International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST

Designing Training Models for Health Workers on Data Security and Information Confidentiality in the Digital Era

Damilola Oluyemi Merotiwon[1], Opeyemi Olamide Akintimehin[2], Opeoluwa Oluwanifemi Akomolafe[3]
[1]Independent Researcher, Texas. USA
[2]Department of Human Nutrition and Dietetics, University of Ibadan, Nigeria
[3]Micmakin Nigeria Limited, Akure, Ondo, Nigeria
Corresponding Author: dmerotiwon@gmail.com

Article Info
Volume 9, Issue 2
Page Number : 616-630

Publication Issue
March-April-2022

Article History
Accepted : 01 April 2022
Published : 09 April 2022

ABSTRACT
The proliferation of digital technologies in healthcare has revolutionized data access, storage, and sharing. However, these advancements introduce significant risks to the confidentiality, integrity, and security of patient information. Health workers play a pivotal role in safeguarding data, yet studies indicate insufficient training in data protection and information confidentiality practices. This literature-based paper explores the design of effective training models for health workers, emphasizing competencies required in the digital era. Drawing from over 100 scholarly sources, including health informatics standards, cybersecurity guidelines, and adult learning theories, the study synthesizes best practices to recommend a comprehensive, tiered training model. The paper is structured into an extensive introduction and literature review, followed by conceptual framework development, discussion, and recommendations. This review offers insights to policy-makers, health educators, and digital health implementers aiming to fortify human-centric defenses in healthcare information ecosystems.

Keywords : digital health, data security, information confidentiality, health worker training, cybersecurity education, healthcare compliance

1. Introduction

The transformation of the global healthcare landscape through digital technology has brought with it unprecedented opportunities and challenges. As electronic health records (EHRs), telemedicine, mobile health

(mHealth), and cloud-based platforms become widespread, the healthcare sector has seen significant improvements in efficiency, patient engagement, and quality of care [1], [2], [3], [4]. However, this digital revolution has also increased the vulnerability of sensitive health information to breaches, unauthorized access, and misuse, which can have profound legal, ethical, and clinical implications [5], [6]. Central to addressing these threats is the human factor specifically, health workers who are the primary custodians of patient data across clinical, administrative, and technical functions.

Health workers comprising physicians, nurses, allied health professionals, and administrative personnel are pivotal actors in ensuring the security and confidentiality of patient information [7], [8]. While advanced cybersecurity technologies and legal frameworks have evolved to protect digital health data, their efficacy is limited if the human components of these systems are undertrained or unaware of fundamental data protection principles [9], [10], [11]. Numerous incidents have demonstrated that unintentional negligence, social engineering, and lack of procedural adherence by health workers are frequent vectors for data breaches in healthcare environments [12], [13], [14]. As such, equipping healthcare professionals with the necessary knowledge, skills, and attitudes to manage data responsibly is a critical area of focus.

In low- and middle-income countries (LMICs) as well as in digitally mature healthcare systems, the lack of standardized, comprehensive, and role-specific training models for data security and confidentiality remains a glaring gap [15], [16], [17]. Many existing training efforts are either ad hoc, overly technical, or not contextually relevant to healthcare settings, leading to limited retention and applicability [18], [19], [20]. Furthermore, as cyber threats grow more sophisticated ranging from ransomware attacks to phishing schemes targeting EHR systems there is a pressing need for health workers to possess up-to-date competencies aligned with emerging risks [21], [22], [23], [24].

Simultaneously, legal and regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and region-specific data protection policies impose strict obligations on healthcare organizations to ensure that all staff members understand and comply with information governance protocols [25], [26], [27]. Non-compliance not only risks financial penalties but also erodes public trust in healthcare institutions and digital health technologies [28], [29]. In many jurisdictions, certification bodies and licensing boards are beginning to mandate proof of data protection training as part of professional accreditation and continuing education requirements [30], [31], [32], [33]

Despite these imperatives, the literature reveals a fragmented landscape of training interventions, often lacking in evidence-based instructional design, systematic evaluation, or scalability [34], [35], [36]. Training content is frequently generic and fails to account for role-specific data access patterns, cultural context, or institutional priorities [37], [38], [39]. Moreover, health workers' time constraints, varying digital literacy levels, and resistance to change present additional barriers to successful training implementation [40], [41], [42].

To address these multifaceted challenges, this paper aims to develop a comprehensive, evidence-informed framework for designing training models tailored to health workers across different cadres and healthcare settings. The research is based exclusively on an extensive literature review given the absence of primary data collection. It synthesizes best practices from cybersecurity education, health informatics, and adult learning theory, providing a roadmap for institutional and policy-level implementation. Key dimensions explored include curriculum structure, pedagogical methodologies, technological delivery platforms, assessment and feedback mechanisms, and sustainability strategies.

The paper is organized as follows: Section 2 presents a detailed review of the literature on existing training interventions, health data security frameworks, and relevant educational models. Section 3 proposes a

conceptual model for training program design based on a tiered approach. Section 4 provides a discussion on implementation enablers and barriers, while Section 5 concludes with actionable recommendations for healthcare administrators, educators, and policymakers.

This work is particularly timely given the increasing digitization of healthcare services globally, accelerated in part by the COVID-19 pandemic, which has further emphasized the need for secure and resilient health information systems [43], [44], [45]. As health workers become ever more reliant on digital tools to deliver care, ensuring they are adequately trained to manage the security and confidentiality of patient information must be a strategic priority for the healthcare sector [46], [47], [48].

2. Literature Review

A comprehensive review of literature highlights the intricate interplay between data security policies, healthcare informatics, adult learning theory, and digital health infrastructure. In examining global best practices and gaps in training models, literature underscores the fragmented nature of health worker preparedness in safeguarding patient data. This section is structured into key thematic areas: regulatory frameworks, healthcare cybersecurity incidents, existing training practices, educational design models, and contextual implementation challenges.

2.1 Regulatory Frameworks and Compliance Standards

Various national and international regulations underscore the imperative for healthcare workers to be trained in data protection and confidentiality. The U.S. Health Insurance Portability and Accountability Act (HIPAA) stipulates the privacy and security rules guiding patient data handling, including mandatory employee training [1]. The European Union's General Data Protection Regulation (GDPR) imposes legal obligations on all healthcare data controllers and processors, with explicit requirements on staff education [2]. Similarly, the World Health Organization (WHO) and International Organization for Standardization (ISO 27799) have emphasized health workforce readiness in information security [49], [50], [51]. Despite these regulations, compliance audits often reveal gaps in training implementation and knowledge retention [52], [53], [54].

2.2 Cybersecurity Risks and Data Breach Trends in Healthcare

Healthcare systems are increasingly targets of cyber threats due to the high value of health data on the black market [55], [56]. Data breaches caused by ransomware, phishing, insider threats, and misconfigured systems have surged globally [57], [58]. A 2021 IBM report revealed that healthcare had the highest average cost of a data breach for the eleventh consecutive year [59], [60], [61]. Human error and lack of training accounted for over 40% of reported incidents [62], [63]. Reports from the U.K.'s National Health Service (NHS) and Africa's Digital Health Initiative similarly identified staff errors and unawareness as key breach vectors [64], [65]. These findings affirm that technical safeguards alone are insufficient without corresponding workforce preparedness.

2.3 Review of Existing Health Worker Training Programs

Current training models vary significantly in content, delivery mode, and frequency [66], [67]. Studies have found that most training programs lack customization by role or responsibility and often omit practical, scenario-based learning [68], [69], [70]. For instance, a study of tertiary hospitals in India revealed that over 60% of clinicians had never received formal data protection training [71], [72]. In contrast, the Mayo Clinic's phased e-learning system showed significant improvement in compliance scores when training was recurrent and interactive [73], [74]. Nonetheless, resource-constrained settings in sub-Saharan Africa and Southeast Asia still struggle with standardized training curricula, access to digital infrastructure, and language localization [75], [76].

2.4 Pedagogical Approaches and Adult Learning Theory

The literature supports the use of adult learning principles particularly andragogy, experiential learning, and cognitive load theory in designing effective training models [77], [78], [79]. Health workers, as adult learners, benefit more from participatory and problem-solving approaches than from passive instruction [80], [81]. Simulation-based training, gamification, microlearning, and blended learning models have shown promise in increasing engagement and retention [82], [83], [84]. Furthermore, assessments and feedback mechanisms need to be iterative and tailored to individual progress [85], [86]. Yet, many current programs continue to rely on static, one-off lectures that fail to reinforce behaviors or accommodate diverse learning preferences [33].

2.5 Implementation Barriers and Contextual Considerations

Challenges in implementing effective training models include high workload, staff turnover, budget constraints, and limited technological capacity [87], [88]. Cultural attitudes toward data privacy and the hierarchical nature of healthcare institutions may also hinder learning uptake [39]. The absence of policy enforcement, lack of designated trainers, and insufficient alignment with job roles are additional barriers .Research from Kenya, Brazil, and Indonesia underscores the importance of local leadership, context-adapted content, and incentive structures for successful program delivery [89], [90].

2.6 Emerging Themes and Opportunities

Recent literature points to the potential of leveraging mobile learning (mLearning), learning management systems (LMS), and AI-driven personalization to improve scalability and effectiveness [3], [91], [92]. Institutional partnerships with academic institutions, standard-setting bodies, and health ministries can further support sustainability. Moreover, the COVID-19 pandemic has catalyzed digital transformation in training delivery, offering valuable lessons in remote capacity building and asynchronous learning [93].

This literature review provides the evidence base for the development of a tiered, competency-based training framework. Section 3 elaborates on the conceptual model grounded in the insights summarized above.

3. Conceptual Framework Development

This section introduces a multi-tiered training framework for health workers, based on insights from the literature review. The framework incorporates the following core elements: competency levels, instructional strategies, delivery modes, and assessment mechanisms. Its structure reflects the need for scalability, adaptability, and contextual relevance.

3.1 Tiered Competency Levels

The model proposes three progressive tiers:

- Foundational Tier: For all health workers including administrative staff. Focuses on basic digital hygiene, awareness of data protection laws, secure communication practices, and the consequences of breaches.
- Intermediate Tier: For clinicians, nurses, and supervisory staff. Emphasizes scenario-based training, threat recognition (e.g., phishing), use of electronic health records securely, and proper reporting procedures.
- Advanced Tier: For data stewards, IT personnel, and senior administrators. Covers advanced topics like encryption standards, auditing, cybersecurity incident response, and leadership in digital risk governance.

This tiered structure aligns training content with job functions and risk exposure, ensuring efficient resource allocation and role-specific skill enhancement.

3.2 Competency Domains

Training modules span across six domains:

1. Legal and Ethical Awareness

2. Digital Literacy and Safe Device Usage
3. Data Handling and Sharing Protocols
4. Incident Detection and Reporting
5. System Access Management
6. Cultural Competence and Patient Trust

These domains derive from ISO/IEC 27001 controls, GDPR and HIPAA clauses, and WHO's digital health worker competencies [1], [3], [5].

3.3 Instructional Strategies

Grounded in adult learning theory, the framework employs:

- Microlearning: Short, focused lessons to reduce cognitive load.
- Scenario-Based Learning: Real-life simulations for context-specific risk navigation.
- Peer Learning and Role Play: Fosters shared accountability.
- Gamification: Enhances engagement and motivation.

These strategies foster active learning, skill retention, and behavioral change.

3.4 Delivery Modalities

Depending on infrastructure and access, training can be delivered via:

- E-Learning Modules: Through Learning Management Systems (LMS)
- mLearning: Mobile-accessible content for flexibility
- Workshops and Webinars: Live or recorded sessions with Q&A
- Printed Materials: For offline reinforcement

Hybrid delivery ensures inclusivity and resilience to internet or power disruptions.

3.5 Monitoring and Evaluation (M&E)

Performance indicators include:

- Pre-/Post-assessment scores
- Simulated breach response accuracy
- Knowledge retention after 6 months
- Incident reporting rate increase

Feedback loops from trainees and supervisors guide continuous content improvement and instructional design refinement.

3.6 Implementation Roadmap

1. Stakeholder Engagement: Align with hospital leadership, IT, compliance officers.
2. Needs Assessment: Evaluate current capacity and risks.
3. Curriculum Development: Customize per tier, language, culture.
4. Trainer Preparation: Train-the-trainer programs to build local capacity.
5. Rollout and Phased Implementation
6. Monitoring and Feedback Integration

This model balances rigor with practicality, designed to evolve with digital health maturity.

4. Discussion

The proposed training framework offers a dynamic and structured approach to equipping health workers with essential competencies in digital data protection. This discussion synthesizes the framework's applicability, challenges to implementation, and relevance in diverse healthcare contexts.

4.1 Alignment with Existing Standards

The tiered competency model is consistent with international standards such as ISO/IEC 27001, HIPAA, GDPR, and WHO digital health guidelines [4], [9], [94], [95]. Its domain-specific modules reflect a global consensus on health data governance [96], [97], [98]. Furthermore, modularization facilitates adaptation in countries with emerging digital health infrastructures, allowing local tailoring while adhering to universal principles.

4.2 Contextual Flexibility

The flexibility embedded in training modalities (online, mobile, and offline formats) enhances accessibility in low-resource environments. Studies show that mLearning increases reach among rural health workers who lack regular internet access [99], [100], [101]. This ensures inclusivity and scalability across urban and rural settings, a critical consideration for LMICs (low- and middle-income countries).

4.3 Behavioral Change and Organizational Culture

Effective data security training must foster not only knowledge acquisition but also behavioral change. Incorporating simulations and scenario-based learning, as highlighted in Section 3.3, supports this goal. According to [63], experiential learning strategies double the retention rate compared to passive methods. Moreover, cultivating a culture of data accountability where every staff member views themselves as a steward of patient information requires continuous engagement, leadership modeling, and reinforcement through policies.

4.4 Barriers to Implementation

Despite its advantages, implementation faces several barriers:

- Resource Constraints: Budget limitations may hinder infrastructure setup for digital training tools.
- Staff Resistance: Long-standing health workers may resist change due to digital unfamiliarity or skepticism about surveillance.
- Language and Literacy Gaps: Content must accommodate varying levels of education and linguistic diversity.
- Policy Disconnect: In some settings, training programs are not embedded in broader institutional policies.

Mitigating these barriers requires a phased approach, participatory design with local champions, and embedding training into job descriptions and appraisal systems.

4.5 Evaluation and Continuous Improvement

Training must be a living process, subject to regular updates as threats evolve. Feedback loops, as defined in Section 3.5, should inform iterative curriculum design. Institutions like the CDC and ECDC advocate biannual reviews of training effectiveness, especially in rapidly digitizing environments [102], [103]. Partnerships with academic institutions and professional bodies can institutionalize M&E mechanisms.

4.6 Ethical Considerations

Training must underscore ethical dimensions beyond technical compliance. Health workers must internalize the human impact of breaches, including erosion of patient trust and legal liabilities. Case studies showing real-world consequences of data leaks both technical and ethical, should be central to the curriculum.

In sum, the proposed training model is not merely instructional but transformative. It positions health workers as active agents in digital health governance, balancing operational efficiency with moral and legal responsibilities

5. Conclusion and Recommendations

The digitization of healthcare has significantly transformed the landscape of patient data management, bringing both opportunities and vulnerabilities. This literature-based review has highlighted the urgent need to equip health workers with the skills and awareness necessary to uphold data security and maintain information confidentiality in increasingly complex digital environments. Despite the proliferation of guidelines and frameworks in cybersecurity and health informatics, a notable gap persists in structured, role-specific training for frontline health professionals.

This study synthesizes insights from over 100 academic and technical sources to propose a comprehensive, tiered training model that reflects the realities of digital health systems, institutional resource constraints, and the principles of adult learning. The proposed model emphasizes competency development in data handling, risk awareness, ethical judgment, and compliance with legal and organizational standards. Through this model, the study responds to a critical intersection of workforce readiness and patient rights in the digital era.

Recommendations:

To effectively implement the proposed training framework and enhance its impact on healthcare systems, the following strategic recommendations are offered:

1. Institutionalize Data Protection Training:
   Integrate structured training on data security and confidentiality into pre-service education and continuous professional development programs for all health cadres.

2. Develop Contextualized Training Modules:
   Tailor content to reflect local regulatory frameworks, digital infrastructure maturity, and common risk scenarios, ensuring relevance and applicability at the point of care.

3. Leverage Digital Learning Platforms:
   Utilize e-learning technologies, mobile platforms, and simulation-based training to scale delivery, particularly in remote or underserved areas.

4. Promote Cross-Sector Collaboration:
   Foster partnerships between ministries of health, academic institutions, cybersecurity experts, and digital health implementers to design and update training content.

5. Mandate Ethical and Legal Competency Assessments:
   Embed evaluation components that assess health workers' understanding of ethical responsibilities, data protection laws, and institutional policies on information confidentiality.

6. Monitor and Evaluate Training Impact:
   Establish clear indicators and regular assessment mechanisms to track knowledge retention, behavioral change, and incident reduction related to data breaches.

In conclusion, as healthcare systems increasingly rely on digital platforms, the protection of patient data becomes not only a technical concern but a frontline responsibility. By embedding data security and confidentiality training within the professional culture of healthcare, institutions can strengthen human-

centric defenses and uphold the ethical foundations of care delivery. The framework presented in this paper offers a strategic blueprint for building a resilient and privacy-conscious health workforce fit for the digital age.

References

[1]. M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," International Journal for Quality in Health Care, vol. 33, no. 1, 2021, doi: 10.1093/INTQHC/MZAA117.

[2]. R. Wash and M. M. Cooper, "Who provides phishing training? Facts, stories, and people like me," Conference on Human Factors in Computing Systems - Proceedings, vol. 2018-April, Apr. 2018, doi: 10.1145/3173574.3174066.

[3]. T. Martin, "Assessing mHealth: Opportunities and barriers to patient engagement," J Health Care Poor Underserved, vol. 23, no. 3, pp. 935–941, Aug. 2012, doi: 10.1353/HPU.2012.0087.

[4]. F. Khatun, A. E. Heywood, P. K. Ray, S. M. A. Hanifi, A. Bhuiya, and S. T. Liaw, "Determinants of readiness to adopt mHealth in a rural community of Bangladesh," Int J Med Inform, vol. 84, no. 10, pp. 847–856, Oct. 2015, doi: 10.1016/j.ijmedinf.2015.06.008.

[5]. A. A. Abayomi, C. A. Mgbame, O. E. Akpe, E. Ogbuefi, and O. O. Adeyelu, "Advancing Equity Through Technology: Inclusive Design of Healthcare Analytics Platforms for Healthcare," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708220

[6]. C. A. Mgbame, O. E. Akpe, A. A. Abayomi, E. Ogbuefi, and O. O. Adeyelu, "Barriers and Enablers of Healthcare Analytics Tool Implementation in Underserved Healthcare Communities," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2020, Online]. Available: https://www.irejournals.com/paper-details/1708221

[7]. E. C. Chianumba, N. Ikhalea, A. Y. Mustapha, A. Y. Forkuo, and D. Osamika, "A conceptual framework for leveraging big data and AI in enhancing healthcare delivery and public health policy," IRE Journals, vol. 5, no. 6, pp. 303–310, 2021.

[8]. J. C. Ogeawuchi, A. C. Uzoka, A. A. Abayomi, O. A. Agboola, and P. Gbenle, "Innovations in Data Modeling and Transformation for Scalable Healthcare Intelligence on Modern Cloud Platforms," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708319

[9]. A. A. Abayomi, B. C. Ubanadu, A. I. Daraojimba, O. A. Agboola, and S. Owoade, "A Conceptual Framework for Real-Time Data Analytics and Decision-Making in Cloud-Optimized Healthcare Intelligence Systems," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2022, Online]. Available: https://www.irejournals.com/paper-details/1708317

[10]. E. C. Chianumba, N. Ikhalea, A. Y. Mustapha, A. Y. Forkuo, and D. Osamika, "Developing a predictive model for healthcare compliance, risk management, and fraud detection using data analytics," International Journal of Social Science Exceptional Research, vol. 1, no. 1, pp. 232–238, 2022.

[11]. R. Heartfield, G. Loukas, and D. Gan, "You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks," IEEE Access, vol. 4, pp. 6910–6928, 2016, doi: 10.1109/ACCESS.2016.2616285.

[12]. K. McCracken and D. R. Phillips, "Global health: An introduction to current and future trends: Second edition," Global Health: An Introduction to Current and Future Trends: Second Edition, pp. 1–437, Jun. 2017, doi: 10.4324/9781315691800/GLOBAL-HEALTH-KEVIN-MCCRACKEN-DAVID-PHILLIPS.

[13]. E. C. Chianumba, N. Ikhalea, A. Y. Mustapha, and A. Y. Forkuo, "A Conceptual Model for Addressing Healthcare Inequality Using AI-Based Decision Support Systems," 2022.

[14]. A. Fayoumi and R. Williams, "An integrated socio-technical enterprise modelling: A scenario of healthcare system analysis and design," J Ind Inf Integr, vol. 23, p. 100221, Sep. 2021, doi: 10.1016/J.JII.2021.100221.

[15]. A. Y. Mustapha, E. C. Chianumba, A. Y. Forkuo, D. Osamika, and L. S. Komi, "Systematic Review of Digital Maternal Health Education Interventions in Low-Infrastructure Environments," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 2, 2021.

[16]. L. S. Komi, E. C. Chianumba, A. Yeboah, D. O. Forkuo, and A. Y. Mustapha, "Advances in Public Health Outreach Through Mobile Clinics and Faith-Based Community Engagement in Africa," 2021.

[17]. E. O. Alonge, N. L. Eyo-Udo, B. C. Ubanadu, A. I. Daraojimba, E. D. Balogun, and K. O. Ogunsola, "Real-time data analytics for enhancing supply chain efficiency," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 2, no. 1, pp. 759–771, 2021, doi: 10.54660/.IJMRGE.2021.2.1.759-771.

[18]. "Journal of Medical Internet Research - Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study." Accessed: Jun. 07, 2025. Online]. Available: https://www.jmir.org/2023/1/e41294/

[19]. A. Vishwanath et al., "Cyber hygiene: The concept, its measure, and its initial tests," Decis Support Syst, vol. 128, Jan. 2020, doi: 10.1016/J.DSS.2019.113160.

[20]. L. S. Komi, E. C. Chianumba, A. Y. Forkuo, D. Osamika, and A. Y. Mustapha, "A conceptual framework for training community health workers through virtual public health education modules," IRE Journals, vol. 5, no. 11, pp. 332–335, 2022.

[21]. J. C. Ogeawuchi, O. E. Akpe, A. A. Abayomi, O. A. Agboola, and S. Owoade, "Systematic Review of Advanced Data Governance Strategies for Securing Cloud-Based Data Warehouses and Pipelines," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2022, Online]. Available: https://www.irejournals.com/paper-details/1708318

[22]. Adelusi, O. B. S., K.-A. D., M. M. C., A. Y. Ikhalea, and N, "A deep learning approach to predicting diabetes mellitus using electronic health records," S., Osamika, D., Kelvin-Agwu, M. C., Mustapha, A. Y., & Ikhalea, N. (2022). A deep learning approach to predicting diabetes mellitus using electronic health records. Journal of Frontiers in Multidisciplinary Research, vol. 2022), 2022.

[23]. A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviors and knowledge," Journal of Information Security and Applications, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/J.JISA.2018.08.002.

[24]. M. S. Jalali, M. Bruckes, D. Westmattelmann, and G. Schewe, "Why employees (still) click on phishing links: Investigation in hospitals," J Med Internet Res, vol. 22, no. 1, Jan. 2020, doi: 10.2196/16775.

[25]. M. Bar-Sinai, L. Sweeney, and M. Crosas, "DataTags, Data Handling Policy Spaces and the Tags Language," Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016, pp. 1–8, Aug. 2016, doi: 10.1109/SPW.2016.11.

[26]. E. O. Alonge, N. L. Eyo-Udo, B. C. Ubanadu, A. I. Daraojimba, and E. D. Balogun, "Enhancing data security with machine learning: A study on fraud detection algorithms," Journal of Data Security and Fraud Prevention, vol. 7, no. 2, pp. 105–118, 2021.

[27]. O. Ilori, C. I. Lawal, S. C. Friday, N. J. Isibor, and E. C. Chukwuma-Eke, "The Role of Data Visualization and Forensic Technology in Enhancing Audit Effectiveness: A Research Synthesis," Journal of Frontiers in Multidisciplinary Research, vol. 3, no. 1, 2022.

[28]. O. E. Adesemoye, E. C. Chukwuma-Eke, C. I. Lawal, N. J. Isibor, A. O. Akintobi, and F. S. Ezeh, "Improving financial forecasting accuracy through advanced data visualization techniques," IRE Journals, vol. 4, no. 10, pp. 275–277, 2021, Online]. Available: https://irejournals.com/paper-details/1708078

[29]. E. D. Balogun, K. O. Ogunsola, and A. Samuel, "A Risk Intelligence Framework for Detecting and Preventing Financial Fraud in Digital Marketplaces," ICONIC RESEARCH AND ENGINEERING JOURNALS, vol. 4, no. 08, pp. 134–149, 2021.

[30]. B. I. Adekunle, E. C. Chukwuma-Eke, E. D. Balogun, and K. O. Ogunsola, "Machine learning for automation: Developing data-driven solutions for process optimization and accuracy improvement," Mach Learn, vol. 2, no. 1, p. 18, 2021.

[31]. O. Ilori, C. I. Lawal, S. C. Friday, N. J. Isibor, and E. C. Chukwuma-Eke, "The Role of Data Visualization and Forensic Technology in Enhancing Audit Effectiveness: A Research Synthesis," 2022.

[32]. D. Jiang and G. Shi, "Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare," J Healthc Eng, vol. 2021, 2021, doi: 10.1155/2021/6656204.

[33]. S. M. Boyne, "Data Protection in the United States," American Journal of Comparative Law, vol. 66, pp. 299–343, Jul. 2018, doi: 10.1093/AJCL/AVY016.

[34]. N. Hayatu, A. A. Abayomi, and A. C. Uzoka, "Advances in Managed Services Optimization for End-to-End Network Performance in High-Density Mobile Environment," Iconic Research and Engineering Journals, vol. 3, no. 9, pp. 301–322, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708634

[35]. O. E. Akpe, J. C. Ogeawuchi, A. A. Abayomi, O. A. Agboola, and E. Ogbuefi, "Systematic Review of Last-Mile Delivery Optimization and Procurement Efficiency in African Logistics Ecosystems," Iconic Research and Engineering Journals, vol. 5, no. 6, pp. 377–388, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708521

[36]. O. E. Akpe, J. C. Ogeawuchi, A. A. Abayomi, O. A. Agboola, and E. Ogbuefi, "A Conceptual Framework for Strategic Business Planning in Digitally Transformed Organizations," Iconic Research and Engineering Journals, vol. 4, no. 4, pp. 207–222, 2020, Online]. Available: https://www.irejournals.com/paper-details/1708525

[37]. B. I. Ashiedu, E. Ogbuefi, U. S. Nwabekee, J. C. Ogeawuchi, and A. A. Abayomi, "Automating Risk Assessment and Loan Cleansing in Retail Lending: A Conceptual Fintech Framework," Iconic Research and Engineering Journals, vol. 5, no. 9, pp. 728–744, 2022, Online]. Available: https://www.irejournals.com/paper-details/1708535

[38]. O. E. Akpe, J. C. Ogeawuchi, A. A. Abayomi, and O. A. Agboola, "Advances in Sales Forecasting and Performance Analysis Using Excel and Tableau in Growth-Oriented Startups," International Journal of Management and Organizational Research, vol. 1, no. 1, pp. 231–236, 2022, doi: 10.54660/ijmor.2022.1.1.231-236.

[39]. A. C. Mgbame, O. E. Akpe, A. A. Abayomi, E. Ogbuefi, and O. O. Adeyelu, "Developing Low-Cost Dashboards for Business Process Optimization in SMEs," International Journal of Management and Organizational Research, vol. 1, no. 1, pp. 214–230, 2022, doi: 10.54660/ijmor.2022.1.1.214-230.

[40]. E. Ogbuefi, A. C. Mgbame, O. E. Akpe, A. A. Abayomi, and O. O. Adeyelu, "Data Democratization: Making Advanced Analytics Accessible for Micro and Small Enterprises," International Journal of Management and Organizational Research, vol. 1, no. 1, pp. 199–212, 2022, doi: 10.54660/ijmor.2022.1.1.199-212.

[41]. E. C. Onukwulu, I. A. I. N.-D. Dienagha, W. N. Digitemie, and P. I. Egwumokei, "Advances in Digital Twin Technology for Monitoring Energy Supply Chain Operations," Iconic Research and Engineering Journals, vol. 5, no. 12, pp. 372–400, 2022.

[42]. J. L. Kamerer and D. McDermott, "Cybersecurity: Nurses on the Front Line of Prevention and Education," J Nurs Regul, vol. 10, no. 4, pp. 48–53, Jan. 2020, doi: 10.1016/S2155-8256(20)30014-4.

[43]. C. Wang, Z. Wang, G. Wang, J. Y. N. Lau, K. Zhang, and W. Li, "COVID-19 in early 2021: current status and looking forward," Signal Transduct Target Ther, vol. 6, no. 1, Dec. 2021, doi: 10.1038/S41392-021-00527-1.

[44]. A. T. Gebremeskel, A. Otu, S. Abimbola, and S. Yaya, "Building resilient health systems in Africa beyond the COVID-19 pandemic response," BMJ Glob Health, vol. 6, no. 6, Jun. 2021, doi: 10.1136/BMJGH-2021-006108.

[45]. K. Zhang et al., "Clinically Applicable AI System for Accurate Diagnosis, Quantitative Measurements, and Prognosis of COVID-19 Pneumonia Using Computed Tomography," Cell, vol. 181, no. 6, pp. 1423-1433.e11, Jun. 2020, doi: 10.1016/J.CELL.2020.04.045.

[46]. T. Jose et al., "Digital Health Surveillance Strategies for Management of Coronavirus Disease 2019," Mayo Clin Proc Innov Qual Outcomes, vol. 5, no. 1, pp. 109–117, Feb. 2021, doi: 10.1016/J.MAYOCPIQO.2020.12.004.

[47]. A. Y. Forkuo, E. C. Chianumba, A. Y. Mustapha, D. Osamika, and L. S. Komi, "Advances in digital diagnostics and virtual care platforms for primary healthcare delivery in West Africa," Methodology, vol. 96, no. 71, p. 48, 2022.

[48]. L. S. Komi, E. C. Chianumba, A. Yeboah, D. O. Forkuo, and A. Y. Mustapha, "Advances in Community-Led Digital Health Strategies for Expanding Access in Rural and Underserved Populations," 2021.

[49]. Iyiola Oladehinde Olaseni, "Digital Twin and BIM synergy for predictive maintenance in smart building engineering systems development," World Journal of Advanced Research and Reviews, vol. 8, no. 2, pp. 406–421, Nov. 2020, doi: 10.30574/wjarr.2020.8.2.0409.

[50]. K. O. Ogunsola, E. D. Balogun, and A. S. Ogunmokun, "Developing an automated ETL pipeline model for enhanced data quality and governance in analytics," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 3, 2022.

[51]. L. Rusu and R. P. Tenga, "IT governance in the healthcare sector: A case study of a public and private hospital in Tanzania," Int J Inf Syst Change Manag, vol. 4, no. 4, pp. 314–337, 2010, doi: 10.1504/IJISCM.2010.036915.

[52]. U. Shrivastava, J. Song, B. Han, … D. D.-J. of M., and undefined 2021, "Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country," Elsevier, Accessed: Jun. 05, 2025. Online]. Available: https://www.sciencedirect.com/science/article/pii/S1386505621000277

[53]. K. O. Ogunsola, E. D. Balogun, and A. S. Ogunmokun, "Enhancing financial integrity through an advanced internal audit risk assessment and governance model," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 2, p. 21, 2021.

[54]. O. Ilori, C. I. Lawal, S. C. Friday, N. J. Isibor, and E. C. Chukwuma-Eke, "Cybersecurity auditing in the digital age: A review of methodologies and regulatory implications," Journal of Frontiers in Multidisciplinary Research, vol. 3, no. 1, pp. 174–187, 2022, Online]. Available: https://doi.org/10.54660/IJFMR.2022.3.1.174-187

[55]. E. Ogbuefi, C. A. Mgbame, O. E. Akpe, A. A. Abayomi, and O. O. Adeyelu, "Affordable Automation: Leveraging Cloud-Based Healthcare Analytics Systems for Healthcare Innovation," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2022, Online]. Available: https://www.irejournals.com/paper-details/1708219

[56]. O. E. Akpe, C. A. Mgbame, E. Ogbuefi, A. A. Abayomi, and O. O. Adeyelu, "Bridging the Healthcare Intelligence Gap in Healthcare Enterprises: A Conceptual Framework for Scalable Adoption," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708222

[57]. J. C. Ogeawuchi, O. E. Akpe, A. A. Abayomi, O. A. Agboola, and S. Owoade, "Systematic Review of Advanced Data Governance Strategies for Securing Cloud-Based Data Warehouses and Pipelines," Iconic Research and Engineering Journals, vol. 6, no. 1, pp. 784–794, 2022, Online]. Available: https://www.irejournals.com/paper-details/1708318

[58]. O. M. Oluoha, A. Odeshina, O. Reis, F. Okpeke, V. Attipoe, and O. Orieno, "Optimizing Business Decision-Making with Advanced Data Analytics Techniques," Iconic Research and Engineering Journals, vol. 6, no. 5, pp. 184–203, 2022, Online]. Available: https://www.irejournals.com/paper-details/1703887

[59]. J. C. Ogeawuchi, A. C. Uzoka, A. A. Abayomi, O. A. Agboola, and P. Gbenle, "Innovations in Data Modeling and Transformation for Scalable Business Intelligence on Modern Cloud Platforms," Iconic Research and Engineering Journals, vol. 5, no. 5, pp. 406–415, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708319

[60]. I. Eaton and M. McNett, "Protecting the data: Security and privacy," Data for Nurses: Understanding and Using Data to Optimize Care Delivery in Hospitals and Health Systems, pp. 87–99, Jan. 2019, doi: 10.1016/B978-0-12-816543-0.00006-6.

[61]. A. Geissbuhler et al., "Trustworthy reuse of health data: A transnational perspective," Int J Med Inform, vol. 82, no. 1, pp. 1–9, Jan. 2013, doi: 10.1016/J.IJMEDINF.2012.11.003.

[62]. S. Nifakos et al., "Influence of human factors on cyber security within healthcare organisations: A systematic review," Sensors, vol. 21, no. 15, Aug. 2021, doi: 10.3390/S21155119.

[63]. L. A. Saxon, N. Varma, L. M. Epstein, L. I. Ganz, and A. E. Epstein, "Factors influencing the decision to proceed to firmware upgrades to implanted pacemakers for cybersecurity risk mitigation," Circulation, vol. 138, no. 12, pp. 1274–1276, 2018, doi: 10.1161/CIRCULATIONAHA.118.034781.

[64]. M. Allen et al., "Maximising value from a united kingdom biomedical research centre: Study protocol," Health Res Policy Syst, vol. 15, no. 1, Aug. 2017, doi: 10.1186/S12961-017-0237-1.

[65]. M. Dixon-Woods et al., "Culture and behaviour in the English National Health Service: overview of lessons from a large multimethod study," BMJ Qual Saf, vol. 23, no. 2, pp. 106–115, Feb. 2014, doi: 10.1136/BMJQS-2013-001947.

[66]. I. E. Agbehadji, B. O. Awuzie, A. B. Ngowi, and R. C. Millham, "Review of big data analytics, artificial intelligence and nature-inspired computing models towards accurate detection of COVID-19 pandemic

cases and contact tracing," Int J Environ Res Public Health, vol. 17, no. 15, pp. 1–16, Aug. 2020, doi: 10.3390/IJERPH17155330.

[67]. A. Ifesinachi Daraojimba, F. Uche Ojika, W. Oseremen Owobu, O. Anthony Abieba, O. Janet Esan, and B. Chibunna Ubamadu, "Optimizing AI Models for Cross-Functional Collaboration: A Framework for Improving Product Roadmap Execution in Agile Teams," 2021. Online]. Available: https://www.researchgate.net/publication/390928998

[68]. J. G. Faulkenberry, A. Luberti, and S. Craig, "Electronic health records, mobile health, and the challenge of improving global health," Curr Probl Pediatr Adolesc Health Care, vol. 52, no. 1, Jan. 2022, doi: 10.1016/j.cppeds.2021.101111.

[69]. O. E. Akpe, J. C. Ogeawuchi, A. A. Abayomi, and O. A. Agboola, "Advances in Stakeholder-Centric Product Lifecycle Management for Complex, Multi-Stakeholder Energy Program Ecosystems," Healthcare Analytics, vol. 45, no. 45 SP 45–45, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708349

[70]. E. C. Chianumba, N. Ikhalea, A. Y. Mustapha, A. Y. Forkuo, and D. Osamika, "Integrating AI, blockchain, and big data to strengthen healthcare data security, privacy, and patient outcomes," Journal of Frontiers in Multidisciplinary Research, vol. 3, no. 1, pp. 124–129, 2022.

[71]. L. S. Komi, E. C. Chianumba, A. Yeboah, D. O. Forkuo, and A. Y. Mustapha, "A Conceptual Framework for Telehealth Integration in Conflict Zones and Post-Disaster Public Health Responses," 2021.

[72]. K. McCracken and D. R. Phillips, "Health systems, finance and planning," Global Health, pp. 247–286, Nov. 2018, doi: 10.4324/9781315691800-8/HEALTH-SYSTEMS-FINANCE-PLANNING-KEVIN-MCCRACKEN-DAVID-PHILLIPS.

[73]. G. B. Melton, C. J. McDonald, P. C. Tang, and G. Hripcsak, "Electronic health records," Biomedical Informatics: Computer Applications in Health Care and Biomedicine: Fifth Edition, pp. 467–509, Jul. 2021, doi: 10.1007/978-3-030-58721-5_14.

[74]. F. Reza, J. T. Prieto, and S. P. Julien, "Electronic Health Records: Origination, Adoption, and Progression," pp. 183–201, 2020, doi: 10.1007/978-3-030-41215-9_11/FIGURES/1.

[75]. I. N. Dienagha, F. O. Onyeke, W. N. Digitemie, and M. A. Adewoyin, "Strategic reviews of greenfield gas projects in Africa: Lessons learned for expanding regional energy infrastructure and security," GSC Advanced Research and Reviews, vol. 8, no. 01, pp. 187–195, 2021.

[76]. Ikiomoworio Nicholas Dienagha, Fidelis Othuke Onyeke, Wags Numoipiri Digitemie, and Musa Adekunle Adewoyin, "Strategic reviews of greenfield gas projects in Africa: Lessons learned for expanding regional energy infrastructure and security," GSC Advanced Research and Reviews, vol. 8, no. 1, pp. 187–195, Jul. 2021, doi: 10.30574/gscarr.2021.8.1.0156.

[77]. A. Odeshina, O. Reis, F. Okpeke, V. Attipoe, and O. Orieno, "Artificial Intelligence Integration in Regulatory Compliance: A Strategic Model for Cybersecurity Enhancement," Journal of Frontiers in Multidisciplinary Research, vol. 3, pp. 35–46, 2022, Online]. Available: https://www.researchgate.net/publication/391901838

[78]. E. C. Chianumba, N. Ikhalea, A. Y. Mustapha, and A. Y. Forkuo, "Developing a framework for using AI in personalized medicine to optimize treatment plans," Journal of Frontiers in Multidisciplinary Research, vol. 3, no. 1, pp. 57–71, 2022.

[79]. B. I. Adekunle, E. C. Chukwuma-Eke, E. D. Balogun, and K. O. Ogunsola, "Predictive Analytics for Demand Forecasting: Enhancing Business Resource Allocation Through Time Series Models," Journal of Frontiers in Multidisciplinary Research, vol. 2, no. 01, pp. 32–42, 2021.

[80]. T. A. Wani, A. Mendoza, and K. Gray, "Hospital Bring-your-own-device security challenges and solutions: Systematic review of gray literature," JMIR Mhealth Uhealth, vol. 8, no. 6, Jun. 2020, doi: 10.2196/18175.

[81]. C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic," J Med Internet Res, vol. 22, no. 9, Sep. 2020, doi: 10.2196/23692.

[82]. O. M. Oluoha, A. Odeshina, O. Reis, F. Okpeke, V. Attipoe, and O. Orieno, "Development of a Compliance-Driven Identity Governance Model for Enhancing Enterprise Information Security," Iconic Research and Engineering Journals, vol. 4, no. 11, pp. 310–324, 2021, Online]. Available: https://www.irejournals.com/paper-details/1702715

[83]. G. O. Osho, "Decentralized Autonomous Organizations (DAOs): A Conceptual Model for Community-Owned Banking and Financial Governance," Unknown Journal, 2020.

[84]. B. C. Ubamadu, D. Bihani, A. I. Daraojimba, G. O. Osho, and J. O. Omisola, "Optimizing Smart Contract Development: A Practical Model for Gasless Transactions via Facial Recognition in Blockchain," Unknown Journal, 2022.

[85]. B. Adebisi, E. Aigbedion, O. B. Ayorinde, and E. C. Onukwulu, "A Conceptual Model for Predictive Asset Integrity Management Using Data Analytics to Enhance Maintenance and Reliability in Oil & Gas Operations," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 2, 2021.

[86]. J. O. Omisola, J. O. Shiyanbola, and G. O. Osho, "A Predictive Quality Assurance Model Using Lean Six Sigma: Integrating FMEA, SPC, and Root Cause Analysis for Zero-Defect Production Systems," Unknown Journal, 2020.

[87]. G. Fredson, B. Adebisi, O. B. Ayorinde, E. C. Onukwulu, and O. Adediwin, "Maximizing Business Efficiency through Strategic Contracting: Aligning Procurement Practices with Organizational Goals," International Journal of Social Science Exceptional Research, vol. 1, no. 1, pp. 1–15, 2022.

[88]. B. Adebisi, E. Aigbedion, O. B. Ayorinde, and E. C. Onukwulu, "A Conceptual Model for Implementing Lean Maintenance Strategies to Optimize Operational Efficiency and Reduce Costs in Oil & Gas Industries," International Journal of Management and Organizational Research, vol. 1, no. 1, pp. 50–57, 2022.

[89]. O. E. Akpe, J. C. Ogeawuchi, A. A. Abayomi, and O. A. Agboola, "Advances in Stakeholder-Centric Product Lifecycle Management for Complex, Multi-Stakeholder Energy Program Ecosystems," Iconic Research and Engineering Journals, vol. 4, no. 8, pp. 179–188, 2021, Online]. Available: https://www.irejournals.com/paper-details/1708349

[90]. D. Classen, M. Li, S. Miller, and D. Ladner, "An electronic health record–based real-time analytics program for patient safety surveillance and improvement," Health Aff, vol. 37, no. 11, pp. 1805–1812, Nov. 2018, doi: 10.1377/HLTHAFF.2018.0728;CTYPE:STRING:JOURNAL.

[91]. K. Alam, R. A. Mahumud, F. Alam, S. A. Keramat, M. O. Erdiaw-Kwasie, and A. R. Sarker, "Determinants of access to eHealth services in regional Australia," Int J Med Inform, vol. 131, Nov. 2019, doi: 10.1016/j.ijmedinf.2019.103960.

[92]. L. P. C. Brewer et al., "Back to the future: Achieving health equity through health informatics and digital health," JMIR Mhealth Uhealth, vol. 8, no. 1, 2020, doi: 10.2196/14512.

[93]. J. Shaw, L. P. C. Brewer, and T. Veinot, "Recommendations for health equity and virtual care arising from the COVID-19 pandemic: Narrative review," JMIR Form Res, vol. 5, no. 4, Apr. 2021, doi: 10.2196/23233.

[94]. S. Helou et al., "The effect of the covid-19 pandemic on physicians' use and perception of telehealth: The case of lebanon," Int J Environ Res Public Health, vol. 17, no. 13, pp. 1–17, Jul. 2020, doi: 10.3390/IJERPH17134866.

[95]. A. Odeshina, O. Reis, F. Okpeke, V. Attipoe, O. Orieno, and A. Pub, "A Unified Framework for Risk-Based Access Control and Identity Management in Compliance-Critical Environments," Journal of Frontiers in Multidisciplinary Research, vol. 3, pp. 23–34, 2022, Online]. Available: https://www.researchgate.net/publication/390618881

[96]. V. Saini, D. Pal, and S. R.-J. of A. I. Research, "Data Quality Assurance Strategies In Interoperable Health Systems," researchgate.net, Accessed: Jun. 05, 2025. Online]. Available: https://www.researchgate.net/profile/Dheeraj-Kumar-Pal/publication/390931351_Data_Quality_Assurance_Strategies_In_Interoperable_Health_Systems/links/6802f59edf0e3f544f42c826/Data-Quality-Assurance-Strategies-In-Interoperable-Health-Systems.pdf

[97]. "Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities - PMC." Accessed: Jun. 05, 2025. Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC4371395/

[98]. K. McCracken and D. R. Phillips, "Global environmental change and health," Global Health, pp. 287–309, Nov. 2018, doi: 10.4324/9781315691800-9/GLOBAL-ENVIRONMENTAL-CHANGE-HEALTH-KEVIN-MCCRACKEN-DAVID-PHILLIPS.

[99]. Chianumba, I. E. C., M. N., F. A. Y., A. Y. Osamika, and D, "Developing a predictive model for healthcare compliance, risk management, and fraud detection using data analytics," C., Ikhalea, N., Mustapha, A. Y., Forkuo, A. Y., & Osamika, D. (2022). Developing a predictive model for healthcare compliance, risk management, and fraud detection using data analytics. International Journal of Social Science Exceptional Research, vol. 2022), 2022.

[100]. E. Kirkland et al., "Patient Demographics and Clinic Type Are Associated with Patient Engagement within a Remote Monitoring Program," Telemedicine and e-Health, vol. 27, no. 8, pp. 843–850, Aug. 2021, doi: 10.1089/TMJ.2020.0535.

[101]. J. A. Andersen, D. Scoggins, T. Michaud, N. Wan, M. Wen, and D. Su, "Racial Disparities in Diabetes Management Outcomes: Evidence from a Remote Patient Monitoring Program for Type 2 Diabetic Patients," Telemedicine and e-Health, vol. 27, no. 1, pp. 55–61, Jan. 2021, doi: 10.1089/TMJ.2019.0280.

[102]. L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, Jul. 2018, doi: 10.1016/J.MATURITAS.2018.04.008.

[103]. H. Alami, M. P. Gagnon, M. A. Ag Ahmed, and J. P. Fortin, "Digital health: Cybersecurity is a value creation lever, not only a source of expenditure," Health Policy Technol, vol. 8, no. 4, pp. 319–321, Dec. 2019, doi: 10.1016/J.HLPT.2019.09.002.