Information Security, Cybersecurity and Personal Data Protection Governance Policy

Praram 9 Hospital Public Company Limited

1. Policy Statement

Praram 9 Hospital Public Company Limited (the "Company" or the "Hospital") places the utmost importance on the governance of information security, cybersecurity, personal data protection and continuity of medical services. Health information, patient information, personnel data, business information and the Hospital's information technology systems are critical assets that directly affect patient safety, quality of service, stakeholder confidence and business continuity.

This Policy is established as a public disclosure framework for the management of information security and cybersecurity risks. It is based on the Hospital's internal policies and programs, including the Cybersecurity Policy, Information Management and Data Security Policy, Information Technology System Security Policy and Response for Cyberattack Program.

The Hospital's internal policies require appropriate cybersecurity measures, an annual cybersecurity risk assessment and at least one annual test of the relevant response plans. The scope covers employees, contractors, third parties and all information technology systems of the Hospital.

2. Scope of Policy

This Policy covers the governance and management of the following key areas:

1) Information security.
2) Cybersecurity.
3) Protection of personal data and patient health information.
4) Access control for information and information systems.
5) Data classification and confidentiality management.
6) Data backup, data recovery and continuity of services.
7) Management of external service providers and third parties involved in information systems.
8) Monitoring, inspection and response to information security incidents.
9) Employee training and awareness.
10) Continuous policy review and improvement.

3. Governance Principles

The Hospital requires information security and cybersecurity governance to be integrated into its enterprise risk management system. Roles, duties and responsibilities are appropriately assigned to management, the Information Technology function, the Quality function, personnel, service providers and relevant third parties.

The Hospital monitors domestic and international cyber threat situations, as well as technological developments, in order to assess risks and continuously improve preventive measures. Internal policies also define the roles of relevant management and committees in acknowledging policies, monitoring situations and providing recommendations to hospital management on cybersecurity matters.

4. Information Security and Cybersecurity Risk Management

The Hospital conducts an information security and cybersecurity risk assessment at least once a year to identify, assess and prioritize risks, and to establish appropriate risk mitigation plans.

Risk management covers risks arising from unauthorized access, data leakage, cyberattacks, disruption of information systems, external service providers, mobile devices and risks that may affect the continuity of patient care services.

The Hospital's Information Management and Data Security Policy requires an annual, organization-wide information security risk assessment, including risk prioritization and the development of risk mitigation plans.

5. Data Classification and Confidentiality

The Hospital establishes a data classification approach based on the importance, sensitivity and legal requirements of the data. This includes patient information, health information, personnel information, financial information, management information, quality data, adverse event data, complaint information and other information related to the Hospital's operations.

Sensitive or confidential information is protected through appropriate measures, such as access restriction, secure storage, designation of authorized approvers, control of disclosure and disposal of information in accordance with prescribed retention periods.

The internal HP-MOI-03 document sets out the Hospital's data classification, including financial information, employee information, quality information, incident reports, patient complaints and information that must be accessible only by relevant authorized persons.

6. Access Control for Information and Information Systems

The Hospital requires access to information and information systems to be controlled on a need-to-use basis and in accordance with the duties and responsibilities of users. Personnel, service providers and third parties are granted access only to the information or systems necessary for their work.

Access rights management covers authorization requests, role-based access assignment, access review, termination of access rights when duties or contracts end, and control of access to critical areas or systems.

The Hospital has physical and information technology access control measures, including requirements for user authentication, password confidentiality and reporting of abnormal system usage.

7. Protection of Personal Data and Patient Information

The Hospital recognizes that personal data and patient health information are highly sensitive. Accordingly, the Hospital implements measures to protect such data in accordance with the Personal Data Protection Act, applicable laws governing medical services and professional ethical principles.

The Hospital is committed to maintaining the confidentiality, accuracy, completeness and availability of patient information. Access is restricted to persons with relevant duties, and appropriate procedures are established for the use, transfer, storage, request, disclosure and disposal of information.

8. Protection of Information Systems and Critical Infrastructure

The Hospital implements preventive and control measures to safeguard information systems, networks, computers, mobile devices, electronic medical record systems, clinical support systems and medical devices connected to the Hospital's information systems.

These measures include network control, malware protection, control of external devices, appropriate data encryption, mobile device security, data backup, system testing and monitoring of abnormal events.

The Hospital's internal policies address the protection of information, networks and medical devices against unauthorized access, cyberattacks and data breaches that may affect patient safety, service continuity and confidentiality.

9. Management of External Service Providers and Third Parties

The Hospital requires external service providers, contractors, system installers, system administrators, maintenance providers and other third parties involved with the Hospital's information systems to comply with the Hospital's requirements on information security, confidentiality and data protection.

Access to the Hospital's systems, information or critical areas by external parties must be subject to authorization, control and recording in accordance with the Hospital's procedures in order to prevent risks arising from unauthorized access to information or systems.

The internal HP-MOI-15 document sets out controls for access to critical areas such as the Data Center. Vendors, system installers, external specialists and other external parties are required to be controlled and their entry and exit recorded as prescribed.

10. Data Backup, Data Recovery and Business Continuity

The Hospital establishes data backup, data recovery and information system disruption response measures to support continuity of patient care services and reduce the impact of unexpected events, such as information system failures, cyber threats, disasters or events affecting system availability.

The Hospital tests and reviews response plans for both planned and unplanned information system downtime at least once a year in order to strengthen readiness and information technology security.

11. Cybersecurity Incident Response

The Hospital has established a Response for Cyberattack Program to ensure clear, timely and healthcare-appropriate procedures. The program focuses on threat containment, impact reduction, continuity of patient services, system recovery and prevention of recurrence.

The Hospital's cybersecurity incident response principles are as follows:

1) Contain and isolate the threat promptly.
2) Activate the information system downtime response plan when necessary.
3) Prioritize patient safety and continuity of medical services.
4) Recover systems and data in accordance with the established plan.
5) Analyze the root cause and vulnerabilities after the incident.
6) Establish preventive measures to avoid recurrence.
7) Review lessons learned after the incident to improve controls.

The Response for Cyberattack Program aims to ensure information system availability, data integrity and business continuity, and to ensure that personnel understand their duties in the event of a cyberattack.

12. Training and Awareness

The Hospital provides training and awareness programs on information security, cybersecurity, appropriate use of information and personal data protection for relevant personnel, both upon onboarding and through periodic refresher training as appropriate.

Training covers the use of information systems, confidentiality of information, cyber threat prevention, awareness of electronic fraud and social engineering, reporting of abnormal events and the role of personnel in protecting patient and hospital information.

The HP-MOI-03 policy requires training on information systems, information security and principles for the use and management of information, including the use of electronic medical records according to each role and responsibility. The training is provided to new personnel and refreshed for existing personnel at least annually.

13. Monitoring, Review and Continuous Improvement

The Hospital requires continuous monitoring, surveillance, inspection and review of information security and cybersecurity measures to ensure that controls remain effective and aligned with changing risks.

The Hospital reviews abnormal events, vulnerability assessments, threat monitoring activities, response plan test results and improvement measures to enhance the effectiveness of its control system.

14. Disclosure and Security Limitations

The Hospital discloses this Policy to demonstrate its governance framework and management approach for information security, cybersecurity and personal data protection to stakeholders.

However, in order to preserve the security of the Hospital's information systems and critical data, the Hospital does not publicly disclose technical details, system architecture, operational incident response procedures, details of backup systems, recovery timelines for individual systems, internal escalation channels, names of operational responsible persons or any other information that may increase the organization's security risk.

15. Policy Review

The Hospital will review this Policy at appropriate intervals or when there are significant changes, including changes in laws, international standards, cybersecurity risks, technology, information systems or governance structure, in order to ensure that the Policy remains appropriate, adequate and effective.