1. Overview and Objectives

The protection of personal data, as well as compliance with privacy and data protection laws and regulations, is important to Chetan Meditech Pvt Ltd and its affiliates (“we”, “us”, “Biotek”, the “Company”). We do take it seriously and we aim to ensure the privacy rights of our employees, business contacts and customers when we handle information about them.

This Global Privacy Policy (this “Policy”) establishes a comprehensive governance framework for managing privacy and data protection risks.

This Policy, and supporting documents lay out processes and tools that deliver a consistent approach to privacy risk management across the organization. The protection of personal data of employees, business contacts and customers are fundamental to preserving employee, business partner and customer trust.

In particular, this Policy:

sets out the data protection principles that underpin our global privacy framework;

identifies and explains the data protection roles and responsibilities;

establishes the Privacy Program;

identifies the internal policies, procedures and standards which support this Policy and, together with this Policy, constitute our organization's privacy framework; and

sets out a (non-exhaustive) list of the requirements that employees, contractors, consultants and anyone providing support or service to us must comply with in order to preserve the confidentiality and security of the personal data they handle.

This Policy does not provide an exhaustive list of permitted or prohibited conduct or set forth every rule. This Policy is not a substitute for the responsibility to exercise good business judgment and proper care. Individuals should continue to seek proper advice through appropriate channels in relation to any specific concerns and issues that are not specifically addressed in this Policy.

2. Scope and Enforcement

This Policy applies to all directors, managers, employees, contractors, consultants and anyone else supporting or servicing within our organization with respect to all our operations around the world which involve the processing of personal data.

It is the responsibility of every director, manager, employee, contractor, consultant and any anyone else supporting or servicing our organization to comply with this Policy. Acknowledgment and understanding of this Policy is required through contracts and mandatory training. Failure to comply with this Policy may be a breach of the terms of employment and may lead to disciplinary actions up to and including termination of employment or services contracts.

Senior management is ultimately responsible for ensuring adherence to this Policy. The Legal department in coordination with Internal Audit is responsible for monitoring compliance with this Policy.

Terms & Definitions

Data subject(s) or individual(s) is any living individual to whom the personal data or sensitive data relates. Examples of data subjects are consumers, business contacts and employees, contractors, consultants and anyone else providing support or service to the Company.

Data protection laws means any applicable laws, regulations, regulatory requirements and codes of practice relating to the protection of individuals regarding the processing of personal data including information security.

Data breach or incident means any actual or suspected event where the security, confidentiality, integrity or availability of personal data has been or could be compromised, leading to the accidental, unlawful or unauthorised destruction, loss, alteration, disclosure of or access to personal data, or any other unlawful use of personal data (e.g.

an email with personal data is inadvertently sent to the wrong recipients; a paper record with personal data is lost or stolen; a cyber-attack has been carried out by hackers; a work laptop is lost or stolen).

Data processing or processing means any use of personal data by our organization (or a third party on behalf of our organization), including data collection, data sharing and data storage. The mere storage of data is processing.

Personal data means any information relating to an individual that identifies the individual or could reasonably be used to identify the individual regardless of the medium involved (e.g. paper, electronic, video, audio). Examples of personal data include contact details, financial data, passwords, IP addresses, pictures, online search history, geolocation information. Unless otherwise stated, personal data is intended to include sensitive data (as defined below).

Sensitive personal data means personal data about racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life, genetic data (e.g. an individual's gene sequence), biometric data (e.g. Fingerprints, facial recognition, retinal scans), criminal offences committed or alleged to have been committed.

3. Data Protection Principles

Our organization's business operations must, always, be consistent with the Data Protection Principles set out below. These principles are binding across all our businesses.

Lawful, fair, and transparent processing

Our organization only uses personal data in a way that is lawful, fair, and transparent.

We comply with data protection and privacy laws within each of the jurisdictions in which we operate. Where required by the law, we are also committed to helping individuals understand what information we collect, how we use it and what choices they have. We explain this to employees, contractors, consultants and other workers, consumers and business contacts in a simple and clear way in our privacy statements. We review our privacy statements regularly to keep them up to date, and to ensure they match our internal practices.

Purpose limitation

We only collect personal data for specified, clear and legitimate purposes and we only collect as much personal data as we need to achieve those purposes. Though personal data helps us improve the services we provide, we only use it in ways which are proportionate to clear goals.

Data accuracy

We take steps to ensure that the personal data we hold is accurate, up-to-date and relevant to the purposes for which it is collected.

Data retention

We only keep personal data in an identifiable form for as long as is necessary for the purposes for which we are using it.

Rights of the individuals

We are fully committed to facilitate the privacy rights of individuals with respect to our processing of their personal data, in accordance with applicable laws.

Information security

We use appropriate physical, technical and organizational measures to keep personal data secure and ensure its integrity, confidentiality and availability across all systems at all times.

We are also committed to ensure that our vendors and suppliers which may process personal data on our behalf preserve the confidentiality, integrity and availability of such data.

International transfers of personal data

Our organization is a global business and as such we have to transfer information internationally. We are fully committed to ensure that there are adequate safeguards in place, as required by the applicable laws, to protect the personal data we transfer to countries that do not have adequate data protection laws.

Accountability

We are all responsible for upholding the Data Protection Principles and respecting individual privacy rights. We have a collective and individual duty to protect the personal data of our employees, contractors, consultants and other workers, consumers and business partners. In order to create an environment of trust and to comply with applicable data protection laws, all individuals operating within or on behalf of our organization must comply with our privacy policies and help the organization to uphold its commitments to the protection of personal data.

4. Roles and Responsibilities

Different stakeholders at different corporate levels within our organization play a role in ensuring overall privacy risk management and data protection compliance. The following offices and employees have been identified as having specific roles and responsibilities:

The Legal department is responsible for promoting and ensuring privacy compliance, overseeing the overall privacy management and compliance program, responding to data subject queries and requests, responding to regulatory requests about data protection, liaising with the IT department where required to ensure information security which is a core part of personal data protection.

The IT department is responsible for safeguarding and monitoring our internal networks and systems and, in particular, ensuring that personal data stored, transferred, accessed and used across these networks and systems is adequately protected from data breaches.

The HR department is responsible for handling the personal data properly of employees, contractors, consultants and anyone else providing services and supports and in compliance with the applicable laws. The HR department is also responsible for addressing requests from employees, contractors, consultants and other workers for the exercise of their data protection rights and escalating any further query or complaint to the Legal department. The HR department should also inform the Legal department regarding new processing activities which impact on the personal data of employees, contractors, consultants and other workers. The HR department should be engaged in performing DPIAs of new HR processing activities, updating privacy notices to employees, contractors, consultants and other workers and making them aware of their duties and responsibilities regarding personal data protection (including this Policy).

In addition, any business function which processes personal data is responsible for:

managing the privacy risk related to the processing carried out by the function;

consulting the Legal department when required by the internal policies and procedures;

ensuring the security of the personal data it processes; and

handling and escalating any privacy incidents as required.

All directors, managers, employees, contractors, consultants and workers are responsible for preserving the confidentiality of the personal data they use and for handling this information securely and in accordance with this Policy and any other supporting policies, procedures and standards (as identified below at "Policy Framework").

5. Privacy Program

Our Legal department will supervise our Privacy Program, which provides a comprehensive, coordinated approach to managing privacy risk while serving business needs and strategies.

Our organization must operate at all times in compliance with this Policy, the Code of Conduct and Business Ethics and all internal policies, procedures and standards. Please note that these may, from time to time, be updated or replaced and the scope of the list below may be expanded to additional policies.

The Legal department will also be responsible for ensuring and supervising the development of any additional records which may be required to demonstrate compliance under applicable data protection laws.

6. What Employees, Contractors, Consultants and Workers Must Do

Apply the Data Protection Principles to the collection and use of personal data and follow the policies, procedures and standards regarding privacy. They are also expected to complete all required data protection training.

Non-compliance may result in disciplinary action up to and including termination of employment or business relationship, as well as legal action

7. Reporting and Questions

Biotek personnel may report any concerns through an anonymous and confidential email to info@biotekortho.com. A Company Representative may also make confidential reports to his/her supervisor, HR, the Compliance Officer.

8. Amendments to the Policy

The Legal department will review this Policy and recommend appropriate changes.

9. Exceptions and Escalations

Any exceptions to this Policy must be reviewed and approved by the Legal department.

The Legal department is responsible for resolving questions about the appropriate interpretation of this Policy in light of legal and regulatory requirements. The Legal department is responsible for addressing questions about interpreting this Policy.