Signify Health

California Applicant and Candidate Privacy Policy

Last updated date: January 1, 2024

Thank you for your interest in Signify Health. This Applicant and Candidate Privacy Policy explains:

- What information we collect during our application / recruitment process and why we collect it;
- How we use and share that information; and
- Our retention policy for that information.

Please review this policy carefully. If you have any questions, you may contact us at privacy@signifyhealth.com.

The Types of Information We Collect

This policy covers the information you share with us and/or which may be acquired or produced by Signify Health, its subsidiaries and its affiliates during the application or recruitment process. The information may include:

CATEGORY	EXAMPLES
Personal Identifiers	Name, alias, postal or mailing address, email address, telephone number, social security number, driver's license or state identification card number, passport number.
Contact Information	Home, postal or mailing address, email address, home phone number, cell phone number.
Pre-Hire Information	Information provided in your job application or resume, information gathered as part of background screening and reference checks, pre-hire drug test results, information recorded in job interview notes by persons conducting job interviews for the Company, information contained in candidate evaluation records and assessments, information in work product samples you provided, and voluntary disclosures by you.
Employment History	Information regarding prior job experience, positions held, and when permitted by applicable law your salary history or expectations.
Education Information	Information contained in your resume regarding educational history and information in transcripts or records of degrees and vocational certifications obtained.

Internet, Network, and Computer Activity	Internet or other electronic network activity information related to a job applicant's usage of Company networks, servers, intranet, or Company-owned computers and electronic devices, including system and file access logs, security clearance level, browsing history, search history, and usage history.
Mobile Device Security Information	Data identifying a job applicant's device accessing Company networks and systems, including cell phone make, model, and serial number, cell phone number, and cell phone provider.
Online Portal and Mobile App Access and Usage Information	Where a job applicant or candidate must create an account to apply for a job, collect the applicant's username and password, account history, usage history, and any information submitted through the account.

Of the above categories of Personal Information, the following are categories of Sensitive Personal Information the Company may collect:

- Personal Identifiers (social security number, driver's license or state identification card number, passport number)

Personal information ***does not*** include:

- Publicly available information from government records.
- Information that a business has a reasonable basis to believe is lawfully made available to the general public by the job applicant or from widely distributed media.
- Information made available by a person to whom the job applicant has disclosed the information if the job applicant has not restricted the information to a specific audience.
- De-identified or aggregated information.

How We Use the Information We Collect

Your information will be used by Signify Health for the purposes of carrying out its application and recruitment process that includes:

- Assessing your skills, qualifications and interests for our career opportunities;
- Verifying your information and carrying out reference checks and/or conducting background checks (where applicable) if you are offered a job;
- Communications with you about the recruitment process and/or your application(s), including, in appropriate cases, informing you of other potential career opportunities at Signify Health;
- Creating and/or submitting reports as required under any local laws and/or regulations, where applicable;
- Conducting or arranging for health screenings, drug tests or similar activities;
- Performing any related credentialing or privileging process or review, if applicable;

- Making improvements to Signify Health's application and/or recruitment process;
- Complying with applicable laws, regulations, legal processes or governmental requests; and/or
- Conducting research about your educational and professional background and skills and contacting you if we think you would be suitable for a role with Signify Health.
- To fulfill or meet the purpose for which you provided the information. For example, if you share your name and contact information to apply for a job with the Company, we will use that Personal Information in connection with your candidacy for employment.
- To comply with local, state, and federal law and regulations requiring employers to maintain certain records (such as travel records, personnel files, wage and hour records, payroll records, accident or safety records, and tax records), as well as local, state, and federal law, regulations, ordinances, guidelines, and orders relating to COVID-19.
- To evaluate and improve our recruiting methods and strategies.
- To engage in lawful monitoring of job applicant activities and communications when they are on Company premises, or utilizing Company internet and WiFi connections, computers, networks, devices, software applications or systems.
- To evaluate job applicants and candidates for employment or promotions.
- To obtain and verify background checks on job applicants and to verify employment references.
- To engage in corporate transactions requiring review or disclosure of job applicant records subject to non-disclosure agreements, such as for evaluating potential mergers and acquisitions of the Company.
- To promote and foster diversity, equity, and inclusion in the workplace.
- To evaluate, assess, and manage the Company's business relationship with vendors, service providers, and contractors that provide services to the Company related to recruiting or processing of data from or about job applicants.
- To improve job applicant experience on Company computers, networks, devices, software applications or systems, and to debug, identify, and repair errors that impair existing intended functionality of our systems.
- To protect against malicious or illegal activity and prosecute those responsible.
- To verify and respond to consumer requests from job applicants under applicable consumer privacy laws.

We will also use your information to protect the rights and property of Signify Health and our applicants, candidates, employees or the public as required or permitted by law.

If you are offered and accept employment with Signify Health, the information collected during the application and recruitment process will become part of your employment record.

We collect and process your information where it is necessary in order to take steps, at your request, prior to our potentially entering into a contract of employment with you.

Who May Have Access to Your Information

Signify Health takes appropriate steps to protect information about you that is collected, processed, and stored as part of the application and recruitment process.

- Your information may be shared with our affiliates, subsidiaries or joint ventures in the US and in other jurisdictions, in relation to the purposes described above. If you have been referred for a job at Signify Health by a current Signify Health employee, with your consent, we may inform that employee about the progress of your application and let the Signify Health employee know the outcome of the process.
- Signify Health may also use service providers acting on Signify Health's behalf to perform some of the services described above including for the purposes of the verification / background checks. These service providers may be located outside the country in which you live or the country where the position you have applied for is located.
- Signify Health may sometimes be required to disclose your information to external third parties such as clients or customers, local government authorities, courts and tribunals, regulatory bodies and/or law enforcement agencies for the purpose of complying with applicable laws and regulations, or in response to legal process.
- We will also share your personal information with other third parties if we have your consent (for example if you have given us permission to contact your references), or to detect, prevent or otherwise address fraud, security or technical issues, or to protect against harm to the rights, property or safety of Signify Health, our users, applicants, candidates, employees or the public or as otherwise required by law.
- It is your responsibility to obtain consent from references before providing their personal information to Signify Health.

Our Retention of Your Information

If you apply for a job at Signify Health and your application is unsuccessful (or you withdraw from the process or decline our offer), Signify Health will retain your information for a period after your application. We retain this information for various reasons, including in case we face a legal challenge in respect of a recruitment decision, to consider you for other current or future jobs at Signify Health and to help us better understand, analyze and improve our recruitment processes.

If you do not want us to retain your information for consideration for other roles, or want us to update it, please contact us at privacy@signifyhealth.com. Please note, however, that we may retain some information if required by law or as necessary to protect ourselves from legal claims.

Rights Under the CCPA and CPRA

This section of the Privacy Policy applies only to California residents who are natural persons; it does not apply to any entities (whether business, non-profit or governmental). If you are a California resident, you have the following rights, subject to certain exceptions:

1. Right to Know. The right to request, up to 2 times in a 12-month period, that we identify to you (1) the categories of personal information we have collected about you going back to January 1, 2022, unless doing so would be impossible or involve disproportionate effort, or unless you request a specific time period, (2) the categories of sources from which the personal information was collected, (3) the business or commercial purpose for collecting, selling, or sharing this information, (4) the categories of third parties with whom we share or have shared your personal information;
2. Right to Access. The right to request, up to 2 times in a 12-month period, that we disclose to you, free of charge, the specific pieces of personal information we have collected about you going back

to January 1, 2022, unless doing so would be impossible or involve disproportionate effort, or unless you request a specific time period;

3. Right to Delete. The right to request, up to 2 times in a 12-month period, that we delete personal information that we collected from you, subject to certain exceptions;
4. Right to Correct. The right to request that we correct inaccurate personal information (to the extent such an inaccuracy exists) that we maintain about you;
5. The right to designate an authorized agent to submit one of the above requests on your behalf. See below for how you can designate an authorized agent; and
6. The right to not be discriminated or retaliated against for exercising any of the above rights, including an applicant's and independent contractor's right not to be retaliated against for exercising the above rights.

You can submit any of the above types of consumer requests through any of the 2 options below:

1. Submit an online request on our website at:

   https://www.signifyhealth.com/ccpa-request

2. Call our privacy toll-free line at 855-484-1673.

How We Will Verify That it is Really You Submitting the Request

If you are a California resident, when you submit a Right to Know, Right to Access, Right to Delete, or Right to Correct request through one of the methods provided above, we will ask you to provide some information in order to verify your identity and respond to your request. Specifically, we will ask you to verify information that can be used to link your identity to particular records in our possession, which depends on the nature of your relationship and interaction with us. For example, we may need you to provide your name, email, phone number, IP address, browser ID, amount of your last purchase with the business, and/or date of your last transaction with the business.

Responding to Your Right to Know, Right to Access, Right to Delete, and Right to Correct Requests

Upon receiving a verifiable request from a California resident, we will confirm receipt of the request no later than 10 business days after receiving it. We endeavor to respond to a verifiable request within forty-five (45) calendar days of its receipt. If we require more time (up to an additional 45 calendar days, or 90 calendar days total from the date we receive your request), we will inform you of the reason and extension period in writing. We will deliver our written response by mail or electronically, at your option. The response we provide will also explain the reasons we cannot comply with a request, if applicable.

We do not charge a fee to process or respond to your verifiable request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request.

For a request to correct inaccurate personal information, we will accept, review, and consider any documentation that you provide, and we may require that you provide documentation to rebut our own documentation that the personal information is accurate. You should make a good-faith effort to provide us with all necessary information at the time that you make the request to correct. We may deny a request to correct if we have a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. If we deny your request to correct, we shall inform you of our decision not to comply and provide an explanation as to why we believe the request is fraudulent.

If You Have an Authorized Agent:

If you are a California resident, you can authorize someone else as an authorized agent who can submit a request on your behalf. To do so, you must either (a) execute a valid, verifiable, and notarized power

of attorney or (b) provide other written, signed authorization that we can then verify. When we receive a request submitted on your behalf by an authorized agent who does not have a power of attorney, that person will be asked to provide written proof that they have your permission to act on your behalf, and we will also contact you and ask you for information to verify your own identity directly with us and not through your authorized agent. We may deny a request from an authorized agent if the agent does not provide your signed permission demonstrating that they have been authorized by you to act on your behalf.

Changes to this Applicant and Candidate Policy

We may change this policy from time to time. We will post any changes to this policy on this page.