Holland & Hart

Cameron McCue

Associate
208.383.5110
Boise
clmccue@hollandhart.com

AI Chatbots and HIPAA: What Healthcare Providers Need to Know

Insight — June 19, 2026

Generative AI tools like ChatGPT, Google Gemini, and Microsoft Copilot are increasingly embedded in healthcare workflows—drafting clinical notes, summarizing patient records, composing patient messages, and supporting documentation. But the convenience these tools offer can create significant HIPAA exposure if providers are not careful about what information enters the tool, how it gets there, and who controls it on the other end.

1. Key Takeaways

- **Know your tool.** Before using any AI product with patient information, confirm whether a BAA is available and executed for the specific product tier and environment you are using.
- **Know your data.** Identify whether the information you are entering constitutes PHI, and whether it falls into a special category—psychotherapy notes, SUD records, or state-protected data—that requires additional consent or authorization beyond what a BAA provides.
- **Know your environment.** Ensure that workforce members understand which specific accounts and platforms are BAA-covered. The same chatbot accessed through a consumer account versus an enterprise account may have entirely different compliance profiles.
- **Apply the minimum necessary standard.** Limit what you input to what is reasonably needed for the task.
- **Do not assume "treatment purpose" is a safe harbor.** A treatment purpose may support the underlying use of PHI, but it does not eliminate the need for a BAA with a third-party vendor or patient authorization where otherwise required.

2. Who Is Regulated?

The HIPAA Privacy, Security, and Breach Notification Rules apply to **covered entities** (health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically) and **business associates**. 45 C.F.R. §§ 160.102(a)–(b), 160.103. Business associates are persons or entities that create, receive, maintain, or transmit PHI on

behalf of a covered entity—including for data analysis, billing, practice management, and consulting—or that provide legal, accounting, or other services involving PHI disclosure. *Id*. § 160.103. Post-HITECH, business associates are directly regulated and can face civil and criminal penalties for violations. *See* HITECH Act §§ 13401, 13404.

3. What Information Is Protected?

The HIPAA Privacy Rule protects **protected health information (PHI):** individually identifiable health information created or received by a covered entity that relates to a patient's past, present, or future health condition, care, or payment for care. 45 C.F.R. § 160.103. **Individually identifiable health information entered into or generated by a generative AI tool (clinical notes, diagnostic summaries, treatment histories) will typically meet the definition of PHI.**

Information properly de-identified under the expert determination or safe harbor method (removal of eighteen specified identifiers plus no actual knowledge of re-identification) is not PHI. 45 C.F.R. § 164.514(a)–(b).

4. The Core Question: Is PHI Leaving Your Control?

When a provider types or pastes patient information into a generative AI tool—even for something as routine as a chart note—that information may be leaving the provider's environment and entering the AI vendor's servers. This constitutes a disclosure of PHI, and the vendor—if it creates, receives, maintains, or transmits PHI on the provider's behalf—is a business associate under 45 C.F.R. § 160.103.

5. The Business Associate Agreement Requirement

A covered entity may disclose PHI to a business associate only if it "obtains satisfactory assurance that the business associate will appropriately safeguard the information" through a compliant **Business Associate Agreement (BAA)**. 45 C.F.R. §§ 164.502(e), 164.504(e). The BAA must be executed **before** the vendor accesses PHI. **Without a BAA, the disclosure of PHI to a generative AI vendor is generally impermissible, regardless of the provider's intent or purpose.**

This is where many providers may run into trouble. The same AI model may be available through multiple product tiers, and BAA availability varies by tier. For example, major AI vendors such as OpenAI (ChatGPT), Google (Gemini), and Microsoft (Copilot) offer both consumer AI tools—which typically are not available with a BAA—and enterprise AI tools, some of which may be offered with a BAA and some of which may not.

6. Same Tool, Different Environment—Different Risk

Given the wide range of AI offerings—and their differing BAA availability—it is easy for a provider to move between environments without realizing they have left the protected one. A clinician using an enterprise, BAA-covered AI tool on their work computer may later open the same chatbot on a personal phone or consumer web browser, not logged into the enterprise account. In that consumer environment, there is no BAA and no HIPAA-compliant configuration, meaning any PHI entered is a

disclosure to a third party without required safeguards in place.

The AI interface may look identical, but **a single prompt containing PHI entered in the wrong environment can constitute an impermissible disclosure**-one the provider may not even recognize has occurred.

Providers should ensure workforce members understand not just *which* tools are approved, but *which specific* environments and accounts are covered, and that using AI with PHI outside those approved environments is prohibited.

7. A BAA Is Necessary, But Not Sufficient

Even with a valid BAA in place, providers must still comply with HIPAA's broader requirements:

1. **Minimum Necessary Standard.** When using or disclosing PHI for purposes other than treatment, covered entities must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. 45 C.F.R. § 164.502(b)(1). Although the minimum necessary standard does not apply to disclosures for treatment, 45 C.F.R. § 164.502(b)(2)(i), it does apply to uses and disclosures for healthcare operations and payment. *See id*. § 164.502(b). **Pasting an entire patient record into a chatbot to draft a single letter likely exceeds what is reasonably necessary for the task.**

2. **Permissible Purpose.** A covered entity may use or disclose PHI without patient authorization for its own treatment, payment, or healthcare operations (TPO) activities. 45 C.F.R. §§ 164.501, 164.506(a), (c)(1). **But when a covered entity relies on a third-party AI vendor to assist with TPO functions, the permissible TPO purpose does not eliminate the need for a BAA.** The BAA requirement applies independently. *See* 45 C.F.R. § 164.502(e)(l)(i).

3. **No Expanded Use by the Vendor.** A BAA permits a vendor to handle PHI on the provider's behalf. It does not expand the categories of permissible use or disclosure under HIPAA. Business associates may use or disclose PHI “only as permitted by the [BAA], or as required by law,” and may not use or disclose PHI “in a manner that would violate [the HIPAA Privacy Rule] if done by the covered entity.” 45 C.F.R. § 164.502(a)(3); 45 C.F.R. § 164.504(e)(2)(i)–(ii).

   If a particular disclosure would require patient authorization when made directly by the covered entity, the same authorization is required before the information is shared with the business associate. *See* 45 C.F.R. § 164.508. For more information on this topic, see our separate client alert, Business Associates' Use of Information for Their Own Purposes.

4. **Access Controls and Security.** Providers should confirm that the AI tool is configured with appropriate administrative, technical, and physical safeguards—including encryption, access logging, and restrictions on secondary use or model training—consistent with the Security Rule's requirements to protect the confidentiality, integrity, and availability of ePHI. *See* 45 C.F.R. §§ 164.302–.318.

8. Special Categories Require Extra Caution

Certain types of health information carry heightened protections that a BAA alone cannot satisfy.

1. **Psychotherapy Notes.** HIPAA defines psychotherapy notes as notes recorded by a mental health professional documenting or analyzing counseling session contents, maintained separately from the medical record. 45 C.F.R. § 164.501. (medication monitoring, session times, treatment modalities, clinical test results, and summaries of diagnosis, treatment plan, symptoms, prognosis, and progress are excluded). HIPAA generally requires a separate, specific patient authorization before psychotherapy notes may be used or disclosed—even to a business associate, and even for treatment purposes. 45 C.F.R. § 164.508(a)(2).

   Limited exceptions exist for use by the originator for treatment, training or supervision, defense of a legal action by the patient, and disclosures required by law. *See id.* § 164.508(a)(2)(i)–(ii). **Entering psychotherapy notes into an AI tool—even one operating under a BAA—without patient authorization is likely an impermissible disclosure.** For more information, see our client alert, HIPAA, Psychotherapy Notes, and Other Mental Health Records.

2. **Substance Use Disorder (SUD) Records.** Records protected under 42 C.F.R. Part 2 are subject to a separate federal confidentiality rule that is generally stricter than HIPAA and applies in addition to it. Part 2 applies to "Part 2 Programs," entities that hold themselves out as providing and do provide SUD diagnosis, treatment, or referral for treatment. 42 C.F.R. § 2.11. Protected information includes any information identifying a person as having sought, received, or been referred for SUD treatment—including diagnosis, counseling notes, assessments, and even the fact of enrollment. *See* 42 C.F.R. §§ 2.12–.13; 42 U.S.C. § 290dd-2. Disclosure generally requires written patient consent unless a Part 2 exception applies. 42 C.F.R. § 2.31.

   However, Part 2 permits disclosure without consent to a "qualified service organization" (QSO)—essentially a business associate—that enters into a written QSOA acknowledging it is bound by Part 2. 42 C.F.R. § 2.11. As amended, a Part 2 program may also disclose to a HIPAA business associate without patient consent if the BAA contains the required QSOA elements. *See id*. (definition of "Qualified service organization," para. (3)). **If Part 2 applies, providers must comply with Part 2 even where HIPAA would**

otherwise permit the disclosure.

3. **State Law.** Many states impose additional protections on mental health records, substance use treatment information, HIV/AIDS status, reproductive health data, and other sensitive categories. Providers must generally comply with the most restrictive applicable federal or state law; that is, the law that affords greater protection to the patient's information or greater control to the patient over their information. *See* 45 C.F.R. § 160.203.

9. Individual Rights and AI-Generated Records

The HIPAA Privacy Rule establishes individual rights that have direct implications for AI use in clinical settings.

1. **Right to Access.** An individual has the right to inspect and obtain a copy of PHI in a designated record set. 45 C.F.R. § 164.524(a)(1). A "designated record set" includes medical records and billing records maintained by or for a covered entity, as well as any records used to make decisions about individuals. 45 C.F.R. § 164.501. If an AI-generated clinical note or summary is saved in the patient's medical record and used to make treatment or payment decisions, it likely becomes part of the designated record set and is subject to the patient's access right. *See id*. Drafts or internal AI artifacts that are not saved or relied upon clinically are typically not part of the designated record set. Psychotherapy notes remain excluded from the access right if properly maintained separately. 45 C.F.R. § 164.524(a)(1)(i).

2. **Right to Request Restrictions.** A patient may request that a covered entity restrict uses or disclosures of PHI for treatment, payment, or healthcare operations. 45 C.F.R. § 164.522(a)(1)(i). For example, a patient might ask that their information not be processed by AI tools for documentation, messaging, or quality improvement. The covered entity is generally not required to agree to such a request. 45 C.F.R. § 164.522(a)(1)(ii). However, if the covered entity does agree, it must comply with the restriction. 45 C.F.R. § 164.522(a)(1)(iii). A practice may later terminate an agreed-to restriction, but only prospectively.

3. **Right to Request Amendment.** An individual has the right to request amendment of PHI in a designated record set. 45 C.F.R. § 164.526(a)(1). AI-generated clinical summaries may contain subtle inaccuracies — a well-documented risk of generative AI tools. A covered entity may deny an amendment request if it determines the information is "accurate and complete," 45 C.F.R. § 164.526(a)(2)(iv), but whether an AI-generated summary meets that standard will be a fact-specific inquiry. A covered entity may also deny the request if the PHI was "not created by the covered entity," 45 C.F.R. § 164.526(a)(2)(i), but HHS would likely attribute AI-generated documentation to the provider who deployed the tool and is responsible for the patient's care. Business associates are

independently required to make PHI available for amendment and incorporate amendments. 45 C.F.R. § 164.504(e)(2)(ii)(F).

10. Breach Risk Is Real

If PHI is entered into an AI tool without a BAA or proper authorization, the disclosure may constitute a breach under the HIPAA Breach Notification Rule—defined as acquisition, access, use, or disclosure of PHI not permitted by the Privacy Rule that compromises its security or privacy. 45 C.F.R. § 164.402. An impermissible disclosure is presumed to be a **breach** unless a risk assessment demonstrates a low probability of compromise.

If a breach is confirmed, the covered entity must notify:

- Affected individuals without unreasonable delay and no later than 60 calendar days after discovery. 45 C.F.R. § 164.404(a)(2), (b).
- The Secretary of HHS within 60 days for breaches affecting 500 or more individuals; annually for smaller breaches. 45 C.F.R. § 164.408(b)–(c).
- Prominent media outlets when a breach affects more than 500 residents of a state or jurisdiction. 45 C.F.R. § 164.406(a).

Violations may result in civil monetary penalties of up to $50,000 per violation (as adjusted for inflation), with annual caps ranging from $25,000 to approximately $2 million depending on the level of culpability, as well as corrective action plans and reputational harm. *See* 42 U.S.C. §§ 1320d-5, 1320d-6; 45 C.F.R. §§ 160.306–.316. Criminal penalties may apply for knowing or intentional misuse of PHI, including fines and imprisonment. 42 U.S.C. § 1320d-6.

The breach analysis does not turn on intent. An inadvertent disclosure to an unsecured AI tool is still a disclosure.

11. Practical Takeaways

1. **Know your tool.** Before using any AI product with patient information, confirm whether a BAA is available and executed for the specific product tier and environment you are using. The same AI model accessed through a consumer account versus an enterprise account may have entirely different compliance profiles.
2. **Know your data.** Identify whether the information you are entering constitutes PHI, and whether it falls into a special category such as psychotherapy notes under 45 C.F.R. § 164.501, SUD records under 42 C.F.R. Part 2, or state-protected data — that requires additional consent or authorization beyond what a BAA provides.
3. **Know your environment.** Ensure that workforce members understand which specific accounts and platforms are BAA-covered. A clinician who switches from an enterprise tool on a work computer to the same chatbot on a personal phone may be

disclosing PHI to a consumer product with no BAA and default data retention and model-training settings.

4. **Apply the minimum necessary standard.** Limit what you input to what is reasonably needed for the task. 45 C.F.R. § 164.502(b).

5. **Do not assume "treatment purpose" is a safe harbor.** A treatment purpose may support the underlying use of PHI, but it does not eliminate the need for a BAA with a third-party vendor or patient authorization where otherwise required. *See* 45 C.F.R. §§ 164.502(e), 164.506, 164.508.

6. **Document your compliance.** Maintain records of BAAs, vendor due diligence, workforce training, and any patient authorizations related to AI use.

7. **Train your workforce.** Staff may be using AI tools without realizing the HIPAA implications. Clear policies and regular training are essential. The HIPAA Security Rule requires covered entities to ensure compliance by their workforce members. *See* 45 C.F.R. § 164.308(a)(5).

8. **Prepare for patient questions.** Patients have the right to request restrictions on AI-related uses of their PHI under 45 C.F.R. § 164.522(a), and the right to request amendment of AI-generated records under 45 C.F.R. § 164.526. Providers should have policies in place for responding to these requests consistently.

12. Looking Ahead

The regulatory landscape around AI in healthcare is evolving rapidly. But the foundational HIPAA obligations—BAAs, minimum necessary, authorization requirements, and breach notification **apply now**, regardless of whether AI-specific regulations have caught up.

---

seek the advice of your legal counsel.