

PUBLIC PRIVACY STATEMENT RESEARCH

[ABRIDGE](#)
[APPLE](#)
[GOOGLE](#)
[META](#)
[HYPOCRITIC AI](#)
[SUKI](#)

ABRIDGE - <https://www.abridge.com/about>

[Location on Website](#)

[Structure and Sections Included](#)

1. [First Section: Updates/Changes](#)
2. [Second Section: Definitions](#)
3. [Third Section: Applicability](#)
4. [Fourth Section: Hyperlinks](#)

[Content and Disclosures Expected](#)

1. [HIPAA](#)
2. [Handling of PHI](#)
3. [Customer data usage](#)
4. [AI Model training policies](#)
5. [Prompts/outputs](#)
6. [Data retention](#)
7. [Subprocessors](#)
8. [Cookies](#)
9. [Security Practices](#)
10. [Compliance expectations](#)

[Biometric Privacy Act](#)

1. Location on Website:
 - a. Very bottom of the page there is a section for the links to all the different places in the website (e.g; Resources, About, Policies)
 - b. Under Policy there is a “[Policy Statement](#),” “Terms,” and “Cookie Preferences.”
2. Structure and Sections Included:
 - a. The first section notes the most recent update or change to the statement, which notes what was changed.
 - b. The second section defines a few terms. Explains that the company (ABRIDGE) is referred to as we, our, or us; that the Privacy Policy is referred to as “policy;” that they have “services;” and they collect info from users who visit the www.abridge.com “sites.”
 - c. Third Section is Applicability. It notes that data collected by Clinics and Hospitals that is stored in their services is not governed in this policy. So the “Customer Data” is solely governed in the BAA’s with the external companies in the B2B agreement.
 - d. The Fourth Section serves as an index for the remainder of the statement. It has links to each of the sections, and they are listed as follows:
 - i. Information Company Collect
 - ii. How Company Use Your information
 - iii. How Company Share Your Information
 - iv. Your Privacy Choices
 - v. California Users and Notice at Collection
 - vi. Your Privacy Rights
 - vii. Your Privacy Rights in Respect of Customer Data
 - viii. Security
 - ix. International Data Transfer
 - x. Data Retention and Deletion
 - xi. Applicant & Candidate Texting Privacy Policy
 - xii. Children’s Privacy
 - xiii. Change to this Privacy Policy
 - xiv. How to Contact Us
3. Content and disclosures expected:
 - a. HIPAA:

- i. To my surprise, there is not a single mention of HIPAA in the entire Privacy Statement.
- b. Handling of PHI/health data
 - i. “Abridge processes Customer Data, which may include Protected Health Information (PHI), solely on behalf of our customers. Our processing of such information, which Company refer to as “Customer Data,” is governed exclusively by the terms of our agreements with those customers, including our Business Associate Agreements (BAAs).”
 - 1. PHI processing is not governed by this Policy
 - 2. The Policy then makes a statement to patients whose healthcare provider uses their services. They tell them to refer to their proverbial Notice of Privacy practices to see how they handle PHI. Abridge is purely a business associate to the provider and processes the patients data only on their instruction.
- c. Customer data usage
 - i. Customer data is governed exclusively by the terms of Abridges’ agreements with customers, including BAAs
 - ii. “If personal information pertaining to you as an individual has been submitted to the Service by or on behalf of a Abridge customer and you wish to exercise any data protection rights you may have in respect of that information under applicable law, including (as applicable) the right to access, correct, amend or delete such information, please inquire with the relevant Abridge customer directly and refer to that customer’s privacy notice.”
 - 1. Any person, as allowed by the law (no specific law mentioned), has the right to access, correct, amend or delete their information. They have to reach out to their provider and refer to that customer’s privacy notice.
- d. AI model training policies
 - i. Not mentioned in the Policy Statement
- e. Prompts/outputs
 - i. Not mentioned in the Policy Statement
- f. Data retention
 - i. “Company retain personal information Company collect from you where Company have an ongoing legitimate business need to do so (for example, to comply with applicable legal, tax or accounting requirements, to enforce our agreements or comply with our legal obligations). When establishing a retention period for specific categories of personal information, Company consider who Company collected the data from, our need for the personal

information, why Company collected the personal information, and the sensitivity of the personal information. When Company have no ongoing legitimate business need to process your personal information, Company will either permanently delete or anonymize it or, if this is not possible (for example, because your personal information has been stored in backup archives), then Company will securely store your personal information and isolate it from any further processing until deletion is possible. When processing Customer Data on behalf of our customers, Company will retain Customer Data as described in our agreement with that customer.”

1. They retain information they have collected when they have a legitimate business need to (e.g; tax or accounting requirements, enforce agreements, or comply with legal obligations). Of course complying with applicable law.
2. When there is no means for business they will permanently delete or anonymize it. If that is not possible they will securely store it and isolate it from any further processing until deletion is possible.

g. Subprocessors

- i. Need to look more through small mentions of third party partners, but there is no direct mention in Policy Statement about subprocessors.
- ii. Service providers; business partners in connection with purposes Company aim to make clear to you at or prior to collection:
 1. They are provided with: Identifiers (e.g., name, email, phone number, IP address, account username/password
 2. Customer records/account
 3. Characteristics which may be protected classifications under State or federal law (such as gender and marital status)
 4. Commercial information such as transaction data
 5. Internet or network activity
 6. Geolocation data
 7. Professional or employment related information (e.g., specialty, employer, NPI number)

h. Cookies

- i. Information that is automatically collected when the site is visited.
- ii. When I first clicked on the website it had a pop up that said, “This website utilizes technologies such as cookies to enable essential site functionality, as well as

for analytics, personalization, and targeted advertising. To learn more, view the following link: [Manage Preferences](#)”

1. Language settings, mobile device carrier, radio/network information, general location information, information about activities such as access times and pages viewed.
2. Explains what cookies are. Explains that cookies may include “session cookies” that are deleted when a session ends. “Persistent cookies” are there longer. “First party” Cookies that they place, and “third party” cookies that their third party business partners and service providers place.
3. Local store technologies like HTML5 store larger amounts of data outside of the visitors browser in connection with specific applications. These are cookie-equivalent in function.
4. The company, service providers, and third party partners can collect personal information for marketing purposes. They collect info through cookies, pixel tags, clear gifs and tracking technologies.
 - a. The cookies delivered by third parties or other websites are not included in this policy.
5. Advertising choices are available for Browser settings. “Changing your internet web browser settings to block third party cookies.
6. “You can control cookies by changing the settings for each category of cookies in Abridge’s Cookies Storage Preferences via Cookie Preferences at the footer of Abridge’s website.”
7. There is another section at the bottom under “POLICIES” that allows you to change your cookie preferences.

i. Security practices

- i. “Company use appropriate administrative, physical, and technical safeguards to protect your personal data. Company evaluate our safeguards to adapt to new threats to the confidentiality, integrity, and availability of your personal data.”
- ii. “Even with the safeguards Company use, Company cannot completely guarantee the security of your personal data. Keep your login details in a safe place. Report any suspected security violations or incidents involving personal information by contacting us.”
- iii. Basically - Company have safeguards but anything can

	still happen. j. Compliance expectations (HIPAA, GDPR, SOC 2) i. None listed 4. Biometric Privacy Act? a. ABRIDGE has a lengthy section on a specific California Law. This is where Company can talk about the Biometric Privacy Act to make sure our clients know how Company follow the state laws.
Apple - https://www.apple.com/legal/privacy/en-ww/ 1. Location on website 2. Structure and sections included 3. Content and disclosures expected a. HIPAA b. Handling of PHI c. Customer data usage d. AI Model training policies e. Prompts/outputs f. Data retention g. Subprocessors h. Cookies i. Security Practices j. Compliance expectations	5. Location on Website: a. Very bottom of the website under internet services. Next to website terms of use. 6. Structure and Sections Included: a. Each section is just a few paragraphs in length. b. The sections are as follows: i. What is personal data at Apple? ii. Your privacy rights at apple iii. Personal data apple collects from you iv. Personal data Apple receives from other sources v. Apple's use of personal data vi. Apple's sharing of personal data vii. Protection of personal data at apple viii. Children and personal data ix. Cookies and other technologies x. Transfer and personal data between countries xi. Our companywide commitment to your privacy xii. Privacy questions 7. Content and disclosures expected: a. HIPAA i. No HIPAA Mentioned b. Handling of PHI/health data i. No mention of PHI ii. HOWEVER, this is what is mentioned about Apple Health:Data relating to the health status of an individual, including data related to one's physical or mental health or condition. Personal health data also includes data that can be used to make inferences about or detect the health status of an individual. If you participate in a study using an Apple Health Research Study app, the policy governing the privacy of your personal data is described in the Apple Health Study Apps Privacy Policy. 1. To participate in any studies you must forest review and sign an informed consent and authorization form. By using an app there is consent to the collection, use, and sharing of information. 2. They collect name, email, phone number, age, gender, state of residence, race,

	3. Height, weight, prior medical diagnosis and testing, current and previous use of certain medications, certain family history, health habits. This information may be collected through in app surveys or other health surveys that you may be asked to complete iii. Protection of your information: 1. “Apple takes the security of your personal information very seriously. Apple has implemented reasonable measures to keep the Study Data it maintains safe, and to protect the confidentiality of your information, including storing it in systems with limited access housed in facilities using physical security measures. Despite our security measures, total confidentiality cannot be guaranteed” a. Common c. Customer data usage i. They treat any data that relates to an identified or identifiable individual or that is linked or linkable to them by Apple as “personal data,” no matter where the individual lives. ii. Data about activity and use of offerings such as app launches within the service, including browsing history, search history, product interaction, crash data, performance and other diagnostic data, and other usage data d. AI model training policies i. Applebot model training and individual privacy rights ii. Apple uses information that is licenses from third parties, publicly available on the internet, and created synthetically. They do not use users’ private personal data or user interactions when training foundational models. iii. Applebot is a web crawler, which crawls information that is publicly available on the internet. Web publishers can use standard robots.tct directives to direct applebot not to crawl their website, or to direct apple not to use their website content to train Apple's foundational models. Applebot does not crawl data from websites that require login credentials or that are protected by a paywall. iv. Take steps to reduce the likelihood of personal data being included in their models, such as by omitting data from websites that aggregate large amounts of personal data and applying filters to remove personally identifiable information like social security and credit card numbers that are publicly available on the internet. v. You can object to the crawling of URLs. To exercise
--	--

	this right visit the inquiries page. e. Prompts/outputs i. No mention f. Data retention i. Uses a lot of language friendly to the user. E.g. “Company strive to collect only the personal data that Company need.” ii. Data collected depends on the interactions. Descriptions of how Apple handles personal data for individual services are available at [external link]. iii. They may collect any of the following information: 1. Account information: details, email address, devices registered, account status, and age 2. Device information: divide serial number, browser type 3. Contact information 4. Payment information: billing address and method of payment. Bank details 5. Transaction information 6. Fraud prevention information 7. Usage data 8. Location information 9. Health information: status of an individual, including data related to one’s physical or mental health or condition. Personal health data also includes data that can be used to make inferences about or detect the health status of an individual. If you participate in a study using an Apple Health Research Study app, the policy governing the privacy of your personal data is described in the Apple Health Study Apps Privacy Policy 10. Fitness information 11. Financial information: including salary, income, assets information where collected, and information related to apple branded financial offerings 12. Government id data: in certain jurisdictions they ask for government issued id. 13. Other information provided to them. iv. Apple receives data from other sources 1. From other individuals, businesses, or third parties acting at the users discretion. v. Use of Personal Data: Apple uses personal data to power services, process transactions, communicate with users, security and fraud prevention, and comply with law. May also use personal data for other purposes with users consent. 1. Retains personal data only for so long as necessary to fulfill the purposes for which it
--	--

was collected, including as described in this privacy policy, service specific privacy notices, or as required by law.

g. Subprocessors

- i. Apple can share personal data with apple affiliated companies, service providers who act on our behalf, partners, developers, and publishers, or others at users discretion. Apple does not share personal data with third parties for their own marketing purposes.
 1. Service providers: perform certain tasks on Apple's behalf, processing or storing data, including personal data, connection with users' use of services and delivering products to customers.
 2. Partners: "Apple may partner with third parties to provide services or other offerings. For example, Apple financial offerings like Apple Card and Apple Cash are offered by Apple and our partners. Apple requires its partners to protect your personal data."

h. Cookies:

- i. Apple may collect:
 1. Information about how you use Apple websites and services, Pages you visit and features you interact with, Search activity on Apple websites, Device and browser information, IP addresses and similar identifiers, Information about ad interactions and effectiveness, Click activity from links in Apple emails, Shopping cart ("Bag") contents on Apple's website, Language, formatting, and browsing preferences
 2. Apple also mentions using: Web beacons, Click-through URLs, Similar tracking technologies beyond standard cookies
 3. Types of Cookies Apple Uses
Communications Cookies
 - a. Used to:
 - b. Enable traffic between your device and Apple's systems
 - c. Detect errors
 - d. Support network functionality
 4. Strictly Necessary Cookies
 - a. Used to:
 - b. Make Apple websites function properly
 - c. Authenticate and verify transactions
 - d. Preserve shopping cart contents
 - e. Display websites in the correct language and format

	f. These are essentially required for core site functionality. 5. Other Cookies a. Used to: b. Analyze how visitors use Apple websites c. Measure advertising and search effectiveness d. Remember your preferences and choices e. Customize your browsing experience 6. What Apple Uses the Data For a. Understand user behavior b. Improve website and service performance c. Prevent fraud and enhance security d. Measure advertising effectiveness e. Personalize experiences f. Evaluate communication effectiveness (such as email link clicks) 7. Apple also states that it may combine cookie-related data with personal data it already has. When combined, Apple treats the resulting information as personal data under its Privacy Policy. a. Does not track users across third-party apps and websites b. Does not combine Apple app data with third-party data for targeted ads c. Does not share user or device data with data brokers i. Security practices i. Encryption, access restriction, monitoring, governance, vendor oversight, incident response, minimizing collected data j. Compliance expectations (HIPAA, GDPR, SOC 2) i. GDPR, CCPA, Global CBPR System, Global PRP System
Google - https://policies.google.com/privacy?hl=en-US 1. Location on Website 2. Structure and Sections Included: 3. Content and Dsiclosures Expected	8. Location on Website: a. Specific space for google account to check on privacy policy. i. The little circle of your google account. 9. Structure and Sections Included: a. Information google collects, why google collects data, your privacy controls, sharing your information, keeping your information secure, exporting and deleting your information, retaining your information, compliance and cooperate with regulators, about this policy, related privacy practices, data transfer frameworks, key terms, partners, updates

- a. [HIPAA](#)
- b. [Handling of PHI](#)
- c. [Customer data usage](#)
- d. [AI Model training policies](#)
- e. [Prompts/outputs](#)
- f. [Data retention](#)
- g. [Subprocessors](#)
- h. [Cookies](#)
- i. [Security Practices](#)
- j. [Compliance expectations](#)

- b. Terms of service: Introduction, your relationship with google, using google services, content in google services, software in google services, software in google services, in case of problems or disagreements, about these terms, updates, definitions, how google handles government requests for user information
 - c. Technologies: How google uses cookies, location information, credit card numbers for payments, how google voice works, google product privacy guide, how google retains data they collect
 - d. FAQ
10. Content and disclosures expected:
- a. HIPAA:
 - i. Does not mention HIPAA
 - b. Handling of PHI/health data
 - i. Does not mention PHI or BAAs
 - ii. Health data is addressed only in the context of fitness/consumer wellness products
 - 1. Collected: height, weight, sleep patterns, heart rate, skin temperature, calories burned, steps taken. This is labeled as a sensitive category and it is excluded from personalized ad targeting
 - c. Customer data usage
 - i. Purposes for data use:
 - 1. Service deliver: processing searches, delivering content, authenticating users
 - 2. Service improvement: tracking outages, fixing bugs, analyzing usage patterns
 - 3. New product development: using data from existing services to develop new ones
 - 4. Personalization: tailored search results, content recommendations, personalized ads
 - 5. Performance measurement: analytics on ad performance and product usage
 - 6. Communications: notifications about account activity or policy changes
 - 7. Safety and fraud prevention: detecting spam, malware, abuse, and security threats
 - 8. Cross service use: data may be combined across google services and devices
 - 9. They will not use information for purposes beyond this policy without consent
 - 10. Personally identifiable information is not shared with advertisers without user consent
 - 11. Drive, gmail, and photos content is not used for personalized ads
 - d. AI model training policies
 - i. Permits training AI models on publicly available data and using automated systems to analyze user content

for personalization and service improvement

1. Publicly available data: google may collect publicly available online information to train AI models for translate, gemini, and cloud ai
2. User content analysis: automated systems analyze user content for tailored results, personalized ads, and abuse detection
3. Algorithm use: algorithms recognize patterns in data
4. Gemini apps: governed by a separate gemini apps privacy notice
 - a. Gemini Apps Privacy notice:
 - b. What data is collected
 - i. What you say to gemini apps, like the prompts you submit or speak, and tasks you ask gemini to do.
 - ii. What you share with gemini apps like files, videos, screens you ask about, photos, imported chats, and page content you share from your browser
 - iii. Transcripts and recording of your interactions with gemini live including audio video and screens
 - iv. Instructions you provide
 - c. Information you provide gemini apps
 - d. Information Company collect as you use gemini apps
 - i. Content that gemini apps generation: like text, code, audio, images, video, music, public links, citations, chat summaries
 - ii. Information about steps our technology takes, prompts, like model thinking steps, information from your apps, browsers, and devices.
 - iii. Supplemental information
 - iv. Location information
 - v. Subscription information. Paying for a Google AI plan.
 - e. How your data is used
 - i. As described in the Privacy Policy:
 - ii. Provide services
 - iii. Maintain and improve

	services iv. Develop new services v. Personalize our services vi. Customize our services vii. Communicate with you viii. Measure performance ix. Protect google, our users, and the public f. How gemini apps get help from google services i. Rely on other google services and infrastructure to provide gemini apps. If youre 18 or older and upgrade to gemini apps, your calling or texting history may be imported from your web and app activity to gemini apps activity in some regions. g. How gemini apps work with connected apps i. Gemini apps work with connected apps, including google apps and third party services. Gemini saves and uses info from connected apps according to this notice, including to provide and improve gemini apps. Connected google apps save and use data, per the policies and the google privacy poloicy, including to provide and improve their services. If you use gemini apps to interact with third party services, they process your data according to their own privacy policies. h. Audio features i. Gemini apps may activate when you didn't intent them to, for example, if there's a noise that sounds like "hey google" or if you activate them accidentally by touch. If Gemini apps respond, they will treat your input like a normal activation. Depending on your settings, this data is
--	---

	used to improve google services. These include Gemini models, other generative AI models that power Gemini Apps, and technologies that reduce unintended activations. i. Canvas j. Configuring your settings i. Links to change settings for different categories such as skills manager, public links, and memory k. How long Company retain your data i. For different periods of time, depending on what it is and how they use it. You can change auto delete setting from 18 months to 3 months, 36 months, or indefinite l. Requisition content removal and exporting your information m. Other things to know n. Respect others' rights e. Prompts/outputs i. Collected through Gemini: What you say to gemini apps, like the prompts you submit or speak, and taks you ask gemini to do. ii. Search terms, queries, and interactions with AI services may be saved to account history f. Data retention i. Some data you can delete whenever, such as personal info or the content you create or upload like photos and documents. You can delete activity information saved in your account, or choose to have it deleted automatically after a set period of time. They keep this data in google account until it is removed. ii. Other data is deleted or anaomyzied automatically after a set period of time such as advertising data in server logs iii. They keep some data until the google account is deleted such as information about how often the user uses the services iv. Some data they retain for longer periods of time when necessary for legitimate business or legal purpose, such as security, fraud and abuse prevention, or financial record-keeping. g. Subprocessors i. Google uses third party service providersand affiliates to process data on its behalf. The policy does not
--	--

publish a specific list of subprocessors

1. Affiliates: google ireland limited, google commerce ltd, google mayment copr, google Dialer inc
2. Service providers: used for data center operations, product delivery, business process improvement, customer support
3. Content review: service providers help review Youtube content for public safety
4. Audio analysis: service providers analyze samples of saved user audio to improve speech recognition
5. Advertising partners: over 2 million non-Google websites and apple partner with Google to show ads
6. Subprocessor list: No public subprocessor list is given
7. Confidentiality: service providers are subject to googles privacy policy and contractual confidentiality obligations
8. Data transfer: personal information may be transferred to affiliates for processing under Google's instructions

- ii. Gemini apps work with connected apps, including google apps and third party services. Gemini saves and uses info from connected apps according to this notice, including to provide and improve gemini apps. Connected google apps save and use data, per the policies and the google privacy poloicy, including to provide and improve their services. If you use gemini apps to interact with third party services, they process your data according to their own privacy policies.

h. Cookies

i. Functionality:

1. Allow user to access features that are fundamental to a service. These cookies are used in order to deliver and maintain google services. These include: remembering choices and preferences, like your choice of language, storing information relating to your sessions, such as the content of a shopping cart; enabling features or performing tasks requested by the user, and product optimizations that help maintain and improve that service.
2. Others can be used to enhance the user experience during a specific session; or to improve the performance of Google services
3. Google uses the SOCS cookie, which lasts for 13 months, to store a user's state regarding

	their cookies choices. ii. Security 1. Uses cookies and similar technologies for security purposes to protect you as you interact with a service by authenticating users, protecting against spam, fraud and abuse, and tracking outages. 2. Some are used to authenticate users help ensure that only the actual owner of an account can access that account. 3. Some cookies and similar technologies are used to detect spam, fraud, and abuse. iii. Analytics 1. Google uses cookies and similar technologies for analytical purposes to understand how you interact with a particular service. These cookies and similar tech’s help collect data that allows Google to measure audience engagement and site statistics. This helps them to understand how services are used, and to enhance their content, quality and features, while also allowing us to develop and improve new services. iv. Advertising 1. Uses cookies and similar technology for advertising purposes, including serving and rendering ads, and personalizing ads. These cookies are also used for limiting the number of times an ad is shown to a user, muting ads you have chosen to stop setting, and delivering and measures the effectiveness of ads. 2. The NID cookie can be used to show ads in google services for signed out users. Some google websites that do not have ads, such as google cloud, do not use the NID cookie for this purpose. The IDE and id cookies are used to show google ads on non-google sites a. The IDE and id cookies last for 24 months in the United States 3. Buisness can advertise in googles servicxs as well as non google sites. v. Personalization 1. Features include more relevant results and recommendations. Another cookie UULE sends precise location information from your browser to Google’s servers so that Google can show you results that are relevant to your location. The use of this cookie depends on your browser settings and whether you have chosen to have location turned on for the users
--	--

	browser. The cookie lasts up to 6 hours. i. Security practices i. Encryption in Transit: Data encrypted while in transit across google services ii. Secure features: safe browsing, security checkup, 2 step verification offered to users iii. Access controls: personal information restricted to employees, contractors, and agents with a legitimate need iv. Confidentiality obligations: All staff with data access subject to strict contractual confidentiality; violations may result int termination v. Threat detection, physical security, investment, expert staff, incidence response j. Compliance expectations (HIPAA, GDPR, SOC 2) i. No mention
META: https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 1. Location on Website: 2. Structure and Sections Included: 3. Content and disclosures expected: a. HIPAA b. Handling of PHI/health data c. Customer data usage d. AI model training policies e. Prompts/outputs f. Data retention g. Subprocessors h. Cookies i. Security practices j. Compliance expectations (HIPAA, GDPR, SOC 2) 4. Biometric Privacy Act?	11. Location on Website: a. Found it on Facebook. These larger companies have the specific page and link designated to the privacy center. 12. Structure and Sections Included: a. Sections on the left with tabs linking to that section. Descriptions on the right. There are links to the other sections throughout the description. i. Sections are as follows: ii. Search iii. Privacy topics iv. More privacy resources v. Privacy policy vi. What is the privacy policy and what does it cover? vii. What information do Company collect? viii. How do Company use your information? ix. How is your information shared on Meta products or with integrated partners? x. How do Company share information with third parties? xi. How do the meta companies work together? xii. How can you manage or delete your information and exercise your rights? xiii. How long do Company keep your information? xiv. How do Company transfer information? xv. How do Company respond to legal requests, comply with applicable law and prevent harm? xvi. How will you know the policy has changed? xvii. Privacy notice for United States residents - xviii. How to contact meta with questions xix. Why and how Company process your information xx. Other policies and articles 1. Cookies policy 2. Information for people who don't use Meta

	products 3. How Meta uses information for generative AI models and features 4. Data privacy framework disclosure xxi. Settings 13. Content and disclosures expected: a. HIPAA i. No mention of HIPAA b. Handling of PHI/health data i. Health data is included in typical information that the user provides and can be collected by Meta. 1. Processing information subject to special protections under applicable laws that you provide so Company can share it with those you choose, to provide, personalize and improve our products and to undertake analytics. We'll collect, store, publish and apply automated, or sometimes manual, processing for these purposes. c. Customer data usage i. Information that they collect: 1. Info the user gives them when they sign up for their products and create a profile, like email, phone number, or age 2. What the user does on the products. What they click on or like, posts and photos, chats with AI at Meta, messages you send. On some products you can use end-to-end encrypted messages 3. Who friends or followers are and what they don on the products 4. Information from the phone, computer, or tablet you use products on. Like what kind it is and what version of the app the user is using 5. Information from partners about things you do both on and off our products. This could include other websites the user visits, apps the user uses or online games they play. 6. They collect some information about the user even if you don't have an account. d. AI model training policies i. Completely separate section for AI use. 1. What is generative AI? a. Explains what it is 2. Where does Meta get training information? a. They use information that is publicly available online and licensed information. They use information shared on Meta products. They do not use the content of private messages
--	---

	with friends and family to train AI unless someone in the chat chooses to share those messages with their AIs. Some AI features use private processing technology b. Data collected from public information may have personal information. They do not link this data specifically to any Meta account. c. Even if someone doesn't use their products or have an account, they can still process information about the user to develop and improve Ai and Meta. 3. Privacy and generative AI a. Have a "robust" internal privacy review process that helps ensure they are using data at Meta responsibly for their products. They work to identify potential privacy risks that involve the collecting, use, or sharing of personal information and develop ways to reduce those risks to people's privacy. b. 5 Foundational values: Privacy and security, fairness and inclusion, robustness and safety, transparency and control, governance and accountability c. Cross-disciplinary team whose mission is to help ensure that AI and meta benefits people and society. d. Briefly explains why they collect this data. Because it requires a lot of information to train the data. e. Prompts/outputs i. "Company use the information people share when interacting with our generative AI features... to improve our products and for other purposes." ii. This includes the prompts and questions that are typed, the content uploaded, generated outputs and responses and other interaction data with Meta AI features. f. Data retention i. They keep information as long as they need it to provide products, comply with legal obligations or protect the companies or other's interests. They decide how long they keep it on a case-by-case basis. ii. They consider: 1. "If Company need it to operate or provide our Products. For example, Company need to keep some of your information to maintain your account. .
--	---

	2. The feature Company use it for, and how that feature works. For example, messages sent using Messenger’s vanish mode are retained for less time than regular messages. . 3. How long Company need to retain the information to comply with certain legal obligations. . 4. If Company need it for other legitimate purposes, such as to prevent harm; investigate possible violations of our terms or policies; promote safety, security and integrity; or protect ourselves, including our rights, property or products.” g. Subprocessors i. Partners: 1. Advertisers and audience network publishers a. Ads and commercial content people engaged with, if any b. When people engaged with ads and commercial content c. Where that ad or commercial content was shown 2. Partners who use analytical services a. How many people interacted with their partners’ content, products or services b. The general demographics and interests of the people who interacted with it c. How people use their partners’ products and services to connect to Meta products and the performance of their connection and networks 3. Partners who offer goods or services on our products and commerce services platforms a. Information to complete the users transaction, like order, payment, contact and shipping information b. Information to help ensure the security of the transaction, like information about your device or connection c. Any information required by applicable regulation d. Other information you choose to share with them 4. Integrated partners ii. Vendors: 1. Measurement vendors a. Share information with their measurement vendors who aggregate
--	---

	or compile it to provide their reports. 2. Marketing vendors a. Serving our advertisements across the internet, including on mobile, desktop and connected television devices b. Tracking and categorizing your online and mobile app activity c. Providing us information about your interests and community and advertising interactions. iii. Service providers: 1. Service Providers: 2. Share: a. Investigating suspicious activity b. Detecting and stopping threats to their personnel and property c. Facilitating payments d. Providing customer support e. Improving the functionality of their products f. Providing technical infrastructure services g. Analyzing how their products are used h. Conducting research and surveys i. Marketing and promoting their products iv. Third parties: 1. External researchers a. Promote their business or mission b. Social good c. Technological advancement d. Safety and security on their products e. Public interest f. Health and well-being 2. AI Integrations v. Other third parties: h. Cookies i. Cookies provide, protect, and improve the Meta products, such as personalising content, tailoring or measuring ads, and providing a safer experience. ii. Authentication: “Company use cookies to verify your account and determine when you’re logged in so that Company can make it easier for you to access the Meta Products and show you the appropriate experience and features.” iii. Security, site and product integrity: “Company use cookies to help us keep your account, data and the Meta products safe and secure.” “Company also use cookies to combat activity that violates our policies or otherwise degrades our ability to provide the Meta
--	---

	products.” iv. Advertising, recommendations, insights and measurement: “Company use cookies to help us show ads and to make recommendations for businesses and other organisations to people who may be interested in the products, services or causes they promote.” 1. Company also use cookies to help measure the performance of ad campaigns for businesses that use the Meta Products. 2. Cookies help us serve and measure ads across different browsers and devices used by the same person. 3. Cookies also allow us to provide insights about the people who use the Meta Products, as well as the people who interact with the ads, websites and apps of our advertisers and the businesses that use the Meta Products. v. Site features and services: 1. “Company use cookies to enable the functionality that helps us provide the Meta products.” 2. “Company also use cookies to help provide you with the content relevant to your locale.” vi. Third-party websites and apps: 1. “Our business partners may also choose to share information with Meta from cookies set in their own websites' domains, whether or not you have a Facebook or Instagram account or are logged in. Specifically, cookies named <code>_fb</code> or <code>_fbp</code> may be set on the domain of the business partner whose site you're visiting. Unlike cookies that are set on Meta's own domains, these cookies aren't accessible by Meta when you're on a site other than the one on which they were set, including when you are on one of our domains. They serve the same purposes as cookies set in Meta's own domain, which are to personalise content (including ads), measure ads, produce analytics and provide a safer experience, as set out in this Cookies Policy.” i. Security practices i. Two-factor authentication, account protection tools, hacked account recovery, security settings review ii. Detecting suspicious activity, preventing spam and abuse, automated and human review for safety, Protecting platform integrity iii. Protecting messages, managing shared settings, harassment and abuse protections, platform safety controls
--	---

	iv. External data misuse team made up of data scientists, analysis, and engineers focused on their efforts to detect, block and deter scraping. j. Compliance expectations (HIPAA, GDPR, SOC 2) i. No mention 14. Biometric Privacy Act? a. No mention but they do comply with the Biometric Privacy act. It cannot be found on the website however.
Hippocratic AI - https://hippocraticai.com/privacy-policy/ 15. <u>Location on Website:</u> 16. <u>Structure and Sections Included:</u> 17. <u>Content and disclosures expected:</u> a. <u>HIPAA</u> b. <u>Handling of PHI/health data</u> c. <u>Customer data usage</u> d. <u>AI model training policies</u> e. <u>Prompts/outputs</u> f. <u>Data retention</u> g. <u>Subprocessors</u> h. <u>Cookies</u> i. <u>Security practices</u> j. <u>Compliance expectations (HIPAA, GDPR, SOC 2)</u> 18. <u>Biometric Privacy Act?</u> Given the smaller nature of the website and language, I have provided direct verbiage from the policy.	19. Location on Website: a. Noticing a pattern... at the bottom of the website page again along with numerous other links to different places on the website. 20. Structure and Sections Included: a. This one is much much smaller than the previous ones. Which is not surprising, because we're going from Apple and Google to a company I had not heard of before this research. No index provided. So here's what's included: i. What personal information do Company collect? ii. For what purposes do Company use your personal information? iii. What about cookies and other identifiers? iv. Do Company share your personal information? v. How secure is the information you collect about me? vi. What choices do I have? vii. Are Children allowed to use our services? viii. Conditions of use, notice, and revisions ix. Examples of information collected x. Additional State - Specific Privacy Disclosures 21. Content and disclosures expected: a. HIPAA i. No mention except at the bottom of the page it says, "Excerpt from a real patient call, de-identified in compliance with HIPAA." b. Handling of PHI/health data i. No mention of handling specific health data c. Customer data usage i. They collect: Information the user gives them. Such as name, email, phone number, Automatic information: collect and store information about the user's use on the website. They use cookies and other unique identifiers, and they obtain certain types of information when the web browser or device accesses the site. ii. They use information as such: 1. Communicate with you. Company use your personal information to communicate with you in relation to our services via different channels (e.g., by phone, email, chat). 2. Comply with legal obligations. In certain cases, Company collect and use your personal

	information to comply with laws. d. AI model training policies i. No mention e. Prompts/outputs i. No mention f. Data retention i. Communicate with you. Company use your personal information to communicate with you in relation to our services via different channels (e.g., by phone, email, chat). ii. Comply with legal obligations. In certain cases, Company collect and use your personal information to comply with laws. g. Subprocessors i. Third-Party Service Providers: Company employ other companies and individuals to perform functions on our behalf. Examples include sending postal mail and email, analyzing data, providing marketing assistance, processing payments, and providing customer service. These third-party service providers have access to personal information needed to perform their functions, but may not use it for other purposes. ii. Business Transfers: As Company continue to develop our business, Company might sell or buy other businesses or services. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). In the event that Company or substantially all of our assets are acquired, customer information will of course be one of the transferred assets. h. Cookies i. Automatic information: collect and store information about the user’s use on the website. They use cookies and other unique identifiers, and they obtain certain types of information when the web browser or device accesses the site. ii. Conducting research and diagnostics to improve our content, products, and services. iii. Preventing fraudulent activity. iv. Improving security. v. The user can manage the browser cookies through browser settings. vi. They use cookies, pixels, and other technologies to recognize the browser or divide, learn more about the users interests, and provide the user with essential features and services and for additional purposes i. Security practices i. “Company design our systems with your security and
--	--

	privacy in mind. ii. Company work to protect the security of your personal information during transmission by using encryption protocols and software. Company maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of customer personal information. Our security procedures mean that Company may ask to verify your identity before Company disclose personal information to you.” j. Compliance expectations (HIPAA, GDPR, SOC 2) i. No mention 22. Biometric Privacy Act? a. No mention, but it does refer to specific state laws otherwise
Suki: https://www.suki.ai/privacy-policy/ 23. Location on Website: 24. Structure and Sections Included: 25. Content and disclosures expected: a. HIPAA b. Handling of PHI/health data c. Customer data usage d. AI model training policies e. Prompts/outputs f. Data retention g. Subprocessors h. Cookies i. Security practices j. Compliance expectations (HIPAA, GDPR, SOC 2) 26. Biometric Privacy Act? This website has a lot of what you requested, which I assume is what Company are looking for. This might be a good one to parallel	27. Location on Website: a. Same as others, at the bottom of the website next to the other links. 28. Structure and Sections Included: a. About the policy b. What the policy covers c. Information they collect d. Practice users e. Prospective customers f. Personal data that is provided through the services g. Non-identifiable data: h. Cookies i. Log files j. Aggregated personal data k. Our use of your personal data and other information l. Online tracking m. Our disclosure of your personal data and other information n. Processing of medical practice data o. Service providers and business partners p. Business transfers q. Related companies r. Agents, consultants and related third parties s. Legal requirements t. Your choices u. Retention v. Exclusions w. Children x. Links to other web bites y. Security z. Access to information; contacting company 29. Content and disclosures expected: a. HIPAA i. “Some of the Personal Data received by the Company in connection with the Services may be provided by health care providers that are subject to laws and regulations, such as rules issued under the Health

	Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), that govern providers’ use and disclosure of certain individually identifiable health-related Personal Data (“Protected Health Information”).” ii. “When Company act as a Business Associate, Company may be subject to certain laws and regulations, including certain HIPAA rules that govern our use and disclosure of Protected Health Information and that may be more restrictive than otherwise provided in this Privacy Policy.” b. Handling of PHI/health data i. “Some of the Personal Data received by the Company in connection with the Services may be provided by health care providers that are subject to laws and regulations, such as rules issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), that govern providers’ use and disclosure of certain individually identifiable health-related Personal Data (“Protected Health Information”). When Company receive Protected Health Information, Company may do so as a “Business Associate” of our health care provider customers under an agreement that, among other things, prohibits us from using or disclosing the Protected Health Information in ways that are not permissible by the health care provider itself, and requires us to implement certain measures to safeguard the confidentiality, integrity, and availability of the Protected Health Information. When Company act as a Business Associate, Company may be subject to certain laws and regulations, including certain HIPAA rules that govern our use and disclosure of Protected Health Information and that may be more restrictive than otherwise provided in this Privacy Policy.” ii. “Some of the Personal Data received by the Company in connection with the Services may be provided by health care providers that are subject to laws and regulations, such as rules issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), that govern providers’ use and disclosure of certain individually identifiable health-related Personal Data (“Protected Health Information”). When Company receive Protected Health Information, Company may do so as a “Business Associate” of our health care provider customers under an agreement that, among
--	---

other things, prohibits us from using or disclosing the Protected Health Information in ways that are not permissible by the health care provider itself, and requires us to implement certain measures to safeguard the confidentiality, integrity, and availability of the Protected Health Information. When Company act as a Business Associate, Company may be subject to certain laws and regulations, including certain HIPAA rules that govern our use and disclosure of Protected Health Information and that may be more restrictive than otherwise provided in this Privacy Policy.”

c. Customer data usage

- i. Authenticate access to the account and provide access to the services
- ii. Provide, operate, maintain and improve the services
- iii. Send technical notes, updates, security alerts and support and administrative messages
- iv. Provide and deliver the services and features you request, process and complete transactions, and send you related information, including confirmations and invoices
- v. Respond to comments, questions, and requests and provide customer service and support
- vi. Communicate with the user about services, features, surveys, newsletters, offers, promotions and events, and provide other news or information about the company and their selected partners
- vii. Investigate and prevent fraudulent transactions, unauthorized access to the services, and other illegal activities
- viii. Personalize and improve the services, and provide content, features, and/or advertisements that match the interests and preferences or otherwise customize the experience on their services.
- ix. Monitor and analyze trends, usage, and activities in connection with the
 1. Services and for marketing for advertising purposes; and for other purposes about which the company will notify you and seek the users consent, or which may be reflected in the services agreement with the user.
 2. The company and its affiliates may use this information to contact the user in the future to tell them about services they believe will be of interest to the user. If they do so, each marketing communication they send will contain instructions permitting the user to opt-out of receiving future marketing communications.

d. AI model training policies

	i. No mention e. Prompts/outputs i. No mention f. Data retention i. “Company will keep Personal Data for as long as it remains necessary for the identified purpose or as required by law, which may extend beyond the termination of our relationship with you. Company may retain certain data as necessary to prevent fraud or future abuse, or for legitimate business purposes, such as analysis of aggregated, non-personally-identifiable data, account recovery, or if required by law. Unless otherwise set forth in the applicable Terms of Use or a separate agreement with you governing the applicable Services, if you cease using such Service, Company may retain or destroy, at our discretion, all Personal Data and non-personally identifiable information Company collects through your use of such Service. All retained Personal Data will remain subject to the terms of this Privacy Policy (or an applicable Business Associate Agreement).” g. Subprocessors i. “The Company uses third-party service providers in order to collect, store and process Personal Data about Prospects. The Company use these third-party service providers to identify Prospects and locate contact information to contact Prospects about our Services.” ii. “By voluntarily providing us with Personal Data, you are consenting to our use of it in accordance with this Privacy Policy. If you provide Personal Data to the Services, you acknowledge and agree that such Personal Data may be transferred from your current location to the offices and servers of the Company and the authorized third parties referred to herein located in the United States.” iii. The Company may use third-party tracking services that use log files, cookies, and possibly other techniques to track non-Personal Data about visitors to the Services in the aggregate. These services capture usage and volume statistics as well as geographical location data to compile usage reports and maps for optimization and troubleshooting purposes. iv. The Company may also disclose aggregated user statistics in order to describe our services to current and prospective business partners, and to other third parties for other lawful purposes v. Certain circumstances in which they share personal data with third parties without notice to you 1. Processing of medical practice data 2. Service providers and business partners
--	---

	a. Company may from time to time employ third parties to perform tasks on our behalf and Company may need to share Personal Data with them to provide certain services. Unless the Company tells you differently, such third parties do not have any right to use the Personal Data the Company shares with them beyond what is necessary for them to provide the tasks and services on our behalf. Company currently engage third party companies and individuals employed by us to facilitate our Services, including the provision of maintenance services, database management, Web analytics and general improvement of the Services, and businesses who engage our Services 3. Business transfers 4. Related companies 5. Agents, consultants vi. This Privacy Policy applies only to the Services and does not apply to the practices of companies that we do not own or control. The Services may contain links to other web sites not operated or controlled by the Company (the “Third Party Sites”). The policies and procedures we described here do not apply to the Third Party Sites. The links from the Services do not imply that the Company endorses or has reviewed the Third Party Sites. h. Cookies i. They collect information about the device and browser, network connection, IP address, and information about the cookies installed on the device. Logged to help diagnose technical problems for analytics and for quality control purposes. ii. Cookies Section on Website:“In operating the Services, we may use a technology called “cookies.” A cookie is a piece of information that the computer that hosts our Services gives to your browser when you access the Services. Our cookies help provide additional functionality to the Services and help us analyze Services usage more accurately. For instance, our Site may set a cookie on your browser that allows you to access the Services without needing to remember and then enter a password more than once during a visit to the Site. In all cases in which we use cookies, we will not collect Personal Data except with your permission.
--	--

On most web browsers, you will find a “help” section on the toolbar. Please refer to this section for information on how to receive notification when you are receiving a new cookie and how to turn cookies off. We recommend that you leave cookies turned on because they allow you to take advantage of some of the Service features.”

i. Security practices:

- i. The company takes steps to protect PHI provided via the services from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. “However, no internet or email transmission is ever fully secure or error free.” They recommend taking special care in deciding what information the users send through email. They encourage users not to email PHI to the company unless prior arrangements have been made with the company to ensure the email is encrypted.

j. Compliance expectations (HIPAA, GDPR, SOC 2)

i. HIPAA and HITECH

1. As previously stated from website: Some of the Personal Data received by the Company in connection with the Services may be provided by health care providers that are subject to laws and regulations, such as rules issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), that govern providers’ use and disclosure of certain individually identifiable health-related Personal Data (“Protected Health Information”). When we receive Protected Health Information, we may do so as a “Business Associate” of our health care provider customers under an agreement that, among other things, prohibits us from using or disclosing the Protected Health Information in ways that are not permissible by the health care provider itself, and requires us to implement certain measures to safeguard the confidentiality, integrity, and availability of the Protected Health Information. When we act as a Business Associate, we may be subject to certain laws and regulations, including certain HIPAA rules that govern our use and disclosure of Protected Health Information and that may be more restrictive than otherwise provided in this Privacy Policy.

30. Biometric Privacy Act?

	a. No mention
--	---------------