Saudi Journal of Medicine and Public Health

https://saudijmph.com/index.php/pub

https://doi.org/10.64483/202412337

The Human Firewall Imperative: A Narrative Review of Interprofessional Collaboration for Cybersecurity in Patient-Centric Digital Healthcare

Hamad Hamdan Saad Al-Qahtani [(1)] , Salah Mohammed H Alshhry , Ruba Abdullah A Hadadi [(1)] , Ebtehal Turqi Alotaibi [(1)] , Ahmed Ali Abuazzam [(2)] , Sultan Shami Ali Othaibi [(3)] , Hadi Rasheed Mohammed Kumait [(3)] , Abdullah Ali Abdullah Dighriri [(4)] , Shaker Nayyaf Bader Alotaibi [(5)] , Alabbas Ibrahim Hussian Althurwi [(6)] , Atiah Abulrazaq Abdullah Mohmmed [(7)] , Norah Ghalib Alrowaili [(8)] , Baha Haweidi Aldosari [(9)]

(1) Erada Hospital For Mental Health In Al-Kharj,Ministry of Health, Saudi Arabia,
(2) Erada And Mental Health Complex In Riyadh, Third Health Cluster,Ministry of Health, Saudi Arabia,
(3) Erada Mental Health Hospital In Jazan,Ministry of Health, Saudi Arabia,
(4) Samta General Hospital,Ministry of Health, Saudi Arabia,
(5) Primary Care Center Rafai Aljamsh,Ministry of Health, Saudi Arabia,
(6) Aledabi General Hospital, Ministry of Health, Saudi Arabia,
(7) King Fahad Central Hospital-Jazan,Ministry of Health, Saudi Arabia,
(8) Haddah Primary Health Center,Ministry of Health, Saudi Arabia,
(9) King Salman Bin Abdulaziz Hospital,Ministry of Health, Saudi Arabia

Abstract

Background: The digitization of healthcare, while transformative, has exponentially expanded the attack surface for cyber threats. Patient-centric care models, which rely on seamless data flow across disciplines such as nursing, radiology, and family medicine, create unique vulnerabilities where clinical efficiency can conflict with security protocols. Cybersecurity is no longer a sole IT concern but a critical patient safety and care continuity issue.

Aim: This narrative review aims to analyze and synthesize evidence on collaborative frameworks that integrate frontline clinical disciplines—specifically nursing, radiology, and family medicine—with information security professionals to protect health data.

Methods: A comprehensive search of PubMed, CINAHL, IEEE Xplore, and Scopus databases (2010-2024) was conducted. Keywords included interdisciplinary teams, cybersecurity, health information security, nursing informatics, radiology information systems, and primary care. Empirical studies, review articles, and framework proposals were included.

Results: Successful cybersecurity is predicated on moving beyond technical silos to embrace an interprofessional stewardship model. Nurses are pivotal in access control and phishing defense; radiologists govern high-risk imaging data workflows; family physicians balance accessibility with security in shared records. Effective frameworks incorporate embedded security champions, simulation-based training, and collaborative incident response protocols that prioritize clinical needs. A recurring theme is the tension between usability and security, mitigated through co-designed workflows.

Conclusion: Protecting patient data requires reconceptualizing cybersecurity as a shared, clinical-adjacent competency. Institutional strategies must foster authentic collaboration between IT security and frontline clinicians, investing in role-specific education, joint governance structures, and workflow-integrated security tools.

Keywords: Interprofessional Collaboration, Health Information Security, Cybersecurity, Human Factors, Clinical Workflow.

Introduction

The modern healthcare ecosystem is a paradox of profound vulnerability embedded within revolutionary capability (Gastaldi et al. 2018). The shift to patient-centric, digitally integrated care—epitomized by interconnected Electronic Health Records (EHRs), picture archiving and communication systems (PACS), and telehealth platforms—has dismantled traditional information silos, enabling holistic and continuous care (Kruse et al., 2017). This very interconnectedness, however, has made healthcare a prime target for cyberattacks. Healthcare data is uniquely valuable, often containing a complete identity and financial footprint, making it lucrative for theft and ransomware attacks (Abdulhameed et al., 2021). The ramifications of breaches extend far beyond financial penalties and reputational damage; they directly threaten patient safety through disrupted care pathways, corrupted clinical data, and the loss of patient trust (Aldossri & Hafizur Rahman, 2023; Offner et al., 2021).

*Corresponding author e-mail: Hhmmhhm8@Gmail.Com (Hamad Hamdan Saad Al-Qahtani).

Receive Date: 12 December 2024, Revise Date: 30 December 2024, Accept Date: 31 December 2024

Historically, cybersecurity has been relegated to the domain of specialized IT departments, operating in a silo separate from clinical operations (Patel et al., 2023; Frumento, 2019). This "bolt-on" security model, where protocols are designed by technologists and imposed upon clinicians, has proven fundamentally flawed. It creates friction in critical workflows, leading to workarounds that inadvertently create vulnerabilities, a phenomenon well-documented in studies on nursing informatics (Sittig et al., 2020). The frontline clinicians—nurses, radiologists, and family physicians—are not just end-users of technology; they are the operational custodians of patient data and the first line of defense against a multitude of threats, from phishing emails to physical endpoint security. Their daily workflows encompass the most sensitive data transactions: nurses documenting real-time care and managing myriad system access points; radiologists transmitting and interpreting vast diagnostic image sets; family physicians synthesizing longitudinal records across care settings (Mumtaz et al., 2023).

This review posits that effective cybersecurity in a patient-centric paradigm is an interprofessional imperative. It requires moving from a siloed, technical-centric model to a collaborative framework where information security professionals (InfoSec) and frontline clinicians are co-architects of a secure care environment. The core thesis is that the most critical vulnerability—and the most potent defense—in healthcare cybersecurity is the human factor. Therefore, this narrative review aims to synthesize the emerging literature from 2010 to 2024 on collaborative frameworks that integrate nursing, radiology, and family medicine with cybersecurity initiatives. It will explore the unique vulnerabilities and responsibilities of each discipline, analyze models for effective collaboration, and emphasize the design of secure workflows that align with, rather than obstruct, the primary goal of safe patient care. The ultimate objective is to outline the principles for building a resilient "human firewall," where every member of the care team is a knowledgeable and empowered steward of information security.

The Clinical Frontline

The attack surface in healthcare is heterogeneous, with different clinical disciplines facing distinct threats based on their workflow patterns, technology interfaces, and data privileges. Understanding these discrete vulnerabilities is the first step toward building targeted, collaborative defenses (Sittig & Singh, 2010).

Nursing

Nurses represent the largest user group of health IT systems and are physically present at the most vulnerable endpoints—workstations on wheels, bedside monitors, and medication dispensing systems (Melnick et al., 2021). Their workflow, characterized by urgency and multitasking, creates specific risks. The constant need for rapid access to patient information can lead to "access creep" (shared login credentials), failure to properly log out of systems (session management), and the use of personal devices for work communications (shadow IT) (Zadvinskis et al., 2018). Furthermore, nurses are highly targeted by phishing and social engineering attacks due to their central communication role; a single-click link can serve as the entry point for network-wide ransomware (Ghahremani & Farnia, 2021). Their stewardship role is therefore foundational: they are the guardians of the physical and logical point-of-care perimeter. Effective nursing engagement in cybersecurity involves integrating security checks (e.g., verifying patient identity before record access, secure disposal of printed materials) into routine clinical checks, akin to the "Five Rights" of medication administration. Figure 1 highlights the cybersecurity exposure points encountered by nurses at the bedside, including phishing attacks, unauthorized system access, and data breaches, while emphasizing the role of frontline clinical workflows and secure device management in protecting health information.

Figure 1: The Clinical Frontline: Nursing-Centered Cybersecurity Vulnerabilities and Safeguards

Radiology

Radiology departments operate at the nexus of high-value data and critical, time-sensitive workflows (Mun et al., 2023). PACS and Radiology Information Systems (RIS) are among the most data-intensive and interconnected systems in a hospital, often with direct external links to referring physicians and imaging centers. A breach here can lead to massive exfiltration of sensitive data or the complete halting of diagnostic services, directly impacting emergency and surgical care (Folasole et al., 2023). Radiologists and technologists face threats related to the integrity and availability of imaging data. This includes the risk of malware corrupting images (a patient safety issue), ransomware locking access to prior studies for comparison, and the secure transmission of studies containing identifiable metadata (Zhang et al., 2023). Their collaboration with InfoSec is crucial for ensuring secure, encrypted

data transmission (e.g., via DICOM standards with encryption), robust access controls for external sharing, and disaster recovery plans that prioritize the restoration of diagnostic capabilities (Choudhri et al., 2015; Zeb et al., 2022).

Family Medicine

In the era of patient portals, health information exchanges (HIEs), and integrated care records, family medicine practitioners (FMPs) manage the most longitudinal and comprehensive patient narratives. Their vulnerability stems from the tension between accessibility and security. They require seamless access to records from hospitals, specialists, and labs to provide coordinated care, often across multiple unaffiliated digital platforms (Mahou et al., 2021). This proliferation of access points increases the risk of credential compromise. Furthermore, the use of patient portals, while empowering, introduces risks like weak patient passwords and family member access issues. FMPs are also frequent targets of prescription fraud and medical identity theft schemes. Their collaborative role involves advocating for secure yet interoperable health information exchange protocols, educating patients on digital health literacy and security, and implementing rigorous identity verification processes within their practice workflows, especially for telehealth encounters (Koppel et al., 2023).

Table 1: Threat Landscape and Collaborative Stewardship Roles by Clinical Discipline

Clinical Discipline	Primary Cybersecurity Vulnerabilities	Key Collaborative Stewardship Actions with InfoSec
Nursing	- Phishing & social engineering - Poor session management (shared logins, walk-away failures) - Insecure use of mobile devices & workstations - Physical security of endpoints	- Act as "first reporters" of suspicious emails/activity. - Co-design rapid log-in/log-out workflows for busy settings. - Participate in securing medication dispensing systems & IoT devices. - Integrate privacy checks into patient hand-offs.
Radiology	- Ransomware targeting PACS/RIS - Unsecured external data transmission (DICOM) - Data integrity attacks on images - Unauthorized access to sensitive imaging (e.g., neuro, reproductive)	- Collaborate on secure external image sharing protocols. - Test and validate disaster recovery plans for imaging systems. - Advocate for network segmentation to isolate imaging data. - Ensure audit trails for access to sensitive studies.
Family Medicine	- Credential compromise across multiple portals/HIEs - Insecure telehealth platforms & data transmission - Patient portal-related risks (weak passwords, proxy access) - Medical identity theft & prescription fraud	- Co-design secure, user-friendly patient identity verification. - Advocate for standardized, secure APIs in health information exchange. - Provide patient education on digital health security. - Implement robust access controls for staff in small practice settings.

Frameworks for Collaboration

Moving from recognizing vulnerabilities to implementing effective defense requires structured models of collaboration. The literature points to several key frameworks that facilitate the integration of clinical and cybersecurity expertise.

Embedded Security Champions and Liaison Models

A highly effective strategy is the deployment of "clinical informaticists" or "cybersecurity champions" within clinical departments. These are clinicians, often nurses or physicians with additional informatics training, who serve as a bidirectional liaison (Carayon & Hoonakker, 2019). They translate clinical workflow needs to the InfoSec team and, conversely, explain security protocols and rationales to their clinical peers in contextually relevant terms. For example, a nurse informaticist can work with the security team to design a two-factor authentication process that is feasible for a nurse moving between patient rooms, rather than one that leads to workarounds. In radiology, a designated physician or PACS administrator can collaborate directly on testing the impact of network security policies on image retrieval speeds (Kelly et al., 2023).

Interprofessional Simulation and Education

Didactic training on security policies is often ineffective. Instead, interprofessional, simulation-based education—where clinicians and IT staff respond jointly to a simulated cyber-incident—has shown promise. Tabletop exercises simulating a ransomware attack on a radiology department or a phishing breach originating in a family medicine clinic force collaborative problem-solving (Williams & Woodward, 2015; Aljuraid & Justinia, 2022). These exercises expose communication gaps, clarify roles during a crisis, and build mutual understanding. Education must also be role-specific: nurses need training on identifying sophisticated phishing lures mimicking hospital administrators; radiologists need to understand the forensic implications of accessing systems during an attack; FMPs need guidance on evaluating the security of third-party health apps they recommend to patients (Hadlington et al., 2021; Graber et al., 2019).

Co-Design of Secure Clinical Workflows

The most sustainable security is "security by design," embedded into the clinical workflow itself. This requires InfoSec professionals to partner with clinicians from the inception of any new technology implementation or workflow redesign. Using human-centered design principles, teams can map clinical processes and identify where security controls (authentication, encryption, access logging) can be inserted with minimal disruption (García-Sánchez et al., 2022). For instance, a co-design team might create a single-sign-on (SSO) solution that satisfies security requirements for access control while meeting the nurse's need for speed, thereby eliminating the password-on-a-post-it vulnerability. In family medicine, co-design can focus on building secure, standardized patient intake forms within the EHR that minimize the need for unsecured external email.

Table 2: Models for Interprofessional Cybersecurity Collaboration

Collaborative Model	Core Mechanism	Example Implementation	Measurable Outcomes
Embedded Clinical Security Champion	A clinician (e.g., Nurse Informaticist, Radiologist Lead) with dedicated time to bridge clinical units and the InfoSec team.	A nurse champion pilots a new secure messaging app on a unit, gathers feedback, and works with IT to refine it before hospital-wide rollout.	- Reduced clinician workarounds. - Higher adoption rates of new security tools. - Faster resolution of clinical-user security issues.
Joint Incident Response Team (JIRT)	A pre-defined team with members from InfoSec, Clinical Leadership (Nursing, Medicine), Legal, and Communications that activates during a breach.	During a phishing incident, the JIRT coordinates: IT containment, clinical guidance on downtime procedures, legal reporting, and patient communication.	- Reduced incident response time. - Improved regulatory compliance post-breach. - Maintained clinical operations during crisis.
Interprofessional Security Design Sprint	Intensive, time-bound workshops where clinicians, IT, security, and designers co-create or retrofit a specific workflow.	A sprint to redesign the patient discharge process to ensure all printed materials are automatically logged and that digital copies are securely transmitted to the FMP.	- Workflows with security & privacy built-in. - Increased user satisfaction with IT systems. - Decreased vulnerabilities in high-risk processes.
Simulation-Based Training (Tabletop Exercises)	Realistic, scenario-driven simulations of cyber-attacks requiring coordinated response from different professional groups.	A simulation of a ransomware attack on PACS: Radiologists practice downtime reading, IT executes recovery, and administrators manage patient rescheduling.	- Improved interprofessional communication. - Clarification of roles and responsibilities. - Identification of gaps in response plans.

Overcoming Barriers and Charting a Path Forward

Despite clear imperatives, significant barriers impede interprofessional cybersecurity collaboration. These include cultural divides (the "us vs. them" mentality between clinical and technical staff), resource constraints (lack of time for clinicians to engage in security activities), misaligned incentives (security measured by technical metrics, not clinical outcomes), and knowledge asymmetry (clinicians lacking cyber literacy, InfoSec lacking clinical context) (Keshta & Odeh, 2021; Martínez-Pérez et al., 2015).

To overcome these, healthcare institutions must take decisive steps. First, cybersecurity must be formally integrated into clinical governance structures, with representation from nursing, medicine, and allied health on IT security committees. Second, investment in interprofessional roles, like clinical informaticists, must be viewed not as an IT cost but as a critical patient safety investment. Third, metrics for success must evolve to include clinical indicators, such as "reduction in workflow interruptions due to security controls" or "clinician compliance rates with security protocols," alongside traditional technical metrics like "number of blocked attacks" (Razaque et al., 2019).

Future research should focus on longitudinal studies measuring the impact of collaborative frameworks on both security outcomes (e.g., time to detect breaches) and clinical outcomes (e.g., care delays during incidents). There is also a need to develop and validate standardized interprofessional competencies in health cybersecurity and to explore the ethical dimensions of security decisions that impact care access.

Conclusion

The protection of patient data in the digital age is a quintessential interprofessional challenge. It cannot be solved by firewalls and filters alone but requires the construction of a robust "human firewall" composed of informed, vigilant, and collaborative clinicians. Nurses, radiologists, and family physicians, in partnership with information security professionals, hold the keys to a secure, patient-centric healthcare system. By moving from imposed security to co-designed stewardship, healthcare organizations can build resilient defenses that protect not only data but also the integrity and continuity of care itself. The imperative is clear: cybersecurity is patient safety, and safeguarding it is the shared duty of every member of the healthcare team.

References

1. Abdulhameed, I. S., Al-Mejibli, I., & Naif, J. R. (2021). The security and privacy of electronic health records in healthcare systems: A systematic review. *Turkish Journal of Computer and Mathematics Education*, *12*(10), 1979-1992.
2. Ajami, S., & Arab-Chadegani, R. (2014). The effects of applying information technology on job empowerment dimensions. *Journal of Education and Health promotion*, *3*(1), 84. DOI: 10.4103/2277-9531.139250
3. Aldossri, R., & Hafizur Rahman, M. M. (2023). A Systematic Literature Review on Cybersecurity Issues in Healthcare. *Computational Vision and Bio-Inspired Computing: Proceedings of ICCVBIC 2022*, 813-823. https://doi.org/10.1007/978-981-19-9819-5_58
4. Aljuraid, R., & Justinia, T. (2022). Classification of challenges and threats in healthcare cybersecurity: a systematic review. *Advances in Informatics, Management and Technology in Healthcare*, 362-365. doi:10.3233/SHTI220739
5. Carayon, P., & Hoonakker, P. (2019). Human factors and usability for health information technology: old and new challenges. *Yearbook of medical informatics*, *28*(01), 071-077. DOI: 10.1055/s-0039-1677907
6. Choudhri, A. F., Chatterjee, A. R., Javan, R., Radvany, M. G., & Shih, G. (2015). Security issues for mobile medical imaging: a primer. *Radiographics*, *35*(6), 1814-1824. https://doi.org/10.1148/rg.2015140039
7. Folasole, A., Adegboye, O. S., Ekuewa, O. I., & Eshua, P. E. (2023). Security, privacy challenges and available countermeasures in electronic health record systems: a review. *European Journal of Electrical Engineering and Computer Science*, *7*(6), 27-33. https://doi.org/10.24018/ejece.2023.7.6.561
8. Frumento, E. (2019). Cybersecurity and the evolutions of healthcare: challenges and threats behind its evolution. In *M_Health current and future applications* (pp. 35-69). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-02182-5_4
9. García-Sánchez, S., Somoza-Fernández, B., de Lorenzo-Pinto, A., Ortega-Navarro, C., Herranz-Alonso, A., & Sanjurjo, M. (2022). Mobile health apps providing information on drugs for adult emergency care: systematic search on app stores and content analysis. *JMIR mHealth and uHealth*, *10*(4), e29985. https://doi.org/10.2196/29985
10. Gastaldi, L., Appio, F. P., Corso, M., & Pistorio, A. (2018). Managing the exploration-exploitation paradox in healthcare: Three complementary paths to leverage on the digital transformation. *Business Process*

Management Journal, *24*(5), 1200-1234. https://doi.org/10.1108/BPMJ-04-2017-0092

11. Ghahremani, T., & Farnia, F. (2023). Investigating the Effect of Moral Disengagement and Organizational Culture on Behaviors Related to Information Security Awareness; Case Study Saderat and Mellat Banks. *Iranian Journal of Information Processing and Management*, *39*(2), 453-476. https://doi.org/10.22034/jipm.2023.709000
12. Graber, M. L., Siegal, D., Riah, H., Johnston, D., & Kenyon, K. (2019). Electronic health record–related events in medical malpractice claims. *Journal of patient safety*, *15*(2), 77-85. DOI: 10.1097/PTS.0000000000000240
13. Hadlington, L., Binder, J., & Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information security awareness. *Computers in Human Behavior*, *114*, 106557. https://doi.org/10.1016/j.chb.2020.106557
14. Kelly, B. S., Quinn, C., Belton, N., Lawlor, A., Killeen, R. P., & Burrell, J. (2023). Cybersecurity considerations for radiology departments involved with artificial intelligence. *European radiology*, *33*(12), 8833-8841. https://doi.org/10.1007/s00330-023-09860-1
15. Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183. https://doi.org/10.1016/j.eij.2020.07.003
16. Koppel, R., Kuziemsky, C., Elkin, P. L., Monkman, H., Lesselroth, B., & Nøhr, C. G. (2023). Differential Perceptions of What Constitutes a Medical Error Associated with Electronic Medical Records. In *Context Sensitive Health Informatics and the Pandemic Boost* (pp. 21-25). IOS Press. DOI: 10.3233/SHTI230361
17. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1-10. https://doi.org/10.3233/THC-161263
18. Mahou, X., Barral, B., Fernández, Á., Bouzas-Lorenzo, R., & Cernadas, A. (2021). eHealth and mHealth development in Spain: promise or reality?. *International Journal of Environmental Research and Public Health*, *18*(24), 13055. https://doi.org/10.3390/ijerph182413055
19. Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. *Journal of medical systems*, *39*(1), 181. https://doi.org/10.1007/s10916-014-0181-3
20. Melnick, E. R., West, C. P., Nath, B., Cipriano, P. F., Peterson, C., Satele, D. V., ... & Dyrbye, L. N. (2021). The association between perceived electronic health record usability and professional burnout among US nurses. *Journal of the American Medical Informatics Association*, *28*(8), 1632-1641. https://doi.org/10.1093/jamia/ocab059
21. Mumtaz, H., Riaz, M. H., Wajid, H., Saqib, M., Zeeshan, M. H., Khan, S. E., ... & Vohra, L. I. (2023). Current challenges and potential solutions to the use of digital health technologies in evidence generation: a narrative review. *Frontiers in digital health*, *5*, 1203945. https://doi.org/10.3389/fdgth.2023.1203945
22. Mun, S. K., Lo, S. C. B., Wong, K., Koh, D. M., & Prior, F. (2023). Emerging value-based radiology in the era of artificial intelligence. *Medical Research Archives*, *11*(5). https://doi.org/10.18103/mra.v11i5.3915
23. Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2021). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Health Security Intelligence*, 92-121.
24. Patel, A. U., Williams, C. L., Hart, S. N., Garcia, C. A., Durant, T. J., Cornish, T. C., & McClintock, D. S. (2023). Cybersecurity and information assurance for the clinical laboratory. *The journal of applied laboratory medicine*, *8*(1), 145-161. https://doi.org/10.1093/jalm/jfac119
25. Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. *IEEE access*, *7*, 168774-168797. https://doi.org/10.1109/ACCESS.2019.2950849
26. Sittig, D. F., Wright, A., Coiera, E., Magrabi, F., Ratwani, R., Bates, D. W., & Singh, H. (2020). Current challenges in health information technology–related patient safety. *Health informatics journal*, *26*(1), 181-189. https://doi.org/10.1177/1460458218814893
27. Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *BMJ Quality &*

Safety, *19*(Suppl 3), i68-i74. https://doi.org/10.1136/qshc.2010.042085

28. Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, 305-316.
29. Zadvinskis, I. M., Smith, J. G., & Yen, P. Y. (2018). Nurses' experience with health information technology: Longitudinal qualitative study. *JMIR medical informatics*, *6*(2), e8734. https://doi.org/10.2196/medinform.8734
30. Zeb, S., Mahmood, A., Khowaja, S. A., Dev, K., Hassan, S. A., Qureshi, N. M. F., ... & Bellavista, P. (2022). Industry 5.0 is coming: A survey on intelligent nextG wireless networks as technological enablers. *arXiv preprint arXiv:2205.09084*. https://doi.org/10.48550/arXiv.2205.09084
1. Zhang, B., Rahmatullah, B., Wang, S. L., Zaidan, A. A., Zaidan, B. B., & Liu, P. (2023). A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations. *Multimedia Tools and Applications*, *82*(14), 21867-21906. https://doi.org/10.1007/s11042-020-09629-4.