Workforce Member Privacy Policy

Last Updated: May 6, 2024

Our Commitment to Privacy

Generations Healthcare ("Generations Healthcare," "we," or "us") has developed and implemented this privacy policy ("Workforce Member Privacy Policy") to demonstrate its commitment to privacy for individuals who are or are seeking to become a member of Generations Healthcare' workforce. This Workforce Member Privacy Policy is designed to assist workforce members and candidates ("you") in understanding how we collect, use, share, and safeguard personal information as part of your working relationship with us.

To Whom This Workforce Member Privacy Policy Applies

This Workforce Member Privacy Policy applies to individuals in connection with their status as a workforce member or candidate (collectively "workforce members"). Our privacy practices with respect to personal information collected in other contexts, including visiting the Generations Healthcare Website, can be found in our Generations Healthcare Privacy Policy.
Except as may be specifically required by law, this Workforce Member Privacy Policy does not apply to information available from a public source (such as a telephone directory) or to aggregated or de-identified information we may collect about our workforce, nor to references to workforce members in company work product.

How We Define Personal Information

Personal information (sometimes called "personal data") is a broadly defined term whose legal definition varies across jurisdictions. When used in this Workforce Member Privacy Policy, "personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an individual.

What Personal Information We Collect

The Personal Information that we collect and use about you may include:

- **Application information** as part of your candidacy to become a workforce member, for example, your resume, C.V., application form information, transcripts, recommendations letters, interview recordings and transcripts, and other application materials.
- **Contact information** including your name, email address, telephone number, postal address.
- **Personal details** including your title, name preferences, and date of birth.
- **Right to Work information** including your work permit and visa application information.
- **Payroll information** including your bank account details and tax information.
- **Benefits information**, for example, information to provide and maintain retirement, health, and other benefit program services or products.

- **Medical and/or health information**, for example, medical examination results, vaccination status, reported medical and health conditions disclosed to us.
- **Performance evaluation information** including information about, and assessments of, your performance which are collected as part of the personnel review process.
- **Location information**, including through GPS tracking technology on devices owned by us or other devices owned by you which you use in connection with your services to Generations Healthcare.
- **Attendance records**, for example, time clock records, vacation days, or personal time off available/ taken.
- **Security information**, for example, security badge information, premises surveillance recordings, premises access logs, and parking access records.
- **Safety and disciplinary information**, for example, information in connection with disciplinary action or investigations.
- **Systems information** which includes information about your use of our systems or information that you provide to us through our systems, e.g., information from your company email account, information posted on our website, information you submit through applications or software made available to you.
- **Expenses and transaction information**, for example, payment receipts you provide for goods, services, and other expenses you incur in your capacity as workforce member, such as travel expenses.
- **Sensitive Personal Information**, including your social security number, driver's license number, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, and biometric information.
- **Other information.** Any other information that you provide directly to us or that we receive in connection with your working relationship Generations Healthcare.

How We Collect and Disclose Workforce Member Personal Information

The purpose for which personal information will be collected and processed will be consistent with your role as a workforce member at Generations Healthcare. Because each workforce members relationship with the company varies based on that person's role, location, experience, performance, and other factors, the type, nature, and amount of personal information Generations Healthcare may seek to collect from you or process about you will vary.

Collecting Personal Information

We collect personal information about our workforce members from a variety of source, but primarily from the members themselves. In addition, we gather personal information through workforce members' interaction with Generations Healthcare systems and personnel, and we receive personal information from third parties who provide it to us. The following is a list of the sources from which we may collect personal information.

- **Candidate Recruiting Partners**. These are the persons or entities who assist in facilitating recruitment and review of candidates to become workforce members. These entities include recruiting firms, job search services, social media companies (e.g., LinkedIn), and professional recruiting agents. We may also collect personal information from any other person or entity with

whom you provide a reference, including past employers, personal references, former colleagues, and others.

- **Human Resources Service Providers**. These are the persons or entities who assist in providing human resources and workforce management services, including background check providers, human resources software services providers, insurance providers, employee payment and benefits providers, governmental entities, and similar entities.

- **Business Services Providers**. These are those persons or entities with whom we have a relationship to provide business operations services and support to Generations Healthcare. These providers may include the following:

    - **IT Operations Providers**. These include cloud computing service providers, internet service providers, data backup and security providers, functionality and infrastructure providers, and similar service providers.

    - **Professional Service Providers**. These include lawyers, accountants, consultants, security professionals, and other similar parties when disclosure is reasonably necessary to comply with our legal and contractual obligations, prevent or respond to fraud or abuse, defend ourselves against attacks, or protect the rights, property, and safety of us, our customers, and the public.

    - **Operations Providers.** These include service provider with whom we partner to provide day-to-day business operations, including real estate advisors, event planners, food services providers, entertainment providers, payment processors, banks, facilities management providers.

    - **Affiliates.** Our affiliates include our parent company, subsidiaries, joint venturers, or other companies that we control or that are under common control with us, including Generations Healthcare.

    - **Governmental Entities**: These are governmental agencies that may provide information about workforce members.

We may also collect personal information from any other person or entity with whom you interact in the scope and course of a workforce members affiliation with Generations Healthcare. For example, we may collect personal information about you from customers, business contacts, and the public.

Disclosing Personal Information

We may disclose personal information to any of the entities identified as sources of personal information. We may also disclose any personal information to the following:

- **Legally Required Parties.** Persons to whom we are required by law to provide information, such as pursuant to a subpoena or a court order, or to a regulatory agency.

- **Reorganization Recipients.** Persons involved in the consideration, negotiation, completion of a business transaction, including the sale, merger, consolidation, acquisition, change in control, transfer of substantial assets, bankruptcy, or reorganization, and any subsequent integration.

- **Authorized Recipients:** To any party when authorized by the individual to whom it pertains to share it.

How We Use Workforce Member Personal Information

We use the personal information we collect as follows:

- **To Process Employment Applications and Onboard New Hires**: We collect most personal information to evaluate your candidacy, including to open and maintain candidate records, communicate with you, conduct employment related background screening and checks, and evaluate your application.
- **Recruiting and Workforce Member Communications**. We use personal information to communicate with you as part of the candidacy process and as part of your workforce relationship with us. Personal information may be used to evaluate career development, consider candidates for roles and positions, and to communicate company policies.
- **Business operations.** We use personal information to conduct our business operations, including management of staffing resources, financial planning, corporate compliance, internal audits, and other business administration needs.
- **Compensation and Benefits Management**. We collect and process personal data to provide payment and benefits to our workforce members and to ensure we are legally compliant when doing so.
- **Onboarding and Training**. We collect data for integrating new hires into our systems and to provide staff training, feedback, disciplinary procedures, and investigations to meet our business interests in ensuring our staff are best able to carry out their roles.
- **For Diversity and Equal Opportunity Monitoring.** Where permitted by law, you have the option to provide certain sensitive personal information, such as race or ethnic origin, for the purposes of equal opportunities monitoring. If you decide not to provide this information, your application will not be prejudiced. You may also tell us if you have a disability, so that we can make appropriate arrangements for you to attend our offices and/or participate in an interview.
- **To Maintain Security at Our Premises**. If you attend in-person interviews at our offices or facilities, we may collect information related to your access to our building. This may include data related to your use of security control systems, audio and video captured on security cameras, and visitor logging information.
- **To Conduct Evaluations.** We collect and review your personal information from multiple sources to assess your suitability for employment or work with Generations Healthcare. This may include obtaining pre-employment background checks.

- **Safety and Security Purposes**. We use personal information in connection with the monitoring of our physical and digital ecosystem (which includes using technology to monitor your interaction with our devices and systems). We also us it to report on security and safety incidents, notify emergency contacts, and provide reasonable care when applicable.
- **Travel and Entertainment**. We use information to travel and entertainment administration.
- **Enforce our Generations Healthcare Policies**. We use personal information to support and maintain compliance with our company policies, procedures, and operations.
- **Required Disclosures:** We may disclose personal information to comply with applicable legal and regulatory requests and obligations (including investigations).
- **Legal Defense:** We may process personal information to establish or defend legal claims and allegations.
- **Security Purposes:** We process personal information in connection with the prevention, detection, or investigation of fraud, suspected or actual illegal activity, or other misconduct and the resultant harms or impacts to individuals.
- **Professional Advice:** We may process personal information in connection with seeking advice from lawyers, auditors, and other professional advisors.
- **For Similar Purposes**: When necessary or advisable we may process your personal information for purposes like those mentioned above, and consistent with the purpose for which you provided your personal information.

Retention of Personal Information

We will retain personal information only for so long as necessary to fulfill the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider: (i) the amount, nature, and sensitivity of the personal information; (ii) the potential risk of harm from unauthorized use or disclosure of your personal information; (iii) the purposes for which we process your personal information and whether we can achieve those purposes through other means; and (iv) the applicable legal requirements. In some circumstances, you may ask us to delete your personal information. Additionally, we may anonymize your personal information (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

How We Protect Personal Information

We have implemented and maintain reasonable security procedures and practices, appropriate to the nature of the information, to protect your personal information from unauthorized access, destruction, use, modification, or disclosure. However, no security measure is perfect, so we cannot guarantee the security of your personal information. Periodically, our operations and business practices are reviewed for compliance with policies and procedures governing the security, confidentiality, and quality of our information. Our corporate values, ethical standards, policies, and practices are committed to the

protection of customer information. In general, our business practices limit employee access to confidential information and limit the use and disclosure of such information to authorized persons, processes, and transactions.

Children's Personal Information

We do not consider candidates for employment under the legal working age for the jurisdiction in which employment is to be offered. We do not knowingly collect, process, sell or share the personal information of individuals under the age of 18. If you believe that a child under 18 may have provided us their personal information, please contact us at 800-461-3560.

Your Privacy Choices

Some jurisdictions provide covered individuals with specific privacy rights which can be exercised against covered entities. Depending on the jurisdiction, these rights may include:

- **Access.** The right to know (or confirm) what personal information a business has collected about you.
- **Deletion**. The right to request that a business delete personal information it has collected from you, subject to certain exception.
- **Correction**. The right to request correction of inaccurate personal information maintained by the business.
- **Opt-Out of the Sale/Sharing of Your Personal Information**. The right to opt-out of the sale of your personal information to third parties. The term "sale" varies by jurisdiction, but sometimes includes the right to opt-out of the use of personal information for targeted advertising purposes.
- **Limitation**. The right to limit a business's use or disclosure of certain information, typically sensitive personal information. However, Generations Healthcare does not use or disclose sensitive personal information for any purpose other than for permissible purposes under California law.
- **Opt-out of Profiling:** The right to opt- out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning you.
- **Non-Discrimination**. The right not to be discriminated against for exercising any of the rights conferred at law.

Generations Healthcare will honor the privacy rights afforded to individuals in accordance with applicable law.

You may make a request at any time to exercise your privacy rights listed above by emailing us at hrsupport@lifegen.net. We will respond to your request within a reasonable period (if properly submitted) and in accordance with applicable law. If we need more time to process and respond to your request, we

will notify you of that fact along with the reason for the delay. If we decline to act regarding your request, we will inform you of our decision and the reason for it, and, if applicable, with instructions on how you may appeal our decision.

International Data Transfers

Generations Healthcare is based in the United States, and we operate our websites and portals from there. The laws that apply to the use and protection of personal information in the United States, or other countries or jurisdictions in which we transfer or process personal information, may be different from the laws and protections in your country. By submitting personal information to us, including by accessing our website and portals, you understand that we may process, store, and transfer your personal information in and to jurisdictions foreign to you, including the United States. Whenever we engage a service provider, we require that its privacy and security standards adhere to this policy and applicable privacy laws.

Updates to Our Workforce Member Privacy Policy

We may update this Workforce Member Privacy Policy from time to time. If we make changes, we will notify you by revising the date at the top of the Notice and, in some cases, we may provide you with additional notice (such as adding a statement to our website homepage or sending you a notification).

Contacting Us

To ask questions or comment about this Workforce Member Privacy Policy and our privacy practices, contact us at hrsupport@lifegen.net.

Supplemental Notice for Residents of California

This section supplements our notice provided above and applies to residents of the State of California. The California Consumer Privacy Act requires that we describe the personal information we collect, disclose, and sale/share based on certain defined categories. To make it easier to read and understand our policy, we have presented the relevant information in a chart explaining our collection, use, and disclosure practices related to workforce members.

Categories of Personal Information	Categories of Sources from which the Information was Collected	Categories of Third Parties to whom this type of Personal Information is Disclosed for a Business Purpose	Types of Third Parties with Whom this Category of Personal Information Is Shared/ Sold
Identifiers (e.g., name, signature, address, telephone email, account name, SSN, DL number, passport number, online identifier, IP address)	• Workforce Members directly • Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	• Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We do not sell or share personal identifiers in the context of a workforce member relationship. Please see our general privacy policy for the identifiers we sell about consumers generally.
Customer Records (as defined in Cal. Civ. Code § 1798.80(e))	• Workforce Members directly • Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	• Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We do not sell or share
Protected Classifications (e.g., Age, race, color, ancestry, national origin, citizenship, religion or creed, marital status).	• Workforce Members directly • Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	• Human Resources Service Providers • Business Operations Service Providers • Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We do not sell or share

Commercial Information (e.g., records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies).	We do not collect commercial information in the context of a workforce member relationship. Please see our general privacy policy for the commercial information we collect about consumers generally.	• Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We do not sell or share commercial information in the context of a workforce member relationship. Please see our general privacy policy for the commercial information we sell about consumers generally.
Biometric Information (e.g., fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data).	• Workforce Members directly	• Other Workforce Members • Human Resources Service Providers • Business Services Providers	We do not sell or share
Internet/Network Activity (e.g., you interactions with device, software, websites, and networks we operate or use).	• Workforce Members directly • Business Services Providers	• Business Services Providers	We do not sell or share this information in the context of a workforce member relationship. Please see our general internet information we sell about consumers generally.
Geolocation Data	We may gather your geolocation based on your address, IP address, or other data associated with a particular location. If you are using company-equipment that collects geolocation, we may associate that geolocation with you.	• Business Services Providers	We Do Not Sell
Sensory Data (e.g., Audio, electronic, visual, thermal, olfactory, or similar information).	We may collect your image, voice, electronic activity, or other sensory data through recording devices such as a security camera, call recording device, or thermal image scanner.	• Other Workforce Members • Business Services Providers • Affiliates • Governmental Entities	We Do Not Sell
Professional or employment-related information (e.g., Current or past job history or performance evaluations).	• Workforce Members directly • Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Affiliates • Governmental Entities	• Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We Do Not Sell

Education Information (e.g., Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records).	• Workforce Members directly • Educational institutions • Candidate Recruiting Partners	• Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We Do Not Sell
Inferences drawn from other personal information (e.g., profile information reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes).	We do not collect inferences but we may make inferences about workforce members based on the personal information we have collected. For example, we may make inferences regarding a workforce members' suitability for a particular position or task.	We do not disclose inferences we make outside of the company, but we may store inferred personal data with our Business Service Providers (for example, our cloud storage providers).	We Do Not Sell
Sensitive Personal Information	• Workforce Members directly • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	• Other Workforce Members • Candidate Recruiting Partners • Human Resources Service Providers • Business Services Providers • Affiliates • Governmental Entities	We Do Not Sell

Exercising Your CCPA Rights

California Residents have certain rights under the CCPA. For information on how to exercise these rights, please see below.

Submitting Access, Deletion, and Correction Requests

To make an access, deletion, correction, or limitation request, please email us at hrsupport@lifegen.net, or call us at 714-241-5600.

After we receive your request, to ensure the security of the information we store and consumers' privacy, we will verify that you are appropriately affiliated with the subject of the request, either as the consumer or as an authorized agent or guardian of the consumer. We may ask you to provide a few pieces of information to confirm your identity in our records.

You may designate an authorized agent to exercise your rights under the CCPA on your behalf. You must provide the authorized agent written permission to exercise your rights under the CCPA on your behalf and we may deny a request from an agent on your behalf if we cannot verify that they have been

authorized by you to act on your behalf. Even if you use an authorized agent to exercise your rights under the CCPA on your behalf, pursuant to the CCPA we may still require that you verify your own identity directly to us. This provision does not apply if you have provided a power of attorney under the California Probate Code.

Limiting the Use of Your Sensitive Personal Information

Californian's have the right to limit a business's use or disclosure of sensitive personal information. However, Generations Healthcare does not use or disclose sensitive personal information for any purpose other than for permissible purposes under the CCPA.

Opting Out of the Sale/Share of Your Personal Information

Generations Healthcare does not sell or share personal information related to the workforce member relationship. Please review the Generations Healthcare Privacy Policy for more information about opt-out rights for website visitors.

Contact Us Regarding Your Privacy Rights

If you would like additional information related to your privacy, please email us at hrsupport@lifegen.net Please submit your CCPA rights requests using the methods described above.