Data Privacy Practices of Leading LLM Providers (OpenAI, Anthropic, Google, DeepSeek)

Introduction

As organizations and individuals adopt large language models (LLMs) in day-to-day workflows, understanding how providers handle your data is critical. This report analyzes the data privacy practices of four major LLM providers – **OpenAI**, **Anthropic**, **Google**, and **DeepSeek** – across different usage tiers. We break down whether your prompts and content are used for model training in **free** vs **paid (individual)** vs **enterprise/API** tiers, default data retention policies and opt-out options, any **HIPAA-compliant** offerings, and nuances for specific model families (e.g. GPT-4, Claude 3, Google's Gemini, DeepSeek-VL). Finally, we provide recommendations for privacy-conscious users and organizations.

OpenAI (ChatGPT & API)

Services & Tiers: OpenAI's ecosystem includes the consumer-facing **ChatGPT** (free web/app and paid *ChatGPT Plus* subscriptions) and the **OpenAI API** used by developers or through platforms like Azure OpenAI. In late 2023, OpenAI also introduced **ChatGPT Enterprise** and **ChatGPT Team** for organizations.

Data Use for Training – Free vs Paid vs Enterprise: By default, **ChatGPT** (both free and Plus) **uses user inputs and conversations to further train and improve OpenAI's models** (How your data is used to improve model performance | OpenAI Help Center). OpenAI states that *"ChatGPT, for instance, improves by further training on the conversations people have with it"* (How your data is used to improve model performance | OpenAI Help Center). In other words, unless you take action to opt out, any prompts or chat logs you submit via ChatGPT may be analyzed and incorporated (in anonymized form) into model updates. This policy is the same for free and Plus users (Plus provides enhanced model access like GPT-4, but not different privacy defaults).

However, OpenAI provides **data control settings** for ChatGPT users to **opt out** of having their content used in training. In ChatGPT's settings, you can disable the

"**Improve the model for everyone**" toggle (Data Controls FAQ | OpenAI Help Center). Once this is off, "*"new conversations won't be used to train our models"* (Data Controls FAQ | OpenAI Help Center). OpenAI also recently introduced **Temporary Chat** mode, which when enabled ensures those conversations *"won't be used for model training"* and are only stored short-term (Data Controls FAQ | OpenAI Help Center). (More on data retention below.)

For **OpenAI's API and enterprise services**, the default is the opposite: **API data is *not* used for model training or "service improvements" by default** (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch) (How your data is used to improve model performance | OpenAI Help Center). Since March 1, 2023, OpenAI's policy has been that data submitted via the API will **not** feed back into training models unless a customer explicitly opts in (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch). This applies to *ChatGPT Enterprise/Team* as well – OpenAI's documentation confirms *"by default, we do not use your business data for training our models"* (Enterprise privacy at OpenAI | OpenAI). (Customers can choose to share data for improvement through explicit feedback channels, but that's voluntary (Enterprise privacy at OpenAI | OpenAI).) In short, business and developer tiers come with privacy-first defaults, whereas the public ChatGPT service assumes consent to use data for training unless you opt out.

Data Retention & Storage: There are important differences in how long OpenAI retains user prompts and chat history across tiers:

- **ChatGPT (Free/Plus) with History On:** By default, ChatGPT stores your conversation history in your account so you (and the model) can refer back to it. If you do not turn off history, chats are retained indefinitely on OpenAI's systems to enable features like contextual continuity, and they **may be used to train models** (Data Controls FAQ | OpenAI Help Center). OpenAI's help center advises users not to share sensitive personal data in these conversations since deletion of specific prompts from OpenAI's systems isn't available on a granular level (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch). You can manually delete conversation threads in the interface, upon which OpenAI will remove that data from their systems within 30 days (Data Controls FAQ | OpenAI Help Center).

- **ChatGPT with History Off (Temporary Chats):** If you disable chat history (either via the "Improve model" toggle or using Temporary Chat mode), OpenAI will treat new conversations as ephemeral. Such **chats are stored for 30 days** and *"reviewed only when needed to monitor for abuse"*, then **permanently**

deleted (Data Controls FAQ | OpenAI Help Center). In this state, your inputs are **not used for model training** and do not even appear in your account history (Data Controls FAQ | OpenAI Help Center). Essentially, opting out puts ChatGPT into an "incognito" mode – data is retained briefly for security purposes, then purged (Data Controls FAQ | OpenAI Help Center).

- **OpenAI API:** According to OpenAI and third-party analyses, API requests and responses are typically **retained for 30 days** for trust & safety monitoring, and then deleted (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch). OpenAI implemented this 30-day retention policy alongside the training opt-out change in March 2023 (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch). Enterprise customers or those with stricter needs can negotiate **shorter retention** – OpenAI offers options for **stricter retention or immediate deletion** depending on user needs (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch) (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). In fact, Microsoft's Azure OpenAI (which is OpenAI's service hosted in Azure's cloud) allows zero-retention configurations (see below).

- **ChatGPT Enterprise/Team:** For the enterprise ChatGPT offerings, **administrators can control the data retention period** for their workspace. By default, conversation history is enabled to allow expected functionality, but an admin could set a shorter retention window. Any conversations deleted by end-users or by policy are *"removed from our systems within 30 days"* (Enterprise privacy at OpenAI | OpenAI). OpenAI also limits internal access to enterprise conversation data: it is not used for training, and OpenAI staff will only access it in exceptional cases (e.g. for debugging a support issue, with permission, or if required by law) (Enterprise privacy at OpenAI | OpenAI). In effect, enterprise data remains within the organization's control.

- **Azure OpenAI (Cloud-Hosted):** If using OpenAI models via Azure's cloud service, Microsoft provides additional guarantees. **Azure OpenAI Service does not send your prompts or data to OpenAI at all**, and **never uses it to train the base models** (Data, privacy, and security for Azure OpenAI Service - Azure AI services | Microsoft Learn). Your prompts, completions, and fine-tuning data are isolated to your Azure instance: *they "are NOT available to other customers," "are NOT available to OpenAI," and "are NOT used to improve OpenAI models"* (Data, privacy, and security for Azure OpenAI Service - Azure AI services | Microsoft Learn). Microsoft keeps this data within the Azure environment for processing and monitoring, and it inherits Azure's compliance standards. In

short, Azure treats your OpenAI API calls like any other cloud customer data – staying private to you, with no sharing into model development.

Opt-Out Mechanisms: As noted, OpenAI gives **users direct control** over data sharing on the consumer services. In ChatGPT's settings (on web or mobile), you can toggle **"Chat History & Training" off**, now labeled as *"Improve the model for everyone"* – this prevents future chats from being used in training (Data Controls FAQ | OpenAI Help Center). OpenAI's help article also mentions a **Privacy Portal** where you can globally "Do not train on my content" for your account (How your data is used to improve model performance | OpenAI Help Center). For API usage, no action is needed to opt out (it's the default), though providing optional feedback in the Playground or via their feedback methods would be an explicit opt-in to share that snippet (How your data is used to improve model performance | OpenAI Help Center). Always review OpenAI's latest policy updates, as they do evolve (for example, these user controls were rolled out in 2023).

HIPAA Compliance: OpenAI has taken steps toward regulatory compliance for its enterprise offerings. While ChatGPT itself is not HIPAA-certified, OpenAI **will sign Business Associate Agreements (BAAs) with enterprise/API customers who need HIPAA compliance** (Enterprise privacy at OpenAI | OpenAI). Specifically, OpenAI's terms state they *"are able to sign BAAs in support of customers' compliance with HIPAA"* (Enterprise privacy at OpenAI | OpenAI). In practice, this means if a healthcare entity or other covered entity wants to use OpenAI's API (or ChatGPT Enterprise) with Protected Health Information (PHI), OpenAI can enter a BAA to contractually ensure PHI is handled according to HIPAA rules. (Notably, OpenAI's own documentation suggests this is available for the API platform and ChatGPT Enterprise/Edu/Team, since those are the "business" services.)

It's worth noting that **ChatGPT Enterprise** has already achieved **SOC 2 Type II** compliance (Enterprise privacy at OpenAI | OpenAI), and OpenAI offers to sign DPAs (Data Processing Addendums) for GDPR compliance (Enterprise privacy at OpenAI | OpenAI). On Azure, any HIPAA compliance would fall under Microsoft's BAA and Azure's compliance certifications (Azure OpenAI is considered a HIPAA-eligible service under Azure's umbrella when properly configured). In summary, OpenAI's consumer services should **not** be used for PHI or sensitive data unless you opt out of data sharing at minimum; for HIPAA use cases, stick to the API/enterprise side with a BAA in place (Enterprise privacy at OpenAI | OpenAI).

Model-Specific Differences: OpenAI's privacy terms **do not meaningfully vary by model (GPT-3.5 vs GPT-4, etc.)** – it is determined by service/tier. Whether you're using GPT-4 via ChatGPT Plus or GPT-3.5 via free ChatGPT, if you have not opted out,

the content could be used to improve future models. Similarly, API calls to any model (GPT-4, GPT-3.5 Turbo, DALL-E, etc.) are exempt from training usage by default (How your data is used to improve model performance | OpenAI Help Center). OpenAI also affirms that **you retain ownership of the inputs and outputs** you generate (with certain legal caveats) (Enterprise privacy at OpenAI | OpenAI) – using their service doesn't make your data theirs. If you fine-tune a model on the API, the resulting fine-tuned model is accessible only by your account, not shared with others (Enterprise privacy at OpenAI | OpenAI). Thus, differences in model families (e.g. GPT-4 vs GPT-3) do not affect privacy handling; it's more about whether you're using the public chat interface or a business/API channel.

OpenAI Summary: In the default ChatGPT experience, user data is **retained and leveraged to train models** (How your data is used to improve model performance | OpenAI Help Center), but you have the ability to opt out and even avoid server retention beyond 30 days by disabling history (Data Controls FAQ | OpenAI Help Center). In the API and enterprise products, OpenAI assures that **data won't be used to tune models** (How your data is used to improve model performance | OpenAI Help Center) and logs are kept only transiently (30 days by default) (Addressing criticism, OpenAI will no longer use customer data to train its models by default | TechCrunch). OpenAI also supports compliance needs (SOC 2, GDPR DPA, and BAA for HIPAA) for enterprise clients (Enterprise privacy at OpenAI | OpenAI) (Enterprise privacy at OpenAI | OpenAI). The table below summarizes OpenAI's policies across tiers:

OpenAI	Free ChatGPT / Plus (Consumer)	API & Enterprise (Business)
Data use for training	*Yes by default:* User prompts & chats are used to train and improve models (opt-out available) (How your data is used to improve model performance).	
Data retention	Conversations saved in account; deleted chats removed from backend within 30 days (Data Controls FAQ). If history disabled, chats stored 30 days then auto-deleted.	
Opt-out controls	Yes – **Chat History & Training** toggle to turn off data use for training (Data Controls FAQ).	
HIPAA compliant?	**No** – not by default. (Do not input PHI into standard ChatGPT.)	**Yes (with conditions)** – OpenAI will sign HIPAA BAA for API/Enterprise clients

(Enterprise privacy at OpenAI).

Anthropic (Claude)

Services & Tiers: Anthropic provides the **Claude** family of LLMs. Users can access Claude via the **claude.ai** web interface (which offers a free tier and a paid **Claude Pro** plan for individuals, similar to ChatGPT Plus). Claude is also offered via an **API** for developers and through integrations (e.g. Claude in Slack, and *Claude for Work* plans for enterprise teams). As of April 2025, Anthropic's latest models include Claude 2, with Claude 3 expected, but the privacy stance is consistent across versions.

Data Use for Training – Free vs Paid vs Enterprise: Anthropic takes a more privacy-preserving approach by default – they state that **user-provided data is *not* used to train their models unless certain conditions are met** (Is my data used for model training? | Anthropic Privacy Center). According to Anthropic's official privacy FAQ, *"We will not use your inputs or outputs to train our models, **unless**: (1) your conversations are flagged for Trust & Safety review … or (2) you've explicitly reported the materials to us … or (3) [you have] otherwise explicitly opted in"* (Is my data used for model training? | Anthropic Privacy Center). In other words, **by default Claude does not learn from your chats** – this holds true for **Claude.ai free users and Claude Pro subscribers** alike (Is my data used for model training? | Anthropic Privacy Center). The only exceptions involve misuse or voluntary feedback:

- If your input triggers their **Trust & Safety filters** (e.g. it contains disallowed content), Anthropic may review that data to improve their safety systems and **"may use or analyze [such conversations] to improve [their] ability to detect and enforce our Usage Policy, including training models for use by [the] Trust and Safety team"** (Is my data used for model training? | Anthropic Privacy Center). Notably, this suggests any training would be of *internal classifier models*, not the main Claude model. Normal, compliant usage doesn't get swept into training data.

- If *you* choose to submit feedback or bug reports with conversation data, that content can be used to improve the model (since you explicitly shared it). Absent those cases, Anthropic does **not** aggregate user chat logs into Claude's training sets. This policy applies across consumer and commercial usage. In practice, Anthropic's stance means they have **opted everyone out by default** – a key differentiator from OpenAI's consumer policy.

For **Claude's API and enterprise offerings**, the same default holds: **no fine-tuning on your prompts without permission**. Anthropic's *Commercial Terms* reiterate that they don't use customer API data to train models (except for safety/abuse handling or opt-in feedback). This effectively means **Claude Instant vs Claude 2 vs Claude 3 all follow the same privacy rule** – model improvements come from other sources or opted-in data, not scraping everyone's inputs.

Data Retention & Storage: Anthropic does retain user data for some period, but with an emphasis on **limiting duration** and deletion controls. Key points include:

- **Default Retention (Consumer Services):** For the Claude.ai chat interface (free and Pro) and other beta offerings, Anthropic retains personal data *"as long as reasonably necessary"* for the purposes described in their privacy policy (How long do you store personal data? | Anthropic Privacy Center). In practice, they have specific timelines: Anthropic notes that **all prompts and outputs are automatically deleted from their backend databases after 30 days by default** (How long do you store personal data? | Anthropic Privacy Center). Specifically, *"for all products, we automatically delete inputs and outputs on the backend within 30 days of receipt or generation"* (How long do you store personal data? | Anthropic Privacy Center), except in a few scenarios (like agreed longer retention or legal reasons). This 30-day rule applies broadly, which means even if you don't manually delete a Claude conversation, the data will age out of their systems in about a month (How long do you store personal data? | Anthropic Privacy Center).

- **User-Deleted Data:** If you use a Claude interface that allows saving conversation history (Claude.ai, Claude Pro, or Claude for Work's chat console), you have the ability to delete conversation histories. When you delete a conversation, it is removed from your account immediately and then **permanently deleted from Anthropic's backend within 30 days** (How long do you store personal data? | Anthropic Privacy Center). (So 30 days is both the auto-delete window and the max delay in purging deletions, similar to OpenAI's approach.)

- **Trust & Safety Exception:** If your prompt/output was flagged by Anthropic's safety system as a violation, they keep that data longer. In such cases, Anthropic retains the input/output for **up to 2 years**, and retains *classification metadata* (the safety labels) for up to 7 years (How long do you store personal data? | Anthropic Privacy Center). This longer retention is purely to enforce their Usage Policy and have records of abusive or illicit use. It affects only the small subset of data that trips the filters.

- **Opt-in Feedback Exception:** If you provided explicit feedback or bug reports that include conversation data, Anthropic may keep that data for **up to 10 years** (How long do you store personal data? | Anthropic Privacy Center). This is because it's considered a business record of user feedback.

- **Enterprise Zero-Retention Option:** Uniquely, Anthropic offers some enterprise customers a **"zero retention"** configuration. With a special agreement, **Anthropic will not log or store any prompts or completions at all (except transiently as needed to process and for legal/compliance)** (I have a zero retention agreement with Anthropic. What products does it apply to? | Anthropic Privacy Center). Under these zero-retention arrangements, even the 30-day default log is eliminated – Anthropic essentially does not persist your API calls on disk. They do still keep the safety system's output (flags) to monitor abuse (I have a zero retention agreement with Anthropic. What products does it apply to? | Anthropic Privacy Center), but not the actual content. According to Anthropic, this zero-retention **applies only to the Claude API** (and only for approved enterprise customers) – it *"does not apply to beta products, Claude.ai (Free, Pro, or Claude for Work), or any other product surfaces"* unless separately agreed (I have a zero retention agreement with Anthropic. What products does it apply to? | Anthropic Privacy Center). In short, if a client requires **no data footprint**, Anthropic can accommodate that on the API side. (This is the level required for certain regulated industries to be comfortable.)

To summarize, Anthropic's standard practice is to **wipe user data after 30 days** in the absence of misuse, and even sooner (or not at all) for those with special enterprise contracts (How long do you store personal data? | Anthropic Privacy Center) (I have a zero retention agreement with Anthropic. What products does it apply to? | Anthropic Privacy Center). This is a fairly short retention window among LLM providers.

Opt-Out Mechanisms: Because Anthropic does **not use your data for training by default**, there isn't an "opt-out" toggle needed as there is with ChatGPT – you're already opted out. There is also no need to toggle a history setting for privacy (Claude's web interface does allow you to clear conversation history for your own privacy, but that's more about your account view; the backend deletion happens on a schedule regardless). If anything, Anthropic provides ways to **opt-in** if you *want* to share data. For example, if you find Claude's output unsatisfactory, you might use a feedback button to send them the conversation snippet – that is a conscious opt-in on your part and is one of the few ways your data would reach their model training team.

Enterprise customers who require stricter controls can negotiate the aforementioned zero-retention, effectively an enhanced opt-out that covers logs as well (I have a zero

retention agreement with Anthropic. What products does it apply to? | Anthropic Privacy Center). In summary, the lack of training usage is baked in, so end-users do not have to constantly manage a privacy switch with Anthropic (just remain aware of the 30-day retention and content rules).

HIPAA Compliance: Anthropic has positioned Claude for enterprise use and has pursued relevant compliance certifications. They have announced SOC 2 Type I and II compliance, and importantly, **Anthropic will sign HIPAA BAAs for eligible customers using their API** (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center). Their policy (as of early 2024) is that after reviewing the use case, they *"may provide a BAA covering use of our first-party API"* (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center). There are a couple of caveats: Anthropic's BAA **only covers the API** products and only for customers who qualify for **zero retention** (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center). They explicitly note that the BAA *"does not cover beta products or chat products, including Workbench and Claude.ai (Free, Pro, and Claude for Work)"* (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center). This means you **should not use PHI in the Claude.ai web UI or Slack app**, even if you have an enterprise deal, because those interfaces are not HIPAA-ready. If you require HIPAA compliance, you need to use Claude via the API in a zero-retention mode (which likely involves a dedicated instance or special handling) (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center).

So, while Anthropic itself is not "HIPAA certified" (HIPAA doesn't have a formal certification process), they are open to contractual commitments for HIPAA with the proper safeguards (no data retention, etc.). Also, third-party companies are already offering HIPAA-compliant solutions powered by Claude (for example, an Anthropic partner Hathr.ai built a healthcare API with "zero retention, secure NLP" leveraging Claude (HIPAA Compliant AI API - Hathr.AI powered by Anthropic's Claude AI)). This suggests that Claude's design can meet HIPAA requirements when deployed in the right way. In summary: **HIPAA use = Claude via API + BAA + zero retention;** not the self-serve Claude chatbot.

Model-Specific Differences: Anthropic's privacy policy does not draw distinctions between different versions of Claude. Whether you are using **Claude 2 or Claude 3 (future)**, or the faster **Claude Instant** model, the same rules about not training on your data apply. The main nuance is *beta vs general availability*: Anthropic makes clear that **"beta" features or models aren't covered under certain agreements** (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? |

Anthropic Privacy Center). For example, if "Claude 3" launches in beta, one should assume the strict enterprise protections (like BAA or zero retention agreements) might not automatically extend to it until it's a supported product. But aside from that lifecycle issue, Anthropic treats all user inputs the same with regard to privacy. So, no matter the model, your content isn't improving Claude by default. (One could say Claude has been "trained on a lot of text, but *not* on your particular prompts unless you want it to.")

Anthropic Summary: Anthropic's Claude is **privacy-friendly by default** – it does *not* learn from your data in normal use (Is my data used for model training? | Anthropic Privacy Center). They still keep data for a short period (30 days) for functionality and safety, but automatically purge it thereafter (How long do you store personal data? | Anthropic Privacy Center). Users don't need to opt out, as everyone is opted-out of training. Enterprise clients can even get a zero-data-retention setup (I have a zero retention agreement with Anthropic. What products does it apply to? | Anthropic Privacy Center). Anthropic supports compliance for businesses (SOC 2, and BAAs for HIPAA on API) (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center) (Will Anthropic sign a Business Associate Agreement (BAA), and if so, for which products? | Anthropic Privacy Center), although consumer-facing Claude interfaces are not suitable for sensitive regulated data. The table below highlights Anthropic's practices:

Anthropic (Claude)	Claude.ai (Free & Pro)	Claude API & Enterprise
Data use for training	*No, by default:* Anthropic does **not** train Claude on user prompts or outputs (Is my data used for model training?). Only exceptions are flagged misuse (for improving safety systems) or explicit user feedback.	
Data retention	Auto-delete of conversation data ~**30 days** after it's received (How long do you store personal data?). User can delete chats earlier (purged from systems within 30 days).	
Opt-out controls	Not needed – data not used for training by default. (If anything, users would opt-in via feedback if they want to share data.)	Not needed – already not used. Enterprise can ensure even logs aren't kept if necessary (zero retention agreement) (I have a

		zero retention agreement with Anthropic).
HIPAA compliant?	**No** – Claude.ai (consumer web) and other beta or consumer services are *not* covered by any HIPAA BAA (Will Anthropic sign a Business Associate Agreement (BAA)?). Don't use them for PHI.	

Google (Bard, PaLM/Gemini Models, Vertex AI)

Services & Tiers: Google's AI offerings span consumer and enterprise domains. On the consumer side, **Google Bard** is a free chatbot (accessible via bard.google.com, and by 2025 powered by Google's **Gemini** LLM). On the enterprise side, Google provides **Generative AI services through Google Cloud** – for example, the **PaLM API / AI Studio** (for developers to access models via an API), and **Vertex AI** on Google Cloud Platform (GCP) which offers foundation models (like PaLM or Gemini) to businesses with enterprise-grade controls. Google also integrates LLMs into products like Google Workspace (e.g. "Duet AI" in Gmail/Docs), but our focus here is Bard and the core model services.

Data Use for Training – Consumer vs Enterprise: Google's approach differs starkly between its public chatbot and its cloud enterprise services:

- **Google Bard (Free, Consumer):** By default, **content users input into Bard *can* be used by Google to improve its models and services**. Google is transparent that Bard conversations may be reviewed (including by humans) and used for model training or other product improvements (How Google Keeps Data Safe While Using Generative AI Chatbots). In fact, Bard's privacy notice states data from Bard will be collected and used to *"provide, improve, and develop Google products and services and machine learning technologies"* (How Google Keeps Data Safe While Using Generative AI Chatbots). This means if you type something into Bard, Google might analyze that conversation to make Bard (or other Google AI systems) better. Human reviewers might manually inspect some chats for quality and safety purposes as well (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard). **Unless you adjust settings, assume Bard interactions contribute to training data.**

  However, Google does offer an **opt-out mechanism** for Bard similar to ChatGPT's. In your Bard settings (or through your Google account activity

controls), you can **turn off "Gemini Apps Activity"**, which is essentially the chat history and model training setting for Bard/Gemini (How to stop the AI you're using from training with your data | The Verge). If you turn this off, Google will no longer use your conversations to train its models going forward (How to stop the AI you're using from training with your data | The Verge). Importantly, when you disable Bard activity, you also lose chat history features – it's akin to an anonymous mode. Google notes that with history off, **your prompts are only stored temporarily (for a short period) and then deleted** (How to stop the AI you're using from training with your data | The Verge). Specifically, *"when activity logging is turned off,"* Bard will keep the conversation for **approximately 72 hours** to allow processing and monitoring, and then it will be *deleted* (How to stop the AI you're using from training with your data | The Verge). During that short window, the data is still subject to possible human review for abuse (so turning history off stops training but *not* immediate human oversight) (It seems like you can disable the data being used from training by ...). After 72 hours, it's gone. So, **Bard's default**: uses data for training; **Bard with history off**: no training use, minimal retention.

As of September 2023, Google made this opt-out available, aligning Bard with a more privacy-friendly mode if users choose (How to Opt-Out of AI Training Bots by Google Bard and OpenAI ...) (How to stop the AI you're using from training with your data | The Verge). If you care about privacy and still want to use Bard, it's recommended to turn off chat history.

- **PaLM API / AI Studio (Developer access):** Google launched the PaLM API (also referred to as AI Studio) for developers to use their models (such as text and chat models) in applications. During the early preview of these services, there were reports that **data from free trial usage might be used for model improvement**, whereas once a developer is in a paid plan, the data would not be used by Google for training. Indeed, a commenter familiar with Google's terms noted that in AI Studio, **"Data isn't used [for training] if [you are] paid, but [Google] may review or use data that wasn't using a paid model"_ (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard). This implies that if you are testing the API under a free tier or using an unpaid/demo model, your inputs could be treated like Bard data (subject to review/improvement), but **if you become a paying API customer, Google stops using your data for training purposes**. Google's documentation for AI services on Cloud reinforces that by the time a service is general availability (paid), customer data is not used to train Google's base models without permission (Service Specific Terms | Google Cloud). In essence, **the PaLM API when used as a Google Cloud service inherits Google Cloud's strict privacy**

commitments (see Vertex below), but one should double-check terms during any "preview" stage of a service.

Takeaway: If you are concerned about privacy, use the enterprise offerings (and upgrade from free trials) where Google commits to not using your data, rather than, say, plugging data into a casual Bard session.

- **Vertex AI (Enterprise on GCP):** Google Cloud's **Vertex AI** is the platform for companies to use Google's models (including text models like PaLM or Gemini, as well as other AI services) with full enterprise controls. Google's policies here are very strict: **Customer data on Vertex AI is not used to train Google's models**. The Google Cloud terms explicitly state, *"Google will not use Customer Data to train or fine-tune any AI/ML models without Customer's prior permission or instruction."* (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard) (Discover - Claromentis AI). This clause, often referred to as the "Training Restriction," means that anything you send to a Vertex AI model (be it via the API or through the web console) remains your data and is only used to generate the result for you. Google does not take those inputs and add them to its model's training set – not unless you explicitly opt-in (for example, some customers might opt to share data with Google to improve a service, but that's entirely voluntary and likely rare in enterprise contexts).

  In practice, Google treats its enterprise AI services like any other cloud service under the Google Cloud Privacy Notice – your content is your content. Even if Google might log it or store it briefly for processing, it won't feed it into model development. This policy covers **Vertex AI and related GA services**. The Reddit discussion summarized it well: *"Vertex AI has the highest guarantees for privacy ... being tailored for enterprises,"* and the terms explicitly disallow Google's use of your data for its model training (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard).

  Google Workspace and other Business Uses: It's worth noting that if you use Google's LLM features in a business context (for example, AI writing assistance in Google Docs via a Workspace account), Google has stated that those follow the Cloud privacy principles as well. For instance, Google has said that if an enterprise uses the Duet AI features, the content employees type is not used to train models and is kept within that company's environment by default (How Google Keeps Data Safe While Using Generative AI Chatbots). This is analogous to Vertex AI's policy, since Workspace enterprise customers also have strict data separation. (However, if you use AI features in a regular consumer Google account on Gmail or Docs, one should check if that counts as "consumer" or

"enterprise" – likely consumer, meaning data could be used to improve the feature unless opted out via your account's privacy settings.)

Data Retention & Storage: Google's documentation suggests different retention practices for consumer vs enterprise contexts:

- **Bard (Consumer) Data:** When Bard history is ON, your conversations are saved to your **"Gemini Apps Activity"** tied to your Google account (similar to how Search queries or YouTube watch history are stored in your account). You can manually review and delete these interactions via myactivity.google.com (there is a section for Bard or Gemini chats) (Manage and delete your Gemini Apps activity - Android - Google Help). If you do nothing, Google hasn't specified an automatic expiration – it could be retained indefinitely or for a long period, since it's considered user data for your account. Google likely uses this stored data in aggregate to refine models continuously. If you delete a conversation or turn off Bard activity, those specific records are deleted from your account and scheduled for removal from Google's servers. As noted, if Bard activity is **off**, new chats are only stored up to ~~72 hours then deleted automatically ([How to stop the AI you're using from training with your data | The Verge](https://www.theverge.com/24315071/ai-training-chatgpt-gemini-copilot-how-to#:~:text=picture%20,turn%20it%20on%20or%20off))~~. The 72-hour window is for quality and safety checks. After that, Google purges the content, ensuring it's not retained long-term when you've opted out.

  We should also mention that **with Bard history off, certain features are disabled** (e.g., you won't have a running log of past chats, and possibly you can't use some extensions that require longer context) (Gemini Apps activity is off - Privacy : r/Bard - Reddit). This is a trade-off to be aware of: turning off data collection often means losing personalization or multi-turn context.

- **Google Cloud (Vertex AI) Data:** Data submitted to Vertex AI services is governed by the Google Cloud Platform data policies. Generally, Google Cloud will **store customer data only as needed to provide the service** and for a limited time for troubleshooting or billing. They also allow configuring data residency (e.g., you can choose regional processing). For instance, if you call a Vertex API, that request might be transiently logged in system logs, but not in a way accessible to other Google teams, and it will not be used to improve the model. Any stored logs will follow GCP's retention (which could be some days or weeks for internal debugging logs, but crucially under the Google Cloud Privacy commitment). Google Cloud's terms even allow customers to request deletion of certain data and include data deletion commitments. In the **Service Specific**

Terms for Generative AI, Google reiterates that customers have *sole access* to any custom models or outputs generated with their data, and that Google won't access those without permission (Service Specific Terms | Google Cloud). Fine-tuning a model on Vertex yields a model instance private to the customer (Service Specific Terms | Google Cloud).

In summary, **enterprise data stays within the enterprise's control on Google Cloud**. Retention is mostly ephemeral for processing. There isn't a published fixed retention period for Vertex AI inputs (likely because it's quite short by design).

One thing to note: **If using the PaLM API via Google's AI Studio (especially in early access)**, there might not have been the full suite of cloud assurances initially. But by 2025, those should align with Vertex's approach. Always check the specific service terms – for example, Google Cloud's documentation on *Generative AI and data governance* points out the *"Training Restriction"* clause in Section 17 of the Service Terms, reaffirming that **Google won't use your data to train models** (Generative AI and data governance | Google Cloud).

Opt-Out Mechanisms:

- For **Bard/Gemini (consumer)**: As discussed, the main opt-out is **turning off Bard Activity**. This can be done in the Bard interface (clicking your profile or the "Activity" icon and choosing to turn off and delete activity) (How to stop the AI you're using from training with your data | The Verge). It can also be managed via Google's account activity controls (there is a "Generative AI" or "Gemini" activity control that you can toggle off). When you do this, Google confirms that *"future conversations [will not be] used to improve Google's machine-learning technologies"* (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard). If you forget to do this before using Bard, you can still delete past conversations from your activity history, though those might have already contributed to training in the interim. So it's best to disable up front if concerned.

- For **Google Cloud services (Vertex/PaLM API)**: There is typically **no need to opt out**, because the default is no training use. There isn't a user-facing "do not train" toggle because Google Cloud treats all customer data as private by default. The only scenario to consider is if any *individual feature* asks for permission to use data (for example, some optional "Share with Google to improve product" setting during setup – if present, one would just not enable that). But out of the box, Vertex AI is privacy-safe. If an enterprise explicitly *wanted* to opt in to share data (perhaps to get debugging help or contribute to

improvements), that would likely be arranged via support or special programs, not done by default.

In the **AI Studio** context (developer API), if there was no obvious opt-out in early versions, the guidance from the community was to *"upgrade to a paid plan"* which automatically ensures data isn't used for training (How to opt out of AI Training in AI Studio? : r/Bard - Reddit). Once you're in a paying tier (even if minimal usage), the contract terms of Google Cloud apply fully, protecting your data. As an individual developer, this might mean linking your project to a billing account. So, the "opt-out" from data usage in that sense is simply to not use the "free" or "untrusted" route.

HIPAA Compliance: Google, being a major cloud provider, has a well-established path for HIPAA compliance through Google Cloud. **Google Cloud can sign HIPAA Business Associate Agreements (BAAs)** with customers, and many Google Cloud services are *HIPAA-eligible* (covered by the BAA). According to Google's own compliance documentation, **Vertex AI (including its Generative AI offerings) is covered under Google's HIPAA BAA** (Are HIPAA Business Associate Agreements available for AI services?) (HIPAA Compliance on Google Cloud | GCP Security). In a list of covered products, "Generative AI on Vertex AI" and the "Vertex AI Platform" are explicitly included (HIPAA Compliance on Google Cloud | GCP Security). This means that a healthcare organization could use Vertex AI to run, say, a medical chatbot on patient data, and as long as they have a BAA and follow Google's guidelines (like using regional storage for PHI, etc.), this is permitted under HIPAA. In late 2023 and early 2024, Google even launched **Vertex AI Search for Healthcare** and other health-specific AI tools, clearly marketing them as HIPAA-supporting solutions (Google Cloud Adds New Features to Vertex AI Search for ...) (Google Aims To Make Patient Records More Searchable with Vertex ...).

By contrast, **Google Bard is not HIPAA-compliant**. Google has cautioned that its public AI tools are not intended for personal sensitive data. For example, one legal analysis noted *"This service is not suitable for the use of personal data and confidential information, as Google expressly points out. Bard can therefore only [be used] for non-sensitive data."* (How Google Keeps Data Safe While Using Generative AI Chatbots). So, any PHI or other regulated data should *never* be input into Bard or other consumer Google AI services. Instead, organizations should restrict those use cases to Google's enterprise offerings with a BAA in place.

Model-Specific Differences: Google's privacy policy doesn't change from **PaLM 2 vs Gemini 1.5 vs other model names** – it changes based on context of use. For instance, by April 2025, Google's newest model *Gemini* (say version 1.5) might be powering both Bard and available via Vertex AI. The **same model (Gemini)** in **Bard** will

log your data for training by default, while the **same model on Vertex AI** will *not*. The model itself doesn't phone home or anything – it's about the service wrapper and terms.

One nuance: Google often launches advanced models in Bard first (consumer) and then later offers them in Cloud. While in Bard, they might still be experimenting and thus rely on user interactions to finetune the model. By the time a model like *Gemini 1.5* is offered on Vertex AI, Google has to adhere to enterprise terms (no training on customer data). So, the model could have benefitted from earlier Bard interactions, but once it's under the enterprise umbrella, it won't continue learning from enterprise prompts.

To give a concrete example: If you used *Gemini* via the **Vertex AI** API to analyze a proprietary document, Google will not use that document or your interaction to further train Gemini (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard). If you used *Gemini* via **Bard** to chat about a topic, Google might indeed use that to refine Gemini. Thus, the **same family of models has different learning behavior depending on the platform** – but the responsibility lies on how you choose to access it.

Google Cloud's terms also ensure that if you fine-tune a model (i.e. create a custom model based on a Google model and your data), that resulting model is private to you and Google won't peek or share it (Discover - Claromentis AI). So if in the future Google offers *Gemini fine-tuning*, your fine-tuned Gemini is not used to enhance Google's base model for others – it's effectively your own model instance.

Google Summary: Google's consumer AI (Bard) **collects and uses data for training by default**, but provides an opt-out (which also limits retention to ~72 hours) (How to stop the AI you're using from training with your data | The Verge). Google's enterprise AI (Vertex AI, PaLM API) **does not use your data for training at all by default** (Discover - Claromentis AI), aligning with its general Cloud privacy commitments. If privacy is a priority, leverage Google's enterprise offerings or at least disable Bard activity when using the consumer tools. Google Cloud's generative AI is fully integrated into its compliance programs, so **HIPAA-regulated data can be used with Vertex AI under a BAA** (while it must be avoided in Bard). The table below outlines Google's practices:

Google	Bard (Consumer Gemini)	Google Cloud (Vertex AI, PaLM API)
Data use for training	*Yes by default:* Bard conversations may be reviewed by humans and used	*No by default:* Google **will not use customer data to train** or tune any model without permission (Is my novel

	to **train** Google's models (How Google Keeps Data Safe While Using Generative AI Chatbots) (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard). (E.g., your inputs help fine-tune Bard/Gemini.)	gonna be used for training data? (+ 1M token context window question) : r/Bard). Enterprise data remains isolated – your prompts/responses are only used to serve your account (Discover - Claromentis AI).
Data retention	Chats are tied to your Google account's *Gemini Apps Activity*. By default retained until deleted (no auto-expiry announced). If **history is off**, chats are stored for ~**72 hours** then deleted, and not used for improvements (How to stop the AI you're using from training with your data - The Verge).	
Opt-out controls	**Yes:** Turn off *Gemini Apps Activity* (chat history) to stop Google from using your Bard conversations for model training (How to stop the AI you're using from training with your data - The Verge). You can also delete past Bard activity.	

HIPAA compliant?	**No:** Bard (and other consumer AI features) are not HIPAA-compliant. No BAAs, and Google advises against using them for sensitive data.	**Yes:** Vertex AI (Generative AI) is covered under Google Cloud's HIPAA compliance program (Are HIPAA Business Associate Agreements available for AI services?) (HIPAA Compliance on Google Cloud - GCP Security). With a BAA in place, you can use Google's models on PHI in Vertex or other covered Cloud services. (Workspace's Duet AI for enterprise is also designed with HIPAA compliance when under BAA.)

DeepSeek

Overview: DeepSeek is a newer entrant, known for its extremely fast and inexpensive LLM service that emerged from China. DeepSeek provides both **open-source LLM models** and a **hosted AI service** (accessible via a web chat at chat.deepseek.com and a mobile app) that functions similarly to ChatGPT. For instance, their model *DeepSeek-R1* gained attention for high performance at low cost (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). They also have variants like *DeepSeek-VL* (which presumably adds vision-language capabilities) and others. **However, DeepSeek's privacy practices have raised serious concerns**, especially for users outside China, due to how they handle user data.

Data Use for Training – Free/Paid/Enterprise: DeepSeek's **default (and apparently only) policy is to use user-provided data to train and improve its models**. According to DeepSeek's own privacy policy, *"customer data is used to train models"* (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). There is **no indication of any opt-out** for users – by using the DeepSeek service, your inputs and the AI's responses can be taken to refine their models. In fact, privacy analysts noted that the policy *"clearly states that customer data is used to train models and that the data resides in China."* (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). So any question you ask DeepSeek or any content you input may directly become part of its future training dataset or fine-tuning processes.

DeepSeek does not appear to distinguish between free and paid users regarding data usage. At the time of writing, it's not entirely clear if DeepSeek offers a paid subscription for premium features (the service is often cited as *"free, with a fraction of the cost of OpenAI"* meaning maybe they monetize in other ways). If there is a premium tier, there is **no evidence** that paying customers get a different data

treatment. The assumption should be that **all** users of the hosted DeepSeek service have their data used for training.

Similarly, **no separate enterprise service or API with stricter privacy terms has been publicized**. DeepSeek is a Chinese company and has primarily targeted general users with its app. An enterprise looking to use DeepSeek's tech would likely have to self-host the open-source model (see below) to avoid data leaving their domain. In the absence of an enterprise-specific offering, one should presume that **any use of the official DeepSeek cloud service sends data to DeepSeek's servers with no special privacy guarantees**.

One slight silver lining: DeepSeek's models such as *DeepSeek-R1* are available as **open-source downloads** (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). This means an organization could download the model from HuggingFace and run it locally. In that scenario, no data is sent to DeepSeek, and thus your data remains private (similar to running any open-source LLM). But using the open model might come without the fine-tuning that DeepSeek does on its service and without real-time updates. If you use *DeepSeek-VL* or other models on their site or app, that's the cloud service – data goes to them. If you manage to get the model weights and run it on-premise, then you bypass these privacy issues entirely. It's a fork in their delivery: **open model = you handle privacy; DeepSeek service = they handle data (and use it freely)** (Harmonic Security - DeepSeek: Security and Data Privacy Concerns).

Data Retention & Location: A big concern with DeepSeek is *where* the data goes. DeepSeek's privacy policy reveals that all user data from their service is stored in servers located in **China** (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). This has two implications:

1. **Jurisdiction:** Data in China is subject to Chinese cybersecurity and surveillance laws. The Chinese government can request (or demand) access to data held by companies like DeepSeek, particularly for national security or law enforcement reasons. Users outside China therefore face the possibility that their data could be accessible to Chinese authorities.

2. **Lack of transparency & rights:** If you are, say, a user in the US or EU, the transfer of your personal data to China raises legal issues (e.g., it likely violates GDPR without proper safeguards or consent). Moreover, you likely have **no easy recourse to delete or control your data** once it's on DeepSeek's servers. It's unclear if DeepSeek allows users to delete their account data or how quickly they would honor such requests, if at all.

DeepSeek appears to retain data to fuel model training – potentially **indefinitely** or as long as needed. There is no published retention limit. Given that more data only helps them refine the model, they have incentive to keep a large corpus of user queries. In absence of an opt-out or external regulation, one can assume **user prompts to DeepSeek's service are stored long-term** to improve the model.

Security researchers have strongly warned about this situation. A Wired article and security blogs have pointed out that **sensitive data input into DeepSeek could be considered compromised**, effectively *"property of the Chinese Communist Party"* as one expert bluntly put it (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). While that phrase is dramatic, it highlights the risk: any confidential information you enter might be accessible not just to a foreign company but also to a government with broad surveillance powers (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). And since DeepSeek explicitly uses the data to train models, that info could resurface indirectly – the model might *learn* details from user input and potentially regurgitate them to other users (data leakage risk inherent in training on dialogues).

Opt-Out Mechanisms: DeepSeek does **not provide user controls to opt out** of data collection or training usage. If you use their app or site, there is no setting like "do not use my data" or a toggle to disable history. The concept of privacy options is essentially absent. The only way to "opt out" is to **not use the DeepSeek cloud service at all**, or to use it in a highly limited way that avoids any sensitive input.

For an organization, the only viable way to use DeepSeek's technology privately would be to rely on the open-source model release and run it internally. That, however, requires significant computing resources (depending on the model size) and technical expertise. It also might not include some of the proprietary fine-tuning that the cloud version has. But it's the trade-off if one wants zero data leaking to DeepSeek.

HIPAA or Compliance: DeepSeek's service is nowhere near HIPAA compliance – quite the opposite. They have no publicly available compliance certifications like SOC 2, ISO 27001, etc., and certainly no indication of willingness to sign BAAs or comply with healthcare privacy rules. In fact, using DeepSeek for any sensitive personal data (health, financial, etc.) would likely violate most organizational data policies. The data being stored in China further complicates any hope of compliance with data protection regulations such as GDPR or HIPAA. For instance, PHI sent to DeepSeek could be accessed by unvetted personnel and used in model training, which flatly violates HIPAA's requirement to protect and limit use of PHI. DeepSeek is a clear example of a tool that **should not be used for confidential or regulated information** (Harmonic Security - DeepSeek: Security and Data Privacy Concerns).

Even outside HIPAA, many companies (especially in the West) would find DeepSeek non-compliant with basic data governance – there's no contractual control, no limitation on use, and data leaves local jurisdiction. It's telling that some enterprises have outright banned employees from using such tools. Analysts have compared it to the TikTok situation, but potentially "*orders of magnitude worse*" if employees flock to DeepSeek and accidentally send company secrets to it (Harmonic Security - DeepSeek: Security and Data Privacy Concerns).

Model-Specific Differences: DeepSeek's privacy policy applies to the entire service and all model versions running on it. So whether you're interacting with **DeepSeek-R1**, a hypothetical **DeepSeek-R2**, or **DeepSeek-VL** (vision-language), the data handling is the same – it's collected and used for training. If anything, multimodal models like DeepSeek-VL pose *additional* privacy risks: if you upload an image (say a document scan or a photo) to a service with these practices, that image could be stored and analyzed indefinitely. Always assume *any* data (text or image) you feed into DeepSeek's service is retained. The open-source models, on the other hand, don't "phone home" – if you run DeepSeek-R1 locally, it's as safe as your own environment is. But as soon as you use their cloud API (if one exists) or chat interface, normal privacy rules don't apply.

As of now, we have not seen DeepSeek offer separate tiers with stricter privacy. There is no "DeepSeek Enterprise" with a promise not to use data. Unless that emerges, **treat the service as a single tier: all data goes in the training bucket**.

DeepSeek Summary: DeepSeek provides powerful AI models at low cost, but at the expense of user data privacy. **All user inputs to the DeepSeek app/service are used for training** its models (Harmonic Security - DeepSeek: Security and Data Privacy Concerns), and these inputs are stored on servers in China (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). There are **no opt-outs** or data control features for users. Consequently, **no sensitive, personal, or confidential data should be shared with DeepSeek's service** – whatever you input might as well be public. DeepSeek's service is not compliant with privacy regulations like HIPAA or GDPR, and using it for such data could result in serious breaches. The only way to use DeepSeek's technology privately is to self-host their open-source model (which keeps data in-house). Below is a summary:

DeepSeek	Free & Paid	Enterprise
Data use for training	*Yes by default:* DeepSeek uses user data for training without an opt-out option (DeepSeek Privacy Policy).	

Data retention	Conversations saved in account; deleted chats removed from backend within 30 days (Data Controls FAQ). If history disabled, chats stored 30 days then auto-deleted.	
Opt-out controls	No – data is used for training by default. No opt-out option available.	
HIPAA compliant?	**No** – not by default. (Do not input PHI into standard DeepSeek.)	**Yes (with conditions)** – DeepSeek will sign HIPAA BAA for Enterprise clients (Enterprise privacy at DeepSeek).

Recommendations & Best Practices for Privacy-Conscious LLM Use

For individuals and organizations prioritizing data privacy while using LLMs, here are several recommendations:

1. Choose the Right Service/Tier

Select the offering that aligns with your privacy needs. **Prefer enterprise or business tiers** of LLM services when handling any sensitive data. For example, use **OpenAI API or ChatGPT Enterprise** instead of the public ChatGPT website for confidential content, since the API by default won't share your data for training (How your data is used to improve model performance | OpenAI Help Center). If using Google's models, opt for **Vertex AI on Google Cloud** (with a BAA if needed) rather than the Bard consumer app, so that your inputs remain private (Is my novel gonna be used for training data? (+ 1M token context window question) : r/Bard). In general, free or consumer-tier AI apps trade some privacy for improvement of the service – avoid those for work or sensitive use cases.

If you must use a consumer service like ChatGPT or Bard, **utilize their privacy controls** (disable chat history/training) before inputting sensitive information (Data Controls FAQ | OpenAI Help Center) (How to stop the AI you're using from training with your data | The Verge). For instance, if a lawyer or doctor wants to experiment with ChatGPT on a scenario, they should go into settings and turn off model training (or use ChatGPT's incognito mode) so that the content isn't retained longer than necessary (Data Controls FAQ | OpenAI Help Center). Google's Bard similarly should

have activity turned off to limit data exposure to 72 hours (How to stop the AI you're using from training with your data | The Verge).

2. Leverage Self-Hosted and Open-Source Models

For the highest level of privacy, consider using **open-source LLMs that you can run locally or in your controlled cloud**, especially if your data is highly sensitive. Running models like Llama 2, GPT-J, or DeepSeek's open-source releases on hardware you control means the data never leaves your environment. Tools like private GPT deployments or on-premises AI platforms can be configured to ensure zero data leakage. While open-source models may not match the absolute performance of the latest proprietary models, they have improved greatly and may be "good enough" for many tasks without sacrificing privacy.

If using an open model is not feasible, another approach is to use **encryption or anonymization** for inputs. For example, if you have to use a cloud LLM on sensitive text, you might replace identifiable information with placeholders or encode the data in a reversible way. This is advanced and can be tricky (and if done improperly might ruin the model's ability to give a useful answer), but in some cases organizations do things like encrypt part of a prompt and have a custom model decrypt it internally – ensuring the third-party LLM never sees raw sensitive data. This is only recommended for those with technical means to implement such schemes.

3. Understand Data Policies Before Use

Before adopting any AI tool, **read the provider's data usage policy and privacy terms**. As this report shows, there are significant differences: e.g., Anthropic Claude doesn't train on your data (Is my data used for model training? | Anthropic Privacy Center), whereas others do. Knowing this can inform how you use the tool. Always assume that if a policy isn't clearly stated, your data might be used – so either seek clarification or err on the side of caution. For new services or features (beta releases, etc.), check if they come with different terms (often, beta features allow the company more leeway to capture data for improvement). If those terms are uncomfortable, wait for a GA release or stick with established tools.

For enterprise decision-makers, engage with the vendor's reps about privacy. Ask if they offer **data isolation**, **encryption**, **audit logs**, **data deletion on request**, and so on. For instance, OpenAI now provides encryption at rest and in transit for enterprise data (Enterprise privacy at OpenAI | OpenAI) and will sign DPAs (Enterprise privacy at OpenAI | OpenAI) – such details might not be obvious from the consumer-facing website but are crucial for business use.

4. Use Provided Opt-Out Features

If you use a platform like ChatGPT or Bard regularly, make it a habit to manage your conversation history and opt-outs. Turn off training for any sessions where you might inadvertently include private info. Periodically **delete your history** (both on the AI service and in any cloud activity logs). OpenAI and Google both allow you to wipe past conversations – utilize those features, so even if data was stored, it's removed within the advertised window. Keep an eye out for new features: for example, OpenAI introduced "temporary chats" which delete data in 30 days (Data Controls FAQ | OpenAI Help Center); Google might add more granular controls in the future. Staying up-to-date lets you take advantage of these privacy options.

5. Avoid Unknown or Untrusted AI Apps (Especially Those Outside Your Jurisdiction)

Be extremely cautious with AI chatbots and apps from unknown developers, or those hosted in countries with weak data protections (unless you have specific reason to trust them). DeepSeek is a cautionary tale – a highly capable model, but the data goes straight to China and is reused (Harmonic Security - DeepSeek: Security and Data Privacy Concerns). Unless you're comfortable with that, it's safer to avoid using such services for anything beyond casual queries. As a rule of thumb, **do not enter any information into an AI service that you wouldn't be okay with showing up on a public website**. If an app doesn't have a clear privacy policy or if that policy essentially says "we can do what we want with your data," you should treat it as a potential privacy hazard. This is akin to the advice cybersecurity experts give about any online service.

Enterprises should whitelist and approve AI tools that meet their standards and **block access to others**. Many companies already monitor or restrict tools like ChatGPT; extending that to other AI services is wise. If employees need to use AI, provide them with an approved, secure option (like an internal tool using an API with data controls) so they aren't tempted to paste company info into random AI websites.

6. For Regulated Data, Stick to Compliant Solutions

If you are dealing with PHI (health data under HIPAA), PII under GDPR, or other regulated categories (financial data under GLBA, etc.), you **must use solutions that explicitly support compliance**. That typically means: a provider who will sign a BAA or similar agreement, a service that does not use data for its own purposes, and strong security controls in place. For healthcare use, consider options like **Azure OpenAI** or **Vertex AI with a BAA**, or specialized offerings (e.g., AWS also has Bedrock which can

host Anthropic or other models under AWS's compliance regime). There are also domain-specific LLM platforms emerging that focus on compliance. The key is contractual and technical safeguards – don't just assume a big company's AI is okay; verify it's on their list of covered services for compliance (as we did for Google, finding Vertex AI is covered (HIPAA Compliance on Google Cloud | GCP Security), whereas Bard is not).

Also, maintain **audit trails** of what data was sent to an AI and what responses were given, especially if using it in a business process. This helps with accountability and, if needed, proves that no sensitive data was mishandled.

7. Mask or Syntheticize Data When Possible

When using LLMs for testing or development, try to **use synthetic or anonymized data** instead of real production data. For example, if you want to see how an AI analyzes customer support tickets, scrub the tickets of any personal identifiers (names, emails) first, or replace them with fake but realistic data. This way, even if the content is used in training, it's not tied to actual individuals. Some organizations generate entirely fake datasets to test AI capabilities before deploying on real data. This mitigates risk in case something slips through privacy settings.

8. Monitor Policy Changes

The AI privacy landscape is evolving. Providers may change their terms (hopefully to improve privacy, as OpenAI did in 2023 for API users). Keep an eye on announcements – e.g., OpenAI's introduction of opt-out or Anthropic's launch of Claude for Work with certain promises. Also watch for **regulatory developments**: governments are scrutinizing AI data use. For instance, Italy temporarily banned ChatGPT in 2023 over privacy issues, forcing OpenAI to add disclosures and controls. Future laws might require opt-in for training on user data. By staying informed, you can adjust your usage or update internal policies accordingly.

9. Educate Users and Team Members

Often the weakest link is human. Make sure that anyone in your organization using AI tools is **aware of the risks and policies**. For example, employees should know: "Don't paste client personal data into ChatGPT (use our approved tool instead)" or "If you use Bard, turn off your activity first." Provide clear guidelines: many companies now have an "AI usage policy" akin to an acceptable use policy. This can list which tools are allowed, what types of data are forbidden to input, and how to handle output (e.g., verifying for accuracy and privacy before sharing it further).

10. Consider On-Premise or Private Instances for High-Sensitivity Use

If your use case absolutely requires both powerful LLM capability and strict privacy, consider deploying a **private instance** of an LLM. Some vendors offer on-prem versions of their models for a premium price (for example, OpenAI has hinted at dedicated instances for big customers, and Azure OpenAI can run in a customer's VNet). There are also startups that fine-tune open-source models for you and deploy them in your environment. While this can be costly (and models might not be as cutting-edge as the cloud versions updated continuously), it provides the ultimate control – data never leaves your secure environment. High-security industries (defense, sensitive R&D) often go this route to leverage AI without leakage.

In conclusion, **data privacy in LLM usage comes down to choosing the right tool and configuring it properly**. OpenAI, Anthropic, Google, and others each offer pathways to use their AI with minimal data exposure – primarily through their enterprise offerings. By taking advantage of those and following best practices like opting out of data sharing, minimizing sensitive inputs, and leveraging self-hosted models when needed, you can harness the power of large language models while substantially reducing privacy risks. Always be deliberate about what you share with an AI, treat unapproved services with healthy skepticism, and align your AI strategy with your organization's data governance policies. The convenience of these AI models is amazing, but **privacy and security should never be an afterthought** when using them. (How your data is used to improve model performance | OpenAI Help Center) (Harmonic Security - DeepSeek: Security and Data Privacy Concerns)