# Processes & Safety Measures – Compliance

This document outlines processes and safety protocol that Healistic Group Ltd follows to ensure GDPR and GPhC compliance. All technical infrastructure, data transit and operations are set out to provide a seamless, secure and safe user journey, while meeting the standards of the regulators and ensuring trust with partners.

Healistic operates on a lawful basis and transparency. Healistic designs its processes and protocols with the aim of eliminating any potential for breach of legislation and regulation. Any potential for human failure is continuously hard-coded into the prescription flow

Where possible, the activity has been matched to the appropriate GPhC standard(s) for pharmacy premises.

**Operations:**

Healistic's technology and solutions are built to ensure that all contents are validated and appropriately secured at all times – before dispatch, in transit, and upon delivery

Standards 1.7, 4.2 & 4.3
Healistic only uses tamper-proof packaging to provide a clear proof point to the customer that the packaging has not been tampered with in-transit.

Standards 1.7, 4.2 & 4.3
Packaging is discrete and nondescript, and riders have no view of what is within the package, to ensure patient privacy. The patient can therefore access pharmacy services in full confidentiality.

Standard 1.5
Healistic takes out insurance for goods in transit, for the event of damage or loss.

**Partner Pharmacies:**

Before onboarding, Healistic due diligences its partner pharmacies against all professional standards. Partner pharmacies are required to have appropriate levels of professional indemnity, public liability and employer's liability insurance.

The Pharmacy Superintendent of each partner pharmacy is accountable for ensuring that the appropriate risk assessments are in place and that the guidance for providing pharmacy services at a distance is met before the service starts in their organisation.

In addition, Healistic, to the best of its ability, ensures that partner pharmacy teams are appropriately trained and monitored on process compliance, to minimise risk and demonstrate diligence on behalf of Healistic.

**Controlled Drugs**

Prescribers are required to flag Controlled Drugs at prescription issuance via the Healistic Prescriber Interface. Healistic's partner pharmacies will not dispense a Schedule 2 or 3 controlled drug without receipt of physical FP10PCD controlled drug prescription. This is to be sent to the pharmacy by the prescriber via mail.

**Delivery Confirmation**

Standards 4.2 and 4.3 Identity Verification:
Identity verification takes place at parcel handover between Healistic rider and customer. The patient must provide a valid ID document, showing their date of birth. Only then a rider can confirm delivery. The Healistic rider app requires customer DOB entry & ID check confirmation to mark an order as delivered. In event of failure, a 'failed delivery process' is initiated.

Standards 1.6, 4.2 & 4.3 Digital Delivery Checks Logbook:
A complete record of all historic restricted delivery checks is kept. This includes *verification_id*, *rider_id*, *order_id*, *DOB_entry* (date), *id_checked* (true/false), and *created* (timestamp).

Standards 4.2 & 4.3 Failed Delivery Protocol:
If a customer is not present for delivery, Healistic allows the rider to try and contact the customer for 10 minutes. If contact is unsuccessful, Healistic rider must return the order to the pharmacy. The order will then be redelivered at a later date.

**Riders**

Rider services are sub-contracted by Healistic on a scheduled full-time basis to Ryde (Gameplan Technology Limited), a company incorporated in the United Kingdom (company number: 11175220) with registered address at Epworth House, 25 City Road, London, EC1Y 1AA. At any given moment in a rider's shift with Healistic, the rider is solely responsible for Healistic deliveries. Rider vetting documentation is provided by Ryde for Healistic to ensure that Healistic always holds central record of a riders' pre-employment checks.

Standards 1.8, 4.2 & 4.3 Pre-employment Checks:
The rider's Right-To-Work is checked and their identity verified by their employer prior to employment along with a full vehicle check (where applicable). All riders are subject to a basic DBS check. DBS and vehicle checks are repeated annually. Additional RTW checks are completed, if the rider is not a British citizen or does not have indefinite right to remain in the UK; the rider's ability to work with Healistic expires in line with their leave to remain.

Standards 1.2, 1.4, 1.6, 4.2 & 4.3 Quality Assurance includes:

1) Mandatory training modules (incl. safeguarding)
2) Monitored in-app messaging
3) Age-verification refusals log book indicates where there has been ID check and/or refusal by any rider
4) Pharmacy partner feedback – dedicated email address and communication channels, where Healistic's pharmacy partners can log any rider related issues/concerns.
5) Bi-monthly check in with pharmacy partners to review service provision

**Information summary to determine what information Healistic processes and who has access to that information**

1. Processed information: Professional data of prescribers (name, clinic, GMC number), that is needed to demonstrate the legitimacy of issued private prescriptions
    - Maintained by: Authorised Healistic personnel
    - Accessible (read-only) by: Prescriber; Pharmacies that provide dispensing services for patients of that prescriber; Patient of that prescriber
2. Processed information: Information on the pharmacist providing dispensing services that confirms their registration with the GPhC
    - Maintained by: Authorised Healistic personnel
3. Processed information: Medical patient data (full prescription content)
    - Created by: Prescriber
    - Accessible (read-only) by: Pharmacies that provide dispensing services for that patient; Patient of that prescriber
4. Processed information: Medical patient data (prescribed items only)
    - Created by: Prescriber
    - Accessible (read-only) by: Authorised Healistic personnel
5. Processed information: Personal patient data (address, date of birth)
    - Accessible (read-only) by: Authorised Healistic personnel; Couriers assigned to the delivery of that specific order

**Legal justification for Healistic's data processing activities**

The processing of personal medical & health data is necessary for providing the safe and effective supply and delivery of prescribed medication.

**Information about Healistic's data processing and legal justification in Healistic's privacy policy**

Detailed information about Healistic's privacy policy can be found here.

**Data protection by design & default**

Healistic ensures a secure handling of personal data by applying the principle of least privilege. Users can only access data they require to fulfil a task.

**Data handling policies**

Any processed data is encrypted when it is in transit. Users are not able to access personal data that is not required for the fulfilment of a task assigned to them.

**Internal security policies**

Internal security policies are outlined in the Healistic IT Guidelines. These guidelines include policies for work devices, online accounts, data backups and actions in case of data breaches.

Internal IT security & risk awareness training is held quarterly and attended by all Healistic employees to raise awareness for common threats and vulnerabilities as well as to cultivate responsible behaviours in the handling of personal data.

**Responsibility for ensuring GDPR compliance across the Healistic organisation**

Every employee is responsible for ensuring GDPR compliance in their area of responsibility. Where clarity is required or new processes implemented, specialist regulatory and legal advisors are consulted.

**Processing Agreement between Healistic and third parties that process personal data on Healistic's behalf**

All third parties that process data on Healistic's behalf must be able to demonstrate that they meet the requirements of the GDPR and the GPhC standards relating to personal data and confidentiality. Therefore the following checkpoints need to be fulfilled by any third party before and during all times of integration:

- The third party must be GDPR compliant themselves;
- The third party is required to have their data residency in the UK or the EU;
- The third party must ensure that any used sub-processors are GDPR compliant as well;
- A process for handling data breaches and notifying Healistic in the event of a data breach must be in place.

**Right for patients to request and receive all information that Healistic holds on them**

Patients can request information on the data Healistic stores about them, how it is used and how long it is stored for. Healistic will provide this data free of charge within 4 weeks after proof of identity is received. The data will be provided securely in a common machine-readable electronic format.

**Right for patients to request correction of information that Healistic holds on them**

If a patient spots mistakes in the data Healistic holds on them, they can submit a request for the data to be corrected. Healistic commits to correct this data free of charge within 4 weeks after receipt of proof of identity and correct data.

**Right for patients to request deletion of information that Healistic holds on them**

If a patient requests deletion of their data, Healistic will comply with the request, if the deletion is not in conflict with legal obligations and professional requirements to store the data. Healistic commits to delete this data free of charge within 4 weeks after receipt of proof of identity. This request will lead to a halt of services for that patient.

**Right for patients to request that Healistic stops processing information that Healistic holds on them**

If a patient requests to stop processing of their data, Healistic will comply with the request; any existing data will be retained. If this request relates to all kinds of processing, this will lead to the cessation of provision of services for that patient. If this request relates only to the processing of data for marketing purposes, the patient will still be able to access services via the platform.