Privacy Compliance Evaluation Checklist for Customer Data Platforms (CDPs)

Use this checklist to assess whether a Customer Data Platform can meet the operational demands of HIPAA-regulated marketing environments. This list is designed to validate compliance not just at the infrastructure level, but across data handling, suppression, consent, and auditability.

HIPAA & BAA Readiness

□ Vendor provides a signed BAA (standard or on request)
□ Platform documents HIPAA-compliant infrastructure and data flows
□ PHI can be encrypted at rest and in transit
□ Data minimization and purpose limitation policies are published

Consent Enforcement

□ Consent status is captured and stored for all users
□ Consent is enforced at the point of data collection (e.g., tags, forms)
□ Consent flags are used in downstream segmentation and activation
□ Consent decisions are synchronized across web, mobile, and CRM systems

Suppression & De-Identification

□ Platform includes native support for audience suppression
□ De-identification workflows (e.g., tokenization, masking) are available
□ PHI is blocked from flowing to unapproved destinations or tags
□ No third-party scripts are fired prior to consent

Auditability & Role-Based Access

□ Platform maintains logs of user access, exports, and configuration changes
□ Data access can be restricted by role, team, or workspace
□ Admins can view full history of data sharing or profile edits
□ Audit logs are exportable for compliance reporting

Vendor & Ecosystem Controls

□ Platform monitors for non-compliant pixels, destinations, or vendor tags
□ CMP integration is supported or embedded
□ Platform alerts or blocks unapproved data flows
□ All vendor integrations are documented and governed

intros@wheelhousedmg.com www.wheelhousedmg.com