Hightop Health

Privacy Policy

Last Updated: July 30, 2026

1. Introduction and Scope

Hightop Health, LLC ("Hightop Health," "we," "our," or "us") respects your privacy and is committed to protecting the personal information you share with us. This Privacy Policy describes our practices for collecting, using, maintaining, protecting, and disclosing personal information in connection with our website (https://hightophealth.com/), patient portal, services, and electronic communications (collectively, the "Services").

This Privacy Policy applies to information we collect when you visit our website, use our Services, interact with us electronically, or otherwise engage with Hightop Health as a consumer or customer. It does not apply to information collected by third parties, including through any third-party application or content that may link to or be accessible from our Services.

To the extent you access our Services through our website, your use is also governed by our Terms of Use, available at HTTPS://HIGHTOPHEALTH.COM In the event of any conflict between this Privacy Policy and the Terms of Use regarding the treatment of your personal information, this Privacy Policy shall control.

Scope Limitation: This Privacy Policy addresses our website and customer-facing privacy practices under applicable U.S. federal and state law. It does not replace or modify any separate Notice of Privacy Practices that Hightop Health may issue under the Health Insurance Portability and Accountability Act ("HIPAA") or applicable state health privacy laws.

2. Personal Information We Collect

We may collect the following categories of personal information, depending on how you interact with us:

a. Identifiers and Contact Information

- Name, postal address, email address, telephone number, and account credentials.
- Social Security number, driver's license number, or other government-issued identifiers (where necessary for specific services).

b. Customer Records Information

- Billing and payment information (e.g., credit or debit card numbers, bank account information).
- Insurance information, health plan identifiers, or similar account details.

c. Health-Related Information

- Health conditions, symptoms, treatment history, or wellness information you voluntarily provide through our website or Services.

- Medical information, health insurance information, and related data necessary to provide or facilitate healthcare services.

d. Protected Classification Characteristics

- Age, gender, race, ethnicity, disability status, or other characteristics protected under applicable law, where voluntarily provided or necessary for service delivery.

e. Internet and Network Activity

- Browsing and search history on our website, information regarding your interaction with our website or Services, and clickstream data.
- IP address, device identifiers, browser type and version, operating system, system configuration, referring URLs, and network/connection information.

3. Sources and Methods of Collection

We collect personal information from the following sources:

a. Directly From You

- When you create an account, complete a form, submit an inquiry, or otherwise provide information to us directly.
- When you communicate with us via email, telephone, chat, or other means.

b. Automatically Through Your Use of Our Services

- Through cookies, web beacons, pixel tags, log files, and similar tracking technologies deployed on our website.
- Through analytics tools and third-party services that help us understand usage patterns.

c. From Third-Party Sources

- Service providers and business partners who assist in delivering our Services.
- Healthcare providers, health plans, or other entities where necessary to facilitate services.

5. Cookies and Similar Technologies

Our website uses cookies and similar tracking technologies to enhance functionality, analyze usage, and deliver relevant content. We use the following types of cookies:

- **Strictly Necessary Cookies:** Essential for website functionality (e.g., session management, security).
- **Analytics Cookies:** Help us understand how visitors interact with our website (e.g., page views, traffic sources). We may use Google Analytics or similar tools.
- **Personalization Cookies:** Allow us to remember your preferences and settings.
- **recr/Advertising Cookies:** Used to deliver relevant advertisements and measure campaign effectiveness.

Your Cookie Choices: Most web browsers allow you to manage cookie preferences through browser settings. You may also opt out of interest-based advertising through the following mechanisms:

- Network Advertising Initiative (NAI): https://optout.networkadvertising.org/
- Digital Advertising Alliance (DAA): https://optout.aboutads.info/

Please note that disabling cookies may affect your ability to use certain features of our website.

6. How We Use Personal Information

We use personal information for the following purposes:

a. Providing and Managing Services

- To provide, maintain, and improve our products and Services.
- To create and manage your account, process transactions, and fulfill requests.
- To respond to customer service inquiries, technical support requests, and feedback.
- To process payments and billing.
- To determine eligibility for services or programs.

b. Communications

- To send transactional communications (e.g., service updates, account notices, receipts).
- To send promotional communications about products, services, or events that may interest you.
- To conduct surveys, questionnaires, and research to improve our Services.

c. Personalization and Analytics

- To personalize your experience and deliver content relevant to your interests.
- To analyze website traffic, usage patterns, and trends.
- To develop new products, services, features, and functionality.

d. Security and Legal Compliance

- To detect, prevent, and address fraud, unauthorized access, and security incidents.
- To comply with applicable laws, regulations, legal processes, and government requests.
- To enforce our terms of service, contracts, and other agreements.
- To protect the rights, property, and safety of Hightop Health, our users, and others.

e. Business Operations

- To support internal business operations, including auditing, data analysis, and record-keeping.
- To facilitate corporate transactions (e.g., mergers, acquisitions, reorganizations).
- To monitor compliance with internal policies and applicable law.

7. How We Disclose Personal Information

We may disclose your personal information to the following categories of recipients and for the following purposes:

- **Affiliates and Subsidiaries:** We may share personal information with our corporate affiliates and subsidiaries for business operations and to provide integrated services.

- **Service Providers:** We disclose personal information to contractors, vendors, and service providers who perform services on our behalf (e.g., hosting, analytics, payment processing, customer support, IT services), subject to contractual obligations of confidentiality and use limitations.
- **Business Partners:** Where appropriate for joint offerings, referrals, or co-branded services.
- **Healthcare Entities:** Healthcare providers, health plans, or clearinghouses, where necessary to facilitate healthcare services or as required by law.
- **Legal and Regulatory:** To comply with a legal obligation, subpoena, court order, or other legal process; to respond to government or regulatory inquiries; or as otherwise required by law.
- **Protection of Rights:** To protect the rights, property, or safety of Hightop Health, our users, or others, including to enforce our agreements and prevent fraud.
- **Corporate Transactions:** To a buyer, successor, or other party in connection with a merger, acquisition, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets.
- **With Your Consent:** Where you have otherwise directed or consented to the disclosure.

8. Sensitive Personal Information

Under certain U.S. state privacy laws, "sensitive personal information" may include categories such as Social Security numbers, government-issued identifiers, financial account information, precise geolocation, racial or ethnic origin, health information, and biometric data. We collect and use sensitive personal information only for the purposes permitted by applicable law, including to provide the Services you request, ensure security, and comply with legal obligations.

Sale and Sharing of Personal Information

Hightop Health does not "sell" or "share" personal information as such terms are defined under applicable state privacy laws

9. Data Retention

We retain personal information for as long as necessary to fulfill the purposes for which it was collected, including to:

- Provide our products and Services and maintain your account.
- Comply with legal, regulatory, and contractual obligations.
- Resolve disputes, enforce agreements, and protect against fraud or illegal activity.
- Support legitimate internal business purposes (e.g., auditing, analytics, record-keeping).

When personal information is no longer necessary for these purposes, we will securely delete or de-identify it in accordance with our data retention policies and applicable law.

10. Applicant and Recruitment Data

This section describes how we collect, use, disclose, and retain personal information from individuals who apply for employment or independent contractor positions with Hightop Health, whether through our careers website, third-party job boards, recruiting platforms, or other means (collectively, "Applicants").

The other provisions of this Privacy Policy also apply to the personal information we collect from Applicants, except as specifically provided in this section.

This section applies to all personal information we collect in connection with the recruiting and hiring process, including information you provide directly, information we receive from third parties, and information collected automatically when you interact with our careers or application platforms.

If you are hired by Hightop Health, certain information collected during the application process may become part of your personnel file and will be subject to applicable employee privacy policies.

Categories of Applicant Personal Information

In connection with recruiting and hiring, we may collect the following categories of personal information:

Identifiers and Contact Information. Full name, address, email address, telephone number, and other contact details.

Application Materials. Resume or curriculum vitae (CV), cover letter, writing samples, portfolios, or other materials you submit in support of your application.

Professional and Employment History. Current and prior employers, job titles, dates of employment, job duties, compensation history (where permitted by law), and reasons for leaving.

Education and Credentials. Educational institutions attended, degrees, certifications, licenses, professional memberships, and training records.

References. Names and contact information for professional references, and information provided by references.

Assessment and Interview Information. Responses to application questionnaires, skills assessments, interview notes, and evaluation scores; scheduling and communication metadata (e.g., interview dates, recruiter communications).

Background Screening Information. Criminal history, credit history, driving records, or other background check information, where authorized by you and permitted by applicable law.

Eligibility and Compliance Information. Work authorization/eligibility documentation, professional licenses or certifications; voluntary Equal Employment Opportunity ("EEO") and affirmative action demographic data (e.g., gender, race/ethnicity, veteran status, disability status), collected solely for compliance and reporting purposes.

Accommodation Information. Information relating to requests for reasonable accommodations during the application or interview process.

Compensation Expectations. Salary expectations, desired benefits, and availability.

Device and Usage Data. IP address, browser type, device information, and usage data collected when you interact with our careers website or applicant portal.

Sensitive Personal Information (where applicable). Social Security number or government-issued identifiers (only where required for background screening or employment eligibility verification); racial or ethnic origin, religious beliefs (only where voluntarily provided for EEO/accommodation purposes).

Sources of Applicant Information

We collect applicant personal information from the following sources:

- **Directly From You.** When you submit an application, resume, or other materials through our careers website, applicant portal, job fairs, or direct communications.
- **Recruiting Platforms and Job Boards.** Third-party platforms such as LinkedIn, Indeed, Glassdoor, or similar job boards, where you have made your information publicly available or have directed the platform to share it with us.
- **References.** Professional references you have identified.
- **Background Check Providers.** Background check providers engaged to conduct authorized background screenings.
- **Recruiters and Staffing Agencies.** Third-party recruiters or staffing agencies assisting with recruitment on our behalf.
- **Assessment and Skills Providers.** Third-party vendors administering skills assessments, tests, or evaluations.
- **Publicly Available Sources.** Professional profiles, portfolios, or publicly available information relevant to your qualifications.
- **Automated Collection.** Cookies and similar technologies on our careers website or applicant portal (see Section 5 above).

How We Use Applicant Information

We use applicant personal information for the following purposes:

- Recruiting and hiring, including identifying and evaluating candidates for open positions;
- Communicating with you about your application, scheduling interviews, and providing updates on the status of your candidacy;
- Evaluating qualifications, skills, experience, and suitability for the position;
- Conducting background checks and verifying information, where authorized by you and permitted by law;
- Making hiring decisions and extending offers of employment;
- Processing requests for reasonable accommodations;
- Complying with EEO, affirmative action, and other legal and regulatory obligations (e.g., EEOC, OFCCP, state and local employment laws);
- Preventing fraud, ensuring security, and protecting Hightop Health's legitimate business interests;
- Complying with legal obligations, responding to legal process, and defending against legal claims;
- Improving our recruiting processes and practices, including in aggregated or de-identified form where possible; and
- Considering you for future openings (where you have consented or where permitted by law).

Automated Decision-Making and AI-Assisted Recruiting

Hightop Health uses artificial intelligence (AI) and machine learning (ML) technologies, including natural language processing and predictive analytics, to assist in the initial screening of employment applications. These AI/ML tools, provided through the Ashby recruitment platform, assess applications

against the characteristics and qualifications relevant to the applicable job requisition. These tools are designed to help identify potentially qualified candidates, but they do not make automated hiring decisions. AI/ML-generated assessments are one of several factors considered in the hiring process, and our human recruiters thoroughly evaluate each applicant's skills and qualifications to determine suitability for the role.

Opt-Out of AI/ML Screening. If you prefer not to have your application assessed using AI/ML features, you may opt out by selecting the applicable checkbox on your application. Opting out will not negatively impact your application, which will instead be reviewed manually by our recruiting team.

Notice for New York City Applicants. If you are applying for a position located in New York City, AI and ML technologies may be used in connection with your application. Pursuant to New York City Local Law 144, you have the right to take at least ten (10) business days to decide whether to proceed with submitting your information through this process. By continuing with your application, you confirm your understanding of this notice. If you choose to proceed before the ten-business-day period expires, you are making a knowing and voluntary decision to do so.

Notice for Illinois Applicants. If you are applying for a position located in Illinois or are an Illinois resident, Hightop Health may use AI-enabled video analysis to analyze video interviews you submit as part of the application process, if applicable. In accordance with the Illinois Artificial Intelligence Video Interview Act (820 ILCS 42), we will: (1) notify you before the interview that AI may be used; (2) provide information explaining how the AI works and what general characteristics it uses to evaluate applicants; and (3) obtain your consent before using AI analysis. You may request that any video submitted be destroyed within thirty (30) days of making such request, and we will destroy the video within thirty (30) days unless you have otherwise consented to retention.

Notice for Maryland Applicants. If you are applying for a position located in Maryland, Hightop Health will not use facial recognition technology during an interview without your prior written consent, in accordance with Maryland Labor and Employment Code § 3-717.

How We Disclose Applicant Information

We may disclose applicant personal information to the following categories of recipients:

- **Internal Personnel.** Recruiting, human resources, hiring managers, and other authorized personnel involved in the hiring process.
- **Service Providers and Vendors.** Third-party vendors providing services on our behalf, including applicant tracking systems, background check providers, assessment platforms, scheduling tools, and IT service providers. These vendors are subject to contractual obligations to safeguard personal information and use it only for authorized purposes.
- **Affiliates and Subsidiaries.** Our corporate affiliates or subsidiaries, where relevant for recruiting, talent management, or shared services.
- **Recruiters and Staffing Agencies.** Third-party recruiters or staffing agencies assisting with the position.
- **Government Authorities and Regulators.** Where required by law, regulation, subpoena, court order, or government inquiry (e.g., EEOC, OFCCP, state labor agencies).
- **Legal and Professional Advisors.** External legal counsel, auditors, and other professional advisors in connection with legal, audit, or compliance matters.
- **Corporate Transactions.** A buyer, successor, or other party in connection with a merger, acquisition, or other corporate transaction.

No Sale of Applicant Personal Information. Hightop Health does not sell applicant personal information for monetary consideration and does not share applicant personal information for cross-context behavioral advertising purposes.

Sensitive Applicant Information and Equal Employment Opportunity ("EEO") Data

Certain applicant personal information may constitute sensitive personal information under applicable state privacy laws. We collect and use sensitive applicant information only for purposes permitted by law, including:

- Processing and verifying employment eligibility;
- Conducting authorized background screenings;
- Complying with EEO, affirmative action, and reporting requirements (e.g., EEOC, OFCCP);
- Processing accommodation requests; and
- Complying with other legal obligations.

Voluntary demographic data collected for EEO and affirmative action purposes is maintained separately from your application, is not used in hiring decisions, and is used only for compliance and aggregate statistical reporting.

Applicant Data Retention

In addition to the general data retention practices described in Section 9 above, we retain applicant personal information as follows:

- For candidates who are not hired, we generally retain application materials and related records for two (2) years following the conclusion of the recruiting process, unless a longer retention period is required by law or necessary for legal claims;
- For candidates who are hired, application materials become part of the employee personnel file and are retained in accordance with our employee records retention policies;
- Background check reports are retained in accordance with applicable law and provider agreements;
- EEO and affirmative action data is retained in accordance with EEOC and OFCCP record-retention requirements; and
- We will securely delete or de-identify applicant personal information when it is no longer needed for the purposes described above, subject to applicable legal holds or obligations.

11. Data Security

We implement reasonable administrative, technical, and physical security measures designed to protect personal information against accidental loss and unauthorized access, use, alteration, or disclosure. These measures include encryption of data in transit and at rest, access controls limiting personnel access to personal information on a need-to-know basis, and maintenance of an incident response program to address potential security events. However, no method of transmission over the internet or electronic storage is completely secure. While we strive to protect your information, we cannot guarantee absolute security. You are responsible for maintaining the confidentiality of any account credentials.

11. Your Privacy Choices and Rights

a. Marketing Communications

You may opt out of receiving promotional email communications from us by following the unsubscribe instructions in any promotional email or by contacting us at info@hightophealth.com. Even after opting out of promotional communications, we may still send you transactional or service-related messages.

b. Cookies and Tracking

You may manage cookie preferences through your browser settings or using our cookie preference center. See Section 5 above for additional details and opt-out links.

c. SMS Text Message Communications

Hightop Health may offer SMS text messaging communications as part of our Services. SMS messages may include transactional, informational, and service-related communications, such as interview confirmations, application follow-up communications, and candidate status updates, and may also include recurring recruiting outreach messages regarding open positions and career opportunities. This section describes our practices with respect to SMS communications.

Consent to Receive SMS Messages. By providing your mobile phone number and opting in to receive SMS text messages from us, you expressly consent to receive recurring SMS text messages from Hightop Health at the mobile phone number you provide. Your consent to receive SMS messages is not a condition of purchasing any goods or services from us, and you may use our Services without consenting to receive SMS messages. Consent to receive SMS messages may be revoked at any time by following the opt-out procedures described below.

Program Description and Message Content. Our SMS messaging program includes transactional and service-related messages, such as interview confirmations, application follow-up communications, and candidate status updates. We may also send recurring messages to prospective candidates regarding open positions and career opportunities, which may be considered promotional or marketing in nature.

Message Frequency. Message frequency varies based on your use of the Services and account activity. You may receive multiple messages per day or per week depending on service-related events, appointment schedules, or your interactions with our Services.

Message and Data Rates. Standard message and data rates may apply to SMS messages depending on your mobile carrier and wireless plan. You are solely responsible for any fees or charges from your mobile carrier related to SMS messages. Hightop Health is not responsible for any carrier charges or fees.

Opt-Out Instructions. You may opt out of receiving SMS text messages at any time by replying STOP, CANCEL, END, QUIT, or UNSUBSCRIBE to any SMS message you receive from us. After you send an opt-out keyword, you will receive a single final confirmation message confirming that you have been unsubscribed and will receive no further SMS messages from us unless you re-enroll. Opting out of SMS messages will not affect your ability to use our Services or receive communications through other channels (such as email).

Help and Support. For assistance with our SMS messaging program, reply HELP to any SMS message you receive from us. Upon receipt of a HELP request, you will receive a message with customer support contact information and instructions for opting out.

No Sharing of SMS Opt-In Data. We will not sell, rent, loan, trade, lease, or otherwise share or transfer for marketing or promotional purposes any mobile telephone numbers or mobile opt-in information or consent collected in connection with our SMS messaging program to any third parties or affiliates. Any

disclosure of such information to service providers or vendors will be limited to the purpose of facilitating our SMS messaging program and subject to confidentiality obligations.

Privacy Policy and Terms. By opting in to receive SMS messages, you acknowledge that you have reviewed and agree to this Privacy Policy and our Terms of Service. Our collection and use of personal information in connection with SMS communications, including your mobile phone number, is subject to this Privacy Policy.

12. State-Specific Privacy Rights

Depending on your state of residence, you may have additional rights under applicable state consumer privacy laws. These rights may include:

- **Right to Know/Access:** The right to request information about the categories and specific pieces of personal information we have collected, the sources of collection, the purposes of use, and the categories of third parties to whom we disclose information.
- **Right to Delete:** The right to request deletion of personal information we have collected from you, subject to legal exceptions.
- **Right to Correct:** The right to request correction of inaccurate personal information.
- **Right to Data Portability:** The right to receive your personal information in a portable, readily usable format.
- **Right to Opt Out of Sale/Sharing:** The right to opt out of the "sale" of your personal information or "sharing" for cross-context behavioral advertising (as defined by applicable law).
- **Right to Opt Out of Targeted Advertising:** The right to opt out of the processing of personal information for purposes of targeted advertising.
- **Right to Opt Out of Profiling:** The right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects.
- **Right to Limit Sensitive Personal Information:** The right to limit the use and disclosure of sensitive personal information to purposes permitted by law.
- **Right to Appeal:** If we deny your privacy request, you may have the right to appeal our decision.

We will not discriminate against you for exercising any of your privacy rights.

Verification and Authorized Agents

To protect your privacy, we will verify your identity before fulfilling any rights request. We may ask you to provide information that matches information we have on file. If you use an authorized agent to submit a request on your behalf, we may require the agent to provide proof of written authorization and may require you to verify your identity directly with us.

How to Submit a Request

You may submit a privacy rights request by sending us an email at info@hightophealth.com

We will respond to verifiable requests within the timeframe required by applicable law (generally 45 days, with extensions as permitted).

13. Children's Privacy

Our website and Services are not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13. If we become aware that we have collected personal information from a child under 13 without verified parental consent, we will take steps to delete such information. If you believe we have collected information from a child under 13, please contact us at info@hightophealth.com.

14. Third-Party Websites and Services

Our website may contain links to third-party websites, services, or applications that are not operated or controlled by Hightop Health. This Privacy Policy does not apply to the practices of third parties. We encourage you to review the privacy policies of any third-party sites you visit. We are not responsible for the content, privacy practices, or security of third-party websites or services.

15. Contact Information

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us at:

Hightop Health

info@hightophealth.com

16. Dispute Resolution

Any dispute, claim, or controversy arising out of or relating to this Privacy Policy or the collection, use, or disclosure of your personal information is subject to the dispute resolution provisions set forth in our Terms of Use, including the binding arbitration clause and class action waiver contained therein. Please review the Terms of Use for full details.

17. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. When we make material changes, we will update the “Last Updated” date at the top of this Policy. We encourage you to review this Privacy Policy periodically. Your continued use of our website or Services following the posting of changes constitutes your acknowledgment of such changes.