SHIELDS HEALTH SOLUTIONS

ELEVATING SPECIALTY PHARMACY

SHIELDS HEALTH SOLUTIONS
SHIELDS CALIFORNIA WORKFORCE PRIVACY NOTICE

Effective January 1, 2023

INTRODUCTION

This Notice is issued by Shields Health Solutions Holdings, LLC and its subsidiaries (collectively "**Shields**" or "**we**"). Shields is committed to maintaining its workforce members' privacy. This California Workforce Privacy Notice ("**Notice**") explains to Shields' California resident employees and job applicants, Shields' practices regarding the collection and use of **Personal Information** and **Sensitive Information**, about Shields' current and prospective workforce members (collectively "**CA Personal Information**"), as described in more detail below.

SCOPE OF THIS POLICY

This Notice applies only to CA Personal Information, as described herein, processed in the 12-months preceding the effective date of this Notice in the context of Shields' human resources ("**HR**"), employment, and other internal business functions relating to its employees and applicants that are California residents and their family members or beneficiaries, including internal computer systems, networks, online services, benefits, etc. It is issued in accordance with the California Consumer Privacy Act (**"CCPA"**). Capitalized terms herein as defined in the CCPA.

HOW TO CONTACT US

SHIELDS HEALTH SOLUTIONS
Suite 600, 100 Technology Center Drive
Stoughton, MA 02072
Privacy@shieldsrx.com
(844) 974-4353 (844-9SHIELD]

See below for information relating to how to submit requests to exercise your rights in the CA Personal Information we process.

CATEGORIES OF CA PERSONAL INFORMATION

This chart describes the categories of CA Personal Information that Shields may collect in connection with its employment work relationships. Note, all CA Personal Information may be used and disclosed in connection with our Business Purposes.

Category of CA Personal Information & Representative Data Elements	**Common Purposes for Collecting & Sharing**
Contact Data • Honorifics and titles, preferred form of address • Mailing address • Email address • Telephone number • Mobile number	We use your Contact Data to communicate with you by mail, email, telephone, or text about your employment, including sending you work schedule information, compensation and benefits communications, and other Shields information. Contact Data is also used to help us identify you and personalize our communications, such as by using your preferred name.

Category of CA Personal Information & Representative Data Elements	Common Purposes for Collecting & Sharing
Identity Data • Full name, nicknames or previous names (such as maiden names) • Date of birth • Language • Employee ID number • Shields account identifiers and passwords • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	We use your Identity Data to identify you in our HR records and systems, to communicate with you (often using your Contact Data) and to facilitate our relationship with you, to facilitate obligations to unions (including under applicable collective bargaining agreements), for internal record-keeping and reporting (including for data matching and analytics), and to track your use of Shields' programs and assets, and for most processing purposes described in this Privacy Notice, including governmental reporting, employment/immigration verification, background checks, etc.
Government ID Data • Social security/national insurance number • Driver's license information • Passport information • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number)*	We use your Government ID Data to identify you and to maintain the integrity of our HR records, enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks (subject to applicable law), enable us to administer payroll and benefits programs and comply with applicable laws (such as reporting compensation to government agencies as required by law), as well as for security and risk management (such as collecting driver's license data for employees who operate Shields' vehicles, professional license verification, fraud prevention and similar purposes). We may also use Government ID data for other customer business purposes, such as collecting passport data and secure flight information for employees who travel as part of their job duties.
Biographical Data • Resume or CV • Application and screening questionnaires • Data from information publicly available on the Internet • Education and degree information • Employment or other work history • Professional licenses, certifications, and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests and hobbies • Professional goals and interests • Criminal records	We use Biographical Data to help us understand our employees and for professional and personal development, to assess suitability for job roles, and to ensure a good fit between each individual's background and relevant job functions. We also use Biographical Data to foster a creative, diverse workforce, for recruiting, for coaching, and to guide our decisions about internal programs and service offerings.
Transaction and Interaction Data • Dates of Employment • Re-employment eligibility • Position, Title, Reporting Information	We use Transaction and Interaction Data as needed to manage the employment relationship and fulfill standard HR functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g., onboarding, maintenance,

Category of CA Personal Information & Representative Data Elements	Common Purposes for Collecting & Sharing
• Work history information • Time and attendance records • Leave and absence records • Salary/Payroll records • Benefit plan records • Housing records • Travel and expense records • Training plan records • Performance records and reviews • Disciplinary records	evaluations, performance management, investigations, etc.).
Financial Data • Bank account number and details • Shields-issued payment card information, including transaction records • Tax-related information	We use your Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, for tax withholding purposes, and for security and fraud prevention.
Health Data • Medical information for accommodation of disabilities • Medical information for leave and absence management, and emergency preparedness programs • COVID-19 testing and vaccination data and exposure to COVID-19 • Vaccination status • Wellness program participation • Information pertaining to enrollment and utilization of health and disability insurance programs	We use your Health Data as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and analytics related to our HR functions, staffing needs, and other Business Purposes. In response to the COVID-19 pandemic, we have implemented health and other screening procedures, vaccination requirements, vaccination tracking, and other measures to reduce the possibility of transmission to our employees and guests and to comply with applicable public health orders and guidance. We use and may need to share this data to carry out contact tracing, implement and enforce workplace safety rules, and for public safety reasons and compliance obligations.
Device/Network Data • Device information from devices that connect to our networks • System logs, including access logs and records of access attempts • Records from access control devices, such as badge readers • Information regarding use of IT systems and Internet search and browsing history, metadata and other technically generated data • Records from technology monitoring programs, including suspicious activity alerts • Data relating to the use of communications systems and the content of those communications	Shields uses Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. We may also use this information to evaluate compliance with Shields' policies. For example, we may use access logs to verify work hours and attendance records. Shields' service providers may use this information to operate systems and services on our behalf, and in connection with service analysis, improvement, or other similar purposes related to our business and HR functions.

Category of CA Personal Information & Representative Data Elements	Common Purposes for Collecting & Sharing
Audio/Visual Data • Photographs • Video images, videoconference records • Call center recordings and call monitoring records • Voicemails	We may use Audio/Visual Data for general relationship purposes, such as call recordings used for training, coaching, or quality control.
Inference Data • Performance reviews • Results of tests related to interests and aptitudes	We use Inference Data to help tailor professional development programs and to determine suitability for advancement or other positions. We may also analyze and aggregate data for workforce planning. Certain Inference Data may be collected in connection with information security functions (e.g., patterns of usage and cybersecurity risk).
Compliance and Demographic data • Employment eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA, etc. • Occupational safety records and workers' compensation program records • Records relating to internal investigations • Records of privacy and security incidents involving HR records, including any security breach notifications	We use Compliance and Demographic Data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, and as needed for litigation and defense of claims.
Protected Category Data Characteristics of protected classifications under state or federal law, e.g., race, national origin, religion, gender, disability, marital status, sexual orientation, or gender identity	We use Protected Category Data as needed to facilitate the employment relationship or other relationship, for compliance and legal reporting obligations, to evaluate the diversity of our workforce and the success of our diversity and inclusion efforts, and as needed for litigation and defense of claims.
Sensitive Personal Data The following categories of data we collect are considered "Sensitive Personal Data:" • Protected Category Data; • Health Data • Financial Data • Government ID • any other Personal Data revealing: • (i) Social security, driver's license, state identification card, or passport number; (ii) account log-in and password, financial account, debit card, or credit card number; precise location data; (iii) racial or ethnic origin,	We use Sensitive Personal Data only as strictly necessary for the purpose it is collected with your knowledge and consent if required by law (e.g., health information on a health insurance benefits application, COVID-19 vaccination status for staffing or entry into locations where vaccination is required, and requests for accommodation).

Category of CA Personal Information & Representative Data Elements	Common Purposes for Collecting & Sharing
religious or philosophical beliefs, or union membership; (iv) mail, email, and text message content (unless we are the intended recipient); and (v) health.	

SOURCES OF CA PERSONAL INFORMATION

We collect CA Personal Information from various sources, which vary depending on the context in which we process that CA Personal Information.

- **Data you provide us** – We will receive your CA Personal Information when you provide it to us, when you apply for a job, complete forms, via the Shields' employee ADP portal, provide information via a Shields' app, allow us to perform a health-related test or temperature check, or otherwise direct information to us.
- **Data from a third party** – We will receive your CA Personal Information from third parties such as recruiters, credit reporting agencies, or employment screening providers.
- **Data from publicly available sources** – We may collect data that is publicly available on the Internet (e.g., through a Google search of a candidate's name).
- **Data we collect automatically** – We may also collect information about or generated by any device you have used to access internal IT services, applications, and networks.
- **Data we receive from Service Providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer CA Personal Information such as Inference Data based on our observations or analysis of other CA Personal Information processed under this Privacy Notice, and we may correlate this data with other data we process about you. We may combine CA Personal Information about you that we receive from you and from third parties.

DISCLOSURE OF CA PERSONAL INFORMATION

We generally process HR personal data internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

CATEGORIES OF INTERNAL RECIPIENTS

The CA Personal Information identified below may be disclosed to the following categories of recipients in relevant contexts.

- **Personnel of the HR Department** – All CA Personal Information relating to HR and Recruitment.
- **Personnel of the Finance Department** – Elements of CA Personal Information to the extent related to payroll, compensation, expense reimbursements, etc.
- **Supervisors and Managers –** Elements of CA Personal Information to the extent permitted in the jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment or contractual relationship, conduct reviews, handle compliance obligations, and similar matters.

- **Department Managers searching for new employees** – CA Personal Information of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs.
- **IT Administrators** of Shields and/or third parties who support the management and administration of HR processes may receive CA Personal Information as necessary for providing relevant IT related support services (for example, conducting IT security measures and IT support services)**.**
- **Peers and colleagues** – Elements of Personal Data in connection with Shields' address books, intra-Shields and interpersonal communications, and other contexts relevant to the day-to-day operation of Shields business.
- **Personnel of the Legal Department** – Elements of CA Personal Information to the extent necessary to provide legal advice.

CATEGORIES OF EXTERNAL RECIPIENTS

Shields may provide CA Personal Information to external third parties as described below. The specific information disclosed may vary depending on context, but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and Shields. We generally provide information to:

- Our subsidiaries, affiliates, and parent company.
- Service providers, vendors, and similar data processors that process CA Personal Information on Shields' behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, background checks, etc.) or that provide other services for our employees or for Shields.
- To prospective seller or buyer of such business or assets in the event Shields sells or buys any business or assets.
- To future Shields affiliated entities, if Shields or substantially all of its assets are acquired by a third party, in which case CA Personal Information held by it about its employees will be one of the transferred assets.
- To your employment references, to inform them that you have applied with Shields as part of our recruiting process.
- To future prospective employers seeking to confirm your relationship with Shields.
- To government agencies or departments, employee unions, or similar parties in connection with employment related matters.
- To any public authority in relation to national security or law enforcement requests, if Shields is required to disclose CA Personal Information in response to lawful requests by a public authority.
- To Shields' customers, if you will be working on-site at the customer's facility.
- To any other appropriate third party, if Shields is under a duty to disclose or share your CA Personal Information to comply with any legal obligation or to protect the rights, property, health, or safety of Shields, our employees, contractors, customers, or others.

PURPOSES FOR COLLECTING, USING, AND DISCLOSING CA PERSONAL INFORMATION

Shields collects CA Personal Information about its prospective, current, and former employees and other individuals as appropriate in the context of an employment or contractual work relationship (such as

dependents) for various general HR and business purposes, as described below**. We do not sell or "share" (as defined in CCPA) CA Personal Information with third parties in exchange for monetary consideration or for advertising purposes.**

GENERAL HR PURPOSES

Shields collects CA Personal Information about its prospective, current, and former employees, job applicants, and other individuals as appropriate in the context of an employment relationship, including for recruitment and IT/technical support services, and as needed for using internal software, networks and devices. The categories of CA Personal Information we process, along with representative data elements, are listed in the chart below. We may not collect from you or process all of the CA Personal Information identified below, depending on your position or the nature of your relationship with Shields.

We generally process CA Personal Information for the following purposes:

CA Personal Information pertaining to ***prospective*** employees may be processed for:	• Recruitment and staffing, including evaluation of skills and job placement. • Hiring decisions, including negotiation of compensation, benefits, relocation packages, etc. • Risk management, including reference and other background checks. • Our Business Purposes (defined below).
CA Personal Information pertaining to ***current*** employees may be processed for:	• Staffing and job placement, including scheduling and absence management. • Verification of eligibility to work and compliance with immigration laws, rules and regulations. • Administration of compensation, insurance and benefits programs. • Time and attendance tracking, expense reimbursement, other workplace administration and facilitating relationships within Shields. • Technology support uses, such as managing our computers and other assets, providing email and other tools to our workers. • EEO/Affirmative Action programs. • Internal and external directories of Employees. • Health and wellness programs. • Reasonable employment accommodations. • Occupational health and safety programs (including drug and alcohol testing, required injury and illness reporting, disaster recovery and business continuity planning, and workers' compensation management). • Health and safety requirements imposed by Shields, government authorities, or others, depending on the location of employment, engagement or travel (e.g., vaccination status or health screening). • Talent and performance development, skills management and training, performance reviews, employee feedback surveys, and recognition and reward programs. • HR support services, such as responding to inquiries, providing information and assistance.

	• Employee relations, such as implementing and administering HR policies, investigations, and resolving disputes or concerns that you may raise. • Risk management and loss prevention, including employee and premises monitoring. • Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken, such as making adjustments. • Managing statutory leave programs such as family and parental leave. • Succession planning and adjustments for restructuring. • As requested by individuals, including verifying employment and income verifications (e.g., for mortgage applications). • Facilitating obligations to unions, including under applicable collective bargaining agreements • Business Purposes (defined below).
CA Personal Information pertaining to ***former*** employees may be processed for:	• Re-employment. • Administration of compensation, insurance and benefits programs. • Expense reimbursements. • For archival and recordkeeping purposes. • Responding to claims for unemployment benefits and other government inquiries. • As requested by individuals, including employment and income verifications (e.g., for mortgage applications). • EEO/Affirmative Action programs. • Business Purposes (defined below).
CA Personal Information pertaining to individuals whose information is provided to Shields in the course of HR management (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, etc.) may be processed for:	• Administration of compensation, insurance and benefit programs. • Workplace administration. • To comply with child support orders or garnishments. • To maintain emergency contact lists and similar records. • Business Purposes (defined below).

BUSINESS PURPOSES

"Business Purposes" means the following purposes for which CA Personal Information may be collected, used and shared:

- Maintaining comprehensive and up-to-date employment records.
- Establishing, managing, or terminating employment or other working relationships.
- Maintaining a safe and respectful workplace and improving employee satisfaction and performance.
- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials.
- Security, safety, loss prevention, information security, and cybersecurity.

- Legal and regulatory compliance, including without limitation all uses and disclosures of CA Personal Information that are required by court orders and applicable laws, regulations, orders and ordinances, and for compliance with legally-mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics reporting system, and other processing in connection with the establishment and defense of legal claims.
- Corporate audit, analysis, and consolidated reporting.
- To enforce our contracts and to protect Shields, our workers, our clients and their employees and the public against injury, theft, legal liability, fraud or abuse, to people or property.
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research, or analytics.
- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
- For the operations, analysis, upgrade, enhancement, development, or improvement internal IT or other services, operations, and similar matters.
- As needed to facilitate corporate governance.

RETENTION AND DISPOSAL

Shields intends to retain CA Personal Information) for no longer than is reasonably necessary and proportionate to achieve the legitimate business purpose for which it was collected or to satisfy a legal requirement. What is necessary may vary depending on the context and purpose of processing. We generally consider the following factors when we determine how long to retain data (without limitation):

- Retention periods established or necessary under applicable law;
- Industry and human resources best practices;
- Whether the purpose of processing is reasonably likely to justify further processing;
- Risks to individual privacy in continued processing;
- Applicable data protection impact assessments;
- IT systems design considerations/limitations; and
- The costs associated with continued processing, retention, and deletion.

Shields staff must follow any applicable records retention schedules and policies and destroy any media containing CA Personal Information in accordance with applicable Shields' policies. CA Personal Information shall not be processed in a manner that is incompatible with these purposes.

YOUR RIGHTS, INCLUDING YOUR CALIFORNIA PRIVACY RIGHTS

Under the CCPA, California residents may have the following rights, subject to your submission of an appropriately verified request (see below for verification requirements):

Right to Know	You may request any of following, for the 12 month period preceding your request: (1) the categories of CA Personal Information we have collected about you, or that we have sold, or disclosed for a commercial purpose; (2) the categories of sources from which CA Personal Information was collected; (3) the business or commercial purpose for which we collected, sold or shared your CA Personal Information; (4) the categories of third parties to whom we have sold or shared your CA Personal

	Information, or disclosed it for a business purpose; and (5) the specific pieces of CA Personal Information we have collected about you.
Right to Delete	You have the right to delete certain CA Personal Information that we hold about you, subject to exceptions under applicable law.
Right to Correct	You have the right to correct certain CA Personal Information that we hold about you, subject to exceptions under applicable law.
Right of Non-retaliation	You have the right to not to receive discriminatory treatment as a result of your exercise of rights conferred by the CCPA.
Direct Marketing	You may request a list of CA Personal Information we have disclosed about you to third parties for direct marketing purposes during the preceding calendar year, if applicable.
Opt-Out of Sale or Sharing	**We do not sell or share CA Personal Information with third parties in exchange for monetary consideration or for advertising purposes.**
Limit Use and Disclosure of Sensitive Personal Information	You may request that we limit our use of Sensitive Personal Information to that which is necessary to perform the specific HR and business purposes described herein.
Minors'	To the extent we have actual knowledge that we collect or maintain CA Personal Information of a minor under age 16, those minors between the age of 13 and 16 must opt-in to any sharing of CA Personal Information (as defined under CCPA), and minors under the age of 13 must have a parent consent to sharing of CA Personal Information (as defined under CCPA). All minors have the right to opt-out later at any time. Minors under age 13 may have other rights under the Children's Online Privacy Protection Act ("COPPA").

SUBMISSION OF REQUESTS

Current Shields employees can review and update much of their CA Personal Information via the Shields ADP employee portal or you may also contact your HR Office for assistance.

If you are a former employee, beneficiary, dependent, or family member, please contact us at the address or email listed below for assistance with your privacy requests.

To exercise rights available to you under California law and for all other questions or comments about this Notice or our privacy practices, please contact:

SHIELDS HEALTH SOLUTIONS
Suite 600, 100 Technology Center Drive
Stoughton, MA 02072
Re: Data Rights Requests
OR
Privacy@shieldsrx.com
OR
(844) 974-4353 (844-9SHIELD]

VERIFICATION OF REQUESTS

Requests to receive a copy of CA Personal Information, and requests to delete or correct CA Personal Information, must be verified to ensure that the individual making the request is authorized to make that request, to reduce fraud, and to ensure the security of your CA Personal Information. We may require that you log in through the Shields' ADP employee portal (if you are a current employee, and/or that you provide the email address we have on file for you (and verify that you can access that email account) as well as an address, phone number, or other data we have on file, in order to verify your identity.

If an agent is submitting the request on your behalf, we reserve the right to validate the agent's authority to act on your behalf. You and the agent will be required to provide us with proof of the agent's identity and proof that you gave the agent signed permission to submit a request on your behalf. Additionally, you will be required to verify your identity by providing us with certain CA Personal Information as described above or provide us with written confirmation that you have authorized the agent to act on your behalf.

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.

For requests for access or deletion, Shields will first acknowledge receipt of your request within 10 business days of receipt of your request. Shields will provide a substantive response to your request as soon as Shields can, generally within 45 days from when Shields receives your request, although Shields may need to take longer to process your request under certain circumstances. If Shields expects your request is going to take longer than normal to fulfill, Shields will let you know.

Shields usually act on requests and provide information free of charge, but Shields 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. If this is the case, Shields will endeavor to provide you with an explanation as to why.

I acknowledge that on the date indicated below, I received a copy of SHIELDS' CALIFORNIA WORKFORCE PRIVACY NOTICE. I acknowledge that I am expected to read and understand the information in the SHIELDS' CALIFORNIA WORKFORCE PRIVACY NOTICE. I also understand I should ask my manager or Human Resources if I have any questions.

I also acknowledge that the provisions in this SHIELDS' CALIFORNIA WORKFORCE PRIVACY NOTICE are not intended to form or imply an employment contract between SHIELDS and me or any of its other employees. I understand my employment may be terminated "at-will" by me or by SHIELDS at any time for any reason.

Employee Signature: _____

Employee Name (Printed): _____

Date: _____