PROCEEDINGS OF
INTERNATIONAL CONFERENCE ON NEW TRENDS IN APPLIED SCIENCES
https://proceedings.icontas.org/
International Conference on New Trends in Applied Sciences (ICONTAS'23), Konya, December 1-3, 2023.

Human Error and Clinical Data Sharing

Yassine GOUNINE
Faculté des sciences de Rabat, ORCID: 0009-0002-1814-5817
Yassi.gou@gmail.com

Pr.Khalid MINAOUI
Faculté des sciences de Rabat
k.minaoui@um5r.ac.ma

Pr.Mohamed ElAROUSSI
Faculté des sciences de Rabat
mohamed.elaroussi4@gmail.com

ABSTRACT: Computer security issues have a widespread impact across all sectors and are increasingly influencing the healthcare industry. Since 2019, several reported attacks have been specifically aimed at exploiting vulnerabilities in medical network protocols like 'DICOM' and 'HL7,' as well as file formats, particularly those related to digital imaging and medical communications.
While numerous articles delve into subjects such as security and blockchain, they often disregard the significant role that human errors play in compromising security.
Human errors within hospital computer systems can lead to substantial implications for both patient care and data security. This article delves into the various forms of human errors that can occur within such systems and assesses their potential consequences on the overall effectiveness and security of healthcare information management. The study underscores the necessity of effective mitigation strategies to reduce the associated risks of these errors and enhance the dependability of hospital computer systems.

Key words: Data Sharing 1, Human Error 2, Dicom 3, Hl7 4, Clinical Data 5.

I. INTRODUCTION

The concept of clinical data sharing revolves around a continuous flow of patient information among authorized healthcare professionals and organizations. Through interconnected Electronic Health Record (EHR) systems and health information exchanges, data sharing enables practicing physicians to access crucial patient data across various contexts, transcending geographical barriers and streamlining care processes.

In the realm of healthcare and information management, the transparent exchange of clinical data assumes a central role in ensuring effective and efficient patient care. As technology continues to reshape the healthcare landscape, electronic systems and digital platforms have become fundamental tools for storing, retrieving, and disseminating critical medical information. However, amidst these technological advancements, the potential impact of human error on the security and accuracy of clinical data sharing cannot be underestimated. This article delves into the intricate relationship between human fallibility and the sharing of vital clinical data, exploring the types of errors that can arise and the implications they pose for patient outcomes and data integrity. By recognizing and understanding the challenges posed by human errors, we can devise strategies to mitigate risks and foster a safer and more dependable environment for clinical data sharing.

The consequences of human errors in clinical data sharing extend beyond immediate security concerns. Patient outcomes may be adversely affected due to compromised data accuracy, delayed access to critical information, or even unauthorized modifications of medical records.

Data integrity, a cornerstone of reliable healthcare information, is at risk when human errors occur. Inaccurate or incomplete data can lead to misinformed medical decisions, potential harm to patients, and challenges in maintaining trust within the healthcare ecosystem.

In the subsequent sections, we will delve into specific instances of human errors in clinical cybersecurity, examining their real-world impact and proposing proactive measures to mitigate risks. By understanding the intricate interplay between human actions and the security of clinical data sharing, we can pave the way for resilient solutions that prioritize patient welfare and data integrity in our digitally-driven healthcare landscape..

II. The most frequently occurring human mistakes informations in medical

Human errors can jeopardize the security of your business in myriad ways, but certain types of mistakes stand out due to their high frequency. Let's explore some of these notably common errors.

1. Undervalued Human Factors and their Impact on Healthcare Information Security

Human factors are consistently underestimated and neglected, constituting crucial elements that impact the information security hygiene of a clinic or health service. The challenge stems from the diversity of human errors that ultimately grant unauthorized access to sensitive information and other corporate assets, leading to significant data breaches and security lapses. Employee errors pose a risk within the clinic. In fact, the rise and severity of reported security issues in recent years suggest that organizations are more vulnerable than ever.

The principle of confidentiality includes individuals safeguarding others by restricting the sharing of personal or sensitive information without explicit authorization.
The third and final principle safeguards and promotes system functionality by ensuring that data is always available to authorized users. [14][16][12].

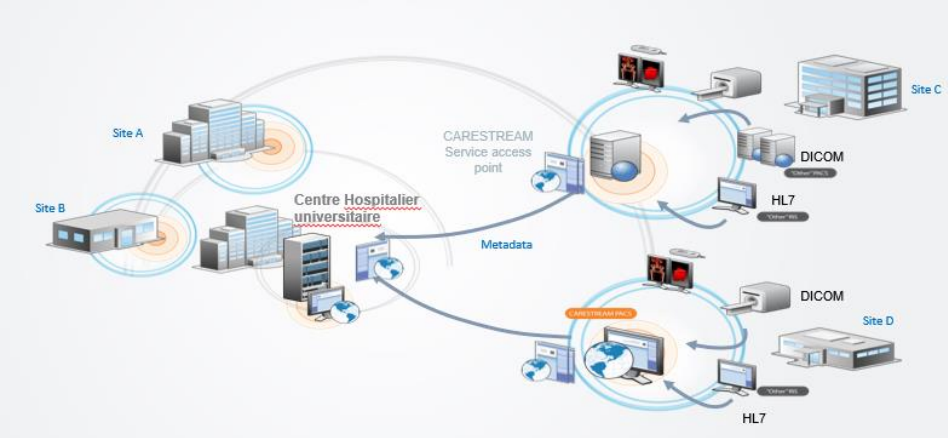

Fig. 1. Data synchronization between sites

2. Deficiency in Education and Awareness

User Awareness: Establishing a coherent organizational policy for employee training and education in cybersecurity best practices is of paramount importance. This training not only shields individuals from hackers but also bolsters the organization's overall protection. Equipping users with relevant knowledge is imperative to prevent them from becoming vulnerabilities. Research conducted by [organization name, if available] highlights the impact of security awareness on employee behavior and its role in influencing compliance with best practices. The lack of awareness and knowledge can lead to breaches of security policy [2][21].

User Habits: User habits play a central role. Education is pivotal in altering online behavior. Educating users on appropriate online conduct can thwart hackers from tracking their patterns. For instance, users should be educated not to comply with requests for account verification but, instead, to contact the organization directly to authenticate such requests. Discouraging practices like clicking hyperlinks is critical, as hackers can manipulate them for deceptive purposes. Users should be encouraged to directly input an organization's correct web address into the browser's address bar to evade phishing risks [2].

Password Management: Insufficient understanding of computer operations, particularly in areas such as password management, is underscored. Education remains paramount. User training should concentrate on conveying best practices in password credential management. Effective password management involves:

- Avoiding writing down passwords.
- Changing passwords every three months.
- Refraining from using personal words or phrases.
- Employing unique passwords for each account.
- Using passwords of a minimum of eight characters.
- Incorporating a combination of uppercase and lowercase letters, numbers, and special characters.
- Avoiding default passwords.

Users should acknowledge their vulnerability and comprehend that hackers invest time in tracking, monitoring, and exploiting vulnerabilities. Awareness of these practices can discourage hackers from breaching security [15][18].

3. Misconfiguration During System Setup

Configuring systems to mitigate vulnerabilities to cybersecurity threats marks the initial step in the security process. When setting up a device, establishing a solid foundation is paramount. If the device's initial setup lacks security, subsequent password usage or training efforts become less effective. [6].

4. Varied Scenarios of Hacking and IT Incidents: Impact on Protected Health Information.

Breaches classified as hacking or IT incidents (HITi) encompass various scenarios, such as instances where a foreign IP address accesses a Covered Entity's (CE) website containing a database of clients' Protected Health Information (PHI) or when an unidentified attacker linked to a foreign IP address attempts to breach the security mechanisms of a computer server owned by a former third-party administrator and Business Associate (BA). These breaches impact numerous individuals. The compromised servers contained PHI of CE participants, including names, addresses, social security numbers, clinical data, and healthcare provider information.

Another case involves breaches where file servers at entity offices are compromised, allowing unauthorized access and potentially exposing prescription records of thousands of individuals via electronic transmission, resulting in a HITi classification. The exposed PHI includes names, addresses, diagnostic codes, prescribed medication names, costs, and certain social security numbers. Instances involving computer malware detected within unencrypted billing software programs used by the CE are also categorized as HITi. In these situations, the entry point of the malware into the system remained unknown. Thousands of individuals were potentially impacted by this malware. The compromised PHI includes demographic, financial (claims data), and clinical information (diagnoses, medications, lab results, and other treatment details).

Lastly, cases where external and unidentified individuals breach database web servers containing electronic Protected Health Information (ePHI) for use as game servers are considered HITi. The breached ePHI on these database web servers includes names, birthdates, types of x-rays, and corresponding dates. [12][8].

III. Strategies under consideration to reduce human errors in the fields of radiology and data sharing

This discussion delves into the strategies currently under consideration aimed at mitigating human errors in the realms of radiology and data sharing. The exploration of these approaches underscores the importance of addressing potential pitfalls to enhance accuracy and efficiency in these critical domains.

1. Enhancing Traditional Workflow for Digital Transformation in the Field of Radiology

n the landscape of digital transformation in radiology, addressing human errors extends beyond the clinical aspects to encompass the intricacies of data interoperability, where standards like HL7 (Health Level Seven) and DICOM (Digital Imaging and Communications in Medicine) play a pivotal role. These standards are fundamental to the

seamless exchange and integration of medical information, ensuring consistency and accuracy throughout the radiological workflow.

The integration of HL7 facilitates the standardized exchange of clinical and administrative data among disparate healthcare systems, reducing the risk of errors associated with inconsistent data formats. Similarly, DICOM, specifically tailored for medical imaging, standardizes the communication of images and accompanying information across different devices and platforms. This integration not only enhances interoperability but also contributes significantly to reducing errors related to miscommunication or misinterpretation of medical images.

As radiology undergoes digital transformation, the synergy between HL7 and DICOM not only streamlines data sharing but also acts as a robust mechanism for addressing human errors associated with data integration and communication within the radiological ecosystem. In optimizing traditional workflows for digital transformation, the harmonious incorporation of these standards emerges as a linchpin, ensuring accuracy, consistency, and integrity in the exchange of medical information while mitigating potential errors arising from data incompatibility or misalignment. [9][3].

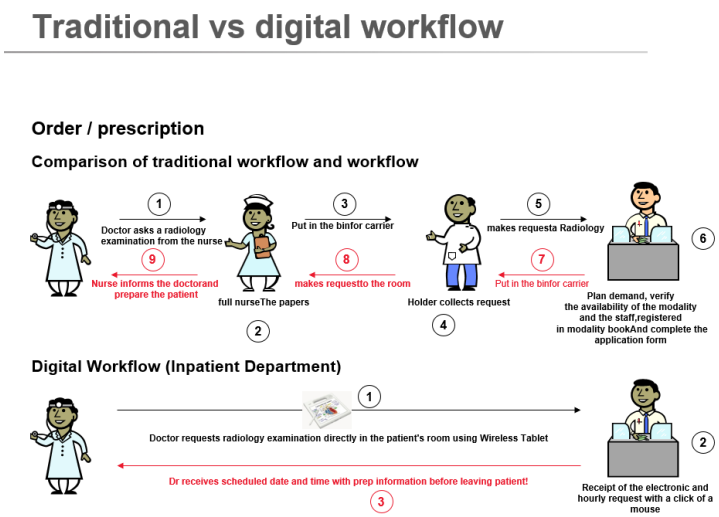

Fig. 2. Difference between traditional and digital IS workflow in a hospital department

2. DICOM Data Sharing

DICOM, or Digital Imaging and Communications in Medicine, is a standardized framework for the exchange of biomedical images and related information in the field of medical imaging. It provides a comprehensive set of specifications, including a data interchange protocol and digital image format, with the primary goal of ensuring seamless interoperability across various medical imaging systems.

DICOM addresses five main application areas, such as network image management and offline storage media management, offering a detailed specification for achieving automatic interoperability in biomedical imaging computer systems. This standard goes beyond defining physical connections and serves as a guide for the information structures and procedures governing data input and output in medical imaging systems [20].

In the context of sharing DICOM images, the potential for human errors becomes a critical consideration. Human errors in the sharing process can lead to a variety of issues, ranging from data inaccuracies to compromised patient care. These errors may manifest during the selection of images for sharing, the transfer process itself, or even in the interpretation of received images. Miscommunication, misinterpretation, or oversight during image sharing could result in incorrect diagnoses or treatment plans. Therefore, it is imperative to implement robust protocols, training, and technological solutions to minimize the risk of human errors in the sharing of DICOM images, ensuring the integrity and accuracy of medical information exchanged among healthcare professionals.

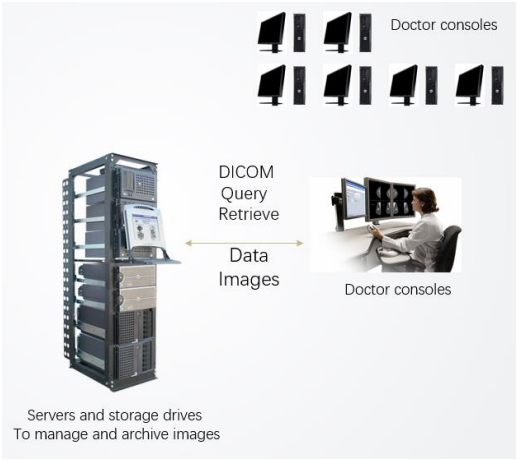

Fig. 3. Sharing of radiological images using the DICOM protocol

3. HL7 Data Sharing

HL7, or Health Level Seven, is a set of international standards for the exchange, integration, sharing, and retrieval of electronic health information. It provides a framework for the seamless communication and interoperability of healthcare systems and applications. HL7 standards define the format and structure of messages, ensuring that health information is accurately and consistently exchanged between different healthcare IT systems [1].

Despite the security measures provided by HL7 standards in the electronic exchange of medical information, human errors continue to pose a challenge. While HL7 establishes rigorous protocols for the secure transmission of health data, persistent risks associated with human errors can compromise the integrity and confidentiality of this information. Trust in these systems relies not only on the robustness of the protocols set by HL7 but also on the vigilance and compliance of users with security procedures. It remains essential to raise awareness and provide training for healthcare professionals and stakeholders involved in the use of HL7 standards to minimize the risks of human errors and enhance the overall security of electronic medical information sharing.

Fig. 4. Sharing patient information using the HL7 protocol

4. Vulnerability of DICOM and HL7 Protocols Due to User Actions

The susceptibility of DICOM and HL7 protocols is a significant concern, largely stemming from user actions in healthcare environments. Despite robust security measures incorporated into these protocols, the risk landscape is heavily influenced by user behavior. Human errors, such as misconfigurations, insufficient training, and lapses in adherence to security protocols, can expose vulnerabilities in both DICOM and HL7 frameworks.

Users, comprising healthcare professionals and system administrators, play a crucial role in upholding the integrity and confidentiality of medical information exchanged through these protocols. Given that these standards rely on responsible and knowledgeable usage by individuals, there is an urgent need to prioritize continuous training, awareness initiatives, and strict adherence to security best practices to mitigate potential risks arising from user actions.

The intersection of advanced protocols with human factors underscores the vital necessity for a comprehensive cybersecurity approach in healthcare settings, emphasizing both technological resilience and user-centric security practices. [11][4].

IV. Cybersecurity with Integrating the Human Factor

Despite the thorough examination of cybersecurity measures within healthcare IT, the article inadvertently overlooks a critical factor that significantly influences the effectiveness of these strategies – human error. While the content adeptly delves into the intricacies of physical and technical layers of security, it fails to explicitly address the considerable impact of human actions on the overall cybersecurity landscape.

The emphasis on standards, regulations, and best practices rightly recognizes the importance of a structured approach, yet the article falls short in underscoring the susceptibility of these measures to errors stemming from human factors. Whether it be misconfigurations, lapses in compliance with security protocols, or inadequate training, human errors remain a persistent challenge that can expose vulnerabilities in even the most robust cybersecurity frameworks.

Integrating a discussion on mitigating human errors, perhaps through enhanced training programs and user awareness initiatives, would fortify the article's comprehensive examination of healthcare IT cybersecurity, ensuring a more holistic and resilient defense against evolving threats. [10][17][7][19].

V. The Integrity of Shared Medical Data and Human Errors

Critiquing articles on the integrity of shared medical data and human errors reveals a nuanced landscape where the balance between technological advancements and human fallibility is carefully navigated. While many articles rightfully emphasize the critical importance of securing medical data through advanced protocols, encryption, and access controls, there is often a tendency to oversimplify the role of human errors in compromising data integrity.

Some articles tend to categorize human errors as mere lapses in judgment or awareness without delving into the complex contextual factors that contribute to such mistakes. Negligence is portrayed as a standalone issue rather than a systemic challenge influenced by factors such as the intensity of healthcare workflows, time constraints, and the evolving nature of cyber threats.

Moreover, the critique extends to the limited exploration of the socio-cultural aspects within healthcare organizations. Organizational culture, leadership commitment to cybersecurity, and the availability of resources for continuous education and training play pivotal roles in shaping how effectively healthcare professionals adhere to security protocols. Articles often fall short in providing a holistic understanding of the organizational dynamics that contribute to or mitigate human errors.

Furthermore, there is a notable gap in some articles regarding the long-term impact of human errors on patient outcomes and data integrity. While acknowledging the occurrence of errors, there is a lack of in-depth analysis of the consequences of compromised medical data for patient safety and trust in healthcare systems.

In conclusion, while the emphasis on technological safeguards is crucial, a more nuanced and holistic approach is warranted in articles discussing the integrity of shared medical data and human errors. Addressing the systemic issues contributing to negligence, considering the organizational context, and exploring the broader implications of human errors are essential for developing comprehensive strategies that truly enhance the security and integrity of shared medical information. [13].

VI. Conclusion

The prevalence of computer security issues has expanded across all sectors, notably impacting the healthcare industry. there has been a surge in targeted attacks exploiting vulnerabilities in medical network protocols such as "DICOM" and "HL7," as well as file formats related to digital imaging and medical communications.

Despite extensive discussions on security and blockchain, a critical aspect often overlooked is the substantial role played by human errors in compromising security . This is particularly relevant within hospital computer systems, where such errors can have significant repercussions on both patient care and data security.

This article has explored various forms of human errors inherent in these systems, evaluating their potential consequences on the overall effectiveness and security of healthcare information management. The study underscores the imperative need for effective mitigation strategies to reduce associated risks, thereby enhancing the reliability of hospital computer systems. Recognizing and addressing human errors becomes paramount in fortifying the security of healthcare information systems, ultimately contributing to the safeguarding of patient data and the overall integrity of healthcare services.
As we navigate the convergence of DICOM, HL7, and cybersecurity in clinical data sharing, it becomes evident that addressing human errors is integral to achieving a truly secure and interoperable healthcare ecosystem. Beyond technological advancements, a comprehensive approach must include ongoing education and training for healthcare professionals, emphasizing the critical role they play in maintaining the security and integrity of clinical data exchanges. By acknowledging and mitigating the impact of human errors, the healthcare industry can foster a resilient environment that upholds the principles of patient privacy, data security, and seamless interoperability.

REFERENCES

[1] Khaled Shaalan Adi A AlQudah, Mostafa Al-Emran. Medical data integration using hl7 standards for patient's early identification. Public Library of Science one, 2021.

[2] M. Alshaikh and B Adamson. toward a model for improving employees' security behavior. Personal and Ubiquitous Computing, 2021.

[3] Miroslav Koncar Bojan Blazona. Hl7 and dicom based integration of radiology departments with healthcare enterprise information systems. Int J Med Inform, 2007.

[4] Stephen A. Clark. Secure integration of information systems in radiol- ogy. Murray State's Digital Commons, 2018.

[5] Shakyawar S.K. Sharma-M. et al. Dash, S. Big data in healthcare: management, analysis and future prospect. J Big Data.

[6] Lara Khansa. Divakaran Liginla, Inkook Sim. How significant is human error as a cause of privacy breaches? an empirical study and a framework for error management.

[7] Esmeralda Kadena Dr. Marsidi Gupi. Human factors in cybersecurity: Risks and impacts. Security Sience Journal, 2021.

[8] Duffy V.G. Lee, B.C. Impact of healthcare information technology systems on patient safety. Lecture Notes in Computer Science.

[9] Thusitha Mabotuwana and Christopher S. Hall. Using hl7 and dicom to improve operational workflow efficiency in radiology. 2017.

[10] Klaus Kleber Marco Eichelberg and Marc Kammerer. Cybersecurity in pacs and medical imaging: an overview. Journal of digital imaging, 2020.

[11] Klaus Kleber Marc Kammerer MD Marco Eichelberg, PhD. Cyberse- curity challenges for pacs and medical imaging. Academic Radiology, 2020.

[12] Helge Janicke Cunjin Luo Ryna Yevseyeva Leandros A. Maglaras Mark Evans, Ying He. Employee perspective on information security related human error in healthcare: Proactive use of is-chec in question- naire form.

[13] T.Jamal Ansari A.Kumar Pandey M.Ahmad A.Agrawal R.Kumar R.Ahmad Khan M.Zarour, M.Alenezi. Ensuring data integrity of healthcare information in the era of digital health. National Library Of Medicine, 2021.

[14] Tabisa Ncubukezi. Human errors: A cybersecurity concern and the weakest link to small businesses. Proceedings of the 17th International Conference on Information Warfare and Security, pages 2–5, 2022.

[15] School of Information and Software Engineering. Human factor a critical weak point in the information security of an organization's internet of things. Proceedings of the 17th International Conference on Information Warfare and Security, 2021.

[16] J Anaesthesiol Clin Pharmacol. Human errors and their prevention in healthcare. Lecture Notes in Computer Science, 2021.

[17] Callari T.C. Tedeschi A Pollini, A. Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn Tech Work, 2021.

[18] Anshul Rajendra Kumar Dwivedi Shivam Pandey, Vanshika. A secure design of healthcare system with blockchain and internet of things (iot).

[19] William J. Triplett. Addressing human factors in cybersecurity leader- ship. Cybersecurity and Privacy, 2022.

[20] MD MS Steven C. Horii MD Fred W. Prior PhD W. Dean Bidgood, Jr. and Donald E. Van Syckle. Understanding and using dicom, the data interchange standard for biomedical imaging. Journal of the American Medical Informatics Association, 1997.

[21]Green K. Johnson C. Cooper J. Wallace, S. and C. Gilstrap. An extended toe framework for cybersecurity adoption decisions. Communications of the Association for Information Systems, page 47, 2020