PIWIK PRO

How to make your analytics HIPAA-compliant: A practical checklist for healthcare marketers

This comprehensive checklist helps healthcare organizations evaluate the HIPAA compliance of their analytics setups.

> *Disclaimer:* This checklist should be reviewed with qualified legal counsel familiar with healthcare privacy law. Compliance requirements may vary based on your specific use case, geographic location, and applicable state laws.

Understanding your compliance landscape

Federal and state privacy laws

Before beginning your assessment, determine which privacy laws apply to your organization:

Federal requirements:

- HIPAA Privacy Rule and Security Rule
- HITECH Act breach notification requirements

State requirements to consider:

- **New York:** NYHIPA
- **California:** CMIA (Confidentiality of Medical Information Act)
- **Illinois:** Genetic Information Privacy Act
- **Texas:** Medical Privacy Act

> *Action item: Consult with legal counsel to identify all applicable privacy laws in your operating jurisdictions.*

- Have you implemented server-side or client-side URL scrubbing that removes PHI (including condition names, patient identifiers, and appointment details) before data reaches your analytics platform?

PHI/ePHI protection & data collection

Protected health information (PHI) and electronic PHI (ePHI) include any individually identifiable health information created, received, maintained, or transmitted by covered entities. This encompasses medical records, billing information, health insurance details, and even IP addresses or geolocation data when linked to health services.

Your HIPAA obligations depend on whether you process PHI/ePHI in your analytics platform.

Key principle: The Minimum Necessary Rule requires that you only collect and process the minimum amount of PHI needed to accomplish your intended purpose.

Using an analytics platform to collect and process ePHI or PHI

You collect identifiable information to analyze individual patient journeys, personalize experiences, and understand specific patient behaviors. This makes compliance with HIPAA requirements necessary, but it also allows sophisticated analytics.

Common use cases for PHI collection:

- Patient portal analytics tracking individual engagement
- Telehealth platform usage monitoring for quality improvement
- Clinical decision support tools analyzing patient-specific data
- Research studies requiring identifiable patient tracking
- Care coordination platforms tracking individual patient journeys
- Population health management requiring individual-level data

If you intentionally collect PHI/ePHI for patient portal analytics, telehealth monitoring, or personalized health experiences, you must address all requirements in this section.

Analytics vendor capabilities

- [ ] Have you verified that your analytics vendor explicitly permits the collection of PHI in their Terms of Service?

- [ ] Are you using a HIPAA-compliant platform (such as Piwik PRO or Adobe Analytics for Healthcare) rather than platforms like Google Analytics, which prohibit the use of PHI?

Geolocation data management

- [ ] Have you implemented AES-256 encryption, role-based access controls, and audit logging for all geolocation data?

URL and parameter protection

- [ ] Have you implemented server-side or client-side URL scrubbing that removes PHI (including condition names, patient identifiers, and appointment details) before data reaches your analytics platform?

Post-login area protection

- [ ] Have you implemented separate tracking configurations for authenticated areas with enhanced encryption?

- [ ] Have you configured secure session management with automatic timeout after 15-30 minutes of inactivity?

- [ ] Have you disabled or modified session recording, heatmaps, and form analytics in areas that display PHI?

Mobile application security

- [ ] Have you implemented app-level encryption using iOS Keychain or Android Keystore for PHI stored on devices?

- [ ] Have you configured secure storage that prevents PHI from being backed up to cloud services?

- [ ] Have you implemented certificate pinning to prevent man-in-the-middle attacks during data transmission?

- [ ] Do your push notifications avoid containing PHI in notification text?

Minimum necessary compliance

- [ ] Have you documented business justification for each specific PHI data point you collect?
- [ ] Have you implemented technical controls (such as form validation and data collection filters) to prevent collecting more than what's documented as necessary?
- [ ] Do you review your PHI collection practices at least quarterly to ensure you're collecting only what's necessary?
- [ ] Have you defined role-based access policies that restrict access to specific types of PHI based on job function?
- [ ] Have you documented and communicated internal policies that define how PHI is accessed, used, and disclosed in accordance with the minimum necessary standard?

Third-party integration protection

- [ ] Have you configured integration filtering to prevent PHI from being transmitted to third-party tools (such as chatbots, heat-mapping, or A/B testing platforms)?
- [ ] Have you executed separate BAAs with vendors that will receive PHI through integrations?
- [ ] Have you implemented technical safeguards (such as payload filtering and field-level controls) to ensure only non-PHI data is shared where applicable?
- [ ] Have you established legal safeguards (such as BAA enforcement and contractual restrictions) for all third parties receiving PHI?

Backup and recovery

- [ ] Do you have backup storage with automated daily encrypted backups that provide maximum recovery capability?
- [ ] Are backups stored in geographically redundant locations?
- [ ] Do you conduct quarterly restoration tests to verify the integrity of your backups?

Using an analytics platform without collecting and processing ePHI or PHI

You configure your analytics to track website visitors, patient portal usage, and marketing campaign performance without collecting any data that could identify specific individuals or their health conditions. This lowers the compliance burden but significantly limits what data you can access and how you can use it.

Without PHI, you lose:

- Individual-level insights about patient behavior
- Ability to segment by specific health conditions or treatments
- Personalization capabilities that improve patient experience
- Detailed ROI tracking for patient acquisition costs

If you've chosen not to collect PHI/ePHI, you must implement strict technical controls to prevent identifiable health information from entering your analytics platform.

Geolocation data

- [ ] Do you ensure your analytics doesn't track any geolocation data (even in hashed/salted IP addresses)?

URL and parameter protection

- [ ] Do you ensure no PHI is transmitted via URLs or custom attributes?

Email and device identifiers

- [ ] Do you ensure you don't track email addresses and device identifiers that could be linked to health activity?

Post-login areas

- [ ] Do you ensure you don't track sensitive data in post-login areas (such as patient portals and appointment systems)?

Unauthenticated pages with PHI

- [ ] Do you adequately protect user data on unauthenticated pages when it includes PHI (such as registration pages, symptom checkers, doctor search tools, and appointment schedulers)?

Configuration verification

- [ ] Do you regularly audit sample data exports to verify no PHI is being accidentally collected?
- [ ] Have you configured your analytics platform to block health-related parameters and form field data?

If you answered "no" to any of the above questions, you may be inadvertently collecting PHI and should follow the compliance requirements in the section for collecting and processing PHI.

De-identification

According to the HIPAA Privacy Rule, once data is properly de-identified using Expert Determination or Safe Harbor methods, you can use or disclose it without limitation and don't have to fulfill most of the HIPAA obligations covered in this document.

De-identified data doesn’t include user identifiers, so you won't be able to personalize content for returning visitors, analyze individual patient journeys, or build detailed conversion attribution models.

Business Associate Agreement (BAA)

A BAA is a legally binding contract between a covered entity and any vendor that creates, receives, maintains, or transmits PHI on its behalf. The BAA establishes each party's responsibilities for protecting PHI and outlines procedures for breach notification, data handling, and compliance verification.

Key principle: BAAs must be executed before any PHI access occurs, even for trials or demonstrations.

BAA requirements

Timing and scope

- [ ] Have you signed a BAA with your analytics platform provider before granting them any access to PHI?
- [ ] Have you executed separate BAAs with all subcontractors in the data chain (such as cloud hosting providers, CDN services, and backup storage providers)?

Essential BAA provisions

- [ ] Does your BAA include specific provisions for breach notification procedures with clear timelines for notifying you?
- [ ] Does your BAA clearly define data processing limitations specific to analytics?
- [ ] Have you included your right to audit the vendor's security practices (at least annually)?
- [ ] Does your BAA specify data return or destruction requirements upon contract termination?
- [ ] Does your BAA address the vendor's obligations in the event of security incidents?
- [ ] Have you established geographic restrictions on where data can be stored and processed (if required)?

HITECH Act compliance

- [ ] Have you updated all existing BAAs to reflect HITECH Act requirements, making business associates directly liable?

Vendor due diligence

- [ ] Have you requested and reviewed the vendor's SOC 2 Type II audit report (that was issued within the past 12 months)?
- [ ] Have you reviewed penetration testing results conducted within the past 6 months?
- [ ] Have you verified the vendor's incident response procedures and track record?
- [ ] Have you confirmed the vendor's experience with healthcare industry compliance?

Hosting infrastructure

Your hosting infrastructure is the foundation of your security architecture. While there's no HIPAA-certified hosting, it’s crucial to choose a provider that understands healthcare compliance requirements and maintains appropriate physical, technical, and administrative safeguards.

Key principle: Whether you choose cloud or on-premises hosting, you must know exactly where your data resides, who can access it, and how it's protected.

For cloud hosting

Infrastructure knowledge

- [ ] Do you know the physical location of your cloud servers and how they replicate data?
- [ ] Have you verified that data residency complies with any state-specific requirements (such as data sovereignty laws)?

Provider certifications

- [ ] Does your hosting provider have ISO 27001- and SOC 2 Type II-certified data centers?
- [ ] Does your provider conduct regular, independent security audits?
- [ ] Does your provider offer compliance documentation or audit reports (such as SOC 2 and ISO 27001) for your review under an NDA?

Contractual protections

- [ ] Do you have a Service Level Agreement (SLA) with security commitments and uptime guarantees?
- [ ] Will your cloud service provider sign a BAA covering their hosting services?

For on-premises hosting

Access controls and monitoring

- [ ] Do you hire independent auditors to verify who accesses and attempts to access PHI in your infrastructure?
- [ ] Have you implemented access controls that limit the number of employees who can view PHI?

Network security

- [ ] Do you use a secure VPN to connect to your infrastructure?
- [ ] Have you implemented network segmentation to isolate systems containing PHI?
- [ ] Do you actively monitor for intrusions and unusual network activity?

Data recovery

- [ ] Are your backup systems encrypted and stored separately from primary systems?
- [ ] Do you conduct periodic disaster recovery tests?

Note: If you host your analytics on-premises, you don't necessarily need to sign a BAA with your analytics partner.

Technical safeguards

Technical safeguards refer to the technology-based policies, procedures, and controls that protect electronic Protected Health Information (ePHI) and regulate access to it. Technical safeguards form the technological backbone of HIPAA compliance and are often the first line of defense against breaches. Organizations with robust technical safeguards can demonstrate that encrypted data rendered unusable doesn't constitute a reportable breach, potentially saving millions in notification costs.

Key principle: Under HIPAA, all the following technical safeguards are required: access control, audit controls, integrity controls, person/entity authentication, and transmission security.

Encryption standards

Data at rest and in transit

- [ ] Are you using AES-256 encryption with FIPS 140-2 Level 2 validated modules for all stored PHI?
- [ ] Are you using TLS 1.3 minimum for all PHI transmission (TLS 1.2 acceptable until 2026)?
- [ ] Have you enabled transparent data encryption (TDE) or equivalent for databases containing PHI?

Key management

- [ ] Are you using Hardware Security Modules (HSM) or cloud key management services for encryption key protection?
- [ ] Do you rotate encryption keys at least every 12 months?

Backup encryption

- [ ] Do you verify backup encryption through regular restore testing?

Access controls and authentication

Authentication requirements

- [ ] Have you implemented multi-factor authentication (MFA) for all users accessing PHI in analytics platforms?
- [ ] Do you enforce strong password policies (such as a minimum of 12 characters and complexity requirements)?
- [ ] Do you enforce 2FA or integrate with an external SSO/identity provider to secure access to systems that handle PHI?

Role-based access

- [ ] Have you implemented role-based access controls that assign permissions based on job function, following least privilege principles?
- [ ] Do you have a documented approval process for assigning or modifying role-based access to systems handling PHI?
- [ ] Are role-based permissions reviewed periodically and updated as needed?

Access management

- [ ] Do you have automated access revocation within 24 hours of employee termination?
- [ ] Do you conduct quarterly access reviews to verify the continued appropriateness of access levels?

Session security

- [ ] Have you configured automatic logoff after 15-30 minutes of inactivity?

Audit controls

Logging and monitoring

- [ ] Have you enabled comprehensive audit logging that captures user identity, timestamps, actions taken, and specific data accessed?
- [ ] Do you retain all audit logs for at least 6 years as required by HIPAA?
- [ ] Have you implemented real-time alerts for suspicious activities (such as multiple failed logins and bulk downloads)?

Transmission security

- [ ] Do you use encrypted channels (HTTPS, SFTP or VPN) for all PHI transmission?
- [ ] Have you verified that SSL/TLS certificates are properly configured and up to date?

Administrative safeguards

Administrative safeguards are the policies, procedures, and processes that govern how your organization manages security measures to protect electronic Protected Health Information (ePHI) and how your workforce conducts itself when handling patient information.

Key principle: If it's not documented, it didn't happen from a compliance perspective. Administrative safeguards require both creating the right policies and consistently following them.

Security management process

Risk assessment

- [ ] Do you conduct comprehensive risk assessments of your analytics platform at least once a year?
- [ ] Do you document identified vulnerabilities with severity ratings and remediation timelines?
- [ ] Do you ensure critical vulnerabilities are addressed within 30 days?

Sanction policy

- [ ] Have you created and communicated sanction policies for workforce members who violate security policies?

Assigned security responsibility

- [ ] Have you designated a specific security official responsible for developing and implementing security policies with documented authority and resources?
- [ ] Do you have designated representatives who will handle an incident if one occurs?

Workforce security

- [ ] Have you established termination procedures to ensure that ePHI access is removed within 24 hours?
- [ ] Do you have a formal onboarding process that assigns ePHI access only after documented approval based on job responsibilities?

Security awareness and training

Training program

- [ ] Do you provide initial HIPAA training before granting analytics access, and do you offer an annual refresher training?
- [ ] Does your training address analytics-specific risks (such as concerning PHI in URLs, data export handling, and password management)?
- [ ] Do you maintain training records for at least 6 years?

Security incident procedures

- [ ] Have you documented incident response procedures and designated a response team?
- [ ] Do you document all security incidents and conduct post-incident analysis?
- [ ] Do you conduct annual tabletop exercises to test breach response procedures?
- [ ] Are procedures and policies accessible to all employees?

Contingency planning

Backup and disaster recovery

- [ ] Have you created data backup plans with documented schedules and encryption requirements?
- [ ] Have you established disaster recovery plans with recovery time objectives (RTO) and recovery point objectives (RPO)?
- [ ] Do you conduct annual testing of your backup, restoration, and disaster recovery procedures?

Evaluation

- [ ] Do you conduct periodic evaluations of your security measures at least annually?
- [ ] Do you document evaluation findings and remediation plans?

Business associate management

- [ ] Do you maintain an inventory of all business associates with current BAA status?
- [ ] Do you have procedures for addressing contract breaches and terminating non-compliant relationships?
- [ ] Do you review certificates for your key partners at least once a year?

Breach response and notification

A breach is the unauthorized acquisition, access, use, or disclosure of PHI that compromises its security or privacy. HIPAA's Breach Notification Rule requires covered entities to notify affected individuals, HHS, and, potentially, the media when breaches occur, within strict timelines.

Key principle: Time is critical. You have 60 days from the date of discovery to notify affected individuals and HHS. Delayed notification can result in additional penalties up to $50,000 per violation.

Breach identification and assessment

Discovery and initial response (0-24 hours)

- [ ] Do you have procedures in place to immediately activate your incident response team upon discovering a potential PHI exposure?
- [ ] Can you quickly implement containment measures to prevent further unauthorized access?

Breach risk assessment (1-10 days)

- [ ] Can you complete a breach risk assessment using the HHS four-factor test within 10 days?
- [ ] Can you identify all affected individuals by querying audit logs and analytics databases?

Notification requirements

Individual and regulatory notification

- [ ] Can you notify the affected individuals within 60 days of discovering the breach?
- [ ] Do you have pre-approved notification letter templates that can be quickly customized?
- [ ] Do you know the notification requirements for HHS (within 60 days for 500+ individuals)?
- [ ] Do you have procedures in place for notifying the media if a breach affects 500 or more individuals in the same state?

Documentation and prevention

Breach documentation

- [ ] Do you document the date of breach discovery, the assessment methodology, and the findings?
- [ ] Do you retain all notification communications for at least 6 years?
- [ ] Do you document remediation actions with completion dates?

Preparedness measures

- [ ] Do you conduct annual tabletop exercises simulating various breach scenarios?
- [ ] Have you trained all employees on procedures for identifying and reporting breaches?

Ongoing compliance activities

- **Monthly:** Review access logs for unusual patterns, verify data retention settings
- **Quarterly:** Conduct access reviews, review and update risk assessments, and test backup restoration
- **Annually:** Comprehensive risk assessment, employee training, BAA reviews, disaster recovery testing, security evaluation

Regulatory resources:

- HHS Office for Civil Rights: https://www.hhs.gov/ocr/
- HIPAA Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/
- Breach Notification Rule: https://www.hhs.gov/hipaa/for-professionals/breach-notification/

Get HIPAA-compliant analytics and access to valuable patient insights without compromise

Piwik PRO offers privacy-compliant analytics and data activation that lets healthcare organizations personalize patient experiences while protecting their privacy. Whether you want to evaluate your analytics use cases or are ready to move to a new, HIPAA-compliant platform, our team is ready to help.

Connect with Piwik PRO today to start making data-driven decisions with complete confidence in your compliance:

Schedule a free demo **Contact us**

Or reach out directly:

North America
+1 (888) 444 0049

EMEA
+48 71 716 69 50

Email
sales@piwik.pro

Visit us at piwik.pro to learn more about our HIPAA-compliant analytics solutions.

This checklist should be reviewed with qualified legal counsel familiar with healthcare privacy law.
Compliance requirements may vary based on your specific use case, geographic location, and applicable state laws.