

Global Privacy Policy

Fisher & Paykel Healthcare Corporation Limited

Purpose

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

This Policy outlines our approach to privacy, including our philosophy of privacy by design, the principles that underpin how we treat personal information, key privacy roles and responsibilities in our organisation, our training and awareness initiatives, management of our privacy policies and procedures at a global and regional level, and the business processes and activities we use to manage privacy.

Scope and Application

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

Privacy by Design

F&P Healthcare 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 Healthcare will endeavour 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 and process personal information to support a specific, legitimate purpose.

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 respects individual dignity, autonomy and right to privacy.

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 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 will endeavour to provide individuals with choice about what personal information is collected about them.
- We will respect individuals’ rights to request to access, 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 Healthcare 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 Healthcare privacy team based in New Zealand responsible for:

- (a) the global management of F&P Healthcare’s privacy policies and procedures;
- (b) privacy risk management, including identifying and reporting privacy risks to relevant F&P Healthcare 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.

Data Protection Officer (DPO) – DPOs will be appointed in the head office in New Zealand and regional offices as required. Their role is to advise and monitor compliance with applicable law, identify and report privacy risks, and cooperate and liaise with regulatory authorities. DPOs must act in an independent capacity, without conflict of interest, and represent the privacy rights and interests of individuals whose personal information is collected or processed by F&P Healthcare.

DPOs will be responsible for implementing local privacy related procedures in compliance with global F&P Healthcare policies and in accordance with applicable law.

The following DPOs have been designated:

JURISDICTION	NAME	EMAIL
New Zealand	Natasha Mazey	privacy@fphcare.com
France	Yann Breton	dpo@fphcare.fr
Germany	Gregor Euteneuer	datenschutz@fphcare.de
United Kingdom & Ireland	Maria Giljam	dpo@fphcare.co.uk

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

- (a) complying with F&P Healthcare privacy policies and procedures; and
- (b) exercising appropriate confidentiality and discretion when interacting with personal information at F&P Healthcare in performance of their roles and responsibilities.

Policies and Procedures

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

Training and Awareness

F&P Healthcare 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 Healthcare. Training and awareness initiatives will have regard to the nature of their roles and responsibilities, and the context, scope and purposes of applicable personal information processing.

Privacy Rights of Individuals

F&P Healthcare will respect and facilitate, where appropriate, individual privacy rights, including the rights of accessibility, correction, portability, erasure and the objection or restriction of personal information processing.

F&P Healthcare will process individuals' privacy requests using a risk based approach and prioritise the processing of high risk personal information when fulfilling a request. When responding to individuals' privacy requests, F&P Healthcare 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 Healthcare will implement an appropriate privacy governance structure to meet the needs and objectives of the organisation, to enable effective privacy management to support the global F&P Healthcare privacy mission and effectively communicate and manage privacy risks with relevant business stakeholders.

F&P Healthcare 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 (DPIAs) shall be performed for activities which pose a high risk to the privacy of individuals whom F&P Healthcare collect or process information about. 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 Healthcare will have privacy incident management processes to record and appropriately respond to privacy incidents.

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

Cross-Border Transfers of Personal Information

F&P Healthcare endeavours to transfer personal information in accordance with applicable law to ensure that international cross-border transfers of personal information occur in a safe, lawful and secure way. F&P Healthcare may use standard contractual clauses and other contractual and legal arrangements to ensure appropriate safeguards are in place for the safe and secure transfer of personal information globally.

Privacy Records

F&P Healthcare will keep an appropriate record of activities to demonstrate privacy compliance with applicable law and reasonably up to date records of processing activities relating to personal information that occur in F&P Healthcare entities.

Policy Review

This policy will be reviewed annually by the Privacy Officer and a relevant VP of F&P Healthcare (or delegates). We reserve the right to amend this policy at any time, at our discretion and will keep F&P Healthcare informed of any material amendments.

Approved on 6 June 2019.