WHITE PAPER

Why WhatsApp, Viber, Telegram, Signal and Other Consumer Apps Are Not HIPAA-Secure Messaging

Encryption alone does not make a messaging app appropriate for protected health information. What healthcare agencies need to know about business associate agreements, administrative controls, and safer workflows.

GooScript | November 2026

This paper is general educational information, not legal advice. Vendor terms change; confirm current terms and consult qualified counsel before making compliance decisions.

Executive summary

Many clinicians and caregivers text patient details through the apps already on their phones. Several of these apps advertise strong end-to-end encryption, which leads to a common assumption: if messages are encrypted, they must be HIPAA compliant. That assumption is incorrect.

HIPAA does not certify apps. Instead, a covered entity or business associate must protect electronic protected health information (ePHI) through a combination of administrative, physical and technical safeguards, and must have a business associate agreement (BAA) with vendors that create, receive, maintain or transmit ePHI on its behalf. Consumer messaging apps generally fail on the organizational side: their providers do not offer BAAs for these consumer services, and the apps lack the central administration, audit trails, access governance and retention controls an agency needs to meet its obligations.

Key conclusions

- Encryption is one safeguard among many. It does not replace a BAA, risk analysis, access controls, audit controls or policies.
- WhatsApp, Signal, Telegram, Viber, Facebook Messenger, WeChat, Snapchat and standard SMS/iMessage are consumer services; their providers do not publicly offer BAAs for them.
- Using them for ePHI shifts uncontrolled risk to the agency: lost or shared phones, personal backups, no remote wipe of a single conversation, and no organization-owned record.
- The COVID-19 telehealth enforcement discretion that tolerated some consumer apps ended on May 11, 2023.
- Agencies should adopt a purpose-built platform with a signed BAA, organization-managed accounts and auditable records.

What HIPAA actually requires

The Security Rule (45 CFR Part 164, Subpart C) requires regulated entities to ensure the confidentiality, integrity and availability of ePHI. For messaging, the most relevant requirements include:

- **Risk analysis and risk management** (164.308(a)(1)): documented evaluation of how ePHI flows through each tool.
- **Business associate contracts** (164.308(b), 164.314(a)): written assurances from vendors that handle ePHI.
- **Access control** (164.312(a)): unique user identification, emergency access, automatic logoff, and encryption as an addressable specification.
- **Audit controls** (164.312(b)): mechanisms that record and examine activity in systems containing ePHI.
- **Integrity and transmission security** (164.312(c), (e)): protection against improper alteration and interception.

- **Workforce security and termination procedures** (164.308(a)(3)): removing access when staff leave.

“Addressable” does not mean optional. An entity must implement the specification when reasonable and appropriate, or document why not and adopt an equivalent alternative.

Why encryption is not enough

HHS guidance on cloud services states that a service provider which stores or transmits ePHI is a business associate even if it holds only encrypted data and has no decryption key, so a BAA is still required. The narrow “conduit” exception covers transmission-only services such as a telephone company or internet provider with transient access, not services that store messages, backups, contact data or metadata.

How popular apps compare

Summary based on publicly available vendor information as of November 2026. “Not offered” means no publicly available BAA for the consumer service; separate enterprise products from the same company may have different terms.

App	Vendor BAA for this service	Default encryption	Key gaps for agencies
WhatsApp	Not offered for consumer app	End-to-end	Personal accounts; cloud backups outside agency control; no agency audit log; Meta metadata collection
Signal	Not offered	End-to-end	No organizational admin, audit trail, user provisioning or retention controls
Telegram	Not offered	Standard chats are cloud chats, not end-to-end; Secret Chats opt-in	Messages stored on vendor servers by default; no agency governance
Viber	Not offered	End-to-end for supported chats	Consumer accounts tied to personal phone numbers; no admin or audit tools
Facebook Messenger	Not offered	End-to-end for personal chats	Consumer platform; data use under consumer terms; no agency controls
WeChat, Snapchat, others	Not offered	Varies	Consumer terms; data residency and retention outside agency control
SMS / MMS	Carriers do not sign BAAs	None end-to-end	Readable by carrier; stored on devices; easily misdirected
iMessage / FaceTime	Not offered for consumer services	End-to-end	Personal Apple IDs; iCloud backups; no agency audit or offboarding

Common gaps across consumer apps

- **No business associate agreement.** Without one, disclosing ePHI to the vendor is generally not permitted.
- **Personal ownership.** Accounts belong to the employee, not the agency. When staff leave, patient conversations leave with them.

- **No audit trail.** The agency cannot show who accessed or sent which records during an investigation or breach review.
- **Uncontrolled backups.** Chats may sync to personal Google Drive or iCloud accounts outside any BAA.
- **Notification previews.** Lock-screen previews can display patient details to anyone nearby.
- **No retention or legal-hold controls.** Disappearing messages can destroy records the agency must keep; permanent chats can retain data longer than policy allows.

Real-world risk

Breaches involving lost or stolen devices, misdirected messages and unauthorized access are recurring categories in breach reports to HHS. HHS also clarified in 2023 that its pandemic-era enforcement discretion for “non-public facing” consumer communication tools ended on May 11, 2023, and providers were given a transition period that has since closed. Agencies continuing to rely on consumer apps for ePHI should treat that as an unresolved compliance risk.

What qualifies as a HIPAA-appropriate messaging platform

No product is “HIPAA certified,” and no software makes an organization compliant on its own. A platform suited to ePHI should, at a minimum, offer:

- A signed BAA covering the messaging service.
- Encryption in transit and at rest.
- Organization-managed accounts with unique user IDs and role-based access.
- Immediate deactivation when staff are offboarded, plus remote session sign-out.
- Audit logs of sign-ins, message activity and administrative changes.
- Configurable retention aligned with agency policy.
- No PHI in push notification previews.
- Support for the agency's risk analysis and documented policies.

Recommended steps for agencies

- Inventory every channel staff use to discuss patients, including personal phones.
- Update policy to prohibit ePHI on consumer apps and SMS, and train staff with examples.
- Select a platform that signs a BAA and provides administrative and audit controls.
- Migrate active care teams, then disable or restrict the old channels.
- Document the change in your risk analysis and review it at least annually.

How GooScript helps

GooScript provides secure messaging designed for healthcare agencies, with a business associate agreement, organization-managed users, role-based access and activity records. It is one part of a

compliance program; agencies remain responsible for their policies, training and risk analysis. Learn more at gooscript.com or request a demo at gooscript.com/book-a-demo.

Sources

1. HHS, Guidance on HIPAA & Cloud Computing: hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing
2. HHS, Business Associates guidance: hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates
3. HHS, Notification of Enforcement Discretion for Telehealth (expired May 11, 2023): hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth
4. 45 CFR 164.308, 164.312, 164.314 (eCFR): ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164
5. Telegram FAQ, Secret Chats: telegram.org/faq