Alpha Psychiatry

Alpha Psychiatry **2025**; 26(3): 44279
https://doi.org/10.31083/AP44279

Editorial

E-mental Health in the Age of AI: Data Safety, Privacy Regulations and Recommendations

Hanwen Zhang[1], Yanna Mao[2], Yibin Lin[1,3], Dexing Zhang[1,3,*]

[1]JC School of Public Health and Primary Care, The Chinese University of Hong Kong, Hong Kong, China
[2]School of Health Management, Southern Medical University, 510091 Guangzhou, Guangdong, China
[3]School of Nursing, The Hong Kong Polytechnic University, Hong Kong, China
*Correspondence: daisy.dx.zhang@polyu.edu.hk (Dexing Zhang)
Submitted: 15 November 2024 Revised: 28 November 2024 Accepted: 2 December 2024 Published: 26 June 2025

1. Mental Health Problems Are a Global Challenge

Mental health problems pose a major public health challenge globally. It has been reported that about 14% of the world's population experienced mental disorders, and 17% of the total years lived with disability were attributable to these disorders in 2021 [1]. An increasing trend of mental health issues has been observed among younger generations; in 2020, depressive and anxiety disorders were most prevalent in the 20–35-year-old age group. Significant unmet needs for mental health treatment persist [2,3], due to underscreening, underdiagnosis, and undertreatment. These issues are compounded by stigma, a lack of public awareness and literacy, and a healthcare system that suffers from insufficient mental health manpower, resources, and access.

2. The Role of E-mental Health (EMH) in Mitigating Growing Global Challenges

EMH interventions have been applied in primary care settings, hospitals, long-term care facilities, and non-clinical settings such as home or community. It showed effectiveness in treating anxiety and depression, eating disorder, work-related stress etc. [4–7], especially in rural area where residents have lower health literacy and limited access to healthcare [8]. Virtual mental health evaluation services has improved patient engagement and continuity of care following hospital discharge, as well as the efficiency in hospital emergency department [9].

EMH treatments yield positive and sustaining effects and remain stable post-treatment across various patient groups and therapy types [10]. There is a growing availability of patient-driven, web-based resources for depression and other chronic care managements in primary care intervention [11]. Digital phenotyping (DP) has been widely integrated into EMH interventions including heart rate estimation, exercise/physical activity monitoring, and sleep tracking, supported by validated effectiveness [12]. One review has indicated DP can directly improve mental health status of college students [13]. Research has also demonstrated the feasibility of using AI chatbots to deliver mental health support, with findings highlighting their effectiveness in alleviating anxiety and depressive symptoms [14]. Innovative approaches such as incorporating avatars and the metaverse into EMH services, have shown early promise but require further research evidence on effectiveness [15].

With the rapid technology development, EMH has gained much momentum and success [16]. Access to EMH can be many forms, such as videoconferences led by a professional, mental health mobile apps, or information and guidance on websites, with or without integration with electronic medical records (EMRs) [17]. It features prominently in delivering timely, effective mental health services by using technologies, at a low cost to reach a large population. Due to the anonymity it offers, EMH interventions also reduced help-seeking barriers, such as shame, stigma, and fear of exposure [18]. Advantages include improved accessibility in rural and remote areas and inner cities as well as multilingual tailor-made services that cater to the specific habits or preferences of users [19]. Use of internet-based mental health information and support is becoming increasingly common among the younger generations; for example over 60% Canadian youth were using it and over 80% prone to use a website if going through a difficult times [20]. The capacity of EMH to be delivered at scale provides an opportunity for the prevention of prevention of mental illness, as well as early detection and intervention [19].

3. Concerns over Data Safety in EMH

Despite advantages and future trends of using EMH, data safety issues remain a significant concern [21]. Personal Health Information (PHI) such as name, age, and state of mental health are recorded and stored, [22] which is one of the main reasons for patients' resistance to EMH services [23]. It is not uncommon to report digital mailbox hacks [24], text message interception [25], and video videoconference overheard or observed by unauthorized parties [26]. Nowadays, the growing wealth of mobile sensing data is being leveraged in health and behavioral sciences through digital biomarkers, aiding in the detection of mental health problems, monitoring progress, and enhancing targeted behavioral interventions [27,28]. The integration of sophisticated sensors in smartphones and wearables enables the unobtrusive and automated collection of detailed, real-time

data on human behaviors, states, and environmental factors [29,30]. However, clients may unknowingly share various sensitive data with developers. In some cases, such data are sold to third parties for commercial purposes without notification or authorization, raising privacy concerns and mistrust from the public [31]. Previous analyses of mobile medical, health, and fitness apps has revealed privacy policies were completely lacking for 40% of paid apps; 40% of the apps collect highly traceable data including full name, health information, financial information, etc. Disturbingly, 83% of the free mobile health and fitness apps store data locally on the device without encryption [32]. According to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) data breach portal, approximately 295 breaches were reported by the healthcare sector in the first half of 2023 alone, with more than 39 million individuals implicated in healthcare data breaches [33]. Despite advancements in data encryption and safety protocols, the risk of data breaches cannot be entirely eliminated.

4. Current Well-known Data Protection Law and Regulations

It is encouraging to witness the significant efforts made by numerous countries in the realm of data protection. Table 1 lists some important regulations. These regulations typically include:

(1) the necessity of obtaining user consent prior to collecting, using, and sharing personal information;

(2) data subject rights such as data access, portability and objection;

(3) accountability and obligations for data controllers/processors;

(4) oversight of cross-border data transfers or third-party sharing;

(5) data breaches reporting to affected parties;

(6) provisions for enforcement and penalties for non-compliance.

The General Data Protection Regulation (GDPR) in the EU is a comprehensive framework that sets a global benchmark for privacy laws. Its key features include:

(1) Standardized Communication: GDPR promotes the use of standardized icons and abbreviations to enhance user understanding of data collection processes.

(2) Informed Consent: It strengthens requirements for informed consent, mandating that data controllers and processors clearly explain the necessity of collecting health data, including legal or contractual obligations and potential consequences of non-disclosure.

(3) Data Management Guidelines: GDPR establishes stringent rules for the collection, storage, and transfer of personal data, ensuring robust data handling practices.

(4) Data Protection Impact Assessments (DPIAs): For high-risk processing activities, organizations are required to conduct DPIAs to identify and mitigate potential risks to individuals' rights and freedoms. Breach Notification: Organizations must report data breaches to supervisory authorities within 72 hours, regardless of their scale, to promote transparency and accountability [34].

(5) Data Protection Officer (DPO): The regulation mandates the appointment of a DPO for many organizations, serving as an independent liaison between data subjects and authorities to ensure compliance [35].

(6) Severe Penalties: Non-compliance can result in hefty fines—up to 2% of global annual revenue or €10 million (USA $11.25 million) for minor breaches, and up to 4% or €20 million (USA $22.50 million) for major breaches—emphasizing the importance of adhering to GDPR standards [36].

Overall, GDPR not only enhances individual privacy rights but also inspires similar regulations globally, such as China's PIPL and Singapore's Personal Data Protection Act (PDPA).

5. Recommendations for Data Safety in the Future

Data protection regulations and actions must evolve rapidly to keep pace with the evolving trend. Inconsistencies exist within different regulations. Some existing frameworks, like Health Insurance Portability and Accountability Act (HIPAA) (nearly 30 years old), are also criticized for failing to address data in digital health applications. EMH providers must immediately strengthen safeguards and implement robust privacy protocols. Key recommendations for essential future action are illustrated in Fig. 1 and outlined as follows.

5.1 Establish a Governance Body

Create a dedicated governance body, to establish and regularly update privacy regulations. The governance body should ideally to be national, supplemented by sub-levels, and Companies are also suggested to have their own. It could be potentially integrated with AI oversight, for example under Hong Kong's "artificial intelligence (AI) Model Personal Data Protection Framework" [37]. The body should also provide training and education, beside monitor regulation compliance and impact. Overall, it should facilitate cross-sector cooperation between government, industry, and healthcare stakeholders, and further provide insights for further actions and research.

5.2 Develop a Proactive Data Breach Protocol

Implement a proactive approach to privacy risk management, incorporating strategies from Privacy by Design (PbD) [38] and National Institute of Standards and Technology privacy framework (NIST) [39]. Along with a robust response plan for data breaches, it should establish clear protocols for identifying data processing roles, data types, and individual privacy needs. Beyond traditional privacy frameworks, consider implementing AI-powered systems

Table 1. Important data protection regulations/enactments globally.

Enactment date	Law/Regulation	Country/Region	Promulgating authority
1 July 1983	Privacy Act	Canada	The Parliament of Canada
13 April 2000	Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada	The Parliament of Canada
12 December 1988	The Privacy Act 1988 (Privacy Act)	Australia	The Australian Parliament
21 August 1996	The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA)	USA	The United States Congress
30 May 2003	Act on the Protection of Personal Information (APPI)	Japan	Japanese Government
15 October 2012	The Personal Data Protection Act (PDPA)	Singapore	Parliament of Singapore
25 May 2018	The European Union General Data Protection Regulation (EU GDPR)	European Union	European Parliament and Council of the European Union
25 May 2018	Data Protection Act 2018	UK	Parliament of the United Kingdom
13 September 2018	The California Consumer Privacy Act (CCPA)	USA	California State Legislature
20 August 2021	The Personal Information Protection Law (PIPL)	China	Standing Committee of the National People's Congress
9 March 2022	The Personal Data Protection Act (PDPA)	Sri Lanka	The Parliament of Sri Lanka

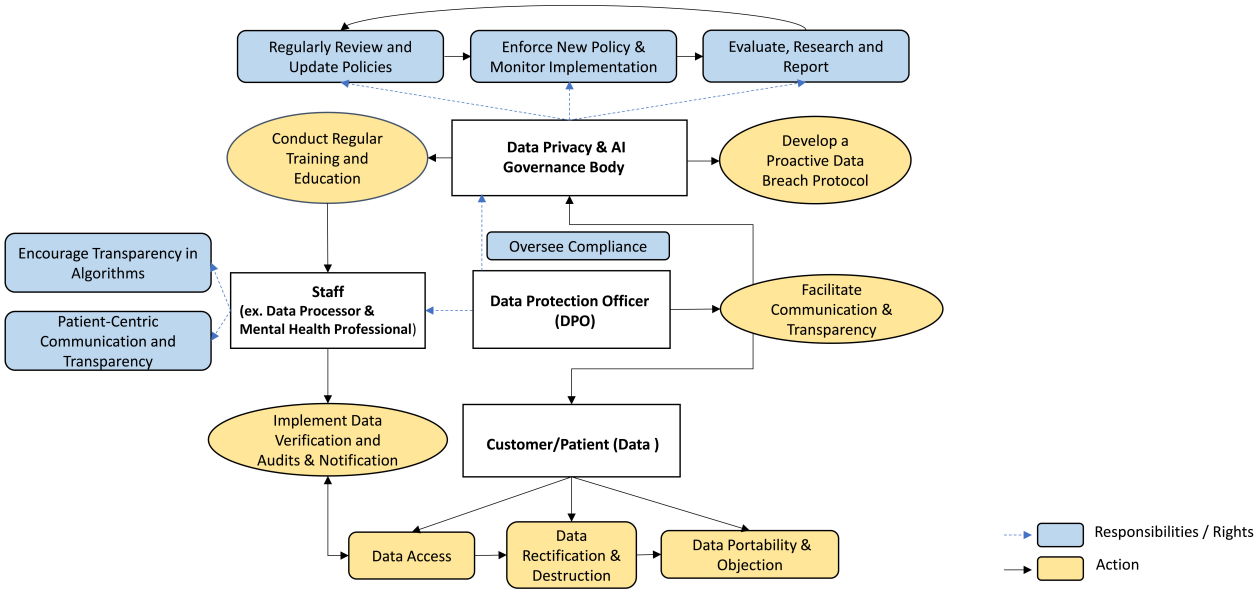

Fig. 1. Key recommendations for data safety governance.

that can dynamically identify, predict, and respond to potential data breaches or privacy risks. By utilizing machine learning models, these systems could analyse patterns in data access and usage to proactively flag unusual activities before they result in a breach.

5.3 Appoint a Data Protection Officer (DPO)

Designate a DPO to oversee compliance and transparency, facilitate clear communication between management and staff (such as mental health professionals), and

address gaps in existing data protection plans. This role is critical for promoting a culture of accountability. The DPO should establish collaborative efforts across healthcare, technology, and regulatory sectors to develop unified standards for AI security in mental health care. These standards should focus on both the ethical use of AI and robust technical safeguards to prevent malicious AI manipulation or misuse.

5.4 Implement Data Verification and Audits

Ensure that patient consent, with terms easy to be understood, is prioritized throughout the data lifecycle. Establish verification procedures for data accuracy and conduct regular audits to maintain data integrity. Allow patients to update and modify their information, thereby enhancing autonomy and personalized mental health care.

5.5 Patient-Centric Communication and Transparency

Foster trust by maintaining open lines of communication with patients regarding data processing practices and respecting their rights to decline unwanted data transmission or access. Promote transparency in AI algorithms used in the care, allowing patients and stakeholders to understand how their data is utilized and the rationale behind AI-driven decisions. Keep patients informed about EMH care and solicit their feedback to align practices with their preferences and needs. Additionally, utilize blockchain technology to provide patients with full control over their data. Blockchain could facilitate secure, transparent, and immutable records of patient consent for data sharing, ensuring that users retain control over their mental health data at all times. This approach would enhance transparency and trust in digital mental health services and AI algorithms.

5.6 Provide User-friendly Procedures of Data Destruction

Furthermore, organizations should pay some attention to Ethical Implications of Data Destruction. Implement guidelines that balance patients' right to delete their data with the clinical and legal responsibilities of healthcare providers. While patients should be able to erase data, this must not compromise the integrity of ongoing care, especially when the data is necessary for treatment or legal reasons. Legally, patients should be informed of their right to request the destruction of their data, and the systems managing mental health records should provide clear, user-friendly processes for data deletion requests.

5.7 Conduct Regular Training and Education

Mandate ongoing training for all stakeholders involved, especially data processors (e.g., IT staff) and mental health professionals, on data privacy and security, emphasizing the protection of PHI and recognizing security threats. This is crucial for building a knowledgeable workforce that prioritizes data protection. Additionally, educational activities should be conducted to enhance the public's awareness and knowledge on this.

5.8 Regularly Review and Update Policies

Establish a framework for periodic review of data protection policies to adapt to emerging technologies and regulatory changes, ensuring ongoing compliance and relevance.

6. Conclusion

Mental healthcare needs are rising rapidly. EMH has proven to be a transformative solution, with a promising future on the horizon. Tackling privacy concerns is a critical first step to propel EMH services to greater heights. However, it demands unwavering commitment from all relevant stakeholders to vouch for it. Collaborative efforts from all key stakeholders is essential. Now is the time to take decisive action to protect sensitive information and build trust in this vital service.

Author Contributions

Conception–HZ, YM, YL, DZ; Design–HZ, YM, YL, DZ; Supervision–DZ; Literature Review–HZ, DZ; Writing–HZ, YM, YL, DZ; Critical Review–HZ, YM, YL, DZ. All authors read and approved the final manuscript. All authors have participated sufficiently in the work and agreed to be accountable for all aspects of the work.

Ethics Approval and Consent to Participate

Not applicable.

Acknowledgment

Not applicable.

Funding

This research received no external funding.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Institute for Health Metrics and Evaluation. Research and analysis-mental health. 2021. Available at: https://www.healthdata.org/research-analysis/health-risks-issues/mental-health (Accessed: 14 November 2024).

[2] Sadeniemi M, Almeda N, Salinas-Pérez JA, Gutiérrez-Colosía MR, García-Alonso C, Ala-Nikkola T, *et al*. A Comparison of Mental Health Care Systems in Northern and Southern Europe: A Service Mapping Study. International Journal of Environmental Research and Public Health. 2018; 15: 1133. https://doi.org/10.3390/ijerph15061133.

[3] Anthes E. Mental health: There's an app for that. Nature. 2016; 532: 20–23. https://doi.org/10.1038/532020a.

[4] Bolinski F, Boumparis N, Kleiboer A, Cuijpers P, Ebert DD, Riper H. The effect of e-mental health interventions on academic performance in university and college students: A meta-analysis of randomized controlled trials. Internet Interventions. 2020; 20: 100321. https://doi.org/10.1016/j.invent.2020.100321.

[5] Linardon J, Torous J, Firth J, Cuijpers P, Messer M, Fuller-Tyszkiewicz M. Current evidence on the efficacy of mental health smartphone apps for symptoms of depression and anxiety. A meta-analysis of 176 randomized controlled trials. World Psychiatry: Official Journal of the World Psychiatric Association (WPA). 2024; 23: 139–149. https://doi.org/10.1002/wps.21183.

[6] Linardon J, Shatte A, Messer M, Firth J, Fuller-Tyszkiewicz M. E-mental health interventions for the treatment and prevention of eating disorders: An updated systematic review and meta-analysis. Journal of Consulting and Clinical Psychology. 2020; 88: 994–1007. https://doi.org/10.1037/ccp0000575.

[7] Carolan S, Harris PR, Cavanagh K. Improving Employee Well-Being and Effectiveness: Systematic Review and Meta-Analysis of Web-Based Psychological Interventions Delivered in the Workplace. Journal of Medical Internet Research. 2017; 19: e271. https://doi.org/10.2196/jmir.7583.

[8] Myers KM, Valentine JM, Melzer SM. Feasibility, acceptability, and sustainability of telepsychiatry for children and adolescents. Psychiatric Services (Washington, D.C.). 2007; 58: 1493–1496. https://doi.org/10.1176/ps.2007.58.11.1493.

[9] Narasimhan M, Druss BG, Hockenberry JM, Royer J, Weiss P, Glick G, *et al*. Impact of a Telepsychiatry Program at Emergency Departments Statewide on the Quality, Utilization, and Costs of Mental Health Services. Psychiatric Services (Washington, D.C.). 2015; 66: 1167–1172. https://doi.org/10.1176/appi.ps.201400122.

[10] Diel A, Schröter IC, Frewer AL, Jansen C, Robitzsch A, Gradl-Dietsch G, *et al*. A systematic review and meta analysis on digital mental health interventions in inpatient settings. NPJ Digital Medicine. 2024; 7: 253. https://doi.org/10.1038/s41746-024-01252-z.

[11] Myers KM, Lieberman D. Telemental health: responding to mandates for reform in primary healthcare. Telemedicine Journal and E-health: the Official Journal of the American Telemedicine Association. 2013; 19: 438–443. https://doi.org/10.1089/tmj.2013.0084.

[12] Lee K, Lee TC, Yefimova M, Kumar S, Puga F, Azuero A, *et al*. Using digital phenotyping to understand health-related outcomes: A scoping review. International Journal of Medical Informatics. 2023; 174: 105061. https://doi.org/10.1016/j.ijmedinf.2023.105061.

[13] Melcher J, Hays R, Torous J. Digital phenotyping for mental health of college students: a clinical review. Evidence-based Mental Health. 2020; 23: 161–166. https://doi.org/10.1136/ebmental-2020-300180.

[14] Omarov B, Zhumanov Z, Gumar A, Kuntunova L. Artificial Intelligence Enabled Mobile Chatbot Psychologist using AIML and Cognitive Behavioral Therapy. International Journal of Advanced Computer Science and Applications. 2023; 14: 137–146.

[15] López Del Hoyo Y, Elices M, Garcia-Campayo J. Mental health in the virtual world: Challenges and opportunities in the metaverse era. World Journal of Clinical Cases. 2024; 12: 2939–2945. https://doi.org/10.12998/wjcc.v12.i17.2939.

[16] Fisher CB, Fried AL. Internet-mediated psychological services and the American Psychological Association ethics code. Psychotherapy: Theory, Research, Practice, Training. 2003; 40: 103.

[17] Lal S, Adair CE. E-mental health: a rapid review of the literature. Psychiatric Services (Washington, D.C.). 2014; 65: 24–32. https://doi.org/10.1176/appi.ps.201300009.

[18] Mol M, van Genugten C, Dozeman E, van Schaik DJF, Draisma S, Riper H, *et al*. Why Uptake of Blended Internet-Based Interventions for Depression Is Challenging: A Qualitative Study on Therapists' Perspectives. Journal of Clinical Medicine. 2019; 9: 91. https://doi.org/10.3390/jcm9010091.

[19] Mental Health Commission of Canana. E-Mental Health. 2024. Available at: https://mentalhealthcommission.ca/what-we-do/e-mental-health/ (Accessed: 14 November 2024).

[20] Lal S. E-mental health: Promising advancements in policy, research, and practice. Healthcare Management Forum. 2019; 32: 56–62. https://doi.org/10.1177/0840470418818583.

[21] Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: a review and recommendations. Journal of Medical Systems. 2015; 39: 181. https://doi.org/10.1007/s10916-014-0181-3.

[22] De-identification of Protected Health Information: How to Anonymize PHI. 2021–2024. Available at: https://www.hipaajournal.com/de-identification-protected-health-information/ (Accessed: 14 November 2024).

[23] Grover S, Sarkar S, Gupta R. Data Handling for E-Mental Health Professionals. Indian Journal of Psychological Medicine. 2020; 42: 85S–91S. https://doi.org/10.1177/0253717620956732.

[24] Elhai JD, Hall BJ. How secure is mental health providers' electronic patient communication? An empirical investigation. Professional Psychology: Research and Practice. 2015; 46: 444.

[25] Lustgarten SD. Emerging ethical threats to client privacy in cloud communication and data storage. Professional Psychology: Research and Practice. 2015; 46: 154.

[26] Wrape ER, McGinn MM. Clinical and Ethical Considerations for Delivering Couple and Family Therapy via Telehealth. Journal of Marital and Family Therapy. 2019; 45: 296–308. https://doi.org/10.1111/jmft.12319.

[27] Opoku Asare K, Terhorst Y, Vega J, Peltonen E, Lagerspetz E, Ferreira D. Predicting Depression From Smartphone Behavioral Markers Using Machine Learning Methods, Hyperparameter Optimization, and Feature Importance Analysis: Exploratory Study. JMIR MHealth and UHealth. 2021; 9: e26540. https://doi.org/10.2196/26540.

[28] Fried EI, Proppert RKK, Rieble CL. Building an Early Warning System for Depression: Rationale, Objectives, and Methods of the WARN-D Study. Clinical Psychology in Europe. 2023; 5: e10075. https://doi.org/10.32872/cpe.10075.

[29] Baumeister H, Montag C. Digital Phenotyping and Mobile Sensing - New Developments in Psychoinformatics. Springer International Publishing: Basel. 2019.

[30] Torous J, Kiang MV, Lorme J, Onnela JP. New Tools for New Research in Psychiatry: A Scalable and Customizable Platform to Empower Data Driven Smartphone Research. JMIR Mental Health. 2016; 3: e16. https://doi.org/10.2196/mental.5165.

[31] Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Medical Ethics. 2021; 22: 122. https://doi.org/10.1186/s12910-021-00687-3.

[32] Filkins BL, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, *et al*. Privacy and security in the era of digital health: what should translational researchers know and do about it? American Journal of Translational Research. 2016; 8: 1560–1580.

[33] McKeon J. Biggest Healthcare Data Breaches Reported This Year, So Far. 2023. Available at: https://www.techtarget.com/healthtechsecurity/feature/Biggest-Healthcare-Data-Breaches-Reported-This-Year-So-Far (Accessed: 14 November 2024).

[34] HIPAA vs. GDPR compliance: what's the difference? 2022. Available at: https://www.onetrust.com/blog/hipaa-vs-gdpr-compliance/ (Accessed: 14 November 2024).

[35] General Data Protection Regulation (GDPR).EU. Art. 39 GDPR Tasks of the data protection officer. 2024. Available at: https://gdpr.eu/article-39-tasks-of-the-data-protection-officer/ (Accessed: 14 November 2024).

[36] Yuan B, Li J. The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. International

Journal of Environmental Research and Public Health. 2019; 16: 1070. https://doi.org/10.3390/ijerph16061070.

[37] Privacy Commissioner's Office Publishes "Artificial Intelligence: Model Personal Data Protection Framework". 2024. Available at: https://www.pcpd.org.hk/english/news_events/media_statements/press_20240611.html (Accessed: 14 November 2024).

[38] Bu F, Wang N, Jiang B, Liang H. "Privacy by Design" implementation: Information system engineers' perspective. International Journal of Information Management. 2020; 53: 102124.

[39] NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0. 2020. Available at: https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf (Accessed: 14 November 2024).