



## PSLT - Healthcare Shield for Application Services (2022v1)

1. **Customer Responsibilities.** Customer is solely responsible for:
  - 1.1 ensuring that Customer creates, receives, maintains, or transmits Permitted Sensitive Personal Data in compliance with all applicable laws, rules, guidelines, regulations, and codes;
  - 1.2 ensuring that Customer retains, exports, and deletes Permitted Sensitive Personal Data in compliance with any applicable laws, rules, guidelines, regulations, and codes;
  - 1.3 ensuring that Permitted Sensitive Personal Data is made available and incorporates any amendments in compliance with all applicable laws, rules, guidelines, regulations, and codes; and
  - 1.4 ensuring that if Customer is a Covered Entity or Business Associate under HIPAA and is creating, receiving, maintaining, or transmitting Permitted Sensitive Personal Data through HIPAA-Ready Application Services, that Customer has executed a BAA with Adobe and is licensing Healthcare Shield.

Adobe will not be responsible for any failure in the operation or security of the Application Services caused by Customer's failure to meet the obligations outlined in sections 1.1 to 1.4 above or caused by Customer Customizations.
2. **Data Retention.** If Customer is required to retain its data for a specific time, Customer must export its data from the Application Services where available prior to the data deletion storage limits set out in the applicable underlying Application Services PSLTs and Product Descriptions.
3. **License Restriction.** Customer may not use, ingest, collect, share, or integrate Permitted Sensitive Personal Data with any non-HIPAA-Ready Products and Services.
4. **Permitted Sensitive Personal Data.** Notwithstanding any restrictions on Sensitive Personal Data in the General Terms, Customer may use the HIPAA-Ready Application Services in connection with Healthcare Shield to create, receive, maintain, or transmit to Adobe, Permitted Sensitive Personal Data, as defined in this PSLT, provided Customer has obtained all necessary permissions, consents, clearances, and authorization required under applicable law or regulation for such use, including marketing, and Customer's activities do not otherwise cause Adobe or Adobe's third party providers to violate any applicable law or regulation.
5. **Additional Claims.** Customer's indemnification obligations set forth in the General Terms will also apply to (a) Customer's use, collection, transmission, and processing Permitted Sensitive Personal Data through non-HIPAA-Ready Products and Services, (b) Customer's use of HIPAA-Ready Application Services in violation of HIPAA, and (c) Customer's use, collection, transmission, and processing of Permitted Sensitive Personal Data in violation of applicable laws, rules, guidelines, regulations, and codes. The additional Claims in this section are treated as Data Privacy Claims or Other Claims as described in the applicable General Terms. The Limitation of Liability provision in the applicable General Terms does not apply to Customer's liability or obligations under this section.
6. **Definitions.** All capitalized terms used herein and not defined below are defined in the Business Associate Agreement or applicable Sales Order.
  - 6.1 **"Application Services"** means the following: (i) Real-Time Customer Data Platform Prime or Ultimate (B2C Edition) and (B2P Edition - Consumer Audiences only); (ii) Adobe Journey Optimizer; and (iii) Customer Journey Analytics.
  - 6.2 **"HIPAA-Ready"** means the Adobe Products and Services: (1) listed on <https://www.adobe.com/trust/compliance/hipaa-ready.html>; and (2) that Customer is expressly

authorized via a written Sales Order to use to create, receive, maintain, or transmit Permitted Sensitive Personal Data in accordance with the BAA and applicable Agreement.

- 6.3 **“Permitted Sensitive Personal Data”** means an individual’s financial information, medical or health information, but specifically excluding substance abuse, mental, or genetic health records, or health records of a minor, full account number, full credit card numbers, government identifiers, and personal information of children protected under any child protection laws (such as the personal information defined under the U.S. Children’s Online Privacy Act (“COPPA”)).