

Marketing analytics designed to support HIPAA compliance.

Backed by a BAA and documented security controls.

01 What Piwik PRO confirms

CONTRACTS

A BAA to anchor the relationship

We provide our BAA for your legal review or are happy to review yours to reach mutual agreement.

A DPA where your obligations require one

A Data Processing Agreement addressing applicable controller/processor obligations, subprocessors, data subject rights, and breach notification requirements.

DATA CONTROL

Data residency you control

US Microsoft Azure hosting for your BAA-covered deployment. No default outbound sharing to ad networks; data reaches third parties only through integrations you configure.

IP address masking

Configurable at the platform level to reduce the risk of inadvertent collection of location data.

PHI PROTECTION

Two ways to handle PHI

Process PHI within BAA-covered services where appropriate, or configure collection to minimize PHI before transmission to meet your compliance requirements.

PHI kept out of storage by design

Data layer rules you define at contract time are enforced at the platform level. Responsibility is set in the BAA and enforced technically, not just on paper.

ACTIVATION & ACCOUNTABILITY

Customer-controlled activation to ad platforms

Activate to supported ad platforms with controls over what data is shared. You remain responsible for ensuring any third-party disclosure is permitted and for obtaining any required authorization.

Exportable audit trail

Full event-level audit logging, user access logs, and data processing records. Export for regulatory review, litigation hold, or OCR inquiry.

02 Compliance & assurance

HIPAA

Piwik PRO undergoes an annual HIPAA compliance assessment as part of its SOC 2 Type II audit process, performed by an independent third party.

Privacy by design

US hosting on Microsoft Azure for BAA-covered deployments, with AES-256 encryption at rest. We don't monetize your data or use it for advertising or model training.

CCPA

Supported where applicable.

03 Documentation available

IMMEDIATELY

- ✓ Standard BAA
- ✓ Data Processing Agreement
- ✓ ISO 27001 certificate
- ✓ SOC 2 Type II report (NDA required)
- ✓ Security whitepaper
- ✓ Subprocessor list
- ✓ MSA

ON REQUEST

- Completed security questionnaires (CAIQ, SIG Lite, custom formats)
- Data flow diagrams
- Penetration test summary
- Incident response policy

GOOD TO KNOW

Why GA4 raises exposure

Google doesn't offer a BAA for Google Analytics, which limits its use where PHI may be disclosed to Google. If PHI reaches Google through URLs, event parameters, or form fields, that may be an impermissible disclosure under HIPAA. HHS OCR and the FTC have both warned healthcare organizations about the privacy and security risks of third-party tracking technologies, including Google Analytics.

Trusted by regulated health systems Each ran their own legal and security review. Each chose Piwik PRO.



Engage directly with our legal and compliance team. Request the documentation package and start your BAA review:

[Get in touch](#) →