Privacy Policy Analysis Template

\*\*Service:\*\* Meta/Facebook

\*\*Category:\*\* Social Media

\*\*Policy URL:\*\* <https://mbasic.facebook.com/privacy/policy/printable/#8>

\*\*Date Accessed:\*\* 4/16/25

## 1. Data Collection

- What personal data is collected?  
- Is location, device, or behavioral data included?  
- Are cookies or trackers used?

* **User-Provided Information:** Includes content you create (posts, comments, audio), contact details, and communications with Meta.
* **Device and Network Information:** Encompasses device characteristics, software, activity (e.g., whether the app is in the foreground), identifiers, device signals, location-related information, and network details like IP addresses.
* **Usage Data:** Covers metadata about content and messages, types of content you interact with, app and feature usage, transaction details, hashtags used, and activity frequency and duration.
* **Information from Partners:** Data collected through Meta’s Business Tools, integrations, and technologies like the Meta Audience Network when you interact with partner sites or apps.
* **Direct Collection:** Data you provide through interactions with Meta Products.
* **Automated Technologies:** Use of cookies, device signals, and other technologies to collect data as you use Meta Products.
* **Third-Party Partners:** Information shared by partners who use Meta’s business tools and technologies.

## 2. Data Sharing

- Who is data shared with (advertisers, partners)?  
- Is there international data transfer?  
- Does the company use third-party processors?

**Third-Party Sharing:**

* Meta shares information with service providers who perform services on its behalf, such as payment processing, customer support, and marketing.
* Information is also shared with external researchers for purposes like advancing scholarship and promoting safety.
* Meta may share information in response to legal requests or to comply with applicable laws.

**International Transfers:**

* User information may be transferred globally, including to countries where Meta operates data centers or has partners.
* Meta ensures appropriate safeguards are in place for international data transfers, such as encryption during transit.

**Service Provider Requirements:**

* Service providers are required to adhere to strict data protection and confidentiality obligations, ensuring the security and integrity of user data.

## 3. User Rights

- Can users access their data?  
- Can users delete or correct their info?  
- Is data portability supported?

**Access Rights:**

* Users can access their data through Meta’s Privacy Center, where they can view and manage the information collected about them.

**Deletion Rights:**

* Users have the right to delete their data. This can be done through account settings, where users can delete specific information or their entire account.

**Portability Options:**

* Meta provides tools for users to download their data, facilitating data portability.

## 4. Opt-Out Options

- Can users opt out of tracking, marketing, or data sales?  
- How easy is the opt-out process?

**Opt-Out Mechanisms:**

* Users can manage their ad preferences and opt out of certain data processing activities through settings.

## 5. Clarity & Readability

| **Feature** | **Meta Privacy Policy** |
| --- | --- |
| **Grade Level** | ~12th to college level |
| **Length & Complexity** | Long and moderately hard to follow |
| **User-Friendly Summaries** | Yes, in the Privacy Center (not in the main document) |
| **Visual Aids** | Minimal (mostly text; some help docs include guides or walkthroughs) |

## Summary Matrix

|  |  |  |
| --- | --- | --- |
| Feature | Yes/No | Notes |
| Access Rights |  |  |
| Deletion Rights |  |  |
| Data Sharing Stated |  |  |
| Opt-Out Available |  |  |
| GDPR/CCPA Mentioned |  |  |

Meta’s privacy policy **generally aligns with the legal expectations** set out in the current U.S. privacy framework, especially for states like California. But it:

* **Pushes the boundaries** of what’s considered “sharing” vs. “selling,”
* **Relies heavily on user action** to limit data use (rather than opt-in by default),
* And **has a history of regulatory violations**, suggesting **operational issues even with compliant policies**.

**Meta has made significant efforts to align with GDPR**, especially in:

* Rights,
* Documentation,
* Transparency, and
* Technical safeguards.

However, it **continues to face enforcement action** for:

* Consent violations,
* Unlawful data transfers,
* And the way it uses personal data for profiling and ads.

\*\*Service:\*\* Walgreens

\*\*Category:\*\* Healthcare

\*\*Policy URL:\*\* <https://www.walgreens.com/privacycenter/privacy-policy?utm_source=chatgpt.com>

\*\*Date Accessed:\*\* 4/16/25

## 1. Data Collection

- What personal data is collected?  
- Is location, device, or behavioral data included?  
- Are cookies or trackers used?

**Types of Data Collected:**

* **Identifiers:** Name, email address, street address, phone number, and IP address.
* **Personal Information:** Information that identifies, relates to, describes, or is capable of being associated with a particular individual.
* **Commercial Information:** Records of products or services purchased, obtained, or considered, and other purchasing or consuming histories or tendencies.
* **Internet Activity:** Browsing history, search history, and information regarding a consumer’s interaction with the website, application, or advertisement.
* **Geolocation Data:** Physical location information, such as ZIP codes entered to see nearby pharmacies and precise location data when visitors grant access.

**Collection Methods:**

* **Direct Collection:** Information provided by users through interactions with Walgreens’ websites, mobile applications, and in-store visits.
* **Automated Technologies:** Use of cookies, web beacons, and similar technologies to collect information about users’ interactions with the website and services.
* **Third-Party Sources:** Information obtained from partners, advertising networks, data suppliers, and social media companies.

## 2. Data Sharing

- Who is data shared with (advertisers, partners)?  
- Is there international data transfer?  
- Does the company use third-party processors?

**Third-Party Sharing:**

* Walgreens may share personal information with service providers for business purposes, such as payment processing and marketing.
* Information may also be shared with third parties for purposes that could be considered a “sale” under certain state laws.

**International Transfers:**

* The privacy policy does not explicitly detail international data transfers.

**Service Provider Requirements:**

* Service providers are contractually obligated to use personal information only for specified purposes and to protect its confidentiality.

## 3. User Rights

- Can users access their data?  
- Can users delete or correct their info?  
- Is data portability supported?

**Access Rights:**

* Users can request access to their personal information collected by Walgreens.

**Deletion Rights:**

* Users have the right to request the deletion of their personal information, subject to certain exceptions.

**Portability Options:**

* Upon request, Walgreens provides users with their personal information in a portable, machine-readable format.

## 4. Opt-Out Options

- Can users opt out of tracking, marketing, or data sales?  
- How easy is the opt-out process?

**Opt-Out Mechanisms:**

* Users can opt out of the sale or sharing of their personal information through the Data Preferences page or by contacting Walgreens at 800-925-4733.

## 5. Clarity & Readability

| **Feature** | **Walgreens Privacy Policy** |
| --- | --- |
| **Grade Level** | Approximately 12th to college level |
| **Length & Complexity** | Long and moderately complex; detailed with legal and technical terms |
| **User-Friendly Summaries** | Available in the Privacy Center with topic-based summaries and FAQs |
| **Visual Aids** | Minimal; primarily text-based with some interactive elements in the Privacy Center |

Walgreens is fully compliant with US privacy laws. It does not meet the EU privacy standards because it does not serve that market.

\*\*Service:\*\* Fidelity

\*\*Category:\*\* Financial Services

\*\*Policy URL:\*\* <https://www.fidelity.com/privacy/policy?utm_source=chatgpt.com>

\*\*Date Accessed:\*\* 4/16/25

## 1. Data Collection

- What personal data is collected?  
- Is location, device, or behavioral data included?  
- Are cookies or trackers used?

**Types of Data Collected:**

* **Personal Identifiers:** Name, Social Security number, address, email, phone number.
* **Financial Information:** Account balances, transaction history, investment preferences.
* **Digital Data:** Device type, browser type, IP address, pages visited, and average time spent on digital offerings.

**Collection Methods:**

* **Direct Interactions:** Information provided by users through applications, forms, and customer service interactions.
* **Automated Technologies:** Use of cookies and similar technologies to collect technical and navigational information.
* **Third-Party Sources:** Information from consumer reporting agencies and other third-party data sources to verify identity and understand product and service needs.

**Purpose Specification:**

* To service, maintain, and protect accounts.
* To process transactions and respond to inquiries.
* To develop, offer, and deliver products and services.
* To operate and manage the business.
* To fulfill legal and regulatory requirements.

## 2. Data Sharing

- Who is data shared with (advertisers, partners)?  
- Is there international data transfer?  
- Does the company use third-party processors?

**Third-Party Sharing:**

* Fidelity may share personal information with service providers for business purposes, such as processing transactions and servicing accounts.
* Information may also be shared with affiliates for marketing purposes, as allowed by law.

**International Transfers:**

* The privacy policy does not explicitly detail international data transfers.

**Service Provider Requirements:**

* Service providers are contractually obligated to use personal information only for specified purposes and to protect its confidentiality.

## 3. User Rights

- Can users access their data?  
- Can users delete or correct their info?  
- Is data portability supported?

**Access Rights:**

* Users can request access to their personal information collected by Fidelity.

**Deletion Rights:**

* Users have the right to request the deletion of their personal information, subject to certain exceptions.

**Portability Options:**

* Upon request, Fidelity provides users with their personal information in a portable, machine-readable format.

## 4. Opt-Out Options

- Can users opt out of tracking, marketing, or data sales?  
- How easy is the opt-out process?

**Opt-Out Mechanisms:**

* Fidelity provides a “Do Not Sell or Share My Personal Information” link for users to opt out of the sale or sharing of their personal information.

**5. Security Measures**

**Storage Practices:**

* Fidelity retains personal information for as long as necessary to fulfill the purposes outlined in the privacy policy, comply with legal obligations, and resolve disputes.

**Protection Methods:**

* Fidelity employs reasonable security measures, including administrative, technical, and physical safeguards, to protect personal information.

**Breach Notification:**

* While specific breach notification procedures are not detailed, Fidelity is committed to protecting personal information and complying with applicable laws regarding data breaches.

## 6. Clarity & Readability

| **Feature** | **Fidelity Privacy Policy** |
| --- | --- |
| **Grade Level** | Approximately 12th to college level |
| **Length & Complexity** | Long and moderately complex; detailed with legal and technical terms |
| **User-Friendly Summaries** | Available in the Privacy Center with topic-based summaries and FAQs |
| **Visual Aids** | Minimal; primarily text-based with some interactive elements in the Privacy Center |

**U.S. Privacy Laws:**

* Fidelity’s privacy practices align with U.S. federal laws, such as the Gramm-Leach-Bliley Act (GLBA), and state laws, including the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA).
* The company provides notices at collection, supports user rights (access, deletion, portability), and offers opt-out mechanisms for the sale or sharing of personal information.

**EU Privacy Laws (GDPR):**

* Fidelity’s privacy policy does not explicitly reference the General Data Protection Regulation (GDPR).
* Key GDPR requirements, such as specifying lawful bases for processing, appointing a Data Protection Officer (DPO), and detailing international data transfer mechanisms, are not addressed in the policy.
* Therefore, Fidelity may not be fully compliant with GDPR standards, especially if offering services to EU residents.

\*\*Service:\*\* React Health

\*\*Category:\*\* Healthcare

\*\*Policy URL:\*\* <https://rhcinfo.reacthealth.com/RHPlusPrivacyPolicyv2.html?utm_source=chatgpt.com>

\*\*Date Accessed:\*\* 4/16/25

## 1. Data Collection

- What personal data is collected?  
- Is location, device, or behavioral data included?  
- Are cookies or trackers used?

**Types of Data Collected:**

* **Usage Data:** Time/duration of use, air/breathing pressure, respiratory indices (AHI, AI, HI, CAI), leak information, serial number, and other information related to the user’s treatment.
* **Personal Information:** Name, email address, birthdate, and device serial number (collected if the user creates an account and registers the device).
* **Feedback and Questions:** Information voluntarily submitted by users, which may include email address, online logs, device logs, and serial number.
* **Facial Recognition Data:** Temporarily scanned facial geometry for optional mask fitting feature; no facial data or images are stored or shared.

**Collection Methods:**

* **Device Integration:** Data received digitally through a modem in the device, via SD card upload by a medical provider, or by scanning QR codes generated by the device using the app.
* **User Input:** Personal information entered by users when creating an account and registering the device.

**Purpose Specification:**

* To make usage data available to medical professionals for monitoring and treatment purposes.
* To perform legal duties or obligations.
* To respond to emergencies, including public health emergencies.
* To maintain the safe and stable operation of the device.

## 2. Data Sharing

- Who is data shared with (advertisers, partners)?  
- Is there international data transfer?  
- Does the company use third-party processors?

**Third-Party Sharing:**

* Usage data may be shared with third-party service providers for data processing, hosting services, maintenance services, compliance risk assessments, data analysis, and customer services.
* Data may also be shared with affiliates, subsidiaries, or companies owned or controlled by React Health.
* In the event of a business transfer, data may be shared with the successor entity.

**International Transfers:**

* All data is stored and processed in a secure cloud infrastructure in the U.S.A.

**Service Provider Requirements:**

* Service providers are contractually obligated to apply adequate security and confidentiality measures and to process data only in accordance with instructions.

## 3. User Rights

- Can users access their data?  
- Can users delete or correct their info?  
- Is data portability supported?

**Access Rights:**

* Users can access their usage data via the app.

**Deletion Rights:**

* Users may delete usage data in the app by deleting the app itself.

**Portability Options:**

* The policy does not explicitly mention data portability options.

## 4. Opt-Out Options

- Can users opt out of tracking, marketing, or data sales?  
- How easy is the opt-out process?

**Opt-Out Mechanisms:**

* Users may request restrictions on the access of their usage data by contacting React Health.

**5. Security Measures**

**Storage Practices:**

* Data is retained for ten (10) years from the date of receipt.

**Protection Methods:**

* Data is stored in secure servers with access limited to relevant personnel.
* A combination of technical and administrative security controls are utilized to maintain data security.
* Users are encouraged to enable additional security features on their devices, such as PINs, fingerprint security, or facial recognition, and to keep their operating systems and apps up to date.

**Breach Notification:**

* In the event of a confirmed breach, affected users will be notified as required by applicable laws.

## 6. Clarity & Readability

| **Feature** | **React Health Plus App Privacy Policy** |
| --- | --- |
| **Grade Level** | Approximately 12th to college level |
| **Length & Complexity** | Long and moderately complex; detailed with legal and technical terms |
| **User-Friendly Summaries** | Not specified; the policy is primarily text-based |
| **Visual Aids** | Minimal; primarily text-based with some interactive elements in the app |

**U.S. Privacy Laws:**

* The policy indicates compliance with applicable U.S. laws, including HIPAA, by ensuring data is stored and processed in secure servers within the U.S. and by implementing appropriate security measures.

**EU Privacy Laws (GDPR):**

* The policy does not explicitly reference the General Data Protection Regulation (GDPR).
* Key GDPR requirements, such as specifying lawful bases for processing, appointing a Data Protection Officer (DPO), and detailing international data transfer mechanisms, are not addressed in the policy.
* Therefore, React Health may not be fully compliant with GDPR standards, especially if offering services to EU residents.

| **Category** | **Facebook (Meta)** | **Walgreens** | **Fidelity** | **React Health** |
| --- | --- | --- | --- | --- |
| **Unique Features** | AI-driven personalization, Ad controls and dashboards, TLDR summaries | HIPAA-specific disclosures, State-by-state privacy notices | GLBA compliance, “Do Not Sell” option, Financial data tools | CPAP data tracking, Facial scan (not stored), Device data use only |
| **Regulatory Compliance** | ✅CCPA/CPRA  ⚠️ Partial GDPR compliance | ✅ HIPAA  ✅ CCPA  ⚠️ No GDPR reference | ✅CCPA/CPRA  ✅ GLBA  ⚠️ No GDPR reference | ✅ HIPAA safeguards  ⚠️ No GDPR/CCPA reference |
| **Best Practices** | Visual and layered content, Customizable controls, Transparency | Strong HIPAA protections, State law adaptation | Clear opt-out choices, Data use timelines | Clear on CPAP data use, Temporary biometric use |
| **Worst Practices** | Complex wording, Limited GDPR support | Dense legal language, Lacks summary or visual aids | Legalistic wording, No GDPR references | No portability tools, Minimal education or visual explanation |
| **User-Friendliness** | TLDRs, 10th–12th grade level, Easy-to-navigate controls | Text-heavy, Few visual aids | Privacy Center tools, Dense policy text | App offers some controls, No visual summaries |