Workforce Privacy Policy

Effective date: July 5, 2024

This Workforce Privacy Policy talks about how Signify Health (also referred to herein as “Signify," "we," "us," or “our”) may collect and use personal information about our employees, job applicants, former employees, contractors and other Signify professionals located in the United States. This Workforce Privacy Policy does not apply to CVS customers, patients or health plan members.

Job applicants in the European Economic Area, the United Kingdom, and Switzerland (together, for purposes of this section, “EEA”), should refer to the General Data Protection Regulation (GDPR) Candidate Privacy Policy. Access here.

Employees, former employees, contractors, and other Signify professionals in the EEA can reach out to privacy@signifyhealth.com for a copy of the GDPR Workforce Privacy Policy.

If you have any questions or concerns about this Workforce Privacy Policy, how we collect and use your personal information, or questions about which policy applies to information you have provided, please do not hesitate to **contact us**, or call us toll-free at (855) 484-1673.

We may change this Workforce Privacy Policy. The "effective date” at the top of this page shows when it was last revised. Any changes take effect when we post the revised Workforce Privacy Policy.

If you are a California consumer, for more information about your privacy rights, please see the section of this Workforce Privacy Policy called “Your California privacy rights.”

TABLE OF CONTENTS

1. The personal information we collect

We want you to know how we collect and use your personal information. Some examples of the personal information we may collect about you include:

Information from you:

- Contact information including your name, mailing address, personal email address, personal telephone and contact numbers, emergency contacts and language preferences
- Demographic information, such as your age and date of birth, sex and gender, race and ethnicity, sexual orientation and gender identity, disability and health status and military status
- Professional information, such as resumes and cover letters, educational history and transcripts, work history, references, certifications and professional licenses
- Work eligibility and tax information, such as your social security number, spousal and dependent information and marital status
- Vehicle information, such as VIN and license plate number
- ID information, such as driver's license information, passport number, government-issued identification number and immigration/naturalization identification number
- Financial information, such as bank account numbers and beneficiary information
- Social media account information if you share it with us
- Photos or videos you provide to us
- Other information you voluntarily provide

Information created during your workforce relationship with Signify:

- Role information, such as job title, office location, start and end dates, business unit and reporting manager
- Compensation information, such as salary and wages, bonus allocations and payments, hours of work and records of absence
- Benefits information, such as insurance enrollments and 401(k) contributions
- Workforce investigations, grievances and complaints, disciplinary action and performance evaluations
- Background check and investigations information

- Information about your internet activity and related devices, including your computer's IP address and/or mobile device information (e.g., device model, operating system version, unique device identifiers, mobile network information)
- Geolocation information, including from your mobile device(s) or vehicle(s), such as GPS coordinates
- Health information, such as your health conditions
- Images or videos recorded in or around one of our office buildings (e.g., security camera footage)

We may also combine information that does not personally identify you with personal information. If we do, we will treat the combined information as personal information for as long as it stays combined. Please note, we may use and disclose de-identified information that is not in scope of this policy.

2. Sources we collect personal information from

We collect the personal information described above from the following sources.

- **Directly from you.** We collect personal information directly from you when you interact with us or our vendors through communications and automatically when you visit our websites and mobile applications.
- **From subsidiaries and affiliates.** We collect personal information from our subsidiaries and affiliates you interact with as permitted by applicable law.
- **Publicly available information and other sources.** We may collect information about you from both publicly available and other third-party sources to enhance and improve the accuracy of our information about you. We may combine the information we collect from you through the services with information we get from and about you from other online and offline sources. We may use the combined information in accordance with this Workforce Privacy Policy.

3. How we use your personal information

Depending on the nature of your relationship with us, we may use your personal information for the purposes listed below.

- **To communicate with you.** We use your personal information to respond to your requests and otherwise communicate with you. For instance, we may use your personal information to consider you for a role, contact you about your application, send you email alerts, send you newsletters and to provide you with related customer service. We may use your personal information to send marketing communications and administrative information.

- **For our internal business purposes.** We may use your personal information for our internal human resources and business purposes, such as hiring and onboarding, offboarding, financial reporting, training and data analysis. We may also use it for developing our new programs, to assess the effectiveness of our campaigns, and to operate and expand our business activities.
- **For workforce management**. We may use your personal information for payroll and tax, benefits administration, investigations and corrective actions, workforce development programs, diversity, equality and inclusion initiatives.
- **To maintain and enhance the safety and security of the workplace.** We may use personal information to detect, prevent and address safety and security issues, fraud or illegal/malicious activity. We may also use your personal information to protect the health and safety of you and others in our workplace.
- **In connection with a sale or transfer of business assets.** To consider and implement mergers, acquisitions, reorganizations and other business transactions, and where necessary to the administration of our general business, accounting, recordkeeping and legal functions.
- **To protect our legal rights and preventing misuse**. To protect the services and our business operations; to prevent and detect fraud, unauthorized activities and access and other misuse; where we believe necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety or legal rights of any person or third party or violations of our terms and conditions or this Workforce Privacy Policy.

4. How we disclose personal information

We may disclose personal information with the following parties.

- **Vendors.** We may disclose personal Information we collect to our service providers or agents who perform functions on our behalf. These may include, for example, IT service providers, help desk, payment processors, analytics providers, consultants, auditors and legal counsel.
- **Affiliates and subsidiaries**. We may disclose personal information we collect to our affiliates or subsidiaries.
- **Government or public authorities**. We may disclose personal information to a third party if (a) we believe that disclosure is reasonably necessary to comply with any applicable law, regulation, legal process or governmental request, (b) to enforce our agreements, policies and terms of service, (c) to protect the security or integrity of our services, (d) to protect the property, rights and safety of Signify, our users or the public from harm or illegal activities, (e) to respond to an emergency which we believe in the good faith requires us to disclose information to assist in preventing the death or serious bodily injury of any person, or (f) to investigate and defend ourselves against any third-party claims

or allegations.

We may disclose personal information for the following purposes:

- **To provide information to our service providers.** We may disclose personal information to our service providers. They provide services such as website hosting, data analysis, payment processing, order fulfillment, information technology and infrastructure, customer service, email delivery, auditing and other services.
- **In connection with a sale or transfer of business assets.** We may disclose or transfer your personal information to other parties if some or all of our business, assets or stock are sold, transferred or used as security. This includes in connection with any bankruptcy or similar proceeding.
- **To respond to law enforcement officials or enforce our rights.** We may disclose your personal information if required to do so by law enforcement officials or other government authorities. We disclose personal information in matters involving claims of personal or public safety, or in litigation. This may include disclosure of your personal information to allow us to pursue remedies or to limit the damages we may sustain. We may also use or disclose your information to enforce our terms and conditions, to protect our operations or those of any of our affiliates, to prevent misuse of our services, or to protect our rights, privacy, safety or property and/or that of our affiliates, you or others.
- **To maintain and enhance the safety and security of the workplace.** We may disclose personal information to detect, prevent and address safety and security issues, fraud or illegal/malicious activity. We may also disclose your personal information to protect the health and safety of you and others in our workplace.

5. Third-party service and features

The services may contain links to, or make available, third-party websites, services, features or other resources not run by us or on our behalf (the “Third-Party Services.”) We make these Third-Party Services available as a convenience to you and are not affiliated with, endorsing or sponsoring the Third-Party Services.

Any information you give to such third parties is not subject to the terms of this Workforce Privacy Policy. We are not responsible for the privacy or security of the information you give to Third-Party Services or how they handle your information. We also are not responsible for the information collection, use, sharing or security practices of Third-Party Services. You should review the privacy policy of any Third-Party Service to whom you give information in connection with the services.

6. Security

We use reasonable physical, technical and administrative safeguards. Please be aware that despite our efforts, no data security measures can guarantee security. You should take steps to ensure your personal information is protected like using passwords that would be difficult to guess, not using the same password for multiple accounts and periodically changing your password.

7. Cookies and other technologies

What are cookies? Cookies are small computer files we transfer to your computer's hard drive. These are usually small text files. You can set your browser to accept or reject cookies. Instructions for resetting the browser are in the "help" section of most browsers.

How we use cookies. Like many other websites and online services, we collect traffic and usage patterns. We use cookies, web server logs and similar technologies to do this.

We use this information for various purposes:

- To ensure that the services function properly
- To help with navigation (or how you find your way around the site)
- To understand use of the services
- To diagnose problems
- To measure the success of our talent campaigns
- To otherwise administer the services

We also use cookies to collect and receive certain information about a website user, such as the type of web browser used, internet service provider ("ISP"), referring/exit pages, operating system, date/time stamp, clickstream data, device platform, device version and/or other device characteristics including your choice of settings such as Wi-Fi, Bluetooth and Global Positioning System ("GPS"), CPU ID and type, build, model, manufacturer, operating system version, screen size, screen resolution, mobile network status, device locale and carrier ID. We review our web server logs and usage of our sites. This helps us to gather statistics on how many people are using our sites and why.

Internet providers assign your device an IP address number. We may identify and log your IP address automatically in our web server log files when you use our services. We may also collect the time of your visit and the pages you look at. We use IP addresses to do things like gauge usage levels of the services, help find server problems, and administer services.

Our services use tracking technologies to collect and record your activities and movements across our websites throughout your browsing session, including page hits, mouse movements, scrolling, typing, out-of-the-box errors and events and API calls (“Session Data”). We use this information to (1) remember your information so you do not have to re-enter it, (2) track and understand how you use and interact with the services, (3) perform analytics, (4) measure the usability of the services and the effectiveness of our communications; and (5) improve our products, services and your experience. Such tracking may also include recorded sessions, which we may play back for these purposes. We may share session data with our vendors (which may change over time) for these purposes.

Do-Not-Track. Our websites are not designed to respond to “do-not-track” signals received from browsers.

8. Contact information

If you have any questions or concerns about the way we collect and use your information, **contact us.**

If you have any other questions about the content of this Workforce Privacy Policy contact the Signify Health Privacy Office at the address below.

Signify Health
Attn: Privacy Office
4055 Valley View Lane, Ste 400

Dallas, TX 75244
(855) 484-1673

9. Your California privacy rights

This section supplements the Workforce Privacy Policy and applies solely to California employees, job applicants, former employees, contractors and other Signify professionals about whom we have collected personal information from any source, including through the use of our website(s), mobile applications or other online services, or by communicating with us electronically, in paper correspondence or in person (collectively, "you"). Under the California Consumer Privacy Act, as amended by the California Privacy Rights Act of 2020 (the “CCPA”), California residents have the right to receive certain disclosures regarding our information practices related to “personal information,” as defined under the CCPA.

This section does not address or apply to our information practices that are not subject to the CCPA, such as:

- **Publicly available information**. Information that is lawfully made available from government records, information we have a reasonable basis to believe is lawfully made available to the general public by you or by widely distributed media or by a person to whom you have disclosed the information and not restricted it to a specific audience.
- **Deidentified information**. Information that is deidentified in accordance with applicable laws.
- **Aggregated information**. Information relates to a group from which individual identities have been removed.
- **Protected health information**. Information governed by the Health Insurance Portability and Accountability Act or California Confidentiality of Medical Information Act.
- **Activities covered by the Fair Credit Reporting Act**. This includes information we receive from consumer reporting agencies that are subject to the Fair Credit Reporting Act e.g., information contained in background check reports we obtain as part of our vetting process.
- **Trade secret and intellectual property of Signify**. This includes our confidential business information and intellectual property.

The terms used in this section have the same meaning given to them in the CCPA.

A. What personal information we collect

We may collect the following categories of personal information (as enumerated in the CCPA) about you. For more information about the personal information we collect, please see Section 1 above.

- **Identifiers**, which may include your name, mailing address, personal email address, and personal telephone number
- **Professional or employment-related information**, such as your employment history, information relating to your compensation, benefits information, information from background checks or references, information relating to your performance evaluations, hours of work and records of absence and other information that may be provided on your resume
- **Commercial information**, such as VIN or vehicle license plate number
- **Information relating to internet activity or other electronic network activity**, which may include your device and browser information, interactions with our websites or mobile sites, mobile apps, Wi-Fi, emails, communications and social media

- **Geolocation data**, including from your mobile device(s) or vehicle(s), such as Global Positioning System ("GPS") coordinates
- **Audio, electronic or visual information**, which may include images you provide to us (e.g., when you upload photos or videos) or that are viewed or recorded on a security camera
- **Education information**, such as education history, educational degrees and academic transcripts
- **Protected classification characteristics under California or federal law**, such as your age and/or date of birth, gender or gender identity, nationality and national origin, race or ethnicity, marital status, criminal history, drug test results and trade union membership
- **Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))**, such as your health insurance information and workers' compensation claim information, signature and physical characteristics or description

We may also collect the following categories of sensitive personal information about you:

- **Government identification,** such as government issued identifications (e.g., SSN)
- **Account log-in information,** which may include your account username and passwords
- **Demographic information**, such as racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership
- **Precise geolocation data**, such as the GPS coordinates of any corporate devices assigned to you
- **Biometric information**, such as your fingerprint or other biometric identifiers
- **Information concerning your health**, such as your health conditions or information made available via connected health devices (e.g., smart watches, health apps)
- **Information concerning sexual orientation**, as part of our employment reporting obligations and diversity, equality and inclusion initiatives

We do not collect, use or disclose sensitive personal information about employees beyond the purposes authorized by the CCPA.

B. How long we retain personal information

We retain your personal information only as long as necessary and in alignment with our data retention schedules. Information may be retained to comply with applicable law, adhere to contractual requirements, in anticipation of litigation or a legal matter or as otherwise necessary and proportionate to provide you with a product or service.

C. What we do with personal information

We may use your personal information for the purposes described above in Section 3 of our Workforce Privacy Policy and for the following business and commercial purposes specified in the CCPA:

- Performing services, including maintaining or servicing employment related activities, providing customer service, processing or fulfilling requests, verifying your information, processing payments, providing analytics services or providing similar services
- Auditing related to applicant and employment related activities, including, but not limited to, auditing compliance
- Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity and prosecuting those responsible for that activity
- Debugging to identify and repair errors that impair existing intended functionality
- Undertaking internal research for technological development and demonstration
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade or enhance the service or device that is owned, manufactured, manufactured for or controlled by us

D. Sources of collected personal information

We may collect personal information about you from these sources:

- Directly from you or your device, including your use of our websites and mobile applications, and your communications with us
- Our subsidiaries and affiliates
- Our service providers, including but not limited to, technology/website hosting providers, analytics providers, and systems administrators/security and fraud investigations providers
- Advertising networks and social media networks
- Government entities, regulators and law enforcement
- Third parties, including companies that collect and sell publicly available information, or business partners that collect information and provide it to us according to their privacy policies and terms of service

E. What personal information we disclose and who we disclose personal information to

The following table describes the categories of personal information we disclose and the categories of third parties to whom we disclose personal information. For more information about how we disclose personal information, please see Section 4 above.

Categories of Personal Information	Categories of Third Parties
Identifiers	- Subsidiaries and affiliates; clients - Government entities, regulators and law enforcement
Commercial information	- Government entities, regulators and law enforcement
Information relating to internet activity or other electronic network activity	- Subsidiaries and affiliates - Regulators, government entities and law enforcement
Geolocation data	- Subsidiaries and affiliates - Government entities, regulators and law enforcement
Audio, electronic or visual information	- Government entities, regulators and law enforcement
Education information	- Subsidiaries and affiliates - Government entities, regulators and law enforcement
Professional or employment-related information	- Government entities, regulators and law enforcement
Other personal information not listed above and described in California Civil Code § 1798.80(e)	- Subsidiaries and affiliates - Government entities, regulators and law enforcement
Sensitive personal information	- Government entities, regulators and law enforcement
Information not listed above and related to characteristics protected under California or federal law	- Subsidiaries and affiliates - Government entities, regulators and law enforcement

We do not sell or share your personal information to third parties.

We do not knowingly sell the personal information of minors under 16 years of age.

F. Your privacy rights

If you are a California consumer, you have the following rights under the CCPA with respect to your personal information.

- **Right to know/access.** With respect to the personal information we have collected about you, you have the right to request from us (up to twice per year

and subject to certain exemptions): (i) categories of personal information about you we have collected; (ii) the sources from which we have collected that personal information; (iii) our business or commercial purposes for collecting, selling, or disclosing that personal information; (iv) the categories of third parties to whom we have disclosed that personal information; and (v) a copy of the specific pieces of your personal information we have collected.

- **Right to delete.** Subject to certain conditions and exceptions, you may have the right to ask us to delete certain personal information we have collected from you. Please note, Signify is not obligated to delete personal information that is: (i) necessary to provide services that you request (such as benefits and compensation) or (2) required to comply with applicable laws.
- **Right to correction.** You may have the right to ask us to correct inaccuracies in the personal information we have collected.
- **Right to non-discrimination.** We will not discriminate against you if you exercise any of these privacy rights.

How to submit a request

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.

You may also give someone else permission to exercise these rights for you. To submit a request as an authorized agent on behalf of a consumer, write us at privacy@signifyhealth.com or call us at 855-484-1673. We will need proof showing you have asked someone else to make a request on your behalf, which may include a Power of Attorney form or other signed document. If we have information on your minor child, you may exercise these rights for them.

Verifying requests

Before we fulfill a request, we must verify your identity and ability to exercise these rights. There are also some exclusions and exceptions that may apply. You will be asked to give us certain personal information via webform or on the phone we may require you to provide any of the following information: Full legal name, email address, phone number, position(s) applied for, office location applied to and/or home address (depending on the information you may have provided). In addition, if you ask us to provide you with specific pieces of personal information, we may require you to sign a

declaration under penalty of perjury that you are the consumer whose personal information is the subject of the request.