Walgreens California Workforce Privacy Notice

Introduction

At Walgreens, we are committed to maintaining our Workforce Members' privacy. This California Workforce Privacy Notice ("**Workforce Notice**") is intended to explain to Walgreens job applicants and active or former employees and contractors, who are California residents ("**Workforce Members**"), Walgreens practices regarding the collection, use, and disclosure of their "Personal Information" and "Sensitive Personal Information," as defined under California law ("**Workforce Personal Information**"). As described in more detail below, Workforce Members may have rights with regard to how we use and disclose Workforce Personal Information.

Categories of Workforce Personal Information We Collect

The Workforce Personal Information we collect about you may vary depending on whether you are a job applicant, employee, or contractor. In the 12 months prior to the date of this Workforce Notice, we may have collected the following types of categories and specific pieces of Workforce Personal Information, which we may continue to collect:

- **Identifiers,** such as name, address, phone number, email address, government identification numbers, date of birth, social security number, ethnicity, family-related data (e.g., marital status, information on family members);
- **Characteristics of protected classifications,** such as race, gender, ethnicity, disability information (if provided voluntarily), military and veteran status (if provided voluntarily), maternity leave information;
- **Internet and other electronic network activity information,** such as location information, communication information and computer usage information related to your use of company equipment, systems, applications, and other resources;
- **Audio, visual, or similar information** such as photographs, store security video, audio recordings;
- **Professional or employment-related information,** such as previous employment, worker status, organization information, compensation information, payroll information, leave information, performance and talent information, employment background, functional experience, leadership experience, honors or awards, background information commonly used for security screenings, qualifications, evaluations, developmental planning, career interest and development information, and other talent management and team based assessments;
- **Biometric information,** such as fingerprint, face, and voice recordings;
- **Education information,** such as education, training, qualifications, and certifications;
- **Sensitive Personal Information** such as driver's license, state identification card, or passport number, social security number, racial or ethnic origin, union membership, fingerprint, face, voice recordings, account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, the contents of email, and information concerning your sexual orientation (if provided voluntarily) and health; and
- **Other information**, such as sick day information, health information for workplace safety, designated emergency contact information, work-related accidents information, monitoring information, and any other information reasonably necessary for us to carry out our legal and regulatory obligations.

How We Use Workforce Personal Information

We may use Workforce Personal Information to administer the workforce relationship, including to:

- Conduct background checks and determine eligibility for employment;
- Establish, manage, or terminate the employer/employee relationship subject to and in accordance with Walgreens' policies and procedures;
- Administer payroll and company benefits pursuant to Walgreens' employee benefit plans;
- Establish and maintain emergency contacts;
- Process work-related claims (e.g., workers compensation) and leave of absence requests;
- Internal recordkeeping, auditing, and reporting;
- Protect the safety and security of the workforce and facilities; and
- Other activities as needed for legitimate business or legal purposes.

Sources. We may collect certain categories of Workforce Personal Information from you, publicly available sources, and third parties. The categories of sources from which we collected Workforce Personal Information in the 12 months prior to the date of this Workforce Notice include the following:

- When you communicate with us or perform activities as a job applicant or Workforce Member
- Data Suppliers (e.g., recruitment providers or companies that perform background checks)
- Service Providers (e.g., companies that administer company benefits or provide payroll support)

We will continue to collect Workforce Personal Information from these same sources.

Retention. We retain Workforce Personal Information for the purposes described in the "How We Use Workforce Personal Information" section above. Retention of your Workforce Personal Information may also be required to maintain our employment relationship with you, administer employment benefits, or for us to fulfill a legal obligation. Once no longer needed for these purposes, we will not retain your Workforce Personal Information in our systems.

Sharing your Workforce Personal Information for business purposes. In the 12 months prior to the date of this Workforce Notice, we shared and we may continue to share the following categories of Workforce Personal Information with third parties who are considered "service providers" as defined under California law since we disclose Workforce Personal Information to them for our business purposes.

- **Identifiers,** such as name, address, phone number, email address, government identification numbers, date of birth, social security number, ethnicity, family-related data (e.g., marital status, information on family members);
- **Characteristics of protected classifications,** such as race, gender, ethnicity, disability information (if provided voluntarily), military and veteran status (if provided voluntarily), maternity leave information;
- **Internet and other electronic network activity information,** such as location information, communication information and computer usage information related to your use of company equipment, systems, applications, and other resources;
- **Audio, visual, or similar information** such as photographs, store security video, audio recordings;

- **Professional or employment-related information,** such as previous employment, worker status, organization information, compensation information, payroll information, leave information, performance and talent information, employment background, functional experience, leadership experience, honors or awards, background information commonly used for security screenings, qualifications, evaluations, developmental planning, career interest and development information, and other talent management and team based assessments;
- **Biometric information,** such as fingerprint, face, and voice recordings;
- **Education information,** such as education, training, qualifications, and certifications;
- **Sensitive Personal Information** such as driver's license, state identification card, or passport number, social security number, racial or ethnic origin, union membership, fingerprint, face, voice recordings, account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, the contents of email, and information concerning your sexual orientation (if provided voluntarily) and health;
- **Other information**, such as sick day information, health information for workplace safety, designated emergency contact information, work-related accidents information, monitoring information, and any other information reasonably necessary for us to carry out our legal and regulatory obligations.

As described above, examples of business purposes include performing services on our behalf, internal operations, prevention of fraud and other harm, and legal compliance.

The categories of third party service providers to which we may share the above described categories include Benefits Administration Companies, Payroll Service Providers, Recruitment Agencies, Data Analytics Providers, Fraud Prevention Providers, Cloud Storage Providers, IT Service Providers, Professional Service Providers, and Delivery Partners.

In addition, we may share the aforementioned categories of Workforce Personal Information with third parties involved in the evaluation of or entry into the sale or purchase of stores or company assets, mergers, or acquisitions. The categories of third parties to which we may share the above described categories of Workforce Personal Information include potential Business Partners or Purchasers, Professional Service Providers (e.g., consultants, lawyers, accountants), and Data Analytics Providers. In the event of sale, merger, or acquisition, employee information (including Workforce Personal Information) generally is one of the transferred business assets, as is permissible under law.

Sale and Sharing of Workforce Personal Information. In the 12 months prior to the date of this Workforce Notice, we have not "sold" or "shared" your Workforce Personal Information or Sensitive Personal Information with third parties, who are considered "third parties" as defined under California law, for secondary purposes.

Opting Out of the Sale and Sharing of Workforce Personal Information. Although we do not "sell" or "share" your Workforce Personal Information, as defined under California law, you may communicate your preference to prevent any future disclosure of your Workforce Personal Information to these entities for their use for secondary purposes by opting-out of the sale or sharing of your Workforce Personal Information. Should our sharing practices change in the future, such that the sharing may constitute a "sale" or "sharing" of your Workforce Personal Information under California law, we will

update this Workforce Notice and honor any opt-out requests you previously submitted. You can submit an opt-out request through this link **here** or by contacting us at 800-925-4733.

Limiting Use and Disclosure of Sensitive Personal Information. We may collect certain categories of Workforce Personal Information from you and third parties as described in the "Categories of Workforce Personal Information We Collect" section above that may be considered "Sensitive Personal Information" under California law. We use your Sensitive Personal Information to perform services reasonably expected in an employment relationship. Although we do not intend to use or disclose your Sensitive Personal Information in a manner that would be subject to limitation, you may communicate your preference to limit our use and disclosure of your Sensitive Personal Information should our sharing practices change in the future. You can submit a request to limit through this link **here** or by contacting us at 800-925-4733.

California Workforce Rights. As a California resident, you have the right to request and access, including in a portable, machine-readable format, any or all of following types of information regarding the Workforce Personal Information we have collected about you from January 1, 2022, to the date of receipt of your request:

- Specific pieces of Workforce Personal Information we have collected about you;
- Categories of Workforce Personal Information we have collected about you;
- Categories of sources from which such Workforce Personal Information was collected;
- Categories of Workforce Personal Information we sold or disclosed for a business purpose about you; and
- The business or commercial purpose for collecting or selling your Workforce Personal Information.

You also have the right to request correction or deletion of your Workforce Personal Information and to opt out of the sale or sharing and automated processing ("profiling") of your Workforce Personal Information. In addition, you have the right to limit the use and disclosure of your Sensitive Personal Information and appeal our refusal to act on your request.

- **Exercising California Workforce Rights.** You or your authorized agent may submit a request to exercise your California Workforce Rights by using one of the following specifically designated methods:
    - Click the following link and confirm your choices:

      Exercise California Workforce Privacy Rights
    - Contacting our Customer Care Center at 800-WALGREENS (800-925-4733)
- Active Workforce Members may also access and update certain Workforce Personal Information using internal Human Resources tools.

- **Responding to Requests.** For requests for access, correction, deletion, or appeal, we will first acknowledge receipt of your request within 10 business days of receipt of your request. We provide a substantive response to your request as soon as we can, generally within 45 days from when we receive your request, although we may be allowed to take longer to process your request under certain circumstances. If we expect your request is going to take us longer than normal to fulfill, we will let you know.

  For requests to opt out of the sale or sharing or to opt out of automated processing, known as "profiling" under California law, of your Workforce Personal Information or request to limit the use and disclosure of your Sensitive Personal Information, we will comply within 15 business days after receipt of your request.

  We usually act on requests and provide information free of charge, but we may charge a reasonable fee to cover our administrative costs of providing the information in certain situations. In some cases, the law may allow us to refuse to act on certain requests. When this is the case, we will endeavor to provide you with an explanation as to why.

- **Requests By Authorized Agents.** You may designate an agent to submit requests on your behalf. The agent must be a natural person or a business entity that is registered with the California Secretary of State.

  If you would like to designate an agent to act on your behalf, your agent must provide us your Workforce Personal Information as required on the request form and provide signed documentation demonstrating that you authorized the agent to submit a request on your behalf. For access and correction requests, the agent must also follow the verification process outlined below.

  Please note that this subsection does not apply when an agent is authorized to act on your behalf pursuant to a valid power of attorney. Any such requests will be processed in accordance with California law pertaining to powers of attorney.

- **Verification of Requests.** Our verification process depends on the type of request you submit to exercise a California Workforce Right as described above.

  <u>Access and Correction Requests</u>
  For Access and Correction requests, if you are a job applicant or former employee or contractor, you will enter a two-part verification process. You must verify your identity by correctly answering demographic questions powered through LexisNexis® and confirm control over the email address you provide in the request form. Active employees and contractors will be required to complete Single Sign-On instead of LexisNexis®. If you successfully complete the LexisNexis® demographic questions and email confirmation or Single Sign-On (for active employees and contractors), you will proceed to part two of the process in which we will attempt to match the data provided in the request form to the data we maintain. If you are matched to a reasonably high degree of certainty, your request will be processed as follows:

- **Access request:** Your access report will include the specific pieces of Workforce Personal Information not otherwise subject to an exception pursuant to law that we match to you. If requested, your access report will also be provided in a portable, machine-readable format.
- **Correction request:** If we determine the contested data to be inaccurate based on the totality of the circumstances, unless otherwise subject to an exception pursuant to law, your data will be corrected.

Active employee and contractor requests that fail Single Sign-On cannot be completed. If you fail the LexisNexis® demographic questions but successfully complete email confirmation, you proceed to part two of the process in which we will attempt to match the data provided in the request form to the data we maintain. If you are matched to a reasonable degree of certainty, your request will be processed as follows:

- **Access request:** Your access report will include the categories of Workforce Personal Information we match to you unless otherwise subject to an exception pursuant to law.
- **Correction request:** Your correction request cannot be processed if you fail the LexisNexis® demographic questions.

If you fail both LexisNexis® and email confirmation, your Access or Correction request will be cancelled, and you will be notified.

Deletion and Appeal Requests

For Deletion and Appeal requests, you must confirm control over the email address you provide in the request form. If you successfully complete email confirmation, we will attempt to match the data provided in the request form to the data we maintain. If you are matched to a reasonably high degree of certainty, your request will be processed as follows:

- **Deletion request:** All data matched to you and not otherwise subject to an exception pursuant to law will be deleted.
- **Appeal request:** Your appeal request will be reviewed, and you will receive a communication with the outcome of the appeal, including any additional rights you may have.

If you are matched to a reasonable degree of certainty, your request will be processed as follows:

- **Deletion request:** Certain limited data we associate to you will be deleted.
- **Appeal request:** We will review your appeal request and, after considering the totality of the circumstances, will respond accordingly.

If you fail email confirmation, your Deletion or Appeal request will be cancelled, and you will be notified.

Opt-Out Requests and Requests to Limit

Requests to opt-out of profiling or sale and sharing of your Workforce Personal Information and requests to limit the use and disclosure of your Sensitive Personal Information do not require LexisNexis® verification.

Nondiscrimination. Should you wish to request the exercise of your rights as detailed above with regard to your Workforce Personal Information, we will not discriminate against you.

No Sale of Minors' Personal Information. Additionally, California law requires California residents under the age of 16 to opt-in to the sale or sharing of Workforce Personal Information. We have protections in place to prevent the sale and sharing of, and do not intend to and have no actual knowledge that we "sell" or "share" the Workforce Personal Information of California residents under the age of 16.

Metrics. California law requires recording of metrics regarding requests for Access, Correction, Deletion, Opting-out of Sale/Sharing, and Limiting the use of Sensitive Personal Information submitted by California residents pursuant to the California Privacy Rights Act. Our metrics can be found **here.**

Questions

Workforce Members who have questions about this Workforce Notice, or would like to request this Workforce Notice in an alternative accessible format, should contact Walgreens Human Resources Department at askhr@walgreens.com or 800-825-5467 via option 4.

Effective: January 1, 2020 **Updated**: August 15, 2023