HUTCHMED (CHINA) LIMITED

POLICY ON PERSONAL INFORMATION GOVERNANCE

Adopted by the board of directors on 14 March 2017 and amended by the board of directors on 1 January 2023

Table of Contents

1. Policy Statement

HUTCHMED (China) Limited (the "Company"), its subsidiaries and controlled affiliates (collectively, the "Group") recognises that the protection of Personal Information is fundamental to preserving the public's trust. The Group is committed to the safeguard and protection of Personal Information acquired (i) from Employees, agents, consultants, contractors, vendors, service providers, (ii) patients or clinical study subjects who use Group's products and other Customers, (iii) healthcare professionals who study or prescribe Group's products, and (iv) in connection with the Group's investment or business development activities including, the Group's due diligence process, in compliance with Applicable Data Protection Laws in jurisdictions in which the Group operates.

This Policy sets out the Group governance framework for the safeguard of Personal Information (PI) of Employees, Customers and other aforesaid PI Subjects. This Policy should be read in conjunction with the HUTCHMED Information Security Policy and the HUTCHMED Code of Ethics, as well as the local policies and procedures of the Group or its member company.

This Policy applies to the Group, and to all directors, officers and Employees in the Group.

Please contact the Legal Department of each Group company (or the Group Legal Department where appropriate) for any questions in relation to this Policy. Where any Employee becomes aware of any laws or regulations that prevent them from complying with this Policy or taking prescribed action in the event of a breach of this Policy, including a data security breach, such Employee must inform the Legal Department of each Group company (or the Group Legal Department where appropriate) immediately upon becoming aware of such laws or regulations (or of a breach of this Policy).

Appendix 1 and 2 set out a glossary of common terms and a summary of key concepts used in this Policy.

2. Governance Framework

The senior management of each Group company is accountable for the effective implementation of this Policy (including the Data Privacy Principles and Procedures set out below). Senior management is to ensure that this Policy is incorporated and embedded into local policies and procedures, subject to (and in compliance with) Applicable Data Protection Laws.

As the "Personal Information Handler" (also known as "Controller") of Personal Information of its Customers, Employees and other PI Subjects, each Group company must implement its local policies and procedures in such a manner that it can demonstrate compliance with its Applicable Data Protection Laws including (where required):

(a) ensuring that the legislative and regulatory requirements are embedded in all operating procedures and activities involving the processing of Personal Information (e.g. ensuring 'privacy by design' for all new projects involving processing Personal Information);

(b) implementing appropriate technical and organisational measures which are designed to implement the Data Privacy Principles in an effective manner and to integrate necessary safeguards into processing activities, and to protect the rights of PI Subjects as required in the jurisdictions in which they operate;

(c) conducting privacy and data protection awareness training for Employees to ensure awareness and understanding of this Policy and their responsibilities in personal information protection management and privacy;

(d) conducting regular privacy risk assessments of its business to assess the privacy risk (including with respect to third party vendors) and the adequacy of mitigating controls;

(e) ensuring Personal Information is classified and handled according to its sensitivity, and access is restricted on a need-to-know-basis; and

(f) designating appropriate privacy and IT security specialists to support the business in managing its data privacy risks (e.g. the appointment of a data protection officer if required).

All Employees involved in Personal Information processing should understand and comply with this Policy, as well as any related policies, procedures and guidelines implemented by the Group company. Failure to process Personal Information in accordance with this Policy may lead to disciplinary action. Serious and/or deliberate non-compliance with this Policy could result in dismissal for Employees.

3. Data Privacy Principles

The Group shall at all times process Personal Information in line with the following Data Privacy Principles.

3.1. Lawful, Fair and Transparent Processing

(a) Personal Information will only be used in a way that is lawful, fair and transparent.

(b) Use of Personal Information should be in compliance with Applicable Data Protection Laws within each of the jurisdictions in which the Group operates. Each Group company is to be transparent about when, how and for what purpose the Personal Information of Customers, Employees and other PI Subjects is processed, and what choices and rights PI Subjects have in that jurisdiction in relation to the processing of their Personal Information.

(c) Access to Personal Information should be restricted to Employees who need to know the information to fulfil their duties within the Group and Sensitive Personal Information (including access thereto) requires the highest level of protection.

3.2. Purpose and Use

Personal Information should only be collected for specified, clear and legitimate purposes and only to the extent needed to achieve those purposes. Use of Personal Information helps improve the services offered by the Group, but use of such data should be proportionate to clear purposes. Excessive Personal Information collection is prohibited.

3.3. Data Accuracy

Reasonable steps should be taken to ensure that any Personal Information held is accurate and up to date.

3.4. Data Retention

Personal Information should only be kept for as long as is necessary for the purposes for which it is being used. Guidelines around document retention periods should be issued by each Group company to relevant management and staff.

3.5. Rights of the PI Subjects

(a) Personal Information should be processed in accordance with the rights of PI Subjects under the Applicable Data Protection Laws within each of the jurisdictions in which the Group operates.

(b) All requests from PI Subjects to access, amend, delete or otherwise relating to their Personal Information should be handled in a manner compliant with Applicable Data Protection Laws with appropriate processes for receiving and responding to such requests.

3.6. Information Security

(a) Appropriate technical and organisational security measures should be adopted to safeguard the Personal Information the Group is entrusted with against unauthorised or unlawful processing and against accidental loss, destruction or damage to ensure a level of security appropriate to the risk (e.g. the de-identification/pseudonymisation and encryption of Personal Information and/or other security measures as appropriate).

(b) Security measures should be implemented and reviewed regularly to ensure that they offer the appropriate level of protection.

(c) The same level of security should be used to protect the Personal Information that is processed on behalf of third parties (e.g. where any Group company acts as "Contract Processor" or "Data Processor").

3.7. Cross-Border Transfers of Personal Information

The Group is a global business and as such is required to transfer information internationally. Personal Information should not be transferred to a country or territory that does not provide adequate data protection without appropriate safeguards unless such transfer complies with Applicable Data Protection Laws.

4. Procedures

Each Group company is to implement appropriate procedures to ensure that Personal Information is processed fairly and lawfully in accordance with the Data Privacy Principles and Applicable Data Protection Laws.

4.1. Records of Processing

Each Group company should maintain records of processing activities, and documentation related to data protection compliance, if required by Applicable Data Protection Laws. The Group and each Group company shall regularly conduct audits of their Personal Information processing and compliance with Data Privacy Principles and Applicable Data Protection Laws.

4.2. Privacy Impact Assessments

Privacy impact assessments should be performed with respect to new products, technologies and business operations, where required by Applicable Data Protection Laws or where appropriate to manage the privacy risk. For instance, if the project involves one or more of the following: processing large amounts of Personal Information or where the processing affects a large number of PI Subjects; using existing Personal Information for a new and/or more intrusive purpose; processing Sensitive Personal Information and/or genetic or biometric data (e.g. fingerprint scanning, face recognition); introducing new and intrusive technology (e.g. CCTV cameras, locator technologies, automated decision-making); transferring Personal Information outbound, contract Personal Information processing, providing Personal Information to non-Group entities or individuals, or disclosing Personal Information, or engaging in any type of employee monitoring (including any recording and/or reviewing of employees' communications or activities, including phone calls, emails and computer files). In addition to self-assessment, security assessment conducted by Privacy Authorities might be required under certain circumstances. For example, a mandatory security assessment conducted by the Cyberspace Administration of China ("CAC") will be required when any Group company operating in mainland China transfers Personal Information that by its nature or quantity will need to be cleared by the CAC.

4.3. Privacy Notices

Each Group company should implement appropriate privacy policies / notices ("Privacy Notices") where required by Applicable Data Protection Laws, including but not limited to explain to Customers Employees, and other PI Subjects what Personal Information is processed and for what purposes using clear and easily understood language. These Privacy Notices should be readily accessible and kept up to date, with simple mechanisms for PI Subjects to opt-out of, or not to agree to, processing of Personal Information when the Applicable Data Protection Laws require.

4.4. Personal Information Subject Requests

All requests from PI Subjects to access, amend, delete or otherwise relating to their Personal Information should be handled according to procedures which are compliant with Applicable Data Protection Laws.

4.5. Disclosure of Personal Information to Law Enforcement Authorities / Other Regulatory Authorities

The Group may have a duty to disclose Personal Information to law enforcement authorities or other regulatory authorities in certain specified and limited circumstances. Responding to official requests for Personal Information should be balanced against the obligation to protect Personal Information. All Employees must follow the relevant procedures and if they are in doubt they must consult with the Group Data Protection Officer (or the Group Legal Department where appropriate).

4.6. Cooperation with Privacy Authorities

The Group is committed to cooperating with enquiries and investigations of the Privacy Authorities, particularly if they have concerns regarding the privacy of the Employees, Customers or users of websites of any Group company, and other PI Subjects. Communications from Privacy Authorities should be referred to the Group Data Privacy Officer ("DPO") (or the Group Legal Department where appropriate) without delay.

4.7. Data Security Incidents

When a Data Security Incident ("DSI") occurs which involves Personal Information, the relevant Group company should aim to mitigate the potential consequences and to secure Personal Information from further unauthorised access, use or damage as quickly as possible. Each Group company should respond rapidly and in accordance with applicable DSI procedures, which may include notifying the Privacy Authorities and/or affected PI Subjects if required. In the event of a DSI involving Personal Information, the Group DPO should be alerted immediately at dpo@hutch-med.com. Further guidance on notification and handling of DSIs should be issued from time to time.

4.8. Use of CCTV

The use of CCTV may involve processing identifiable images of PI Subjects. Where used, each Group company must consider the potentially sensitive nature of the images captured when

using CCTV and processing the data gathered. Employees involved in the use of CCTV should be trained in respect of its use to ensure compliance with Applicable Data Protection Laws.

4.9. Use of Personal Information for Marketing Activities and Sale of Personal Information

Processing of Personal Information for direct marketing purposes and sale of Personal Information are subject to special regulatory requirements under Applicable Data Protection Laws in different jurisdictions. Processing Personal Information for direct marketing purposes must strictly adhere with the regulatory requirements under Applicable Data Protection Laws.

The Group does not sell Personal Information for monetary consideration. If at any time the Group anticipates selling Personal Information, such proposal must be approved by the Group DPO in consultation with the Group Legal Department. If you believe that a disclosure or potential disclosure of Personal Information could constitute a sale, you should immediately contact the Group DPO.

4.10. Third Party Processors

Where third party service providers are engaged as part of business operations which involve the Processing of Personal Information, it is important to ensure that:

(a) appropriate diligence is conducted in the selection of such vendors, with ongoing monitoring and review of third party vendors;

(b) PI Subjects are notified of such disclosure in Privacy Notices and provided an opt-out right or required opt-in consent where required by Applicable Data Protection Laws;

(c) the third party implements adequate privacy and security safeguards in accordance with this Policy;

(d) a contract including data privacy clauses is in place and approved by the Legal Department of the relevant Group company before the processing starts; and

(e) any recommendations arising from the privacy impact assessment (if applicable) relating to the use of the third party are implemented.

Appendix 1: Glossary of Terms

Term	Definition
Applicable Data Protection Laws	means the applicable laws and regulations in the relevant countries ensuring the protection of Personal Information.
Customers	means all customers of a Group company's goods and services, whether online and/or offline, including members of customer loyalty schemes.
Contract Processor or Data Processor	means the entity which processes Personal Information on behalf of the Data Controller (and the meaning of Data Processing shall be construed in accordance with this definition).
Data Processing	means any operation performed upon Personal Information whether or not by automatic means, including collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Information.
Data Security Incident (DSI)	means any actual or suspected event where the security, confidentiality, integrity or availability of Personal Information has been or could be compromised. For example: loss or theft of data or equipment on which Personal Information is stored; sharing or inappropriate use of passwords allowing unauthorised access to Personal Information; IT systems failure; human error; unforeseen circumstances such as a fire or flood; hacking attacks on IT systems; improper handling or disposing of Personal Information; and offences where Personal Information is obtained through deception.
Employee(s)	means all persons who work for the Group including employees with temporary, fixed term and permanent employment contracts.
Personal Information	means information that directly or indirectly identifies a natural person, whether a Customer, Employee or user of a Group Company website, or other PI Subjects.
Personal Information Handler or Data Controller	means the entity which alone or jointly with others determines the purposes and means of processing of Personal Information.
PI Subject(s)	Means a natural person identified or associated with the Personal Information.
Privacy Authorities	means the information commissioners or equivalent regulatory authorities in the relevant countries responsible for administering and enforcing the relevant Applicable Data Protection Laws.
Sensitive Personal Information	means any Personal Information which, due to its sensitive nature, is subject to additional legal controls over processing, including the following special categories of Personal Information: data concerning an PI Subject's racial or ethnic origin, ideology or political opinions, religious or philosophical beliefs, membership of a trade union, physical or mental health, sexual life or orientation, criminal convictions or alleged commission of any offence, as well as any genetic or biometric data.

Appendix 2: Key Concepts

What is "Processing"?

Applicable Data Protection Laws regulate the "processing" (i.e. handling) of Personal Information. Processing is *very* broadly defined and covers a range of activities including collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Personal Information. The rules apply to holding data on computer databases, word processed documents and audio tape, or images identifying a person on video tape, CD, DVD or stored as a digital image. Applicable Data Protection Laws also regulate paper-based information held in filing systems.

What is "Personal Information"?

Data is Personal Information if it relates to a living individual who can be "identified" or who is "identifiable" (a) from those data, or (b) from those data and other information which is in the Group's possession, or is likely to come into its possession. The concept of Personal Information is therefore extremely broad. In some countries, information relating to a corporate entity is treated as Personal Information.

Examples: a telephone number on its own may be Personal Information if it is capable of identifying a living individual. The information contained on a credit card constitutes Personal Information because it contains the name of the card holder. Customer Loyalty card number by itself is regarded as Personal Information under Applicable Data Protection Laws because the loyalty card issuer can identify the individual person behind the number. Footage from a video camera can be Personal Information to the extent individuals are recognisable. Telephone or email log data contain Personal Information because it is possible to directly or indirectly identify the individuals who communicated.

Personal Information also includes any expression of opinion about the individual and any indication of the intentions of the Company or any Group company or any other person in respect of the individual.

What is Sensitive Personal Information?

Sensitive Personal Information refers to various categories of data that are subject to additional legal controls over processing and include data concerning an individual's racial or ethnic origin, ideology or political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health condition, sexual life, criminal convictions or alleged commission of any offence. Please note that the definition may vary by jurisdictions and that in some jurisdictions information relating to offences and proceedings will constitute "judicial data" and be subject to specific rules. More stringent rules apply in many countries to processing of Sensitive Personal Information and judicial data. Where the Company or any Group company relies on consent to process Sensitive Personal Information, such consent must be "explicit" - i.e. the PI Subject needs to take some positive

step to indicate their acceptance. Besides, "separate" consent needs to be obtained under Applicable Data Protection Laws in certain jurisdictions in which the Group is operating, such as the EU and China.

What is the difference between a Data Controller and Data Processor?

A Personal Information Handler or a Data Controller is the entity which controls the manner in which and purposes for which the data is collected, even if it does not physically hold the data itself. As such, the Company and each Group company will be Data Controllers in relation to data relating to their Employees, Customers or other PI Subjects, even if the data is held by a third party, which acts on behalf of the Company and the Group company (e.g. payroll administration is outsourced to a third party). A party which holds and processes Personal Information on behalf of a Data Controller is a Contract Processor or a Data Processor. Where the Company or a Group company together with another party controls the manner and purposes of the processing, the two parties can be joint Data Controllers.

Example: A Group company has certain academic training material which it wishes to distribute to all relevant healthcare professionals. A third party agency is to undertake the processing (e.g. sending academic training materials) on behalf of and under the Group company's instructions. The relevant Group company is the Data Controller and the agency will be a Data Processor.