Curium US LLC California Employee Notice at Collection and Privacy Policy

Last Updated: October 27, 2025

This document is divided into two parts:

1. **Part A: California Notice at Collection for Employees, Contractors, and Applicants.** This is a summary of the personal information we collect and the purposes for which we use it.
2. **Part B: California Employee, Contractor, and Applicant Privacy Policy.** This policy provides a more detailed description of our information practices and your rights under California law.

Part A: California Notice at Collection for Employees, Contractors, and Applicants

Curium US LLC ("Curium," "the Company," "we," "us," or "our") is providing this notice to our job applicants, employees, owners, directors, officers, and contractors ("personnel" or "you"). Any terms defined in the CCPA have the same meaning when used in this notice.

1. Personal Information We Collect

We collect personal information to manage your relationship with us. The following table outlines the categories of personal information we may collect and the purposes for which we may use this information.

Category of Personal Information	Business Purposes for Collection & Use	Is this Information Sold or Shared?	Retention Period Criteria
Identifiers: Such as real name, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, Social Security	Recruiting, hiring, managing the employment relationship, payroll, benefits administration, security, legal compliance, and communication.	No	Duration of employment and for up to 4 years after, subject to legal and regulatory requirements.

number, driver's license number, passport number, or other similar identifiers.			
Personal Information described in Cal. Civ. Code § 1798.80(e): Such as signature, physical characteristics, telephone number, insurance policy number, education, employment history, bank account number, or other financial information, medical information, or health insurance information.	Recruiting, background checks, payroll and direct deposit, administering health and welfare benefits, emergency contacts.	No	Duration of employment and for up to 4 years after, subject to legal and regulatory requirements.
Protected Classification Characteristics: Such as age, race, color, ancestry, national origin, religion, marital status, medical condition, disability, sex (including gender, pregnancy), sexual orientation, veteran or military status.	Equal opportunity and diversity monitoring, providing legally-required accommodations, benefits administration, and compliance with anti-discrimination laws.	No	Duration of employment and for up to 3 years after, subject to legal and regulatory requirements.
Commercial Information: Such as records of company property, products or services purchased or obtained (e.g., for expense reimbursement).	Managing company assets, reimbursing business expenses.	No	Duration of employment and for up to 5 years after for financial and audit purposes.
Internet or Other Electronic Network Activity Information: Such as information regarding your interaction with our	To monitor, secure, and ensure acceptable use of our network and systems; to prevent and investigate security incidents.	No	Retained for up to 180 days unless needed for a security investigation.

internal network, applications, or systems.			
Geolocation Data: Such as the location of a company-issued device or vehicle.	To manage company assets, for safety and security of personnel, and to manage logistics for field-based employees.	No	Retained for up to 180 days unless needed for a security investigation.
Audio, Electronic, Visual Information: Such as security camera footage in our facilities, photographs for employee badges, and call recordings.	Workplace security, safety, quality assurance, and employee identification.	No	Retained for up to 180 days unless needed for a security investigation.
Professional or Employment-Related Information: Such as your work history, performance evaluations, disciplinary records, and professional qualifications.	Recruiting, performance management, compensation and promotion decisions, and succession planning.	No	Duration of employment and for up to 5 years after, subject to legal and regulatory requirements.
Education Information: Such as grades, transcripts, and schools attended.	To verify qualifications for employment and for compliance with educational assistance programs.	No	Duration of employment and for up to 4 years after, subject to legal and regulatory requirements.
Inferences Drawn from Personal Information: Such as a profile reflecting your work preferences, performance, and aptitudes.	Talent management, performance reviews, and career development.	No	Duration of employment and for up to 4 years after, subject to legal and regulatory requirements.
Sensitive Personal Information: This includes your Social Security Number, driver's license, passport number; account log-in	We collect this information for the purposes described above. For example, health information is used for benefits and	No	See the table below for applicable retention periods.

credentials; precise geolocation; racial or ethnic origin; religious beliefs; union membership; the contents of your mail, email, or text messages on company systems; genetic data; biometric information for identification; and health, sex life, or sexual orientation information.	leave administration, and government IDs are used for payroll and legal compliance. We do not use or disclose this information for purposes other than those permitted by the CCPA regulations (§ 7027(m)).		

Sensitive Personal Information

Government-Issued Identification: Social Security number, driver's license number, passport number.	To verify identity and work authorization (I-9), for payroll and tax administration, and benefits enrollment.	No	Duration of employment and for up to 4 years after, subject to legal and regulatory requirements.
Account Log-in Credentials: Your username and password for company systems.	To secure and provide access to our network, email, and other business systems.	No	Duration of your need for access to the system.
Health and Medical Information: Information about your health, medical conditions, or disability status; health insurance information.	To administer health and disability benefits, manage leaves of absence and workers' compensation claims, and provide reasonable accommodations.	No	Duration of employment and for up to 5 years after, subject to legal and regulatory requirements.
Racial or Ethnic Origin; Religious Beliefs; Sexual Orientation (Collected on a voluntary basis).	For equal opportunity monitoring and reporting, and to inform diversity and inclusion initiatives.	No	Duration of employment and for up to 4 years after, subject to legal and regulatory requirements.
Precise Geolocation: Your precise physical location from a company device.	For safety and security of personnel, to manage logistics for field-based roles, and to protect company assets.	No	Retained for up to 180 days unless needed for a security investigation.

2. No Sale or Sharing of Personal Information

Curium does not "sell" or "share" (as those terms are defined in the CCPA) the personal information of its personnel for monetary or other valuable consideration, including for cross-

context behavioral advertising.

3. Full Privacy Policy

For a more detailed description of our practices and your rights, please review our full **California Employee, Contractor, and Applicant Privacy Policy** in [Part B below].

4. Use of Company Equipment

Personnel should not have any expectation of privacy in their use of Company-provided computers, phones, or other communication tools. All communications made using Company-provided equipment or services, including email and internet activity, are subject to inspection by and are the property of the Company. Personnel should keep in mind that even if they delete an email, voicemail or other communication, a copy may be archived on the Company's systems.

Part B: California Employee, Contractor, and Applicant Privacy Policy

Last Updated: October 27, 2025

1. Scope

This California Employee, Contractor, and Applicant Privacy Policy ("Policy") supplements the information contained in Curium's other policies and applies solely to our employees, job applicants, owners, directors, officers, and contractors ("personnel" or "you").

2. Information We Collect

We collect information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household ("personal information"). The "Notice at Collection" in Part A provides a summary of the categories of personal information we have collected from personnel in the prior twelve months and the purposes for which we use it. This includes "sensitive personal information" as defined by the CCPA.

3. Sources of Personal Information

We collect personal information from the following sources:

- *Directly from you*: When you apply for a job, complete onboarding paperwork, or use our systems.
- *Indirectly from you*: From your activity on our networks and systems.
- *From third parties*: Such as from recruiters, background check providers, former employers,

and benefits administrators.

4. How We Use and Disclose Personal Information

We use the personal information we collect for the business purposes identified in the "Notice at Collection" table above. We may disclose the following categories of personal information to the following categories of service providers, contractors, and third parties for a business purpose (auditing, security, debugging, short-term transient use, performing services on our behalf, internal research and development, and quality and safety assurance).

Categories of Third-Party Recipients	**Category of Personal Information Disclosed**
Payroll processors; benefits and leave administrators; background check vendors; IT and network security providers; expense reimbursement services; and recruiting platforms.	Identifiers; Personal Information (Cal. Civ. Code § 1798.80(e)); Professional or Employment-Related Information; Education Information; Government-Issued Identification; Commercial Information; Account Log-in Credentials; Inferences Drawn from Personal Information; Health and Medical Information; Union Membership; Racial or Ethnic Origin; Religious Beliefs; Sexual Orientation
IT and network security providers.	Internet or Other Electronic Network Activity; Geolocation Data; Audio, Electronic, Visual Information
Expense reimbursement services.	Commercial Information

In addition, any category of personal information may be disclosed to:

- *Government and Law Enforcement*: As required by law or in response to a legal process.
- *Outside legal counsel, auditors, and insurers*: To aid in our compliance with applicable law and to protect our business interests.
- *Successor Entities*: As part of a business transaction like a merger, acquisition, or sale of assets.
- *Other Third Parties*: As directed or consented to by you.

4. Sale, Sharing, and Use of Sensitive Personal Information

- *Sale and Sharing*: We do not sell or share (for cross-context behavioral advertising) the personal information of our personnel. We have not done so in the preceding 12 months.
- *Opt-Out Preference Signals*: The CCPA allows consumers to signal their choice to opt out of the sale or sharing of their personal information through a browser-based signal. Because Curium does not sell or share employee personal information, no action is necessary in response to such a signal.

- *Sensitive Personal Information*: We do not use or disclose sensitive personal information for purposes other than those specified in Section 7027(m) of the CCPA regulations. These permitted purposes include ensuring security, providing benefits, performing services for the employment relationship, and other uses necessary to provide the services reasonably expected by you in the employment context. Therefore, we do not provide a right to limit the use of this information.

5. Your California Privacy Rights

California residents have the following rights regarding personal information.

- *The Right to Know*: You have the right to request that we disclose to you the personal information we have collected about you, including:
  - The categories of personal information we have collected.
  - The categories of sources from which the personal information is collected.
  - The business or commercial purpose for collecting the information.
  - The categories of third parties to whom we disclose personal information.
  - The specific pieces of personal information we have collected about you.
- *The Right to Delete*: You have the right to request that we delete personal information that we have collected from you, subject to certain exceptions. For example, we may deny your deletion request if retaining the information is necessary to comply with our legal obligations, complete a transaction, or for other internal and lawful uses.
- *The Right to Correct*: You have the right to request that we correct inaccurate personal information that we maintain about you.
- *The Right to Non-Retaliation*: We will not retaliate or discriminate against you for exercising any of your CCPA rights. This includes denying you goods or services, charging different prices, or providing a different level or quality of services.

These rights are subject to verification and may be limited or denied where permitted by law, such as when an exception applies or fulfilling the request would conflict with legal obligations. We will respond to all valid and verifiable requests in accordance with applicable California privacy laws.

How to Exercise Your California Privacy Rights

If you are a resident of California and wish to exercise your right to know, delete, or correct, please submit a verifiable request to us by either:

- Emailing us at privacy.office@curiumpharma.com
- Calling us at +1 844-591-2749

Only you, or a person you have authorized to act on your behalf, may make a verifiable request related to your personal information.

Verification Process

We cannot fulfill your request if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. To verify your identity, we will match the identifying

information you provide in your request with the personal information we already maintain. For requests for specific pieces of information, we may require a higher degree of verification, which could include a signed declaration under penalty of perjury.

Authorized Agents
You may use an authorized agent to submit a request on your behalf. If you use an authorized agent, we may require you to provide the agent with signed permission to do so, verify your own identity directly with us, and directly confirm with us that you provided the agent permission to submit the request. These requirements do not apply if you have provided the agent with a power of attorney pursuant to California Probate Code sections 4000 to 4465.

6. Accessibility and Languages

This notice is available in Spanish and other languages on request and in alternative formats for individuals with disabilities. Contact HR to obtain a copy.

7. Changes to This Policy

We reserve the right to amend this privacy policy at our discretion and at any time. When we make changes to this policy, we will post the updated notice on our internal employee portal and update the policy's “Last Updated” date.

8. Contact Us

If you have any questions or concerns about this policy, our information practices, or your rights under law, please contact Curium’s Privacy Office at:
Email: privacy.office@curiumpharma.com
Phone: +1 844-591-2749
Mailing Address: Legal Department, Attn: Privacy Office, 111 Westport Plaza, Suite 800, St. Louis, MO 63146