Data Deletion and Retention Policy

Version Control:

Version	Date	Author	Approver	Change
V1	22/08/2024	DNK Security	CTO	Initial Version
V2	20/10/2024	Mellow Software, Inc.	CEO	Rebranding

Contents

References:

SOC 2 Criteria: *CC6.5*

ISO 27001:2022 Requirements: *Clause 7.5.3*

ISO 27001:2022 Annex A: *A.5.1, A.5.33, A.8.13, A.8.10, A.5.1, A.5.33, A.7.10, A.7.14*

Keywords: *Data Retention, Grace Period*

1.1 Purpose

This policy outlines the requirements and controls/procedures Clara Health has implemented to manage the deletion of customer data.

Roles and Responsibilities:

The Chief Information Security Officer (CISO) is responsible for developing and maintaining the Data Deletion Policy. The CISO is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the company's information security management system and program.

1.2 Policy

1.2.1 For Customers

- Customer data must be retained for as long as the account is in active status.
- Data must enter an “expired” state when the account is voluntarily closed.
- Expired account PII data will be encrypted and retained for a maximum of 4 years.
- Customers that wish to voluntarily close their account must download their data manually prior to closing their account.

- If a customer account is involuntarily suspended, then there is a 90 days grace period during which the account will be inaccessible but can be reopened if the customer meets their payment obligations and resolves any terms of service violations.
- If a customer wishes to manually backup their data in a suspended account, they must ensure that their account is brought back to good standing so that the user interface will be available for their use.
    - After 90 days, the suspended account will be closed and the data will enter the “expired” state. PII data must be permanently encrypted and retained indefinitely thereafter (except when required by law to retain).

1.2.2 Return and Deletion

Upon the date of cessation of any Company Services involving the Processing of Customer Personal Data Clara Health must promptly cease all Processing of Customer Personal Data for any purpose other than for storage or as otherwise permitted by the Clara Health DPA.

Subject to Clara Healths DPA, and to the extent technically possible in the circumstances (as determined in Clara Health’s sole discretion), on written request to Clara Health (to be made no later than fourteen (14) days after the Cessation Date, Clara Health must within fourteen (14) days of such request:

1. Return a complete copy of all Customer Personal Data within Clara Health’s possession to Customer by secure file transfer, promptly following which Clara Health shall delete or irreversibly anonymise all other copies of such Customer Personal Data; or
2. either (at its option) delete or irreversibly anonymise all Customer Personal Data within Clara Health’s possession.
3. In the event that during the Post-cessation Storage Period, Customer does not instruct Clara Health in writing to either delete or return Customer Personal Data pursuant to Paragraph 9.2 of the Clara Health Data Processing Addendum, Clara Health shall promptly after the expiry of the Post-cessation Storage Period either (at its option) delete; or irreversibly render anonymous, all Customer Personal Data then within Clara Health possession to the fullest extent technically possible in the circumstances.

4. Clara Health may retain Customer Personal Data where permitted or required by applicable law, for such period as may be required by such applicable law, provided that Clara Health shall:
    1. maintain the confidentiality of all such Customer Personal Data, subject to applicable law; and
    2. Process the Customer Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention.
5. Operational clarification: Certification of deletion of Customer Personal Data, including as described in Clauses 8.5 and 16(d) of the EU SCCs (if and as applicable), shall be provided only upon Customer's written request.

1.2.3 For Visitors to our Website Properties

This policy only applies to data collected from Clara Health's website properties only. By way of example, a form submittal to engage the Clara Health Sales organization. The policy below does not apply to first party data provided by our customers via the Clara Health Platform or Data from 3rd Party Data Sources.

Clara Health will retain personal information collected from our website properties (such as Clara Health.io) for as long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements, to establish or defend legal claims, or for Compliance and protection purposes.

To determine the appropriate retention period for personal information, consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of your personal information, the purposes for which we process the personal information and whether we can achieve those purposes through other means.

When we no longer require the personal information we have collected about visitors, we will either delete or anonymize it or, if this is not possible (for example, because such personal information has been stored in backup or opt-out archives), securely store the personal information and isolate it from any further processing until deletion is possible. Anonymize personal information (so that it can no longer be associated with the visitor) but kept in a state where we may use this information indefinitely without further notice to the visitor.