SutureHealth Privacy Policy

This privacy notice for Suture Health, Inc (doing business as SutureHealth) ("SutureHealth," "we," "us," or "our") describes how and why we might collect, store, use, and/or share ("process") your information when you use our services ("Services"), such as when you:

- Visit our website at www.SutureHealth.com or www.SutureSign.com, utilize SutureHealth applications and/or services, or visit any website or application of ours that links to this privacy notice
- Engage with us in other related ways, including any sales, marketing, or events.

As part of the day-to-day business operations of Suture Health, Inc. ("SutureHealth"), including the operation of the website www.SutureSign.com and/or www.SutureHealth.com (the "Website"), we receive and maintain certain health-related and personal information regarding Individuals. Information received from the website depends in part on what you do when you visit and interact with the website. SutureHealth respects the privacy of every Individual who visits our website. Therefore, we would like to define the types of information we receive and describe how it is maintained in this privacy policy ("Privacy Policy", "Privacy Notice"). This policy refers only to the information collected and maintained from the Website.

For the purpose of this Privacy Policy, the following definitions describe the types of users who may access and use the information, products, and services offered by SutureHealth:

An "Individual" is any person visiting the public sections of the Website.

A "Provider" is a physician, facility, group practice and/or their authorized representatives that may access SutureHealth's products or services available on the Website.

A "Registered User" (User) is any Provider authorized to enter the secure sections of www.SutureHealth.com.

USING THIS WEBSITE CONFIRMS YOUR CONSENT AND AGREEMENT TO OUR PRIVACY POLICY, INCLUDING COLLECTION, USE AND DISCLOSURE OF INFORMATION BY SUTUREHEALTH AS DESCRIBED HEREIN. YOUR USAGE ALSO SIGNIFIES YOUR COMPLIANCE WITH OUR APPLICABLE TERMS OF SERVICE.

SutureHealth, through its products and services, provides private and secure access to health-related and personal information. In addition, SutureHealth provides private and secure access to Provider information.

Questions or concerns? Reading this privacy notice will help you understand your privacy rights and choices. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at support@SutureHealth.com.

Summary of Key Points

This summary provides key points from our privacy notice, but you can find more details about any of these topics by reviewing the relevant sections of this privacy notice.

What personal information do we process? When you visit, use, or navigate our Services, we may process personal information depending on how you interact with SutureHealth and the Services, the choices you make, and the products and features that you use.

Do we process any sensitive personal information? We may process personal information when necessary with your consent or as otherwise permitted by applicable law.

Do we receive any information from third parties? We may receive information from public databases, marketing partners, social media platforms, and other outside sources.

How do we process your information? We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with the law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so.

In what situations and with which types of parties do we share personal information? We may share information in specific situations and with specific categories of third parties.

How do we keep your information safe? We have organizational and technical processes and procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, we cannot promise or guarantee that hackers,

cybercriminals, or other unauthorized parties will not be able to defeat our security and improperly collect, access, steal, or modify your information.

What are your rights? Depending on where you are located geographically, the applicable privacy law may mean you have certain rights regarding your personal information.

How do you exercise your rights? The easiest way to exercise your rights is by contacting us. We will consider and act upon any request in accordance with applicable data protection laws.

Privacy Notice

What information do we collect?

Registered Users
Providers must register to access the secure areas of SutureHealth. Privacy and security are top priorities at SutureHealth. For that reason, SutureHealth has implemented a process that helps protect Protected Health Information ("PHI"), as that term is defined by the Health Insurance Portability & Accountability Act of 1996, as amended ("HIPAA"), contained on our site from inappropriate access. Before a Registered User can access medical information available on our site, the user must first be authenticated as being a provider or a representative of a provider as defined above.

Personal information you disclose to us – we collect personal information that you voluntarily provide to us when you register on the Services, express an interest in obtaining information about us or our products and Services, when you participate in activities on the Services, or otherwise when you contact us.

Providers: Do not send e-mails containing personal information to SutureHealth. SutureHealth cannot secure personal information sent by e-mail because such information can be accessed by other Internet users. If you send SutureHealth a question by e-mail, SutureHealth' use or disclosure of that information will be limited to the minimum necessary for responding to your question.

Personal information provided by you – the personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the products and features that you use. The personal information we collect may include the following:

- Names
- Phone numbers
- Email addresses
- Mailing addresses
- Job titles
- Usernames
- Passwords
- Contact preferences
- Contact or authentication data
- Billing addresses

SutureHealth collects personal data during the registration process, including but not limited to names and email addresses. SutureHealth will not sell nor distribute personally identifiable or contact information. SutureHealth reserves the right to provide a service to third parties who may wish to contact you through our network provided that you have given consent for such services to be rendered. As part of the service provided by SutureHealth, you understand that SutureHealth will contact you on the behalf of other healthcare providers.

Sensitive information – when necessary, with your consent or as otherwise permitted by applicable law, we process the following categories of personal information which may be associated either directly with you or with the type of data you process through our Services:

- Health data
- Biometric data
- Genetic data
- Financial data
- Data about a person's sex life or sexual orientation
- Information revealing race or ethnic origin
- Social security numbers or other government identifiers

All personal information that you provide to us must be true, complete, and accurate, and you must notify us of any changes to such personal information. Note, protected health information (PHI) related to patients is covered under our Terms of Service and User Agreement, Section 3, HIPAA Business Associate Agreement.

Information automatically collected – some information, such as your Internet Protocol (IP) address and/or browser and device characteristics, is collected automatically when you visit our Services. We automatically collect certain information when you visit, use, or navigate the Services. This information does not reveal your identity (like your name or contact information), but may include device and usage information, such as your IP address, browser, and device characteristics, operating system, language preferences, referring URLs, device name, country, location, information about how and when you use our Services, and other technical information. This information is primarily needed to maintain the security and operation of our Services, and for our internal analytics and reporting purposes. Like many businesses, we also collect information through cookies and similar technologies.

The information we collect includes:

- Log and usage data. Log and usage data is service-related, diagnostic, usage, and performance information our servers automatically collect when you access or use our Services and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type and settings and information about your activity in the Services (such as the date/time stamps associated with your usage, pages and files viewed, searches, and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called “crash dumps”), and hardware settings).
- Device data. We collect device data such as information about your computer, phone, tablet, or other device you use to access the Services. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model, internet service provider and/or mobile carrier, operating system, and system configuration information.
- Location data. We collect location data such as information about your device’s location, which can be either precise or imprecise. How much information we

collect depends on the type and setting of the device you use to access the Services. For example, we may use GPS and other technologies to collect geolocation data that tells us your current location (based on your IP address). You can opt out of allowing us to collect this information by either refusing access to the information or by disabling your location setting on your device. However, if you choose to opt out, you may not be able to use certain aspects of the Services.

SutureHealth continually strives to enhance the features and services that are offered on our website. In an effort to determine the effectiveness and functionality of our website, we monitor aggregated data regarding the use of our website. For instance, we may track the number of visits to a certain page; direct links from other websites; and frequency of usage for independent services. Although we reserve the right to share this information as indicated above, this statistical data does not contain any personal information that could disclose the user's identity.

Information collected from other sources – We may collect limited data from public databases, marketing partners, and other outside sources.

In order to enhance our ability to provide relevant marketing, offers, and services to you and update our records, we may obtain information about you from other sources, such as public databases, joint marketing partners, affiliate programs, data providers, and other third parties. This information includes mailing addresses, job titles, email addresses, phone numbers, fax numbers, intent data (or user behavior data), Internet Protocol (IP) addresses, social media profiles, social media URLs, and custom profiles, for purposes of targeted advertising and event promotion.

SutureHealth obtains personal information regarding physician providers from a third-party source including but not limited to state medical license numbers. This data is protected within a secure firewall environment, access to which is limited to only SutureHealth and its representatives.

SutureHealth

How do we process your information?

We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with the law. We may also process your information for other purposes with your consent.

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- To facilitate account creation and authentication and otherwise manage user accounts. We may process your information so you can create and log in to your account, as well as keep your account in working order.
- To deliver and facilitate the delivery of services to the user. We may process your information to provide you with the requested service(s).
- To respond to user inquiries/offer support to users. We may process your information to respond to your inquiries and solve any potential issues you might have with the requested service(s).
- To send administrative information to you. We may process your information to send you details about our products and services, changes to our terms and policies, and other similar information.
- To fulfill and manage your orders. We may process your information to fulfill and manage your orders, payments, returns, and exchanges made through the services.
- To enable user-to-user communications. We may process your information if you choose to use any of our offerings that allow for communication with another user.
- To request feedback. We may process your information when necessary to request feedback and to contact you about your use of our Services.
- To send you marketing and promotional communications. We may process the personal information you send to us for our marketing purposes, if this in is accordance with your marketing preferences. You can opt out of our marketing emails at any time.
- To deliver targeted advertising to you. We may process your information to develop and display personalized content and advertising tailored to your interest, location, and more.
- To protect our Services. We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.

- To identify usage trends. We may process information about how you use our Services to better understand how they are being used so we can improve them.
- To determine the effectiveness of our marketing and promotional campaigns. We may process your information to better understand how to provide marketing and promotional campaigns that are most relevant to you.
- To save or protect an individual's vital interest. We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.

What legal bases do we rely on to process your information?

We only process your personal information when we believe it is necessary and we have a valid legal reason (i.e., legal basis) to do so under applicable law, like with your consent, to comply with laws, to provide you with services to enter into or fulfill our contractual obligations, to protect your rights, or to fulfill our legitimate business interests.

<u>If you are located in the EU or UK, this section applies to you:</u>

The General Data Protection Regulation (GDPR) and UK GDPR require us to explain the valid legal bases we rely on in order to process your personal information. As such, we may rely on the following legal bases to protect your personal information:

- Consent. We may process your information if you have given us permission (i.e., consent) to use your personal information with a specific purpose. You can withdraw your consent at any time.
- Performance of a Contract. We may process your personal information when we believe it is necessary to fulfill our contractual obligations to you, including providing our Services or at your request prior to entering into a contract with you.
- Legitimate interests. We may process your information when we believe it is reasonably necessary to achieve our legitimate business interest and those interests do not outweigh your interests and fundamental rights and freedoms. For example, we may process your personal information for some of the purposes described in order to:

    - Send users information about special offers and discounts on our products and services
    - Develop and display personalized and relevant advertising content for our users
    - Analyze how our services are used so we can improve them to engage and retain users
    - Support our marketing activities
    - Diagnose problems and/or prevent fraudulent activities
    - Understand how our users use our products and services so we can improve user experience
- Legal obligations. We may process your information where we believe it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.
- Vital interests. We may process your information where we believe it is necessary to protect your vital interests or the vital interests of a third party, such as situations involving potential threats to the safety of any person.

<u>If you are located in Canada, this section applies to you:</u>

We may process your information if you have given us specific permission (i.e., express consent) to use your personal information for a specific purpose, or in situations where your permission can be inferred (i.e., implied consent). You can withdraw your consent at any time.

In some exceptional cases, we may be legally permitted under applicable law to process your information without your consent, including, for example:

- If collection is clearly in the interests of an individual and consent cannot be obtained in a timely way.
- For investigations and fraud detection and prevention.
- For business transactions provided certain conditions are met.
- If it is contained in a witness statement and the collection is necessary to assess, process, or settle and insurance claim.
- If it is reasonable to expect collection and use with consent would compromise the availability or the accuracy of the information and the collection is reasonable

for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.
- If disclosure is required to comply with a subpoena, warrant, court order, or rules of the court relating to the production of records.
- If it was produced by an individual in the course of their employment, business, or profession and the collection is consistent with the purposes for which the information was produced.
- If the information is publicly available and is specified by the regulations.

When and with whom do we share your personal information?

We may share information in specific situations described in this section and/or with the following categories of third parties.

Vendors, consultants, and other third-party service providers – we may share your data with third-party vendors, service providers, contractors, or agents (“third parties”) who perform services for us or on our behalf and require access to such information to do that work. We have contracts in place with third parties, which are designed to help safeguard your personal information. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will also not share your personal information with any organization apart from us. They also commit to protect the data they hold on our behalf and to retain it for the period we instruct. The categories of third parties we may share personal information with are as follows:

- Cloud commuting services
- Communication and collaboration tools
- Data analytics services
- Data storage service providers
- Finance and accounting tools
- Other fulfillment service providers
- Payment processors
- Performance monitoring tools
- Product engineering and design tools
- Retargeting platforms
- Sales and marketing tools
- Testing tools
- User account registration and authentication services

- Website hosting service providers

We also may need to share your personal information in the following situations:

- Business transfers. We may share or transfer your information in connection with, or during negotiations of, any merger, sales of company assets, financing, or acquisition of all or a portion of our business to another company.
- When we use Google Maps Platform APIs. We may share your information with certain Google Maps Platform APIs (g.g., Google Maps API, Places API). To find out more about Google's Privacy Policy, please refer to this link. We obtain and store your device ("cache") and your location. You may revoke your consent at any time by contacting us at the contact details provided at the end of this document.
- Affiliates. We may share your information with our affiliates, in which case we will require those affiliates to honor this privacy notice. Affiliates include our parent company and any subsidiaries, joint venture partners, or other companies that we control or that are under common control with us.
- Business partners. We may share your information with our business partners to offer you certain products, services, or promotions.
- Other users. When you share personal information (for example, by posting comments, contributions, or other content to the Services) or otherwise interact with public areas of the Services, such personal information may be viewed by all users and may be publically made available outside the Services in perpetuity. Similarly, other users will be able to view descriptions of your activity, communicate with you within our services, and view your profiles.

Disclosure of Non-Public Personal Information: including Personal Health Information (PHI):
We restrict access to nonpublic personal information, including PHI. Information may be shared with entities (i.e. providers and vendors) that assist SutureHealth in providing services to our Registered Users. Information is provided to nonaffiliated third parties as required or allowed by federal and state law. SutureHealth maintains physical, electronic, and procedural safeguards that comply with federal regulations to guard nonpublic personal information, including but not limited to high-level encryption.

Disclosure to Providers: SutureHealth discloses nonpublic personal information including PHI to Providers through their access to the website. This information is disclosed to Providers for treatment, payment or health care operations (TPO) as allowed under HIPAA. To ensure that Providers are only accessing patient information for TPO, SutureHealth has implemented the following safeguards:

- The accompanying Terms of Service outlines acceptable uses of patient information.
- SutureHealth maintains audit trails of user activity.
- SutureHealth requires both a user name and password for access to PHI.
- Providers' default access to PHI is limited to those records with which they or their associates (i.e. providers who are in the same practice or facility) or representatives need to have access for treatment, payment, or health care operations. For some facilities, this is determined by their need to create or modify patient records. Notwithstanding, however, these facilities will only have access to the medical information that they have submitted into the system; thus, alleviating those access concerns which often times arise in a competitive market environment.

Disclosure to Third Parties: SutureHealth operations, maintenance employees and contractors may have limited access to your nonpublic personal information, including PHI, while providing products or services to SutureHealth. These contractors include vendors and suppliers that provide us with technology, services, and/or content for the operation and maintenance of our Web site. Access to your nonpublic personal information, including PHI, by these contractors, is limited to the information reasonably necessary for the contractor to perform its limited function for SutureHealth. We also contractually require that our operations and maintenance contractors 1) protect the privacy of your nonpublic personal information, including PHI, consistent with this Privacy Policy, and 2) not use or disclose your nonpublic personal information, including PHI, for any purpose other than providing us with products and services as required by law.

Disclosure of Aggregate Information: SutureHealth may disclose aggregate information to third parties. This information may contain medical information; however, it is not associated to a specific individual. Depending on the circumstances, SutureHealth may or may not charge third parties for this Aggregate Information. SutureHealth requires

parties with whom aggregate information is shared to agree that they will not attempt to make this information personally identifiable, such as by combining it with other databases.

Do we use cookies and other tracking technologies?

We may use cookies and other tracking technologies to collect and store your information. We may use cookies and similar tracking technologies (like web beacons and pixels) to access or store information. Specific information about how we use such technologies and how you can refuse certain cookies is set out in our Cookie Notice.

A “cookie” is a mechanism that permits a web server to send small pieces of information or text through your browser to be stored on your hard drive. This information or text allows the server to identify frequent visitors of individual websites. SutureHealth may place a cookie on your computer that will allow us to identify users so that we may enhance their experience on our website. Our cookies are not used to track your activity on any site other than SutureHealth.com nor will they be utilized to send unsolicited e-mails or provide us with the User's personally identifiable information.

How long do we keep your information?

We keep your information as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law. We will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice unless a longer retention period is required or permitted by law (such as tax, accounting, or other legal requirements). No purpose in this notice will require us to keep your personal information for longer than seventy-two (72) months past the start of the idle period of the user’s account. The non-public personal information collected and maintained from this website will be retained for six years from the date of its creation or the date when it was last in effect, whichever is later.

When we have no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information or, if this is not possible (for example, because your personal information has been stored in backup

archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

How do we keep your information safe?

We aim to protect your personal information through a system of organizational and technical security measures. We have implemented appropriate and reasonable technical and organizational security measures designed to protect the security of any personal information that we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot guarantee that hackers, cybercriminals, or other unauthorized third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information. Although we do our best to protect your personal information, the transmission of personal information to and from our Services is at your own risk. You should only access Services within a secure environment.

SutureHealth takes precautions to protect its Users' nonpublic personal information. When users submit sensitive information to SutureHealth, the information is protected both online and offline.

While SutureHealth uses SSL encryption to protect sensitive information online, SutureHealth protects User-information off-line. Only employees who need the information to perform their jobs are granted access to personally identifiable information. Furthermore, all employees are kept up-to-date on SutureHealth security and privacy practices. Finally, the servers that store personally identifiable information are kept in a secure environment.

Despite our efforts to protect your nonpublic personal information, including PHI, there is always some risk that an unauthorized third party may illegally gain access to systems or that transmissions of your information over the Internet may be intercepted. If you believe someone has accessed your information without authorization, please contact SutureHealth immediately at 1-800-878-8814 or support@SutureHealth.com.

Breach of non-public information: If there is a breach of non-public, personally identifiable data, we will first determine if PHI was accessed during the breach. If PHI was not accessed, SutureHealth will make a determination of the risk associated with

such a breach and take action as deemed necessary. If PHI was accessed, SutureHealth will comply with all current state and federal regulations. In either case, SutureHealth will take measures to prevent future breaches.

Do we collect information from minors?

We do not knowingly collect data from or market to children under 18 years of age. We do not knowingly solicit data from or market to children under 18 years of age. By using the Services, you represent that you are at least 18 years of age or are the parent or guardian of such minor and consent to such minor dependant's use of the Services. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact support@suturehealth.com.

What are your privacy rights?

In some regions, such as the European Economic Area (EEA), United Kingdom (UK), and Canada, you have rights that allow you greater access to and control over your personal information. You may review, change, or terminate your account at any time.

In some regions (like the EEA, UK, and Canada), you have certain rights under applicable data protection laws. These may include the right (i) to request access and obtain a copy of your personal information, (ii) to request rectification or erasure, (iii) to restrict the processing of your personal information, and (iv) if applicable, to data portability. In certain circumstances, you may also have the right to object to the processing of your personal information. You can make such a request by contacting us using the contact details provided in the section "How can you contact us about this notice?" section below. We will consider and act upon any request in accordance with applicable data protection laws.

If you are located in the EEA or UK and you believe that we are unlawfully processing your personal information, you have the right to complain at your local data protection supervisory authority. You can find their contact details here: https://ec.europa.eu/newsroom/article29/items/612080

If you are located in Switzerland, the contact details for the data protection authorities are available here: https://www.edoeb.admin.ch/edoeb/en/home.html

Withdrawing your consent: If we are relying on your consent to process your personal information, which may be express and/or implied consent depending on the applicable law, you have the right to withdraw your consent at any time. You can withdraw your consent at any time by contacting us the contact details provided in the section "How can you contact us about this notice?" section below or by updating your preferences. However, please not that this will not affect the lawfulness of the processing before its withdrawal, nor when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Opting out of marketing and promotional communications: you can unsubscribe from our marketing and promotional communications at any time by clicking the unsubscribe link in the emails that we send, replying "STOP" or "UNSUBSCRIBE" to the SMS messages that we send, or by contacting us using the details provided in the "How can you contact us about this notice?" section below. You will then be removed from the marketing lists. However, we may still communicate with you, for example, to send you service-related messages that are necessary for the administration and use of your account, to respond to service requests, or for other non-marketing purposes.

Account information: If you would at any time like to review or change the information in your account or terminate your account, you can:

- Log in to your account setting and update your user account under the "My Account" section of your profile.
- Contact us using the contact information provided

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with investigations, enforce our legal terms and/or comply with applicable legal requirements.

Cookies and similar technologies: Most web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and

to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Services.

If you have questions or comments about your privacy rights, you may email us at support@suturehealth.com.

Controls for do-not-track features

Most web browsers and some mobile operating systems and mobile applications include a Do-No-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage, no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this privacy notice.

Do California residents have specific privacy rights?

If you are a California resident, you are granted specific rights regarding access to your personal information. California Civil Code Section 1798.83, also know as the "Shine the Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclose to third parties for direct marketing purposes and the names and addresses of all thirds parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing ot us using the contact information provided below.

If you are under 18 years of age, reside in California, and have a registered account with Services, you have the right to request the removal of unwanted data that you publicly post on the Services. To request the removal of such data, please contact us using the contact information provided below and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Services, but please be aware that the data may not be completely or comprehensively removed from all of our systems (e.g., backups, etc.)

CCPA Privacy Notice

The California Code of Regulations defines a “resident’ as:

1. Every individual who is in the State of California for other than a temporary or transitory purpose and
2. Every individual who is domiciled in the State of California who is outside the State of California for a temporary or transitory purpose.

All other individuals are defined as “non-residents.” If this definition of “resident’ applies to you, we must adhere to certain rights and obligations regarding your personal information.

We have collected the following categries of personal information in the past twelve (12) months:

Category	Examples	Collected
Identifiers	Contact details such as real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, and account name	Yes
Personal information categories listed in the California Customer Records statute	Name, contact information, education, employment history, and financial information	Yes
Protected classification characteristics under California or federal law	Gender and date of birth	Yes
Commercial Information	Transaction information, purchase history, financial details, and payment	Yes

	information	
Biometric Information	Fingerprints and voice prints	No
Internet or similar network activity	Browsing history, search history, online behavior, interest data, interactions with our and other websites, applications, systems, and advertisements	Yes
Geolocation data	Device Location	Yes
Auto, electronic, visual, thermal, olfactory, or similar information	Images and audio, video or call recordings created in connection with our business activities	Yes
Professional or employment-related information	Business contact details in order to provide you our services at a business level or job title, work history, and professional qualifications if you apply for a job with us	Yes
Education information	Sudent records and directory information	No
Inferences drawn from other personal information	Inferences drawn from any other collected personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics	Yes

We may also collect other personal information outside of these categories instances where you interact with us in person, online, or by phone or mail in the context of:

- Receiving help through our customer support channels;
- Participation un customer surveys or contests; and
- Facilitation in the delivery of our Services and to respond to you inquires.

Suture Health, Inc collects and shares your personal information through;

- Targeting cookies/marketing cookies
- Beacons/Pixels/Tags

More information about our data collection and sharing practices can be found in this Privacy Notice.

You may contact us by email at support@suturehealthc.om or by calling toll-free at 1-800-878-8814, by visiting https://www.suturesign.com/contact or by referring to the contact details at the bottom of this document.

If you are using an authorized agent to exercise your right to opt-out, we may deny a request if the authorized agent does not submit proof that they have been validly authorized to act on your behalf.

We may disclose your personal information with our service providers pursuant to a written contract between us and each service provider. Each service provider is a for-profit entity that processes the information on our behalf. We may use your personal information for our own business purposes, such as for undertaking internal research for technological development and demonstration. This is not considered to be "selling" of your personal information.

Suture Health, Inc., has not sold any personal information to third parties for a business or commercial purpose in the preceding twelve (12) months. Suture Health, Inc., has disclosed the following categories of personal information to third parties for a business or commercial purpose in the preceding twelve (12) months:

- Category A. Identifiers, such as personal contact details like your real name, alias, postal address, telephone or mobile contact number, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, and account name.
- Category B. Personal information, as defined in the California Customer Records law, such as your name, contact information, education, employment, employment history, and financial information.
- Category C. Characteristics of protected classifications under California or federal law, such as gender and date of birth
- Category K. Inferences drawn from any of the personal information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

The categories of third parties to whom we disclosed personal information for a business or commercial purpose can be found under the “When and with whom do we share your personal information” section of this privacy notice.

Your rights with respect to your personal data

Right to request deletion of data – Request to delete
You can ask for the deletion of your personal information. If you ask us to delete your personal information, we will respect your request and delete your personal information, subject to exceptions provided by law, such as (but not limited to) the exercise by another consumer of his or her right to free speech, our compliance requirements resulting from a legal obligation, or any processing that may be required to protect against illegal activities.

Right to be informed – Request to know
Depending on the circumstances, you have a right to know:

- Whether we collect and use your personal information
- The categories of personal information that we collect
- The purposes for which the collected personal information is used
- Whether we sell your personal information to third parties
- The categories of personal information that we sold or disclosed for a business purpose
- The categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
- The business or commercial purpose for collecting or selling personal information

In accordance with applicable law, we are not obligated to provide or delta consumer information that is de-identified in response to a consumer request or to re-identify individual data to verify a consumer request.

Right to Non-Discrimination for the Exercise of a Consumer’s Privacy Rights
We will not discriminate against you if you exercise your privacy rights.

Verification Process

Upon receiving your request, we will need to verify your identity to determine if you are the same person about whom we have the information in our system. These verification efforts require us to ask you to provide information so that we can match it with the information you have previously provided us. For instance, depending on the type of request you submit, we may ask you to provide certain information so that we can match the information you provide with the information w already have on file, or we may contact you through a communication method (e.g., phone or email) that you have previously provided to us. We may also use other verification methods as the circumstances dictate.

We will only use the personal information provided in your request to verify your identity or authority to make the request. To the extent possible, we will avoid requesting additional information from you for the purposes of verification. However, if we cannot verify your identity from the information already maintained by us, we may request that you provide additional information for the purposes of verifying your identity and for security or fraud prevention purposes. We will delete such additionally provided information as soon as we finish verifying you.

Other privacy rights

- You may object to the processing of your personal information
- You may request correction of your personal data if it is incorrect or no longer relevant, or ask to restrict the processing of the information
- You can designate an authorized agent to make a request under the CCPA on your behalf. We may deny a request from an authorized agent that does not submit proof that they have been validly authorized to act on your behalf in accordance with the CCPA
- You may request to opt-out from future selling of your personal information to third parties. Upon receiving an opt-out request, we will act upon the request as soon as feasibly possible, not no longer than fifteen (15) business days from the date of the request submission

To exercise these rights, you can contact us by email at support@suturehealth.com, by calling toll-free at 1-800-878-8814, by visiting https://suturesign.com/contact, or by referring to the contact details at the bottom of this document. If you have a complaint about how we handle your data, we would like to hear from you.

Do we make updates to this notice?

We will update this notice as necessary to stay compliant with relevant laws. We may update this privacy notice from time to time. The updated version will be indicated by an updated “revised” date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information. SutureHealth reserves the right to modify, change, and/or update this privacy policy at any time. .

How can you contact us about this notice?

If you have questions or comments about this notice, you may email us at support@suturehealth.com or by post to:

Suture Health, Inc
105 Vulcan Rd., Suite 413
Homewood, AL 35309

How can you review, update, or delete the data we collect from you?

Based on the applicable laws of your country, you may have the right to request access to the personal information we collect from you, change that information, or delete it. To request to review, update, or delete your personal information please contact support@suturehealth.com and provide the following information:

- Your First and Last Name
- The email address you use to access the Service(s)
- Who you are:
    - The person, or the parent/guardian of the person
    - An agent authorized by the user to make this request on their behalf
- Under the rights of which law you are making the request
    - CCPA
    - GDPR
    - Other
- You are submitting the request to:
    - Know what information is being collected from you

    - Have your information deleted
    - Other
- Additional details regarding your action request or question
- Confirmation that:
    - Under penalty of perjury, you declare that all the information above is true and accurate
    - You understand that the deletion or restriction of your personal data is irreversible and may result in the termination of services
    - You understand that you will be required to validate your request by email and that you may be contacted in order to complete the request