Kurz erklärt: Was „HIPAA“ und „PHI“ bedeuten □□□

Wenn du auf einer *Physiotherapie-Website* einen KI-Chat einbauen willst, ist das Thema **Datenschutz im Gesundheitsbereich** tatsächlich sehr wichtig.

Die beiden Begriffe, die du gehört hast, kommen **aus den USA**:

HIPAA

HIPAA steht für *Health Insurance Portability and Accountability Act*.

Das ist ein US-Gesetz, das regelt, **wie Gesundheitsdaten geschützt werden müssen**. Es betrifft vor allem Arztpraxen, Kliniken, Versicherungen und bestimmte Dienstleister, die mit Gesundheitsdaten arbeiten.

Vereinfacht gesagt:
Wenn eine Organisation unter HIPAA fällt, darf sie **bestimmte Gesundheitsdaten nicht einfach an Dritte weitergeben**, außer unter klar geregelten Bedingungen.

PHI

PHI steht für *Protected Health Information*.

Damit sind **schutzbedürftige Gesundheitsinformationen** gemeint, also Daten, die:

1. sich auf den Gesundheitszustand, eine Behandlung oder Bezahlung von Behandlung beziehen, **und**
2. einer bestimmten Person zugeordnet werden können.

Beispiele für PHI:

- Name + Information über Beschwerden
- E-Mail + Angabe „Ich habe seit 3 Monaten Rückenschmerzen“
- Telefonnummer + Frage zu einer konkreten Therapie nach einer OP
- Termin- oder Versicherungsdaten zusammen mit Gesundheitsbezug

Also:
„Ich interessiere mich für Physiotherapie“ → *eher unkritisch*
„Ich bin Max Mustermann, hatte einen Bandscheibenvorfall und brauche Behandlung“ → **klar sensibel**

Warum das für einen Website-Chat relevant ist

Ein Chat auf einer Praxis-Website wirkt für Nutzer oft wie ein Ort, an dem sie **einfach direkt ihr Anliegen schildern**. Genau da entsteht das Risiko:

- Nutzer schreiben spontan persönliche Daten hinein
- Nutzer nennen Symptome, Diagnosen oder Behandlungswünsche
- damit können im Chat **Gesundheitsdaten** verarbeitet werden

Wenn diese Daten dann an einen externen KI-Dienst gehen, ist die entscheidende Frage:

- **Darfst du das rechtlich überhaupt?**
- **Wie wird der Anbieter mit den Daten umgehen?**
- **Wer ist für Sicherheit, Speicherung und Verarbeitung verantwortlich?**

Wichtig: HIPAA ist US-Recht, aber für dich kann auch DSGVO relevanter sein □□□

Falls deine Physiotherapie-Praxis in **Deutschland oder der EU** sitzt, ist für dich oft **nicht zuerst HIPAA**, sondern vor allem die **DSGVO** relevant.

Das heißt:

- **HIPAA** ist relevant, wenn du in den USA tätig bist oder US-Gesundheitsrecht konkret auf dich zutrifft.
- **DSGVO** ist relevant, wenn du personenbezogene Daten von Personen in der EU verarbeitest.

- Gesundheitsdaten sind unter der DSGVO sogar **besonders sensible personenbezogene Daten**.

Für eine deutsche Physiotherapie-Website wäre also meistens die wichtigere Frage:

> „Verarbeitet der Chat Gesundheitsdaten im Sinne der DSGVO — und wenn ja, auf welcher Rechtsgrundlage, mit welchen Schutzmaßnahmen und mit welchem Auftragsverarbeiter?“

Was das bei einer OpenAI-/ChatGPT-Integration praktisch bedeutet

Wenn du „indirekt OpenAIs ChatGPT“ einbinden willst, kommt es sehr darauf an, **wie der Chat genutzt wird**.

Fall 1: Reiner Website-Auskunfts-Chat

Wenn der Bot nur Fragen beantwortet wie:

- „Welche Leistungen bietet die Praxis an?“
- „Welche Therapeuten gibt es?“
- „Habt ihr manuelle Therapie?“
- „Wie sind die Öffnungszeiten?“

…dann ist das deutlich weniger problematisch, **solange Nutzer keine persönlichen Gesundheitsdaten eingeben**.

Fall 2: Nutzer schildern ihre Beschwerden

Wenn Nutzer Dinge schreiben wie:

- „Ich habe seit Wochen Nackenschmerzen“
- „Ich hatte letztes Jahr eine Kreuzband-OP“
- „Welche Behandlung ist für meine Skoliose sinnvoll?“

...dann kann der Chat sehr schnell **sensible Gesundheitsdaten** verarbeiten.

Und genau dann wird es rechtlich und organisatorisch deutlich anspruchsvoller.

Die Kernfrage: Soll der Chat überhaupt persönliche Gesundheitsangaben zulassen?

Das ist der wichtigste Design-Punkt.

Sicherere Variante

Der Chat wird **streng als Informationsassistent für Website-Inhalte** gebaut:

- nur allgemeine Praxisinfos
- keine Diagnosen
- keine Therapieempfehlungen für Einzelfälle
- keine Terminbuchung mit Gesundheitsdetails
- deutlicher Hinweis:
  „Bitte keine persönlichen oder medizinischen Informationen in den Chat eingeben.“

Dann reduzierst du das Risiko erheblich.

Riskantere Variante ⚠

Der Chat darf frei genutzt werden und Nutzer schildern ihr individuelles Anliegen.

Dann musst du sehr viel genauer prüfen:

- Datenschutzrecht
- Anbieter-Verträge
- Speicherorte
- technische und organisatorische Maßnahmen
- mögliche Einwilligungen
- Logging
- Zugriffskonzepte
- Löschkonzepte

- medizinrechtliche Risiken

Was du zu OpenAI besonders bedenken solltest

Bei einer Integration mit OpenAI oder einem ähnlichen Modellanbieter solltest du insbesondere klären:

1. **Werden die Chat-Inhalte gespeichert?**
2. **Werden sie zum Training verwendet oder nicht?**
3. **In welcher Region werden Daten verarbeitet?**
4. **Gibt es einen Auftragsverarbeitungsvertrag / DPA?**
5. **Gibt es für US-Kontexte HIPAA-relevante Zusagen, z. B. ein BAA?**
6. **Welche Daten sendest du technisch überhaupt an das Modell?**

Gerade bei Gesundheitsdaten gilt:
Du solltest **Datensparsamkeit** ernst nehmen.

Das heißt zum Beispiel:

- keine Namen mitschicken
- keine Kontaktangaben mitschicken
- keine Freitext-Eingaben unkontrolliert an das Modell weiterleiten
- idealerweise Eingaben filtern oder blockieren, wenn sie Gesundheitsdaten enthalten

---

Was ist ein BAA?

Wenn wir schon bei HIPAA sind:
Ein **BAA** ist ein *Business Associate Agreement*.

Das ist vereinfacht ein Vertrag zwischen einer HIPAA-regulierten Stelle und einem Dienstleister, der PHI verarbeitet.

Wenn ein externer Anbieter PHI im Auftrag verarbeitet, braucht man in HIPAA-Kontexten oft so einen Vertrag.

Wichtig:
Nicht jeder KI-Dienst oder jedes Produkt ist automatisch für HIPAA-/PHI-Nutzung freigegeben. Man

darf also nicht einfach annehmen:

> „Ist ein großer Anbieter, also wird das schon passen.“

Gerade bei KI ist das etwas, das man **sehr konkret pro Produkt und Vertrag** prüfen muss.

Für deine Idee würde ich praktisch so unterscheiden

Wenn dein Ziel nur ist:

Einen Chat anzubieten, der die Inhalte der Praxis-Website erklärt, z. B.:

- Leistungen
- Team
- Qualifikationen
- Schwerpunkte
- Ablauf
- Öffnungszeiten
- Kontaktwege

Dann ist die beste Strategie meist:

1. **Chat auf reine Website-Auskunft beschränken**
2. **Deutlichen Hinweis einblenden**, dass keine sensiblen Daten eingegeben werden sollen
3. **Technisch filtern**, wenn jemand Diagnosen, Symptome, Namen, Telefonnummern etc. eingibt
4. **Keine medizinische Beratung** durch den Bot zulassen
5. **Keine Chatprotokolle unnötig speichern**
6. **Datenschutzrechtlich prüfen lassen**, insbesondere nach DSGVO

Gute Formulierung für so einen Hinweis

Zum Beispiel:

> „Dieser Chat dient nur zur allgemeinen Information über unsere Praxis, Leistungen und Abläufe. Bitte geben Sie keine personenbezogenen Gesundheitsdaten, Diagnosen, Beschwerden, Versicherungsdaten oder sonstige sensible Informationen ein. Für individuelle medizinische Anliegen kontaktieren Sie uns bitte direkt telefonisch oder über die vorgesehenen Kontaktwege.“

So ein Hinweis ersetzt **keine** rechtliche Absicherung, aber er ist sehr sinnvoll.

Was ich dir konkret empfehle □□

Für einen ersten sicheren Ansatz

Baue den Bot so, dass er nur auf eine kuratierte Wissensbasis zugreift:

- Praxisbeschreibung
- Leistungsseiten
- Therapeutenprofile
- FAQ
- Kontakt/Anfahrt
- Organisatorische Infos

Und zusätzlich:

- Systemseitig untersagen, individuelle Diagnosen oder Therapieempfehlungen zu geben
- Eingaben mit sensiblen Daten abfangen
- Nutzer auf Telefon/E-Mail/Kontaktformular verweisen, wenn es individuell wird

Nicht als erstes bauen

Einen offenen „Beschwerde- und Beratungs-Chat“, in den Patienten frei ihre gesundheitliche Situation schreiben.

Das ist sowohl **datenschutzrechtlich** als auch **fachlich** viel heikler.

Ganz wichtig: Das ist nicht nur ein Technik-, sondern auch ein Rechts- und Prozess-Thema

Selbst wenn die API technisch funktioniert, bleiben Fragen wie:

- Was steht in deiner Datenschutzerklärung?
- Auf welcher Grundlage verarbeitest du die Daten?
- Wer hat Zugriff auf Logs?
- Wie lange speicherst du Chats?
- Was passiert, wenn jemand doch sensible Daten eingibt?
- In welchem Land werden die Daten verarbeitet?
- Ist der konkrete Anbieter-Vertrag dafür geeignet?

Mein pragmatisches Fazit

Ja, ein KI-Chat auf einer Physiotherapie-Website kann sinnvoll sein.
Aber: Du solltest ihn zunächst **nicht als Patienten- oder Beschwerde-Chat**, sondern als **allgemeinen Website-Assistenten** konzipieren.

Merksatz

- **HIPAA** = US-Regeln zum Schutz von Gesundheitsdaten
- **PHI** = geschützte personenbezogene Gesundheitsdaten
- **Für Deutschland/EU** ist meist vor allem die **DSGVO** entscheidend
- **Je individueller und medizinischer die Chat-Eingaben, desto größer das Risiko**

Wenn du möchtest, kann ich dir als Nächstes noch eines von drei

Dingen machen:

1. eine **einfache Risiko-Einschätzung** für deinen konkreten Use Case
2. eine **sichere Architektur-Skizze** für so einen Website-Chat mit OpenAI
3. einen **Beispieltext für Datenschutzhinweis + Chat-Warnhinweis**

Wenn du willst, mache ich dir direkt eine **empfohlene „sichere Minimalversion“** für eine Physiotherapie-Website.

Revision #1
Created 2026-05-19 09:34:42 UTC by art10m
Updated 2026-05-19 09:35:00 UTC by art10m