute to the occurrence of clinical decision support system error.	User distraction might cause data entry errors or inattentiveness to the information being presented by the decision support system

Ways to ensure Health Data Integrity

1. Attribution

All patient data should clearly and accurately demonstrate who observed and recorded it, when and in which patient it is about.

2. Legibility & Transparency

Patient records should be simple and clear to comprehend, and securely stored.

3. Contemporaneous

Recording patient notes & data in real time as observed & at the time

4. Performing Periodic Assessments or Audits to Ensure Accuracy

It is important to assess the accuracy of previous records and make sure that patient data integrity is being upheld properly; these concerns should not be left to chance. Further assessments should also be performed whenever new operational policies go into effect or when changes are made to software, systems & applications used.

5. Staying Up to date with changing Technology and Emerging trends

Practitioners and medical organisations can no longer afford to lag behind the times as new technologies, digital services, and innovations continue to influence and change the business. When it comes to patient data integrity, staying up to date with the latest technology or learning more about the most recent threats & security concerns is of paramount importance.

6. Ensure compliance

Health care providers must update their IT infrastructure with the latest cybersecurity measures.

7. Maintain the Right Digital Infrastructure

All data integrity in health care can be managed through interconnected applications. Linking these systems together it checks for data errors, gaps or duplications while processing patient information & every aspect and care can be streamlined through a coordinated digital infrastructure.

Protecting Healthcare Data

1. Using data encryption
2. Deploying anti-virus applications
3. Using system monitoring applications
4. Enabling multi-factor authentication
5. Deploying ransomware protection
6. Setting up employee training
7. Using technologies like[23]

Technology	Description	Features	Platforms	Open Issues
Electronic Health Records (EHR)	Digital systems that store and manage patient health information	Secure sharing of information between healthcare providers	Modernizing medicine, Greenway health, GE centricity, and NextGen healthcare	Interoperability and data exchange between different systems
Medical imaging	Digital methods for visualizing and analyzing medical images	Integration with Electronic Health Records (EHRs) and remote monitoring	Cloud-based platforms, Mobile devices (smartphones, tablets), and Wearables (smartwatches)	Data privacy and security, interoperability, and the integration with existing healthcare infrastructure
Artificial intelligence	Machine learning to enhance health outcomes	Predictive analysis and early detection of potential health issues	Health applications and portals for patients and healthcare providers	Regulation and standardization of AI in medical applications
Blockchain	Technology for secure health data management through distributed ledgers	Eliminates the need for a central authority to manage the data	Ethereum, hyperledger, and corda	The decentralized characteristic of blockchain technology presents challenges in regulating data privacy, which is a significant issue in the healthcare sector
Telemedicine	Remote medical treatment through technology	Patients are able to track their essential vital signs, including blood pressure, heart rate, and oxygen levels, through the use of wearable devices	Telemedicine services can be accessed by both healthcare providers and patients through web-based portals	Guarantee the preservation of data privacy and security
mHealth	Mobile technology used for health monitoring, diagnosis, and treatment	Remote monitoring and data management and analysis	iOS, Android, and Web-based	mHealth raises concerns about the privacy and security of sensitive health information stored on mobile devices and in the cloud
Wearable Devices	Health-tracking	Continuous	Apple WatchOS,	Limited battery life as

	devices worn on the body	monitoring of vital signs as well as health and fitness tracking	Google Wear OS, and FitbitOS	well as data privacy and security
Robotic process automation	Automation of routine tasks in healthcare	Real-time data processing and analysis	UiPath, Automation Anywhere, Blue Prism, WorkFusion	Data privacy and security concerns
Federated learning	Preserving data privacy and reducing communication costs	The model can be updated in real-time, as new data is collected from the devices	TensorFlow Federated (TFF), PySyft	The battery life of devices can be affected by the high energy consumption of federated learning

CONCLUSION

Health care data records are the most valuable data in healthcare. The best patient care techniques are employed with the protected health information. Practises need to regularly evaluate their systems, policies, and procedures in order to keep up with the rapidly evolving healthcare data landscape. The healthcare sector has a long way to go before it can be considered secure. We mainly reviewed the technologies that have been used recently like encryption and anonymization methods that have been used for data protection. Building a foundation of accurate and consistent data at the organization level is key along with reviewing of the digitization capabilities of healthcare professionals is necessary given the concerns of patient safety. Implementing and continually focusing on data integrity and security puts organizations in the best spot for success, while reducing health disparities among their patient populations.

REFERENCES

1. Al-Hanawi, M. K., Khan, S. A., & Al-Borie, H. M. Healthcare human resource development in Saudi Arabia: emerging challenges and opportunities—a critical review. *Public health reviews*, 2019; *40:* 1-16.
2. Burghard, C. Big data and analytics key to accountable care success. *IDC health insights*, 2012; *1:* 1-9.
3. Healthcare, I. T. Health Information at Risk: Successful Strategies for Healthcare Security and Privacy.
4. https://www.eccu.edu/blog/cybersecurity/the-importance-of -data-security-in-electronic-health-records/
5. https://www.medicaldirector.com/news/data-security/why-dataintegrity-is-critical-for-healthcare/
6. https://www.fda.gov/medicaldevices/digitalhealth.
7. Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., ... & Khan, R. A. Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters*, 2021*8*(3): 66-77.
8. Marques, I. C., & Ferreira, J. J. Digital transformation in the area of health: systematic review of 45 years of evolution. *Health and Technology*, 2020; *10*(3): 575-586.
9. South Tyneside, N. H. S. Foundation Trust. *Harnessing analytics for strategic planning, operational decision making and end-to-end improvements in patient care. IBM Smarter Planet brief*, 2013.
10. Mehta, N., Pandit, A., & Shukla, S. Transforming healthcare with big data analytics and artificial intelligence: A systematic mapping study. *Journal of biomedical informatics*, 2019; *100:* 103311.
11. CynergisTek, R. (2017). BREACH REPORT 2016: Protected Health Information (PHI).
12. Podesta, J., Pritzker, P., Moniz, E. J., Holdren, J., & Zients, J. Big data: seizing opportunities, preserving values (Executive Office of the President). *The White House, Washington, DC*, 2014.
13. Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. Big healthcare data: preserving security and privacy. *Journal of big data*, 2018; *5*(1): 1-18.
14. Chauhan, R., Kaur, H., & Chang, V. An optimized integrated framework of big data analytics managing security and privacy in healthcare data. *Wireless Personal Communications*, 2021; *117:* 87-108.
15. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. Healthcare data breaches: insights and implications. In *Healthcare.*, May, 2020; (8(2): 133). MDPI.
16. He, Y., Aliyu, A., Evans, M., & Luo, C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of medical Internet research*, 2021; *23*(4): e21747.
17. Roski, J., Bo-Linn, G. W., & Andrews, T. A. Creating value in health care through big data: opportunities and policy implications. *Health affairs*, 2014; *33*(7): 1115-1122.
18. https://www.fortinet.com/resources/cyberglossary/healthcare-data-security
19. https://gaine.com/blog/mdm/the-importance-of-data-integrity-in-healthcare/
20. Hersh, W. R. Medical informatics: improving health care through information. *Jama*, 2002; *288*(16): 1955-1958.
21. Sahama, T., Simpson, L., & Lane, B. Security and Privacy in eHealth: Is it possible?. In *2013 IEEE 15th International Conference on e-Health*

Networking, Applications and Services, 2013, October*; (Healthcom 2013);* 249-253. IEEE.
22. https://www.sciencedirect.com/science/article/pii/S2405959523000243?via%3Dihub
23. https://www.medicaldirector.com/news/data-security/why-data-integrity-is-critical-for-healthcare/