

ELEVAR THERAPEUTICS, INC.

U.S. Personnel Privacy Notice

Last Updated: [02/01/2026]

This U.S. Personnel Privacy Notice ("**U.S. Personnel Notice**") explains how Elevar Therapeutics, Inc. and its subsidiaries (collectively, "**Elevar**," "**we**," "**us**", or "**our**") collects, uses, discloses, and otherwise processes personal data about our U.S.-based employees, officers, directors, contractors, freelancers, contingent workers, consultants and other outsourced and temporary workers (collectively, "**personnel**"), and their family members or other individuals about whom we process personal data as a result of the relationships those individuals have with personnel (collectively, "**related persons**"). It is the responsibility of our personnel to make this U.S. Personnel Notice available to their related persons.

This U.S. Personnel Notice is not a contract and does not create any legal rights or obligations not otherwise provided by law. This U.S. Personnel Notice also is not intended to replace other notices or disclosures we may provide to you in connection with your role in our organization, which will supersede any conflicting disclosures contained in this U.S. Personnel Notice.

What is Personal Data?

When we use the term "**personal data**" in this U.S. Personnel Notice, we mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an individual within the context of the individual's role as a member of our personnel or a related person. It does not include aggregated or deidentified information that is maintained in a form that cannot reasonably be used to infer information about, or otherwise be linked to, a particular individual. Where we maintain deidentified data, we will maintain and use the data in deidentified form and not attempt to reidentify the data except as required or permitted by law.

Our Collection and Use of Personal Data

Personnel

Collection of Personal Data

In connection with an individual's role as a member of our personnel, we collect the following professional or employment-related personal data:

- **Contact Information:** such as full name, email address (personal and work), home address, business address, telephone number, and emergency contact information.
- **Identification Materials:** such as image, Social Security number or other national identification number, passport number, driver's license number, or vehicle license plate number.
- **Professional Information:** such as hire date, employment location, business unit, department, supervisor, job title, position/grade, hours and days worked, working arrangement, work

restrictions or accommodations, employee identification number, licenses and certifications, attendance, career goals, performance reviews, disciplinary records, information needed to establish eligibility to work for us, including visa information, and information relating to potential conflicts with the individual's role in the organization.

- **Education & Training Information:** such as highest level of education, schools attended and dates of attendance, degrees, certificates or other educational qualifications earned, and transcripts or training records.
- **Financial Information:** such as salary, bonus, benefits, expenses, stock or equity grants, bank account and routing information, and corporate credit card number.
- **Benefits Information:** such as eligibility for benefits, information about family members and other related persons eligible for or covered by available benefits, and claims relating to available benefits.
- **Equal Opportunity Information:** such as age, race, ethnicity, national origin, citizenship, sex, gender identity or transgender status, sexual orientation, religion, disability or accommodation request, or marital or veteran status when an individual chooses to provide them, but this equal opportunity information will not be used in employment-related decisions unless specifically permitted by law
- **Audio / Visual Recordings:** such as a recording of image or voice in connection with phone calls, virtual meetings and conferences, and other events, where permitted by law.
- **Security Information:** such as work-related accounts and passwords, technical details about the individual's use of work-related devices and information systems (including, for example, device, logs, analytics data, IP address, and general location information derived from such IP address), the content of communications sent through work-related devices and information systems, access to physical and electronic work-related locations, audio recordings and photographs, videos, and other visual images of the individual.
- **Background Check and Reference Check Information:** when permitted by applicable law, we may choose to conduct a background check and/or a reference check in connection with an individual's employment such as to verify professional and educational history and qualifications or identify criminal history that may be relevant for a position with us. The results of the background check and/or reference check may include personal data we do not already have about the individual who is the subject of the check.
- **Other Work-Related Information:** We also may collect any personal data our personnel choose to share with us or to make publicly available, or we otherwise receive from a third party in connection with their work for us, a grievance they are involved in, an agreement they enter into with us or additional roles they take on as a part of our organization.

Although we often collect the personal data described above directly from our personnel, we also collect this information from supervisors, colleagues, customers, vendors, publicly available sources, and other third parties they may interact with as members of our personnel. In addition, we may also collect this information through service providers and other third parties that collect it on our behalf, such as communications providers, payroll providers and benefits providers.

Use of Personal Data

We use the personal data we collect about our personnel to:

- Conduct organizational planning and development, including budget planning and administration;
- Analyze and monitor compliance with our personnel and compliance policies and practices;
- Administer recruiting, onboarding, staffing, leave, personnel evaluations, promotions, performance management, training, discipline, participation in available activities or programs, and any other processing in connection with work-related purposes;
- Authorize, grant, administer, monitor (including by video surveillance), and terminate access to or use of company systems, facilities, records, property, and infrastructure;
- Communicate with and between personnel, as well as with designated emergency contacts;
- Support and manage personnel, including providing resources needed for personnel to perform their roles with us;
- Facilitate personnel compensation, payroll, and benefit planning and administration (e.g., salary, tax withholding, insurance);
- Conduct performance reviews and evaluations, as well as make decisions about promotions and job mobility;
- Manage business travel (e.g., car service/rentals, flights, hotels) and personnel expenses (e.g., reimbursement, corporate credit card).
- Operate our business, including marketing our personnel to customers, facilitating the work of our personnel, and providing the products and services made available to our customers;
- Investigate, document, and report work-related injuries, illness, or grievances;
- Conduct internal investigations, audits, compliance, risk management, problem resolution, and security operations;
- Fulfill contractual obligations to personnel and other third parties;
- Facilitate business transactions and reorganizations impacting the structure of our business;
- Comply with applicable law, rule, regulation, legal proceedings, and government investigations, including relating to tax reporting and immigration.

Personal Data of Related Persons

Collection of Personal Data

At times, we receive identifiers and other personal data about our personnel's family members and other related persons in connection with emergency contacts and the benefits and services we provide. These identifiers and other personal data include:

- **Contact Information:** such as full name, email address, home address, business address, telephone number, and emergency contact information.
- **Other Identification Materials:** such as image, Social Security number or other national identification number, passport number, driver's license, number or vehicle license plate number.
- **Benefits and Services Information:** We also collect personal data necessary to extend benefits and benefit-related services, including insurance-related information, claims-related information, and disbursement-related information.

Although we often collect the personal data described above directly from our personnel, we also may collect this information directly from the related person, and from our benefit administrators. In addition, we may also collect this information through service providers and other third parties that collect it on our behalf, such as communications providers.

Use of Personal Data

We use the personal data we collect about related persons to:

- Communicate about eligibility benefits and services, events, or activities that are happening, or in the event of an emergency;
- Administer benefits and services;
- Respond to requests and inquiries;
- Conduct internal investigations, audits, compliance, risk management, problem resolution, and security operations;
- Fulfill contractual obligations;
- Facilitate business transactions and reorganizations impacting the structure of our business;
- Comply with applicable law, rule, regulation, legal proceeding, and government investigations, including relating to tax reporting and immigration.

Our Disclosure of Personal Data

We may share the categories of personal data outlined above with the following third parties for the purposes described below:

- **Within Elevartx:** We share personal data relating to personnel and related persons within our family of companies for internal administrative purposes and uses that are consistent with this U.S. Personnel Notice. For example, the entity responsible for payroll may receive personal data about personnel employed by another one of our entities in order to determine the proper compensation to be provided.
- **Benefit Administrators:** In order to provide our personnel and related persons benefits and services available to them, we share personal data with the third parties we engage to offer and administer benefits and services on our behalf. These third parties may also collect additional personal data directly from our personnel and their related persons in connection with these benefits and services, which will be subject to the relevant third party's own privacy policies and notices.
- **Compensation, Payroll and Tax Providers:** We share personal data with third parties who assist us in processing our payroll and other compensation-related obligations, including our tax withholding and reporting obligations.
- **Background Check and Reference Check Providers:** When permitted by applicable law, we may choose to conduct a background check and/or reference check in connection with an individual's employment, such as to verify professional and educational history and qualifications or identify criminal history that may be relevant for a position with us. In order to facilitate the background check and/or reference check, we share personal data about the relevant individual with trusted background check and/or reference check providers.
- **Other Service Providers:** In addition to the third parties identified above, we engage other third parties to perform certain functions on our behalf in connection with the uses of personal data described in the [Our Collection and Use of Personal Data](#) section above, including assisting us with our personnel management, benefits and services offerings, and other related business operations. Depending on the function the third party serves, the service provider may process personal data on our behalf or have access to personal data while performing functions on our behalf.

- **Customers:** We share personal data about our personnel with prospective and actual customers in connection with the marketing, negotiation, sale, delivery and provision of the products and services we make available. For example, we may share the images and contact information for the team of personnel who will be responsible for handling a specific customer's account.
- **Public Disclosure:** We may disclose certain personal data about our personnel, such as name, job title, work-related contact information, and experience, publicly in connection with our recruiting and business operations.
- **Business Transaction or Reorganization:** We may take part in or be involved with a corporate business transaction, such as a merger, acquisition, joint venture, or financing or sale of company assets. We may disclose personal data to a third party during negotiation of, in connection with, or as an asset in such a corporate business transaction. Personal data may also be disclosed in the event of insolvency, bankruptcy, or receivership.
- **Legal Obligations and Rights:** We may disclose personal data to third parties, such as legal advisors and law enforcement:
 - in connection with the establishment, exercise, or defense of legal claims;
 - to comply with laws and regulations or to respond to lawful requests and legal process;
 - to protect our rights and property and the rights and property of our agents, customers, and others, including to enforce our agreements, policies, and terms of employment;
 - to detect, suppress, or prevent fraud;
 - to reduce credit risk and collect debts owed to us;
 - to protect the health and safety of us, our personnel, their related persons, our customers, or any person; or
 - as otherwise required by applicable law or legal process.
- **Otherwise with Consent or Direction:** We may disclose personal data about our personnel or their related persons to certain other third parties or publicly with their consent or direction.

California-Specific Disclosures

The following disclosures only apply to residents of the State of California.

Personal Data Disclosures

No Sales or Targeted Advertising

We do not sell personal data about individuals acting in their capacity as personnel or related persons, and we do not share or otherwise disclose personal data about individuals acting in their capacity as

personnel or related persons to third parties for the purpose of displaying advertisements that are selected based on personal data obtained or inferred over time from an individual's activities across businesses or distinctly-branded websites, applications, or other services (otherwise known as "targeted advertising" or "cross-context behavioral advertising").

Sensitive Information

The following personal data elements we collect about our personnel and our personnel's family members and other related persons may be classified as "sensitive" under certain privacy laws ("**sensitive information**"):

- Social Security number, driver's license number, passport number;
- Work-related accounts and passwords;
- Financial account information;
- Credit/debit card number plus expiration date and security code (CVV); and
- Information relating to racial and ethnic origin, religious beliefs, health, disabilities, sexual orientation, and gender identity.

We use this sensitive information for the purposes set forth in the [Our Collection and Use of Personal Data](#) section above.

We do not sell sensitive information about individuals acting in their capacity as personnel or related persons, and we do not share or otherwise disclose sensitive information about individuals acting in their capacity as personnel or related persons for the purpose of targeted advertising, nor use such information for the purpose of inferring characteristics about our personnel or their related persons.

Retention of Personal Data

We retain personal data only for as long as is reasonably necessary to fulfil the purpose for which it was collected. However, if necessary, we may retain personal data for longer periods of time, until set retention periods and deadlines expire, for instance where we are required to do so in accordance with legal, tax, and accounting requirements set by a legislature, regulator, or other government authority.

To determine the appropriate duration of the retention of personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of personal data, and if we can attain our objectives by other means, as well as our legal, regulatory, tax, accounting, and other applicable obligations.

Once retention of the personal data is no longer necessary for the purposes outlined above, we will either delete or deidentify the personal data or, if this is not possible (for example, because personal data has been stored in backup archives), then we will not further process the personal data until deletion or deidentification is possible.

Your Privacy Choices

Residents of California (and other states to the extent applicable under current law) may be able to exercise the following rights in relation to the personal information that we have collected about you, subject to certain limitations:

- **The Right to Know.** You have the right to request any or all of the following information relating to your personal information we have collected and disclosed in the last 12 months, upon verification of your identity:
 - The specific pieces of personal information we have collected about you;
 - The categories of personal information we have collected about you;
 - The categories of sources of the personal information;
 - The categories of personal information that we have disclosed to third parties for a business purpose, and the categories of recipients to whom this information was disclosed;
 - The categories of personal information we have sold or shared about you (if any), and the categories of third parties to whom the information was sold or shared; and
 - The business or commercial purposes for collecting or, if applicable, selling or sharing the personal information.
- **The Right to Access & Portability.** The right to obtain access to the personal data we have collected about you and, where required by law, the right to obtain a copy of the personal data in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.
- **The Right to Request Deletion.** You have the right to request the deletion of personal information we have collected from you, subject to certain exceptions.
- **The Right to Correction.** You have the right to request that any inaccuracies in your personal data be corrected, taking into account the nature of the personal data and the purposes of the processing of your personal data.

You also have the right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights. However, please note that if the exercise of these rights limits our ability to process personal data, we may no longer be able to engage with you in the same manner.

Submitting Privacy Rights Requests

To submit a request to exercise one of the privacy rights identified above, please:

- Email us at privacy@elevartx.com or
- Call 1-866-4ELEVARTX.

Before processing your request, we will need to verify your identity and confirm you are a resident of the State of California. In order to verify your identity, we will generally either require the successful authentication of your work-related account, or the matching of sufficient information you provide us to the information we maintain about you in our systems. We may at times need to request additional personal data from you, taking into consideration our relationship with you and the sensitivity of your request.

In certain circumstances, we may decline a privacy rights request, particularly where you are not a resident of the State of California or where we are unable to verify your identity.

Authorized Agents

In certain circumstances, you are permitted to use an authorized agent to submit requests on your behalf through the designated methods set forth above where we can verify the authorized agent's authority to act on your behalf. To verify the authorized agent's authority, we generally require evidence of either (i) a valid power of attorney or (ii) a signed letter containing your name and contact information, the name and contact information of the authorized agent, and a statement of authorization for the request. Depending on the evidence provided, we may still need to separately reach out to you to confirm the authorized agent has permission to act on your behalf and to verify your identity in connection with the request.

Updates to This U.S. Personnel Notice

We will update this U.S. Personnel Notice from time to time. When we make changes to this U.S. Personnel Notice, we will change the "Last Updated" date at the beginning of this U.S. Personnel Notice. If we make material changes to this U.S. Personnel Notice, we will notify you by email, by prominent posting on our intranet, or through other appropriate communication channels. All changes shall be effective from the date of publication unless otherwise provided in the notification.

Contact Us

If you have any questions or requests in connection with this U.S. Personnel Notice or other privacy-related matters, please contact privacy@elevartx.com.