CHC HEALTHCARE GROUP

Personal Data Protection Policy

Article 1 Purpose and Commitment

CHC HEALTHCARE GROUP (hereinafter referred to as the “Company”) places great importance on the security and privacy of personal data of all stakeholders. In order to protect the personal data of customers, suppliers, employees, and other stakeholders, the Company has established this Personal Data Protection Policy in accordance with the Personal Data Protection Act and other applicable laws and regulations, and has implemented rigorous personal data privacy management and security protection measures.

The Company has adopted reasonable and appropriate security measures, including access control management and periodic review mechanisms by data owners, to ensure that data access and sharing are properly governed and protected, and to maintain the availability, integrity, and confidentiality of personal data.

This Policy applies to the Company and all of its branches, subsidiaries, and operating locations, and covers the personal data of all customers, suppliers, partners, and other stakeholders.

The Company commits to:

• Collecting and processing personal data only for specific, explicit, and lawful purposes.

• Implementing necessary information security measures to prevent unauthorized access, disclosure, alteration, or destruction of personal data.

• Respecting the rights of data subjects and providing appropriate channels for exercising such rights.

Article 2 Scope of Application

This Policy applies to personal data collected, processed, and used by the Company during the course of its operations, including at a minimum:

• **Customers and Consumers**: Contact persons of medical institutions/corporate clients; procurement, finance, clinical, or maintenance contacts; participants in events or training programs; and individuals submitting customer service inquiries or complaints.

• **Other Stakeholders**: Shareholders/investors, suppliers, partners, job applicants, website visitors, and participants in the Company's events or marketing activities.

Article 3 Categories of Personal Data Collected

Depending on business needs, the Company may collect personal data including, but not limited to:

1. **Identification Data**: Name, job title, company/institution name, department, contact telephone number, email address, mailing address, and business card information.
2. **Characteristics and Records**: Transaction records, customer service/maintenance records, event registration and attendance records, and website interaction records.
3. **Financial and Transaction-Related Data**: Invoice, remittance, or payment contact information, and authorized signatory information (limited to what is necessary).
4. **Website Technical Data**: IP address, cookies, device/browser information, and usage behavior records (subject to cookie settings and notices).
5. **Special Categories of Personal Data (if any)**: Where special personal data such as medical or health examination information is involved due to medical projects, legal requirements, or contractual obligations, the Company shall process such data based on the principle of minimum necessity, lawful grounds, and enhanced security measures, and shall restrict access to authorized personnel only.

Article 4 Methods and Sources of Collection

The Company collects or obtains personal data under the following circumstances:

• Voluntary provision by customers/consumers or stakeholders (e.g., contract negotiations, customer service, complaints, event registrations, job applications).

• Business interactions or cooperation processes (e.g., maintenance or training arrangements, project contact communications).

• Official website or online services (forms, cookies, system logs).

• Lawfully available public sources or third parties with the data subject's consent (only when necessary and lawful).

Article 5 Purposes of Collection

The purposes for which the Company collects personal data include, but are not limited to:

• Customer management and services (quotations, contracts, delivery, maintenance, training, customer service, and satisfaction surveys).

• Marketing and event notifications (seminars, courses, and product information; data subjects may opt out at any time).

• Complaint handling, dispute resolution, and protection of rights and interests.

• Supplier and partner management, procurement, and payment operations.

• Human resources recruitment and employment management.

• Legal compliance, internal control and audit, risk management, and security management.

Article 6 Use and Disclosure of Personal Data

The Company uses personal data within the necessary scope and in reasonable relation to the purposes of collection, and does not arbitrarily disclose personal data to third parties. However, this limitation does not apply under the following circumstances:

• Where disclosure is required by law or by lawful orders of judicial or administrative authorities.

• Where written consent has been obtained from the data subject.

• Where necessary to protect the life, property, or other significant interests of the data subject.

• Where the Company entrusts third parties to process personal data for business purposes, provided that statutory notice obligations have been fulfilled and confidentiality obligations are imposed.

Article 7 Information Security and Personal Data Protection Measures

The Company adopts reasonable and appropriate security measures, including but not limited to:

• Data classification and grading, and the principle of least privilege.

• Access control management, including role-based access, authorization approval, and periodic reviews.

• Account and identity authentication, including complex password policies and periodic password changes.

• System and network protection, including firewalls, antivirus software, endpoint protection, and vulnerability patching.

• Data protection, including encrypted transmission, encrypted storage where necessary, backup, and recovery.

• Logging and monitoring, including access logs and detection and tracking of abnormal activities.

• Document and paper record management, including retention controls, printing controls, and secure destruction.

• Physical security controls, including storage of paper-based personal data in locked cabinets and access control measures.

• Education and awareness, including regular training, assessments, or awareness programs.

• Audits and improvements, including internal audits and follow-up on corrective actions.

Article 8 Exercise of Data Subject Rights

Data subjects may exercise the following rights in accordance with applicable laws:

• To inquire about or request access to personal data.

• To request copies of personal data.

• To request supplementation or correction of personal data.

• To request cessation of collection, processing, or use of personal data.

• To request deletion of personal data.

To exercise the above rights, data subjects may submit a request via the Company's official website or customer service hotline and provide sufficient identification documents. The Company shall process such requests within the statutory time limits.

Article 9 Cross-Border Transfers

Where cross-border transfer of personal data is involved, the Company shall comply with the requirements of the Personal Data Protection Act, ensure that the recipient provides an adequate level of personal data protection, and obtain the data subject's consent or satisfy applicable legal exceptions.

Article 10 Policy Updates and Announcement

This Policy shall be reviewed and amended from time to time in accordance with legal requirements and business needs. Material changes will be announced on the Company's website and notified through appropriate means.

Article 11 Contact Information

If you have any questions regarding this Policy or wish to further understand how to exercise your rights, please contact:

Tel: +886-2-6608-1999 ext. 757 (Mr. Liu)

E-mail: terry.liu@chcg.com

Address: No. 88, Xing'ai Rd., Neihu Dist., Taipei City, Taiwan

---

2025 Implementation Status

Based on the results of the Company's implementation of the Personal Data Protection Policy in 2025, the execution status is as follows:

I. Education and Training

• Total number of employees: 180

• Number of employees completing training: 180 (completion rate: 100%)

• Total training hours: 3 hours

• Training content:

- Information security awareness

- Social engineering and phishing email drills

II. Internal Management and Protection

• One (1) annual regular meeting held by the IT, Legal, and HR departments, with revision recommendations proposed based on data breach simulation exercises.

• One (1) annual internal self-assessment conducted, with no major deficiencies identified.

III. Incident Response and Complaint Handling

• Number of personal data-related complaints: 0

• Personal data breach incidents: None

• Number of simulation drills conducted: 1 (ERP core information system recovery drill)