REGULATORY REQUIREMENTS AND CYBERSECURITY RISKS IN DIGITAL HEALTH APPLICATIONS: A COMPARATIVE STUDY OF SOUTH KOREA AND CANADA

[1] Gopinath P *, [1] S. Kavibharathi, [2] Jaganathan K, [3]Senthil Kumar N

[1]Department of Pharmaceutics, JKKMMRF's Annai JKK Sampoorani Ammal College of Pharmacy, Tamil Nadu, India
[2]Department of Pharmaceutics, JKKMMRF's Annai JKK Sampoorani Ammal College of Pharmacy, Tamil Nadu, India
[3]Principal, JKKMMRF's Annai JKK Sampoorani Ammal College of Pharmacy, Tamil Nadu, India

***Corresponding Author** Gopinath P Department of Regulatory Affairs, JKKMMRF's Annai JKK Sampoorani Ammal College of Pharmacy, Tamil Nadu, India Phone: + 91 9025047834 Email: gopinath04633@gmail.com

ABSTRACT

This study provides a comparative analysis of cybersecurity risks and mitigation strategies for digital health applications in South Korea and Canada, highlighting how two leading digital health economies respond to evolving cyber threats. South Korea faces sophisticated, state-sponsored threats, necessitating a centralized, proactive national security approach. Its prescriptive Digital Medical Products Act (DMPA) and investment in resilient infrastructure exemplify a unified, security-first ecosystem. In contrast, Canada contends with decentralized, financially motivated ransomware attacks that exploit supply chain vulnerabilities, causing operational disruption and directly affecting patient care. Canada's multi-jurisdictional regulatory framework and reliance on external cloud services exacerbate data sovereignty risks. The analysis emphasizes that effective cybersecurity extends beyond technical measures, requiring strategic, policy-driven approaches. South Korea's model demonstrates the benefits of centralized oversight and prescriptive regulation, whereas Canada's fragmented system remains vulnerable to systemic failure without urgent reforms. The study concludes that Canada must implement unified standards, enforce foundational security controls, and address data sovereignty challenges. For both nations, continuous investment in AI-driven defensive technologies is essential to counter emerging threats, safeguard patient data, and maintain trust in digital health ecosystems.

Keywords: Cybersecurity, Digital Health, Data Sovereignty, Centralized Regulation, Ransomware, AI-driven Defense.

1. INTRODUCTION

1.1 Overview of Digital Health Applications (DHAs)

Digital Health Applications (DHAs) encompass a broad range of technologies mobile health apps, connected wearables, cloud-based platforms, AI-enabled diagnostic tools, and software-as-a-medical-device (SaMD) designed to support disease prevention, diagnosis, monitoring, and therapeutic management [1-3]. Their rapid expansion is driven by advances in connectivity, artificial intelligence, miniaturized sensors, and widespread smartphone adoption. DHAs now play a central role in modern healthcare systems through telemedicine, virtual monitoring, electronic health records, and digital therapeutics (DTx), offering convenient, personalized, and data-driven care pathways [4-7].

Regulatory agencies globally, including Health Canada, MFDS (South Korea), FDA (U.S.), and EMA (EU), increasingly recognize DHAs as critical components of healthcare delivery, requiring robust oversight to ensure safety, performance, data protection, and cybersecurity [1,5,12]. Evolving legislative frameworks such as Canada's PIPEDA and PHIPA, and South Korea's Digital Medical Products Act (DMPA), are examples of regulatory modernization supporting innovation while safeguarding patient rights [8,11,13,15].

1.2 Categories of Digital Health Technologies

1.2.1 Mobile Health (mHealth) and Wellness Applications

These include fitness trackers, diet apps, step counters, menstrual-cycle trackers, and mental-wellbeing apps that assist users in health management but generally do not provide clinical intervention [2,3].

1.2.2 Software as a Medical Device (SaMD)

SaMD refers to stand-alone software intended for medical purposes such as diagnosis, monitoring, or treatment [5,6]. It includes AI-enabled clinical decision-support systems, digital therapeutics, and algorithms for imaging analysis [12].

1.2.3 Telemedicine and Virtual Care Platforms

Telehealth systems allow remote consultations, remote patient monitoring (RPM), and real-time physiological data transfer [2,5]. With expanding interoperability standards such as HL7, FHIR, SNOMED-CT, and LOINC, telemedicine has become increasingly integrated into national EHR ecosystems [4,30].

1.2.4 AI-Enabled Digital Health Technologies

AI-driven digital therapeutics, predictive analytics tools, generative AI medical applications,

and automated decision-support systems are increasingly used to enhance diagnostic accuracy and clinical workflow efficiency [14,28]. Real-world evidence (RWE) is now recognized as a critical component for ongoing evaluation of such technologies under emerging legislation like South Korea's DMPA [15,27].

1.3 Data Privacy and Regulatory Protection in Digital Health

1.3.1 Canadian Framework: PIPEDA and Provincial Health Privacy Laws

PIPEDA governs the collection, use, and disclosure of personal information in commercial activities across Canada, including health data, and incorporates the Canadian Standards Association's Model Code for privacy protection [11,17]. Several provinces, including Ontario, Alberta, Quebec, and British Columbia, have "substantially similar" privacy laws that supersede PIPEDA at the provincial level, such as PHIPA in Ontario [29,39].

PIPEDA grants individuals the right to understand how their personal information is used, access their data, request corrections, and file complaints [11,17]. The Digital Privacy Act amendment strengthened breach notification requirements and enhanced the Privacy Commissioner's oversight role [11].

1.3.2 South Korea: The Personal Information Protection Act (PIPA)

PIPA is one of the world's most stringent privacy laws, classifying health data as "sensitive information" requiring explicit consent or statutory justification [13,21,36]. Amendments in 2023 introduced data portability (MyData), harmonized online/offline regulations, and expanded lawful cross-border transfer provisions [13,21]. Pseudonymized data may be used for scientific research without explicit consent under strict safeguards, enabling AI model development in healthcare [14,41,45].

1.4 Cybersecurity Risks in Digital Health

Digital health ecosystems process highly valuable personal health information, making them prime targets for cyberattacks [16,19,22,31,32]. Health data is one of the most lucrative black-market commodities, reaching $10 per record, and 44% of data breaches now involve medical data [48]. Large-scale breaches such as Anthem's attack affecting 80 million individuals highlight the magnitude of the threat [49].

1.4.1 Common Cyber Threats in Digital Health Systems

Digital health applications especially those integrating cloud services, IoT devices, and interoperability standards are vulnerable to multiple threats [16,18,40,50-53]:
Digital health systems face critical risks including data breaches, ransomware extortion, and unauthorized access from weak or stolen credentials. Unpatched software, insecure data storage or transmission, and weak authentication further expose sensitive information. Technical flaws

such as injection attacks, XSS, IDOR, and SSRF create additional entry points for attackers. Cloud misconfigurations also remain a major source of accidental health data exposure.

Penetration testing results show an average of 7 vulnerabilities per health application, with at least one high-severity flaw, making robust cybersecurity governance essential [47].

1.4.2 Interoperability-Related Cybersecurity Risks (HL7, FHIR, DICOM)

Healthcare systems use protocols such as HL7, FHIR, and DICOM to exchange medical information [4,30]. However:

- Older HL7 versions transmit data in plaintext.
- FHIR's RESTful architecture exposes APIs to SQL injection, MITM attacks, and cross-site vulnerabilities.
- Misconfigured authentication and authorization can allow unauthorized EHR access.

These weaknesses increase the risk of manipulation, data exfiltration, and patient safety incidents [18,31,40].

1.5 Importance of Post-Market Surveillance in Digital Health

For high-risk DHAs and SaMDs, continuous monitoring is crucial due to frequent software updates, AI model drift, and evolving cybersecurity threats [5,15,27,41]. Countries such as Canada and South Korea integrate mandatory incident reporting, recall mechanisms, update oversight, and real-time threat monitoring into regulatory frameworks [5,15].

1.6 Summary of the Digital Health Landscape

Digital health technologies offer transformative benefits improved accessibility, personalized care, real-time monitoring, and enhanced clinical support [2,3,5]. However, the expansion of digital ecosystems introduces new privacy, safety, and cybersecurity challenges that require coordinated responses from regulators, developers, and healthcare institutions [16,18,19]. A clear understanding of risks, governance frameworks, and regulatory expectations is essential for developing secure, interoperable, and patient-centered digital health solutions [5,11,14].

2. Materials and Methods

2.1. Study Design

A descriptive, comparative, and thematic analysis design was used to evaluate the regulatory, quality, and cybersecurity frameworks applicable to Digital Health Applications (DHAs) in Canada and South Korea. The approach emphasized structured extraction of regulatory requirements, classification rules, quality system obligations, and data-protection legislation, followed by systematic cross-jurisdictional comparison [5,12,15].

2.2. Data Sources

Data were obtained from official regulatory documents (Health Canada, MFDS) [5,12], international frameworks (IMDRF, ISO/IEC standards) [7,41], legislative acts (PIPEDA, PHIPA, PIPA) [11,13,29], scientific publications, cybersecurity advisories, and digital health policy reports [20,27,44].

2.3. Data Collection and Extraction

Documents were screened and categorized into predefined domains: regulatory definitions, SaMD classification, licensing pathways, quality management obligations, data protection laws, cybersecurity vulnerabilities, and post-market surveillance. Extracted data were coded and mapped into comparative matrices for synthesis.

2.4. Comparative Analysis Framework

A structured framework was applied to compare both jurisdictions across regulatory criteria, risk classification models, documentation requirements, quality management systems, and cybersecurity mandates. Emphasis was placed on risk proportionality, AI-specific policies, and lifecycle regulatory controls [5,12,15].

2.5. Cybersecurity Risk Assessment

Cybersecurity risks were identified using the confidentiality–integrity–availability (CIA) model [16,18,48,50-53]. Vulnerabilities associated with digital health systems including outdated software, weak authentication, injection flaws, XSS, IDOR, misconfigured cloud services, and HL7/FHIR protocol risks were documented [4,18,30]. Threats were mapped against relevant regulatory expectations and international standards (ISO 14971, IEC 62304, IEC 62443).

2.6. Development of Mitigation Strategies

Mitigation strategies were derived from regulatory guidance, cybersecurity standards, and known digital health threat patterns. Strategies focused on secure software development, access control reinforcement, encryption, continuous monitoring, AI-update governance, and lifecycle cybersecurity management [14,41,53].

2.7. Quality Management System Evaluation

Quality requirements for both countries were reviewed. In Canada, ISO 13485 via MDSAP is mandatory for Class II–IV devices [5,6]. In Korea, KGMP certification, aligned with ISO 13485, is required for Class II–IV digital medical products [12,15,41]. Technical dossiers were examined to identify software documentation, risk management files, and cybersecurity plans.

3. Results

3.1. Regulatory Framework Comparison Between Canada and South Korea

The analysis identified clear structural differences and convergences in the regulation of Digital Health Applications (DHAs). Canada regulates DHAs primarily under the Food and Drugs Act and Medical Devices Regulations [5,6,10], with classification aligned to risk (Class I–IV). Software as a Medical Device (SaMD) is increasingly addressed with guidance aligned to IMDRF principles. South Korea regulates under the Digital Medical Products Act (DMPA) and MFDS device framework, also applying a risk-based SaMD classification [12,15,27]. Both countries require comprehensive technical documentation, risk management files, and cybersecurity assurances; however, Korea has more explicit processes for AI-enabled devices, including adaptive algorithm oversight and Real-World Evidence (RWE) integration [14,15,27,41].

Table:1- Comparison of the regulatory and legal frameworks for digital health in South Korea and Canada

Feature	South Korea	Canada
Core Data Privacy Law	Personal Information Protection Act (PIPA)	Personal Information Protection and Electronic Documents Act (PIPEDA) & Provincial Laws (e.g., PHIPA)
Digital Health Specific Legislation	Digital Medical Products Act (DMPA)	Generally Implicit; Industry-Specific Guidelines
Central Certification	Korea Information Security Management System (K-ISMS)	None
Regulatory Philosophy	Centralized, Prescriptive, National Security-Oriented	Decentralized, Principle-Based, Risk-Management Focused
Enforcement & Penalties	High fines, administrative penalties, and criminal liability	Varies by jurisdiction; potential fines and legal action
AI & Emerging Tech	Explicitly addressed in recent amendments and legislation	Governed by broad principles; new legislation in development

3.2 Quality Management Systems and Documentation Requirements

Both jurisdictions mandate quality assurance systems aligned with ISO 13485 [5,6,12,41].

Canada requires MDSAP certification for Class II–IV devices, whereas Korea requires KGMP certification for equivalent risk classes. Documentation expectations in both regions include software architecture, validation files, clinical evidence, and post-market surveillance plans. Korea places additional emphasis on AI algorithm transparency, model update governance, and performance validation using locally relevant datasets [14,41].

3.3 Cybersecurity Risk Landscape in Digital Health Applications

Assessment revealed significant cybersecurity threats across digital health platforms, including mobile apps, cloud-based systems, and hospital-integrated software. Common vulnerabilities included outdated software, weak authentication, insecure API configurations, improper session control, unencrypted data, XSS, SQL injection, IDOR, cloud storage misconfigurations, and protocol-specific risks within HL7 and FHIR. High-severity risks such as unrestricted file upload, server-side request forgery (SSRF), and brute-force login vulnerabilities were found to directly compromise patient data confidentiality and system integrity. Mapping these vulnerabilities to the CIA framework demonstrated a heightened risk of data exposure, ransomware events, and unauthorized manipulation of medical information [4,18,30,50-53].

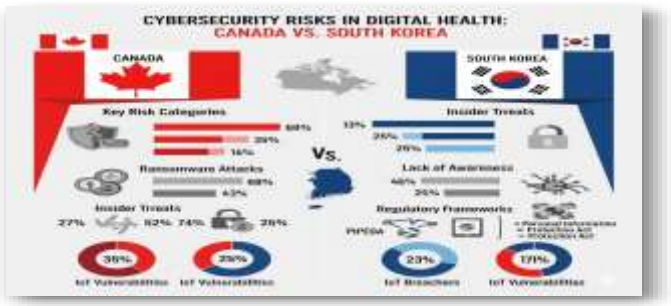

Fig No. 1- A Comparative Analysis of Cybersecurity Risks and Mitigation Strategies for Digital Health Applications: Canada vs. South Korea

3.4 A Comparative Analysis of Cybersecurity Risks and Mitigation Strategies for Digital Health Applications: Canada vs. South Korea

South Korea faces state-sponsored threats and has implemented a centralized, prescriptive framework including PIPA, DMPA, and K-ISMS certification supported by a national cybersecurity strategy. Canada, with a fragmented legal landscape, is primarily exposed to financially motivated ransomware, relying on decentralized, industry-led compliance and business continuity measures. The key distinction is philosophical: South Korea treats cybersecurity as national security, while Canada emphasizes risk management. Both nations must address emerging AI-driven cyber threats through proactive, collaborative defenses to safeguard digital health systems.

3.5 Regulatory Cybersecurity Requirements and Enforcement

Both Canada and South Korea mandate cybersecurity controls but differ in the specificity of enforcement.

- Canada embeds cybersecurity within the Safety and Effectiveness requirements and provides detailed expectations through guidance on software security, patching, and lifecycle management [5,30].
- Korea, under the DMPA and MFDS guidelines, requires explicit cybersecurity validation testing, secure data transmission protocols, and mandatory vulnerability disclosure processes [12,41].

Both countries enforce compliance with international standards (ISO/IEC 27001, ISO 14971, IEC 62304), but Korea's framework includes stricter AI-specific security requirements and continuous monitoring obligations.

3.6 Cybersecurity Threat Profile

Foundational Risks in Digital Health Digital health systems are lucrative targets because PHI has high black-market value. The rapid expansion of interconnected apps, EHRs, wearables, and IoT devices creates a wide attack surface with numerous exploitable vulnerabilities.

South Korea: State-Sponsored Espionage South Korea faces persistent, state-linked attacks mainly from North Korea with over a million daily attempts. These campaigns rely on advanced persistent threats aimed at long-term infiltration and data theft. The 2021 SNUH breach, which exposed data on more than 831,000 individuals, exemplifies espionage-driven motives, requiring a national security–oriented defence posture.

Canada: Financially Motivated Disruption Canada's risk environment mirrors North American trends dominated by ransomware that targets operational disruption. The 2024 Change Healthcare attack demonstrates how compromising a single vendor can cripple healthcare operations. Canada's key vulnerability is supply-chain dependence, making resilience, redundancy, and business continuity essential.

3.7 Market Access, HTA, and Reimbursement Findings

A key finding is the **two-step barrier** faced by manufacturers [5,12,15,27,42]:

1. Regulatory approval (MFDS or Health Canada)
2. Market access and reimbursement (NHIS or Canadian provincial systems)

In Korea, although MFDS approved four digital therapeutics by late 2024 (e.g., Somzz, VIVID Brain), only a subset received reimbursement, highlighting a disconnect between regulatory clearance and clinical adoption.

In Canada, reimbursement pathways remain fragmented due to provincial jurisdiction and lack of dedicated DTx reimbursement policies. Both countries show need for value-based

assessment models tailored to digital therapeutics.

3.8 Use of Real-World Evidence (RWE) in DHA Evaluation

South Korea actively integrates RWE into regulatory evaluation, enabling iterative product improvement and post-market validation [15,27,41]. Canada recognizes RWE within its regulatory modernization framework but lacks DHA-specific implementation pathways [5,7]. Korea's approach was found to be more mature, supported by structured data infrastructures and explicit MFDS guidance.

3.9 Post-Market Surveillance Requirements

Post-market obligations in both countries emphasize continuous safety monitoring and mandatory reporting of adverse events. Korea adopts a full lifecycle management model, requiring ongoing AI performance tracking [14,15,41], cybersecurity monitoring, and routine updates. Canada requires adverse event reporting and field safety corrective actions but does not yet mandate AI-specific performance monitoring [5,7].

3.10 Mitigation Strategy Development Based on Results

Analysis of identified risks and regulatory requirements informed the development of targeted mitigation strategies, including [11,13,16,18,29,34,41,43,48,53]:

- Implementation of robust authentication protocols and role-based access control
- Encryption of data in transit and at rest & Threat modelling and secure SDLC integration
- Periodic vulnerability scanning and penetration testing
- AI algorithm change management plans & Cloud security hardening and logging mechanisms
- Compliance with ISO/IEC cybersecurity standards and national privacy laws (PIPEDA, PHIPA, PIPA)

These results demonstrate alignment between regulatory expectations and practical cybersecurity safeguards required for safe DHA deployment.

Fig No. 2- Cybersecurity mitigation strategies in Digital Health

4. CONCLUSION

Cybersecurity in digital health systems is complex and requires a strategic, proactive approach rather than a purely compliance-driven mindset. South Korea exemplifies a security-first model, with a unified ecosystem that builds resilience against state-level threats through prescriptive regulations and coordinated defense. In contrast, Canada faces challenges from systemic fragmentation and data sovereignty risks, necessitating urgent implementation of essential security measures such as multi-factor authentication, robust backups, and standardized data protocols to protect patient care from financially motivated ransomware attacks. Both countries must invest strategically in AI-driven defenses to address emerging cyber threats and ensure the safety, integrity, and trustworthiness of their digital health ecosystems.

5. References

1. U.S. Food and Drug Administration (FDA). Digital health overview. Available from: https://www.fda.gov/medical-devices/digital-health-center-excellence/whatdigitalhealth
2. Landa C, Lin SY. Wireless medical devices and their role in remote health monitoring. J Biomed Inform. 2020;108:103500.
3. Zhang Y, et al. Wireless technology in digital health: Current trends and challenges. Sensors. 2021;21(12):3980.
4. Armitage D, et al. Cybersecurity risks in wireless medical devices: A regulatory perspective. Front Digit Health. 2022;4:841233.
5. Health Canada. Software as a medical device—guidance document. Available from: https://www.canada.ca
6. PharmaInBrief. Health Canada provides guidance on regulation of SaMD. 2020.
7. DIA Global Forum. Regulatory challenges of software as a medical device. 2019.
8. Dicentra. How digital health is regulated in Canada.
9. National Center for Biotechnology Information. PMC article PMC917005. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC917005
10. Torys LLP. Software as medical devices and digital health in Canada. 2018.
11. Personal Information Protection and Electronic Documents Act (PIPEDA). Official guide on personal data protection and digital health in Canada. Government of Canada; 2021. Available from: https://www.priv.gc.ca
12. Ministry of Food and Drug Safety (MFDS). Digital health and SaMD regulatory information. Available from: https://www.mfds.go.kr/eng/wpge/m_39/de011026l001.do
13. Personal Information Protection Act (PIPA). Data Protection Act of South Korea. Available from: https://www.google.com/search?q=Data+Protection%3A+The+Personal+Information+Protection+Act+(PIPA)
14. Lee Y, Choi H. Cybersecurity in South Korea’s digital health landscape: Current issues and future challenges. J Cybersecurity Health. 2022;9(3):45–60.

15. Korean Ministry of Health. The Digital Medical Products Act (DMPA). Available from: https://www.google.com/search?q=The+Digital+Medical+Products+Act+(DMPA)
16. American Hospital Association. Change Healthcare cyberattack underscores need to strengthen cyber preparedness. 2025.
17. AccountableHQ. All About PIPEDA: Canada's version of HIPAA. Available from: https://www.accountablehq.com
18. Blaze Information Security. Cybersecurity risks in digital health apps. Available from: https://www.blazeinfosec.com/post/cybersecurity-risks-digital-health-apps/
19. Canadian Centre for Cyber Security. Cyber security best practices for Canadian healthcare organizations. Government of Canada; 2020.
20. Center for Strategic and International Studies (CSIS). South Korea's 2024 Cyber Strategy: A Primer. 2024.
21. Chambers and Partners. Data Protection & Privacy 2025: South Korea. 2025.
22. Cluley G. Cancer treatments cancelled after Canadian hospitals hit by ransomware attack. Bitdefender Hot for Security. 2023.
23. Competition Bureau Canada. Unlocking the power of health data. Government of Canada.
24. Council on Foreign Relations. Targeting of South Korean hospital network. 2023.
25. EurekAlert!. Canadian health data security and CLOUD Act commentary. 2025.
26. FirstWord HealthTech. Canadians' health data at risk due to CLOUD Act. 2025.
27. Frankel M. Introducing Korea's Digital Medical Products Act (DMPA). 2025.
28. Georgetown Journal of International Affairs. AI and cybersecurity in digital warfare on the Korean Peninsula. 2024.
29. Google Cloud. PHIPA Canada compliance.
30. Health Canada. Guidance: Pre-market requirements for medical device cybersecurity. 2019.
31. IBM. Canadians' data security under increased threat—2025 Cost of a Data Breach Report. 2025.
32. Swiss Cyber Institute. Lessons learned: LifeLabs data breach. 2021.
33. Korea Health Promotion Institute. AI and IoT healthcare project for senior citizens. 2024.
34. Korea Internet & Security Agency (KISA). K-ISMS certification.
35. Korean National Police Agency / Secure Blink. North Korean hackers attack Seoul Hospital. 2023.
36. Linklaters. South Korea data protection and PIPA. 2024.
37. Ministry of Science and ICT. Digital New Deal. 2020.
38. Norton Rose Fulbright. Digital Health 2024: Canada. 2024.
39. OutsideGC. Quebec's Privacy Law 25. 2025.
40. PwC Canada. Cybersecurity risk insights—Global Digital Trust Survey. 2024.
41. QualTechs. Korea DMPA and mandatory cybersecurity. 2025.
42. Royal College of Physicians and Surgeons of Canada. Breaking down digital barriers. 2025.

43. Seoul National University Hospital. Cloud-based disaster recovery centre (BESTBunker). 2025.
44. Spherical Insights & Consulting. South Korea digital healthcare market forecast to 2035. 2024.
45. Verasafe. South Korea PIPA compliance: Security and encryption.
46. Appari A, Johnson ME. Information security and privacy in healthcare: Current state of research. NIST/U.S. Dept of Commerce; 2008.
47. Stanley N, Coderre M. An introduction to medical device cybersecurity. 2015.
48. Tschider CA. Enhancing cybersecurity for the digital health marketplace. Ann Health Law. 2017;26(1):1. Available from: https://lawecommons.luc.edu/annals/vol26/iss1/3
49. Corman J, DeCesare G. Health Care Industry Cybersecurity Task Force. 2017.
50. Agrawal R, Evfimievski A, Srikant R. Information sharing across private databases. Proc ACM SIGMOD. 2003.
51. Alberts CJ, Dorofee A. Managing information security risks: An OCTAVE approach. Boston: Addison-Wesley; 2002.
52. Hong Y, Lu S, Liu Q, Wang L, Dssouli R. A hierarchical approach to the specification of privacy preferences. Int Conf Innovations Inf Technol. 2007.
53. Hu VC, Ferraiolo DF, Kuhn DR. Assessment of access control systems. NIST Report 7316. 2006.
54. Hung PCK. Towards a privacy access control model for e-healthcare services. Proc Annual Conf Privacy Security Trust. 2004.
55. Hyman DA. HIPAA and healthcare fraud: An empirical perspective. Cato J. 2002;22(1):151–78.
56. Government of Canada. Cybersecurity for healthcare organizations: Protecting against common cyber attacks (ITSAP.00.131).