



Analysis of Electronic Medical Record Security Risk Factors During the Implementation of a New Hospital Information System at Hospital X

Adinda Salsabila, Irda Sari *

Departement of Medical Records and Health Information, Faculty of Health, Politeknik Piki Ganesha, Indonesia

*Email (corresponding author): irdasari13@gmail.com

Abstract. *The implementation of a new Hospital Management Information System (SIMRS) integrated with Electronic Medical Records (EMRs) can improve healthcare services, but it may also introduce risks to patient-data security. This study aimed to analyze EMR security risk factors during the implementation of a new SIMRS at Hospital X. A descriptive qualitative approach was used through interviews and direct observation involving five purposively selected informants: two registration officers, two SIMRS security officers, and one SIMRS information technology staff member. The findings identified risks related to availability, confidentiality, physical and environmental security, human factors, and cybersecurity. A system downtime lasting more than one hour occurred during feature addition, network devices experienced technical disruptions, and failure to log out created a risk of unauthorized account use. Existing controls identified within the study scope included individual usernames and passwords, role-based access restrictions, restricted database access for the IT team, CCTV-supported physical protection, and a firewall. Controls such as automatic logout, two-factor authentication, backup, and encryption were not identified in the available study observations and should not be interpreted as absent across the entire hospital. The study concludes that several controls were identified, while residual risks require continued management and technical verification. Periodic security evaluation, stronger user compliance and training, improved infrastructure reliability, clearer access-control procedures, and regular cybersecurity maintenance are recommended to protect the confidentiality, integrity, and availability of EMR data. By supporting secure, reliable, and resilient digital health services, these improvements are relevant to SDG 3 (Good Health and Well-Being) and SDG 9 (Industry, Innovation and Infrastructure).*

Keywords: *Electronic Medical Records; Information Security; Risk Factors; Hospital Information System; Cybersecurity*

1. Introduction

Advances in health information technology have accelerated the digitalization of hospital services. At Hospital X, a new Hospital Management Information System (SIMRS) has been implemented and integrated with Electronic Medical Records (EMRs). The implementation is intended to improve service quality while supporting the security, integrity, and availability of digitally integrated medical records (Putri & Mulyanti, 2023; Simanullang et al., 2026). Electronic Medical Records contain sensitive patient information, including identity data, diagnoses, examination results, medical procedures, and treatment histories. Because these data are confidential, healthcare organizations must protect their confidentiality, integrity, and availability. Inadequate security may result in data loss,

unauthorized disclosure, or disruption of clinical services (Kementerian Kesehatan Republik Indonesia, 2022).

The implementation of a new SIMRS can improve workflow efficiency, but the early implementation phase may also introduce security risks. The source study identified concerns such as data-entry errors, insufficient attention to account security, service delays caused by limited familiarity with new system features, network disruption, server failure, and system-access problems. These conditions may affect not only information security but also hospital operational continuity. Previous studies have reported comparable challenges. Agustina We'e et al. (2023) identified security and confidentiality issues associated with staff negligence and technical problems, while Sari and Syahputra (2024) emphasized that successful EMR implementation depends on human-resource readiness, management support, training, technological infrastructure, and stronger information-security management. International evidence similarly shows that hospital information security depends on a combination of technical safeguards, organizational governance, access control, workforce behavior, and continuity planning (Argaw et al., 2020; Fernández-Alemán et al., 2013; Jalali & Kaiser, 2018; Mehraeen et al., 2016; Park et al., 2010; Wasserman & Wasserman, 2022). Other literature cited in the source manuscript also highlights access control, cybersecurity, and risk management as important components of EMR protection (Apriliansyah, 2025; Ikawati et al., 2025; Nugraheni et al., 2023).

However, studies specifically examining EMR security risks during the early implementation of a new SIMRS remain limited. Much of the existing literature focuses on systems that have already been established, whereas the transition period may create a distinctive combination of technological, behavioral, physical, organizational, and resource-related vulnerabilities. This constitutes the research gap addressed by the present study. Preliminary observations conducted during field practice at Hospital X indicated potential risks arising from human behavior, technology, and physical and environmental security. Human factors were related to compliance with information-security procedures; technological factors included system and network disruption; and physical and environmental factors concerned protection of the infrastructure supporting the SIMRS. These factors may affect the confidentiality, integrity, and availability of EMR data.

Therefore, this study aimed to analyze the security risk factors affecting Electronic Medical Records during the implementation of a new SIMRS at Hospital X. The study also applied the 5M framework – Man, Method, Machine, Material, and Money – to organize the identified risks and their potential control measures. Strengthening secure and resilient digital health infrastructure can support continuity and quality of healthcare services and the protection of electronic patient information; accordingly, this study is relevant to SDG 3 (Good Health and Well-Being) and SDG 9 (Industry, Innovation and Infrastructure).

2. Methods

This study used a descriptive qualitative design to obtain an in-depth understanding of EMR security risk factors during the implementation of a new SIMRS at Hospital X. The descriptive approach was used to portray field conditions based on the experiences and perspectives of informants (Sugiyono, 2022). The study was conducted at Hospital X in Bandung City during field practice. The research focused on factors that could create risks to EMR security, including human resources, technology, organization, user-access management, and information-security policies associated with the new SIMRS.

Data were collected through in-depth interviews and direct observation. Interviews were conducted with personnel directly involved in the implementation and security of the new SIMRS and addressed system availability, user access, infrastructure, human behavior, and cybersecurity practices. Observation focused on system use, login practices, infrastructure conditions, access restrictions, and security controls encountered during routine service activities. The available study documentation did not specify interview duration, audio-recording or verbatim-transcription procedures, or the formal development and validation process for the interview guide and observation checklist; these procedural details should be verified by the authors before final submission rather than inferred. Five informants were selected using purposive sampling because of their knowledge, competence, and direct involvement in EMR use or SIMRS security management. They consisted of two registration officers, two SIMRS security officers, and one SIMRS information technology staff member.

Data were analyzed descriptively by identifying recurrent security findings and grouping them into five security components: availability, confidentiality, physical and environmental security, human factors, and cybersecurity. The findings were then organized using the 5M approach consisting of Man, Method, Machine, Material, and Money. Interview information and direct observations were compared where both sources addressed the same issue, providing a limited form of source triangulation. Formal member checking, independent peer coding, and a documented audit trail were not reported in the available study materials and therefore are not claimed in this manuscript. Ethical considerations. The study involved interviews and direct observation of hospital personnel. The available manuscript materials do not report the name of an ethics committee, an approval or exemption number, or the specific informed-consent procedure. To avoid fabricating information, these items are not inferred in this revision. The authors should insert the applicable institutional ethical approval/exemption and confirm that participation was voluntary, informant identities were kept confidential, and study reporting did not disclose personally identifiable information before final submission.

3. Results and Discussion

3.1. Identification of EMR Security Risk Factors

Interviews and observations identified several security risks during the implementation of the new SIMRS. As summarized in Table 1, each finding is presented according to what was directly observed or reported by informants within the study scope; the table does not represent a hospital-wide technical security audit.

Table 1. Matrix of Identified Security Risk Factors During New SIMRS Implementation

Security Component	Analysis Variable	Finding at Hospital X	Potential Risk
Availability	SIMRS application stability	The SIMRS experienced downtime for more than one hour during feature addition.	Patient services and workflows may be disrupted when the application is unavailable.

Confidentiality	User access control	Each staff member has an individual username and password.	Account misuse may occur if a user leaves a device without logging out.
Physical and environmental security	Server room and network hardware security	The server room is restricted and monitored by CCTV; network devices such as hubs/routers have experienced disruptions.	SIMRS connectivity may fail because of power/network disruption; unauthorized physical access remains a potential risk if controls fail.
Human factors	User privileges and database authority	Each user has a specific account and role; direct database access is restricted to the IT team.	Unauthorized access may occur through user negligence, particularly failure to log out.
Cybersecurity	Network security and external-threat protection	Within interviews and routine observation, no external data-leakage incident was reported or identified; a firewall was reported to be in use. Incident logs and technical security testing were not reviewed.	External threats may remain undetected without incident-log review, vulnerability assessment, penetration testing, and periodic firewall/network-security maintenance.

Note. Findings reflect interview reports and routine field observations. Statements that a control was 'not identified' indicate only that it was not documented within this limited qualitative study and do not establish hospital-wide absence.

The findings demonstrate that EMR security risks at Hospital X were multidimensional. Although several controls were already in place, the new system remained exposed to risks affecting service availability, confidentiality, physical infrastructure, user behavior, and network security.

3.2. Availability and System Continuity

The SIMRS had experienced downtime lasting more than one hour during the addition of a new feature. An IT informant explained that the update was performed during operational hours and temporarily disrupted patient registration and record retrieval. Direct observation indicated that during downtime, staff could not perform registration or access EMR data. This finding shows that system stability is central to maintaining service continuity and information availability. Preventive maintenance, pre-deployment testing, planned update windows, and recovery mechanisms are therefore important controls.

3.3. Confidentiality and User Access Control

Hospital X had implemented individual usernames and passwords for users, indicating an established basic access-control mechanism. However, users who fail to log out after using the SIMRS may leave authenticated sessions accessible to unauthorized persons.

This behavioral risk can undermine otherwise appropriate technical controls. Continuous education, supervision, and stronger session-management policies are therefore required.

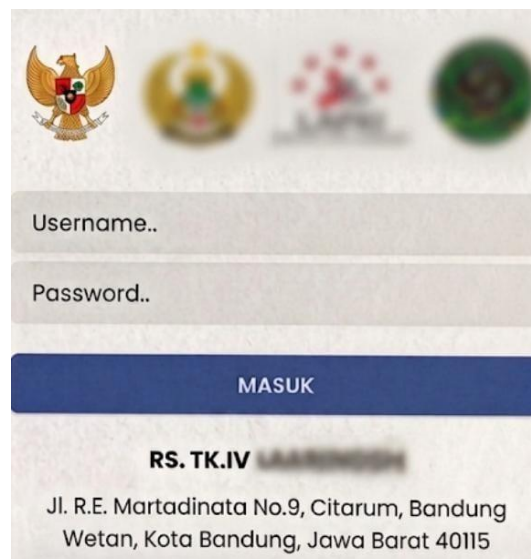


Figure 1. SIMRS login page at Hospital X

As shown in Figure 1, the observed SIMRS login interface used username-and-password authentication as an initial security layer before users could access medical-record data. An additional security feature such as two-factor authentication was not identified during the observation period. This wording indicates a limitation of what was observed, rather than establishing that two-factor authentication was absent across all hospital systems. Stronger authentication may be considered where appropriate to the hospital risk profile (Fernández-Alemán et al., 2013; Liang et al., 2024).

3.4. Physical and Environmental Security

The server infrastructure was reported to be placed in a restricted area and supported by CCTV monitoring. These controls reduce the likelihood of unrestricted physical access. Nevertheless, network devices such as hubs and routers had experienced technical disruption, and power outages were also identified as a potential cause of SIMRS interruption. Periodic infrastructure maintenance and backup power are therefore relevant to system continuity.

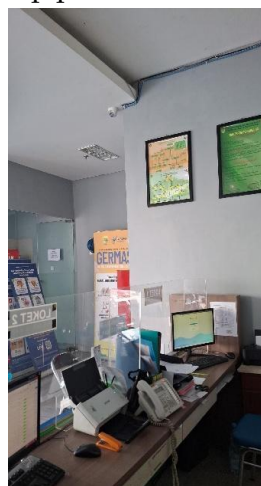


Figure 2. Area identified in the source manuscript as the server room equipped with CCTV at Hospital X

Figure 2 is reproduced from the source manuscript and depicts the area identified there as the server-room environment. According to informant/source descriptions, access to this area was restricted and CCTV monitoring was used. Because the image itself cannot verify all physical-security controls, these features are treated as reported information rather than a complete physical-security audit. Complementary controls such as electronic access restriction, access logging, and periodic review may further strengthen physical protection (Mehraeen et al., 2016; Park et al., 2010).

3.5. Human Factors and Cybersecurity

Role-based access restrictions were already applied, and direct database access was limited to the IT team. Nevertheless, failure to log out remained a recurring human-factor concern. This indicates that technical authorization must be reinforced by user discipline and information-security awareness. Periodic training and compliance monitoring are therefore important components of risk reduction.

For cybersecurity, a firewall was reported to be in use, and no external data-leakage incident was reported by informants or identified during routine observation at the time of the study. This finding must not be interpreted as evidence that the system was adequately protected. The study did not review incident logs and did not include vulnerability scanning, penetration testing, digital-forensic analysis, or other technical verification capable of detecting hidden or unreported compromise. Consequently, cybersecurity effectiveness cannot be established from the present qualitative evidence alone. Regular firewall updates, network monitoring, access-log review, vulnerability assessment, and periodic security testing are therefore recommended (Argaw et al., 2020; Choi et al., 2023; Neprash et al., 2022; Wasserman & Wasserman, 2022; Yeo & Banfield, 2022).

3.6. Security Risk Analysis Using the 5M Approach

The interview and observation findings were further grouped using the 5M framework. Table 2 summarizes the source manuscript's risk interpretation and proposed controls.

Table 2. EMR Security Risk Analysis Using the 5M Approach

5M Aspect	Research Finding	Potential Risk	Proposed Control
Man	Staff may fail to log out.	Unauthorized account use.	Periodic information-security education and training.
Method	An automatic logout/session-lock mechanism was not identified during the observation period.	Unauthorized access when a device is left logged in.	Implement auto-logout policy and strengthen SOPs.
Machine	Downtime, network disruption, and power interruption.	Patient services are disrupted and data become difficult to access.	Periodic maintenance and backup power/UPS.

Material	Backup and encryption controls were not identified in the available interviews/observations; their hospital-wide status was not technically verified.	Potential loss or leakage of patient data.	Formally assess current backup and encryption arrangements and strengthen them where gaps are confirmed.
Money	No direct financial or budget data were collected. Resource constraints are therefore an analytical consideration, not an empirical finding.	If resources are insufficient, infrastructure renewal, maintenance, and training could be delayed.	Conduct a formal resource and budget needs assessment before determining security investment priorities.

Note. The Money component is an analytical inference because no direct budget or financial data were collected. 'Not identified' for Method and Material indicates limitations of the study evidence, not confirmed hospital-wide absence.

The Man component highlights user behavior as a central risk. Individual accounts and role-based permissions had been implemented, but failure to log out could still expose patient data to unauthorized access. Human-factor research in healthcare indicates that security outcomes depend on user behavior as well as technical safeguards, supporting the need for repeated awareness and compliance interventions (Yeo & Banfield, 2022). The Method component reflects that an automatic session-locking mechanism was not identified during the observation period; this is not equivalent to confirming its absence across the entire hospital. Stronger standard operating procedures and appropriately configured session controls should therefore be considered after technical verification.

The Machine component includes application downtime, network-device disruption, and power interruption. These findings indicate that information security depends not only on preventing unauthorized access but also on maintaining reliable infrastructure. Evidence from hospital downtime studies shows that EHR unavailability can disrupt clinical processes, information access, and patient-care continuity (Chen et al., 2017; Fang et al., 2025; Larsen et al., 2018; Larsen et al., 2019). The Material component concerns EMR data as a confidential information asset. Importantly, the available study evidence did not identify a backup or encryption mechanism, but no technical audit was performed to establish whether such controls were absent. The appropriate recommendation is therefore to formally assess existing backup, recovery, and encryption arrangements and strengthen them where gaps are confirmed. Access-control and auditing research likewise supports layered authorization and accountable access to electronic health information (Liang et al., 2024; Ullah et al., 2024).

The Money component is retained only as an analytical consideration. No direct financial data, budget documents, or explicit measurements of funding constraints were collected. Therefore, infrastructure disruptions and maintenance needs should not be presented as proof of inadequate budget allocation. Instead, they indicate areas that may require a formal resource-needs assessment. Any recommendation concerning additional

investment should follow documented assessment of infrastructure condition, security priorities, maintenance requirements, staff competencies, and existing budget capacity.

Overall, the five 5M components are interrelated, but the strength of evidence differs across components. Human behavior, downtime, access practices, and selected infrastructure conditions were identified through interviews and observations, whereas hospital-wide control status and budget adequacy were not established. This distinction is important because cybersecurity risk can increase as health information becomes more interconnected and because ransomware and other cyber incidents can interrupt care delivery (Choi et al., 2023; Neprash et al., 2022). Consequently, EMR security during new SIMRS implementation requires integrated governance, technical validation, continuity planning, and workforce engagement rather than isolated technical interventions.

This study was based on five purposively selected informants from registration and SIMRS/security/information-technology roles. The sample did not include clinicians, medical-record personnel outside the selected roles, hospital management, or other end users. Therefore, the findings describe risks and controls identified within the participating roles and observation scope and should not be generalized to the entire hospital workforce or to the hospital's overall security environment. In addition, the study did not include incident-log analysis, vulnerability assessment, penetration testing, formal configuration review, or financial-data analysis. Controls not identified during interviews or routine observation—such as automatic logout, two-factor authentication, backup, or encryption—cannot be concluded to be absent hospital-wide. Finally, detailed documentation of interview duration, recording/transcription, formal instrument development, member checking, peer coding, audit trail, and ethical approval/exemption was not available in the manuscript materials and should be completed or verified by the authors before final submission.

Conclusions

This study achieved its objective by identifying EMR security risk factors observed or reported during the early implementation of a new SIMRS at Hospital X. Within the limited qualitative scope, identified controls included individual user accounts, role-based access restrictions, restricted database authority, reported CCTV-supported physical security, and firewall use. Residual risks involved system downtime affecting availability, potential account misuse when users failed to log out, network and power-related disruptions, human-factor vulnerabilities, and cybersecurity threats that could not be technically ruled out by the present study.

Using the 5M approach, the evidence was organized into Man, Method, Machine, Material, and Money while distinguishing empirical findings from analytical inference. Hospital X is advised to strengthen staff training and access-control discipline, verify and improve session-management controls, maintain network and power infrastructure, formally assess backup and encryption arrangements, review access and incident logs, and conduct periodic vulnerability assessment and other appropriate technical security testing. Resource recommendations should be based on a formal needs and budget assessment rather than assumed constraints. These measures can strengthen the confidentiality, integrity, and availability of patient information and support secure, reliable digital health services aligned with SDG 3 and SDG 9.

Funding

The authors report that funding information was not available in the submitted manuscript materials and should be confirmed before final publication.

Acknowledgments

The authors may acknowledge Hospital X and participating informants where appropriate and permitted by institutional confidentiality requirements.

Conflicts of Interest

The authors should confirm the journal-required conflict-of-interest declaration before final publication.

References

- Agustina We'e, H., Nugroho, R. H., & Siswatibudi, H. (2023). Evaluasi aspek keamanan dan kerahasiaan rekam medis elektronik di Rumah Sakit X Panti Nugroho. *Jurnal Permata Indonesia*, 14(2), 72–81.
- Apriliansyah, U. (2025). Evaluasi manajemen risiko terkait keamanan data rekam medis elektronik di Rumah Sakit X Mata Undaan Surabaya. *Jurnal Manajemen Kesehatan Yayasan RS Dr. Soetomo*.
- Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20(1), 146. <https://doi.org/10.1186/s12911-020-01161-7>
- Chen, J., Wang, Y., & Magrabi, F. (2017). Downtime in digital hospitals: An analysis of patterns and causes over 33 months. *Studies in Health Technology and Informatics*, 239, 14–20.
- Choi, S. J., Chen, M., & Tan, X. (2023). Assessing the impact of health information exchange on hospital data breach risk. *International Journal of Medical Informatics*, 177, 105149. <https://doi.org/10.1016/j.ijmedinf.2023.105149>
- Fang, Q., Liang, J., Xiang, P., Zhao, M., He, Y., Zhang, Z., Wan, H., Hu, Y., Wang, T., & Lei, J. (2025). Electronic health record downtime events of a hospital: A retrospective analysis from adverse event reports. *Applied Clinical Informatics*, 16(5), 1419–1429. <https://doi.org/10.1055/a-2701-5819>
- Fernández-Alemán, J. L., Carrión Señor, I., Oliver Lozoya, P. A., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), 541–562. <https://doi.org/10.1016/j.jbi.2012.12.003>
- Ikawati, F. R., Ansyori, A., & Permatasari, D. A. S. (2025). Literature review: Analisis keamanan data rekam medis elektronik di fasilitas kesehatan. *Jurnal Manajemen Informasi Kesehatan*.
- Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, 20(5), e10059. <https://doi.org/10.2196/10059>
- Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Kementerian Kesehatan RI.
- Larsen, E., Fong, A., Wernz, C., & Ratwani, R. M. (2018). Implications of electronic health record downtime: An analysis of patient safety event reports. *Journal of the American*

- Medical Informatics Association, 25(2), 187–191.
<https://doi.org/10.1093/jamia/ocx057>
- Larsen, E., Hoffman, D., Rivera, C., & Kleiner, B. M. (2019). Continuing patient care during electronic health record downtime. *Applied Clinical Informatics*, 10(3), 495–504.
<https://doi.org/10.1055/s-0039-1692678>
- Liang, X., Liu, Y., & Ning, J. (2024). An access control scheme with privacy-preserving authentication and flexible revocation for smart healthcare. *IEEE Journal of Biomedical and Health Informatics*, 28(6), 3269–3278. <https://doi.org/10.1109/JBHI.2024.3391218>
- Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in hospitals: The application of security safeguards. *Acta Informatica Medica*, 24(1), 47–50.
<https://doi.org/10.5455/aim.2016.24.47-50>
- Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum*, 3(12), e224873. <https://doi.org/10.1001/jamahealthforum.2022.4873>
- Nugraheni, F., Prasetyo, A., & Handayani, R. (2023). Evaluasi keamanan siber pada sistem informasi manajemen rumah sakit. *Jurnal Informatika Kesehatan*, 10(2), 78–86.
- Park, W.-S., Seo, S.-W., Son, S.-S., Lee, M.-J., Kim, S.-H., Choi, E.-M., Bang, J.-E., Kim, Y.-E., & Kim, O.-N. (2010). Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. *Healthcare Informatics Research*, 16(2), 89–99.
<https://doi.org/10.4258/hir.2010.16.2.89>
- Putri, R. D., & Mulyanti, D. (2023). Tantangan SIMRS dalam penerapan rekam medis elektronik berdasarkan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022: Literature review. *Jurnal Medika Nusantara*, 1(1), 18–28.
- Sari, I., & Syahputra, A. K. (2024). Analisis implementasi rekam medis elektronik di Rumah Sakit Radjak Hospital Group. *EDU RMIK: Jurnal Edukasi Rekam Medis dan Informasi Kesehatan*, 4(2), 179–190.
- Simanullang, R., et al. (2026). Implementasi Sistem Informasi Manajemen Rumah Sakit dalam mendukung keamanan rekam medis elektronik di rumah sakit. *Jurnal Manajemen Informasi Kesehatan Indonesia*.
- Sugiyono. (2022). *Metode penelitian kuantitatif, kualitatif, dan R&D* (2nd ed.). Alfabeta.
- Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., Pathan, M. S., & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, 10, e34407. <https://doi.org/10.1016/j.heliyon.2024.e34407>
- Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, 4, 862221.
<https://doi.org/10.3389/fdgth.2022.862221>
- Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management*, 19(Spring), 1i.

CC BY-SA 4.0 (Attribution-ShareAlike 4.0 International).

This license allows users to share and adapt an article, even commercially, as long as appropriate credit is given and the distribution of derivative works is under the same license as the original. That is, this license lets others copy, distribute, modify and reproduce the Article, provided the original source and Authors are credited under the same license as the original.

