

FinThrive Privacy Policy

Last Updated: September 6, 2023

This general **FinThrive Privacy Policy** (“**Privacy Policy**”) provides information on our information practices. Whether you are new to FinThrive or a long-time partner, please take the time to review our policy. This Privacy Policy also informs you of any rights that you may have with respect to our use of your personal information.

This Privacy Policy reflects the information practices of FinThrive, Inc. and its affiliates and subsidiaries (collectively referred to as “Company”, “FinThrive”, “us”, “our” or “we”).

This Privacy Policy was last updated on September 6, 2023. However, the Privacy Policy can change over time, for example to comply with legal requirements or to meet changing business needs. The most up-to-date version can always be found on our website. By using our websites, services or by interacting with the Company, you accept the terms of this Privacy Policy.

1. Scope

As used in this Privacy Policy, “**personal information**” means information that identifies, links to, or reasonably links to, an identified individual or to an identifiable individual. Personal information does not include publicly available information, de-identified or aggregate data.

This Privacy Policy applies to the collection, use or disclosure of personal information by FinThrive related to the following (collectively, “consumers” or “you”).

- visitors and users of our website at FinThrive.com or other sites that link to this Privacy Policy (collectively referred to as the “**Sites**”)
- attendees of events, such as industry conferences, where FinThrive is represented
- customers and prospective customers and their representatives
- suppliers and business partners and their representatives
- recipients or subscribers to FinThrive’s communications
- visitors to FinThrive facilities

The Privacy Policy does not apply to the following activities:

- **Personal information collected about you by FinThrive customers** which may include, but are not necessarily limited to, healthcare facilities, providers or payers. Our customers are responsible for their own personal information

collection and processing practices, including when customers use FinThrive technology solutions to collect or process your personal information.

- **Personal information you provide on third-party sites not controlled by FinThrive.** We may provide links to other websites, social networks, or other features for your convenience and information. These sites may have their own privacy statements or policies in place, which we recommend you review if you visit any linked websites. We are not responsible for the content of linked sites or any use of the sites.
- **Personal information processed by FinThrive as a Business Associate, Service Provider, Processor, or Contractor.** Personal information made available to FinThrive in these instances is governed by federal data protection regulations, for example the Health Insurance Portability and Accountability Act (“HIPAA”) or state privacy laws, and its use and disclosure is limited by our written agreements with our customers.
- **Personal information made available to FinThrive as an authorized Reseller of certain regulated data.** Some of our products and services include regulated data and is only made available to entities with a permissible purpose to receive it (as defined in the Fair Credit Reporting Act or “FCRA”) or entities with a permitted use under Title V of the Gramm–Leach–Bliley Act or “GLBA” and is not subject to certain data privacy rights and processing limitations imposed by state privacy laws.
- **Personal information collected by FinThrive as part of an employee–employer relationship,** including applicants and candidates for employment with FinThrive. FinThrive maintains separate notices for our use of personal information in these instances. Job applicants or candidates for employment can view the relevant notice in our Privacy Resources page on our website.

2. Information That We Collect

From you directly:

- When you visit our website or otherwise interact with the company online (e.g. through publicly available sites such as social media networks), you choose how much information to provide directly to us. On the website information is typically submitted via forms or requests for contact. Information submitted may include personal information such as name, business or personal email address, phone number, and job level. On social media, any posts or comments you make may reveal personal information to us.
- When you visit us at a conference, industry event or similar, we may collect contact information such as your name, business or personal email address, and phone number. We may also collect information such as the solutions you are interested in learning more about.

- When acting in the role of an employee or representative of one of our customers, service providers or other third-party with whom we do business, we may collect your contact information such as your name, phone number, business email address and work address.
- When you interact with us in person, via video or audio conference or online, we may collect information about your preferences, behaviors, other interests, or any other information you choose to include in your messages, responses, online forums or communities, our support portal, advisory council, focus groups, user groups, surveys, etc.
- When you participate in one of our webinars, podcasts, or similar as a presenter, we may record your voice and image, but only with notice and your consent.
- As a user of one of our technology solutions, whether those sold to customers or used to facilitate interactions with our suppliers or service providers, we collect personal information such as your name, email address, and user login credentials.
- When you subscribe to our communications (e.g. newsletters or online publications), we collect your email address used to register as well as your name, job level and/or area of interest.
- When you visit one of our facilities, we may collect a photo, your full name, signature, email address, phone number and other relevant information as part of our visitor registration process.

Information collected passively:

- Cookies and similar technologies. We automatically collect certain information through browser cookies and other tracking technologies when you access, use or interact with our Sites. A cookie is a piece of data that a website can send to your browser, which may then be stored on your device, sometimes with a code unique to your device. We use cookies for a number of different purposes. Some cookies are necessary to ensure our Sites function properly and some enable us to deliver an individualized online experience.

You have the ability to accept or decline cookies when you visit our site. In addition, most web browsers give you a choice to modify your browser settings to decline some or all cookies. Unless you decline cookies or disable the cookies on your system, by using our Sites, you agree to our use of those cookies. If you decide to decline or disable cookies on your system, then some features of our Sites may not be available, work, or work as designed.

- If you are user of our technology solutions (customers), we may also collect information on your use of our technology solutions, including logs of your activity within the solution, how you navigate within the solution or similar user analytics.

From third parties:

- We may obtain your personal information, including name, contact information or other identifying information, from other sources such as data and analytics providers, social networks, consumer reporting agencies, our customers, vendors, service providers who collect information on our behalf, government agencies or other publicly available sources.

3. Use of Personal Information

We may use the personal information collected about you for the following purposes:

- To provide, administer and communicate with you about our technology solutions, services, events, surveys and promotions (including by sending you marketing communications) or to market our solutions (e.g. your customer references or testimonials, provided only with your consent).
- To facilitate and personalize your experience with our Sites and/or technology solutions and to administer those Sites and technology solutions.
- To determine and manage the effectiveness of our advertising and marketing, for example by engaging in surveys or research to understand our customer-base, conduct analysis of product adoption, evaluate customer success and user behaviors within our solutions.
- To enable you to do business with us, for example, by conducting sales meetings, customer implementation projects, vendor onboarding, contracting processes, or related administrative activities for our customer and vendor management.
- To process, evaluate and respond to your requests, inquiries, or support cases.
- To evaluate, grow and improve our business (including activities such as developing new products and services, enhancing current products or services, market research, quality assessment and improvement activities, cost studies, data aggregation and analytics, customer reference program, advisory councils, etc.).
- To carry out or obligations and enforce our rights arising from any contracts entered into between us and you.
- To protect and secure our Sites, technology solutions, data, assets, network, and business operations, and to detect, investigate, and prevent activities that may violate our policies or be fraudulent or illegal.
- To comply with legal process, such as warrants, subpoenas, court orders, and lawful regulatory or law enforcement requests and to comply with legal, regulatory compliance, or contractual obligations.

- To conduct general business operations such as accounting, recordkeeping, compliance activities and audits.
- To defend the interests of the Company or employees in threatened or actual legal proceedings, investigations or inquiries.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by FinThrive is among the assets transferred.

4. Disclosure of Personal Information

We do not sell or share your personal information to third-parties for direct marketing, or cross-context behavioral advertising.

We may disclose personal information to the following third parties for a business purpose:

- Third-party service providers or contractors we engage to provide services to us or on our behalf. For example, information technology partners, contractors provided by staffing agencies, auditors, accountants, marketing consultants.
- In the case of customer reference data, testimonials or other customer stories related to our solutions, to other customers or prospective customers, but only with prior consent from you.
- Relevant third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings).
- As required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or meet a compliance obligation or respond to government requests, including public and government authorities outside your country of residence, for national security and/or law enforcement purposes.

When third parties are given access to, or receive, personal information, we take appropriate contractual, technical and organizational measures designed to ensure that personal information is processed only to the extent that such processing is necessary, consistent with this Privacy Policy, and in accordance with applicable laws or regulations. For example, when we disclose personal information for a business purpose to a Service Provider, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract.

5. Retention of Information

The Company maintains a Records Retention policy that outlines our practices for retention of business-related information. We are subject to certain legal and regulatory requirements to retain certain information for a defined period of time. Absent a specific requirement to retain personal information based on the retention schedule, a contractual obligation, litigation hold or other legitimate business purpose, the Company deletes information when it is no longer necessary for the proper operation of the Company.

6. How We Protect Your Information

We believe privacy and security must go together. We maintain an Information Security Program with administrative (policies, standards, and processes), physical, and technical controls designed to protect the security and confidentiality of your information both online and offline. We also hold our service providers and other third parties with whom we may share information to confidentiality and security standards. However, while we take precautions, there are inherent risks and limitations to any security program and therefore we cannot guarantee absolute security of your information. Please do your part by keeping any passwords to our systems secure, changing them often and taking other reasonable steps when communicating or sharing personal information with us.

7. Children's Privacy

Our technology solutions and Sites are not directed to children under the age of sixteen (16) and we do not knowingly collect personal information from children under that age for the purposes described in this Privacy Policy. If we become aware that we have inadvertently collected personal information from anyone under the age of sixteen (16), we will delete the information from our records.

8. Communication Choices

Every marketing email from FinThrive contains instructions on how to opt out of receiving further communications. To change your email subscription status or opt out of FinThrive's marketing communications, please follow the instructions indicated. We will comply with your request(s) as soon as reasonably practicable. Please note that if you opt out of receiving marketing-related emails from us, we may still send you important administrative messages.

Likewise, if you are a representative of a customer or FinThrive business partner with whom we do business, you may update your contact information and preferences with us through your account at any time. If you need assistance, please reach out to us at the "Contact Us" information below.

9. State Privacy Laws and Your Rights

If you are a California resident, you have specific rights under the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), regarding your personal data. To review the Notice and a description of your rights, please click on the link below:

[California](#)

10. Contact Us

If you have any questions or comments about this Privacy Policy, please contact us at privacy@finthrive.com.

If you wish to link to our Website, then you must request permission to do so in writing by contacting us by e-mail at notices@finthrive.com or via U.S. mail at FinThrive, 7950 Legacy Drive, Suite 900, Plano, TX 75024, Attn: Legal Department Notices.