Basic Policy on Information Security

As a group that is engaged in medical care, we place the highest priority on the trust of medical facilities and personnel as well as patients. We have established the basic policy for the information assets that we handle from the viewpoint of confidentiality, integrity, and availability as below.

1. Basic statement

We will properly protect important information assets that are within the scope of the application from all threats, whether intentional or accidental, and achieve our business objectives.

2. Compliance

Recognizing the importance of information security, we abide by the laws, regulations and guidelines that we should comply with, the Articles of Incorporation and the rules of employment that we have established, and the information security-related contracts that we have concluded with parties such as customer medical facilities, patients and concerned external organizations.

3. Responsibilities and duties of the top management

We recognize the appropriate protection of information assets as an important management issue, and allocate the necessary management resources for it.

We understand and comply with the agreement made for the information to be protected with the customer medical facilities, patients and concerned external organizations. Furthermore, we shall make adequate amendments when the content is insufficient for the purpose of the business activities of each party. In this way, we will build mutual trust and prosper together.

We set up the Information Security Liaison Group to establish, introduce, operate, monitor, maintain and improve information security across the Company.

We instruct our employees and concerned departments to follow appropriate standards and implementation procedures under this policy.

4. Responsibilities and duties of employees

We fully understand the importance of compliance with this policy and appropriate protection of information assets, and operate accordingly.

When an accident occurs or an employee finds a vulnerability to a threat, he/she is responsible for immediately reporting to the information system department, regardless of directly or indirectly, and will not act in a way where the risk to the information assets to be protected would be increased.

5. Risk assessment

We assume threats to confidentiality, integrity, and availability of information assets to be protected, and evaluate the vulnerabilities to these threats.

Based on the evaluation, we develop and execute control measures to protect and maintain the confidentiality, integrity and availability of each information asset.

6. Internal audit system

We regularly conduct system audits by the Internal Audit Department to check the status of compliance with this policy.

7. Penalties

When an employee breaches this policy and ends up damaging our information assets, the employee who acted as such will be subject to disciplinary action and legal action.

8. Management review

This policy is reviewed regularly or as required.

Moreover, when this policy is revised, we will review the related rules, procedure manuals, etc.

When this policy is revised, we will confirm the validity of the rules, etc. based on this basic policy.