Global Privacy Procedure

Fisher & Paykel Healthcare Corporation Limited

Purpose

Fisher & Paykel Healthcare (F&P) is committed to acting ethically and "doing the right thing" by respecting and protecting the privacy rights of our end users, employees, research participants, customers, shareholders and prospective employees. We seek to ensure the approach we take reflects and upholds our values. Care drives our commitment to privacy.

This Procedure outlines our approach to privacy and sets out the principles which underpin how we treat personal information, including our philosophies of Privacy by Design and Privacy by Default. It enables and supports the implementation of our Digital Technology and Corporate Governance Policies.

Scope and Application

This Procedure applies to all personal information collected or processed by F&P. Compliance with this Procedure is mandatory and applies to all employees and independent contractors of F&P globally.

Privacy by Design

F&P will implement a philosophy of Privacy by Design throughout the lifecycle of personal information, by incorporating privacy principles into the design of our processes, systems and products which involve personal information that we collect or process. This includes technological and organisational controls and procedures.

Privacy Principles

F&P aims to uphold the following privacy principles when collecting or processing personal information, using a risk-based approach which considers the nature, scope, context and purposes of processing.

1. **Purpose**
   - We will only collect personal information to support a specific, legitimate purpose.
   - We will only process personal information to provide products and services associated with that purpose where necessary.
2. **Respect and Care**
   - We will only process personal information when we have a lawful basis to do so.
   - We will process personal information in ways that respect the dignity, autonomy and right to privacy of individuals.
3. **Data Minimisation**
   - We will only process the personal information we need.
   - We will de-identify high-risk personal information before sharing with third parties in accordance with the requirements of applicable law.
   - We will keep personal information only for as long as necessary and permitted by applicable law.
4. **Transparency**
   - We will be open about what personal information we collect and how we use it.
   - We will be open about our reasons for collecting, processing and sharing personal information.
5. **Choice and Control**
   - We use a Privacy by Default approach to ensure appropriate privacy protection when designing our products and services.
   - We aim to provide individuals with choice about what personal information is collected about them by enabling privacy-friendly settings by default and making the sharing of additional personal information optional.
   - We will respect individuals' rights to request access to, correct or erase their personal information, to data portability, and to object to or restrict the use of their personal information in accordance with applicable law.
6. **Confidentiality, Integrity and Accessibility**
   - We will implement appropriate technical and organisational safeguards to protect the confidentiality, integrity and accessibility of personal information from internal and external users.

Roles and Responsibilities

F&P is committed to processing personal information in accordance with its responsibilities under applicable law. These responsibilities are shared by the following roles:

Privacy Team – a centralised internal F&P Privacy team based in New Zealand responsible for:

(a) the global management of F&P's privacy policies, statements and procedures;

(b) privacy risk management, including identifying and reporting privacy risks to relevant stakeholders; and

(c) holding a centralised privacy incident register, Data Protection Impact Assessment (DPIA) register, and other centralised privacy records.

The contact email address for the Privacy team is privacy@fphcare.com.

Local Privacy Representatives – Local Privacy Representatives will be appointed in F&P's offices as necessary. Their role is to implement local privacy related procedures in compliance with global F&P procedures, advise on and monitor compliance with applicable law, identify and report privacy risks, and cooperate and liaise with regulatory authorities. They may also be appointed as Data Protection Officers (DPOs) according to applicable law. DPOs will act in an independent capacity, without conflict of interest, to represent the privacy rights and interests of individuals whose personal information is collected or processed by F&P. Local Privacy Representatives' contact details can be found in F&P's Global Privacy Statement.

Employees and Independent Contractors – all F&P employees and independent contractors are responsible for:

(a) complying with F&P privacy policies, statements and procedures; and

(b) exercising appropriate confidentiality and discretion when interacting with personal information at F&P in performance of their roles and responsibilities.

Policies and Procedures

The Privacy team is responsible for drafting and managing global F&P privacy related procedures. Regional F&P offices may implement relevant privacy procedures at a local level consistent with global F&P privacy procedures and with the support of the Privacy team.

Training and Awareness

F&P will provide privacy training and awareness initiatives to educate employees about their privacy obligations, relevant privacy risks and how to appropriately interact with personal information collected or processed by F&P. Training and awareness initiatives will have regard to the nature of employees' roles and responsibilities, and the context, scope and purposes of applicable personal information processing.

Privacy Rights of Individuals

F&P will respect and facilitate, where appropriate, the exercise of privacy rights by individuals. F&P will process individuals' privacy requests using a risk-based approach and prioritise the processing of urgent or high-risk personal information when fulfilling a request. When responding to individuals' privacy requests, F&P will take care to ensure that other individuals' personal information will not be unreasonably disclosed, altered or used.

Privacy Governance and Risk Management

F&P will implement an appropriate privacy governance structure to meet the needs and objectives of the organisation, to enable effective privacy management by communicating and managing privacy risks with relevant business stakeholders.

F&P will appropriately record and monitor privacy risks in accordance with an organisational privacy risk framework. Operational and enterprise privacy risks will be escalated and communicated to relevant business stakeholders as needed.

Privacy Risk Assessments

Data Protection Impact Assessments shall be performed for activities which pose a high risk to the privacy of individuals whom F&P collect or process information about, including automated decision making, use of artificial intelligence or machine learning, or be performed otherwise at the Privacy team's discretion. DPIAs and risk mitigation activities will follow a risk-based approach and a centralised record of DPIAs will be kept.

Privacy Incident Management

F&P has privacy incident management processes to record and appropriately respond to privacy incidents.

If F&P determines that a privacy breach has occurred, we will notify relevant supervisory authorities and individuals as appropriate, without undue delay and in accordance with applicable law.

Third Party Management

F&P seeks to do business with third parties (e.g. suppliers, service providers) who respect and protect privacy. F&P will aim to protect personal information shared with, or processed by, third parties in accordance with applicable law, consistent with F&P's standards and expectations.

Cross-Border Transfers of Personal Information

F&P aims to use appropriate organisational and technical measures to ensure that international cross-border transfers of personal information occur in a safe, lawful and secure way, using a risk-based approach. These may include standard contractual clauses and other contractual and legal arrangements for the transfer of personal information globally.

Review

This procedure will be reviewed every three years, or sooner as necessary, by the Group Privacy Manager and a relevant VP of F&P (or delegates). We reserve the right to amend this procedure at any time, at our discretion.

Approved by the Board on 27 September 2024.