

NOTICE AT COLLECTION AND PRIVACY POLICY FOR CALIFORNIA APPLICANTS AND EMPLOYEES

LAST UPDATED: AUGUST 1, 2026

Knight Health Holdings, LLC, and/or its affiliates and related companies ("ScionHealth," "Kindred Hospitals," "us," or "we") take your privacy seriously. In compliance with the California Consumer Privacy Act (as amended, CCPA), we are providing you with this Notice at Collection and Privacy Policy for California Applicants and Employees (Privacy Policy) to inform you about how we collect, use, share, and protect your personal information.

California Notice at Collection

ScionHealth collects the personal information identified in Section 1 for the purposes identified in Section 3 and retains it for the period described in Section 5. We do not sell your personal information or disclose it for cross-context behavioral advertising ("sharing"). We also do not process sensitive personal information for the purpose of inferring characteristics about you.

EEO Statement

ScionHealth is an equal employment opportunity (EEO) employer. For more information about ScionHealth's EEO policy, click [here](#).

Assistance For the Disabled

Alternative formats of this Privacy Policy are available to individuals with a disability. Please contact Courage@ScionHealth.com for assistance.

This Privacy Policy explains:

1. The categories of personal information we collect about you
2. The categories of sources from which we collect your personal information
3. The purposes for which we use your personal information
4. How we may disclose your personal information
5. How long we keep your personal information
6. Your rights and how to exercise them
7. Changes to this Privacy Policy

Scope

This Privacy Policy applies to the personal information of California residents in their role as job applicants, employees, and workforce members of ScionHealth, including current and former employees where applicable. For purposes of this notice, "you" refers to California applicants and employees unless a section states otherwise.

"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 a particular applicant, employee, or workforce member.

1) The Categories of Personal Information We Collect about You

Identifiers such as real name, nickname or alias, postal address, telephone number, e-mail address, Social Security number, signature, online identifier, Internet Protocol address, bank account name and number for direct deposits, driver's license number or state identification card number, passport number, credit card number, and debit card number.

Professional or Employment-Related Information such as compensation, bonuses, equity grants, pensions, benefits, hours of work and attendance, evaluations, performance reviews, discipline, personnel files, expenses, education, corporate credit card details, membership in professional organizations, professional certifications, work eligibility documentation, current and past employment history, educational institutions attended, degrees and certifications, work experience, previous employers, and professional memberships and affiliations.

Non-public Educational Information such as academic transcripts, educational discipline records, academic counseling records, and other education information used to determine suitability for employment, internal roles, promotions, training eligibility, or professional licensing.

Background Screening Information such as criminal history, sex offender registration, motor vehicle records, credit history, employment history, drug testing, educational history, and other screening information used to evaluate you for suitability, continued employment, internal roles, or promotions.

Commercial Information such as records of personal property, products or services purchased, obtained, or considered, purchasing or consuming histories or tendencies, travel expense records, business expense records, and reimbursement information.

Internet or Other Similar Network Activity such as browsing history, search history, log-in/log-out records, activity on ScionHealth electronic resources, medical equipment, medical supply storage locations, interactions with ScionHealth websites, applications, job advertisements, and publicly available social media activity.

Sensory or Surveillance Data such as audio or visual recordings of interviews, recordings of customer service telephone calls, and footage from video surveillance cameras used for security, quality assurance, training, compliance, or policy enforcement purposes.

Personal Information Described in California Civil Code § 1798.80(e). To the extent not already included in other categories, for example: photograph, physical description, medical information, and benefits information used for security, internal identification, accommodation, workers' compensation, occupational health and safety, leaves of absence, wellness programs, medical emergencies, and benefits administration.

- a. **Other details**, for example: hobbies and leisure activities or membership in voluntary/charitable/public organizations, such as stated on the applicant's resume.

Inferences and Profile Data such as inferences drawn from personal information to create a profile reflecting preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, aptitudes, team-building information, employee development information, employee engagement information, and employee management information.

Characteristics of Protected Classifications Under California or Federal Law such as race, age, national origin, disability, sex, veteran status, religion, gender, pregnancy, childbirth, breastfeeding or related medical conditions, sexual orientation, gender identity, gender expression, marital status, familial status, ancestry, medical condition, military status, and other protected categories

collected where required by law or on a voluntary basis for legally permissible purposes.

- a. **Sensitive identifiers** such as Social Security, driver's license, state identification card, or passport number.

Biometric Information such as fingerprint or finger-scan templates used for timekeeping, access to medical equipment or medical supply storage, access to secure facilities, or background checks. Where used, ScionHealth does not store a fingerprint image as part of the applicable enrollment or verification process. ScionHealth also collects photographs for identification and security purposes but does not extract faceprints or other identifying metrics from photographs.

Geolocation Data such as information that can be used to determine a mobile device's physical location, vehicle location, or an individual's physical location through an RFID-enabled security badge or similar technology.

Health, Medical, and Benefits Information such as information used to accommodate disabilities, conduct direct-threat analyses, administer workers' compensation, conduct occupational health surveillance, comply with occupational health and safety requirements, conduct fitness-for-duty or pre-employment examinations, administer leaves of absence, sick time, short- and long-term disability benefits, wellness programs, and respond to medical emergencies. Such information may be considered sensitive personal information under the California Consumer Privacy Act.

Note on sensitive personal information and automated decision-making: *ScionHealth does not collect or process sensitive personal information or characteristics of protected classifications for the purpose of inferring characteristics about applicants or employees. ScionHealth does not use automated decision-making technology to make hiring or employment decisions without human review.*

2) The Categories of Sources from Which We Collect Your Personal Information

- **You**, including information in your job application, forms you fill out for us, assessments you complete, surveys you complete, and any information you provide during the course of your application and interview process.
- **Vendors and service providers** such as recruiters.
- **Third parties** such as job references, affiliated companies, professional employer organizations or staffing agencies.

- **Public internet sources** such as social media, job boards, public profiles, and other public online sources.
- **Public records**, including court records, and credentialing and licensing organizations.
- **Automated technologies** on ScionHealth's electronic resources, for example: to track logins and activity on ScionHealth's and other affiliated careers pages.
- **Surveillance/recording technologies installed by ScionHealth**, for example: video surveillance in common areas of ScionHealth facilities, and audio/video recording technologies, with consent, to the extent required by law.
- **Government or administrative agencies** such as law enforcement or public health authorities.
- **Acquired company**: If ScionHealth acquired your employer, ScionHealth might collect personal information from that employer.

Note: This Privacy Policy does not cover background screening conducted by third-party background check vendors subject to the federal Fair Credit Reporting Act. ScionHealth provides a separate disclosure for such screening.

3) The Purposes for Which We Use Your Personal Information

A. Generally Applicable Purposes:

Unless stated otherwise in section 3.B below, we may use applicants' and employees' personal information for the following purposes:

Recruiting:

- To evaluate applicants' qualifications or suitability for employment with ScionHealth,
- To communicate with applicants,
- To conduct a pre-employment or criminal history background check,
- For identification purposes,
- For diversity and inclusion purposes,
- To arrange and manage ScionHealth-sponsored events,
- To create a talent pool for future job openings,
- For recordkeeping purposes,
- To demonstrate applicants' agreement to, or acceptance of, documents presented to them (e.g., pre-employment arbitration agreement, acknowledgment of employment application, offer letter),
- To evaluate employees for other internal positions, promotions, transfers, and succession planning,
- To evaluate and improve the recruiting process, or
- To promote ScionHealth as a place to work.

Monitoring, Security, and Compliance:

- To monitor the use of ScionHealth information systems and other electronic resources or information systems,
- To conduct internal audits,
- To conduct internal investigations,
- To protect the safety and security of ScionHealth's facilities,
- To administer ScionHealth's whistleblower hotline,
- To report suspected criminal conduct to law enforcement and cooperate in investigations,
- To monitor compliance with ScionHealth policies, or
- To exercise ScionHealth's rights under applicable law and to support any claim, defense, or declaration in a case or before a jurisdictional and/or administrative authority, arbitration, or mediation panel.

Conducting Our Business:

- For training purposes or quality assurance with respect to ScionHealth employees conducting the interviews or otherwise assisting with the recruiting and hiring process,
- To administer compensation, bonuses, equity grants, other forms of compensation, benefits, vacation, sick leave, and other leaves of absence,
- To maintain personnel files, internal employee directories, workforce reporting, data analytics, retention programs, career development activities, and employee surveys,
- To facilitate communication, collaboration, team-building, morale-related activities, employee-related emergencies, and company-sponsored events or public service activities,
- For travel and event planning,
- To engage in crisis management, or
- To manage travel reimbursements.

Other Miscellaneous Purposes:

- To manage and operate information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, and strategic planning,
- To manage litigation involving ScionHealth, and other legal disputes and inquiries and to meet legal and regulatory requirements,
- To manage licenses, permits, and authorizations applicable to ScionHealth's business operations,
- In connection with a corporate transaction, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of ScionHealth or any of its subsidiaries or affiliates, and
- To protect the rights, property, or safety of ScionHealth, HR Individuals, customers, or others.

B. Purposes Specific to Certain Categories of Personal Information:

We may use the categories of applicants' personal information listed in this Section 3.B for the purposes stated below:

Purposes for Using Biometric Information:

ScionHealth may use biometric information in the form of fingerprints or finger-scan templates to conduct criminal history background checks, control and monitor access to medical equipment or medical supply storage locations, support timekeeping and attendance systems, control access to secure facilities, monitor use of Company information systems and other electronic resources, and protect the safety and security of ScionHealth facilities. Where applicable systems convert a scan into a numerical or mathematical template, ScionHealth does not store a fingerprint image as part of the enrollment or verification process.

Purposes for Using Geolocation Data:

ScionHealth may use geolocation data to assist with routing, confirm that an applicant or employee has arrived at or left an off-site or ScionHealth work location when scheduled, support customer service, provide training, manage emergencies, monitor safety, monitor compliance with Company policies, protect facilities and personnel, and determine whether employment-related action is appropriate.

Purposes for Using Health, Medical, and Benefits Information:

- To the extent necessary to comply with ScionHealth's legal obligations, such as to accommodate disabilities,
- To protect the health and safety of ScionHealth's employees and facilities, for example: to take the applicant's temperature,
- For occupational health and safety compliance and record-keeping,
- To conduct pre-employment medical examinations,
- To respond to an applicant's medical emergency, or
- To administer workers' compensation, occupational health surveillance, fitness-for-duty evaluations, leaves of absence, sick time, wellness programs, short- and long-term disability benefits, and other benefits.

Note: *This Privacy Policy does not cover health information governed by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), or California's Confidentiality of Medical Information Act (CMIA).*

Purposes for Using Protected Categories of Information:

ScionHealth collects information about race, age, national origin, disability, sex, and veteran status as necessary to

comply with legal obligations, including reporting requirements under the federal Equal Employment Opportunity Act, the federal Office of Contracting Compliance Programs where applicable, and California's Fair Employment and Housing Act, and for legally permissible diversity, equity, inclusion, workforce analytics, and emergency assistance purposes.

ScionHealth also uses protected classification information where necessary to comply with federal and California law related to accommodations, leaves of absence, benefits, tax administration, identity verification, emergency assistance, military and veteran leave requirements, and other legally permissible employment or applicant-related purposes.

ScionHealth collects protected categories of personal information on a purely voluntary basis, except where required by law, and uses the information only in compliance with applicable laws and regulations.

De-identified Information

At times, ScionHealth converts personal information into de-identified information using reasonable measures to ensure that the de-identified information cannot be associated with the individual ("De-identified Information"). ScionHealth maintains De-identified Information in a de-identified form and does not attempt to re-identify it, except that ScionHealth may attempt to re-identify the information solely for the purpose of determining whether its de-identification processes ensure that the information cannot be associated with the individual. ScionHealth prohibits vendors, by contract, from attempting to re-identify ScionHealth's De-identified Information.

4) How We May Disclose Your Personal Information

ScionHealth generally maintains information related to applicants and employees as confidential. However, from time to time, ScionHealth may have a legitimate business need to disclose personal information for one or more of the purposes listed in this Privacy Policy to one or more of the categories of external recipients listed below. In that event, ScionHealth discloses personal information and/or sensitive personal information only to the minimum extent necessary to achieve the purpose of the disclosure and only if the disclosure is permitted by the CCPA and other applicable laws:

- **Service Providers and Contractors:** ScionHealth discloses your personal information to service providers and contractors for the purposes above to assist us in our recruiting efforts and in meeting our business needs and legal obligations.
 - » ScionHealth only discloses your personal information to service providers and contractors subject to writ-

ten contracts as required by applicable law.

- » Service providers and contractors include recruiters, law firms, travel agencies, and any other entity providing services to ScionHealth.
- **Affiliated Companies:** Other companies within the ScionHealth family of companies.
- **Government or Administrative Agencies:** These may include, for example:
 - » Equal Employment Opportunity Commission as required for reporting.
 - » California Department of Fair Employment and Housing as required to respond to employment claims and charges.
 - » Law enforcement in the event of criminal investigations.
- **Required Disclosures:** We may be required to disclose personal information in a court proceeding, in response to a court order, subpoena, civil discovery request, other legal process, or as otherwise required by law.
- **Legal Compliance and Protections:** We may disclose personal information when we believe disclosure is necessary to comply with the law or to protect the rights, property, or safety of ScionHealth, our users, or others.
- **Corporate Transactions:** We may disclose your personal information in connection with a corporate merger, consolidation, bankruptcy, the sale of all – or substantially all – of our membership interests and/or assets, or other corporate change, including to any prospective purchasers.

No sales and no “sharing” (i.e., disclosure for cross-context behavioral advertising):

ScionHealth does not sell the personal information of applicants or employees and does not share their personal information for cross-context behavioral advertising.

5) How Long We Keep Your Personal Information

If ScionHealth hires you, the information collected during the job application process may become part of your personnel file and may be used to administer the employment relationship and for related reporting, compliance, benefits, security, operational, and recordkeeping purposes. ScionHealth will retain this application and employment information for the entire duration of your employment relationship with ScionHealth and for as long thereafter as permitted or required by applicable law, legal process, administrative need, or to exercise or defend legal claims. ScionHealth makes its document retention schedule available to employees for review.

ScionHealth will retain information of applicants who are not hired for four (4) years after the record is collected and may retain longer as required by applicable law or regulation, by legal process, for administrative purposes, or to exercise or defend legal claims.

These records will be retained for our internal recordkeeping and reporting purposes in compliance with California Government Code § 12946. During that time, we may use your information to consider you for positions in addition to the position(s) for which you initially applied.

6) Your Privacy Rights and How to Exercise Them

a. Your California Privacy Rights

Subject to applicable law, exemptions and limitations, you have the following rights:

- **Right to Know:** You have the right to submit a verifiable request for copies of specific pieces of your personal information collected in the preceding 12 months and for information about ScionHealth’s collection, use, and disclosure of your personal information during that same 12-month period. In addition, you have a right to know the categories of your personal information that ScionHealth sold or shared for cross-context behavioral advertising and the parties to which those categories were sold or shared.

Please note that the CCPA’s right to obtain copies does not grant a right to the whole of any document that contains personal information, but only to “specific pieces” of personal information. Moreover, HR Individuals have a right to know categories of sources of personal information and categories of external recipients to which personal information is disclosed, but not the individual sources or recipients. ScionHealth does not always track individualized sources or recipients.

- **Right to Delete:** You have the right to submit a verifiable request for the deletion of personal information that you have provided to ScionHealth.
- **Right to Correct:** You have the right to submit a verifiable request for the correction of inaccurate personal information maintained by ScionHealth, taking into account the nature of the personal information and the purposes of processing the personal information.
- **Right to Opt Out of Sale and Sharing:** You have the right to opt out of the sale of your personal information and the disclosure of your personal information for cross-context advertising. As noted above, ScionHealth does not sell personal information or disclose personal information for cross-context advertising.

- **Right to Restrict Use and Disclosure of Sensitive Personal Information:** You have the right to restrict ScionHealth's use and disclosure of your sensitive personal information to purposes permitted under the CCPA, such as security, quality control, uses required by law, and disclosures to vendors in support of the permitted purposes. This right applies only to sensitive personal information collected or processed by ScionHealth for the purpose of inferring characteristics about you. As noted above, ScionHealth does not collect or process your sensitive personal information for the purpose of inferring characteristics, and therefore this right does not apply.

The CCPA does not restrict our ability to do certain things like comply with other laws or comply with regulatory investigations. We also reserve the right to retain, and not to delete, certain personal information after receipt of a request to delete from you where permitted by the CCPA or another law or regulation.

b. How to Exercise Your Rights

ScionHealth will respond to requests to know, delete, and correct in accordance with applicable law if it can verify the identity of the individual submitting the request. You can exercise these rights in the following ways:

- **Call:** 1-833-326-8724
- **Email:** Courage@ScionHealth.com

We do not sell or share your personal data for targeted or cross-context behavioral advertising. We only use your sensitive personal information for permitted purposes.

c. How We Will Verify Your Request

We verify requests using information we already maintain where feasible and avoid requesting sensitive personal information unless necessary. Any additional information collected for verification is used only for that purpose and deleted when no longer required.

d. Authorized Agents

If an authorized agent submits a request to know, correct or delete on your behalf, the authorized agent must submit with the request either (a) a power of attorney that is valid under California law, or (b) a document signed by you that authorizes the authorized agent to submit the request on your behalf. In addition, we may ask you or your authorized agent to follow the applicable process described above for verifying your identity. You can obtain the "Authorized Agent Designation" form by contacting us at Courage@ScionHealth.com.

e. ScionHealth's Non-Discrimination and Non-Retaliation Policy

ScionHealth will not unlawfully discriminate or retaliate against you for exercising your privacy rights under the CCPA.

7) Use of Certain AI Tools

To ensure accuracy and allow our interviewers to focus fully on our conversation with you, we may use an AI-powered notetaking tool during virtual interviews. This tool will record and transcribe the interview and generate a summary of the discussion to ensure accurate notes for our hiring team's review. The use of this tool helps us maintain consistent and fair evaluation practices across all candidate interviews. The tool analyzes speech patterns for transcription purposes only. The tool does not make any hiring decisions. The generated notes will be used solely for evaluation purposes related to the hiring process, will be stored securely and limited to authorized members of our hiring team, and will not be shared externally or used for any other purpose.

8) Changes to This Privacy Policy

This policy is reviewed periodically and updated as required by law. The "Last Updated" date shows when it was last revised.

For More Information

For questions or concerns about ScionHealth's privacy policies and practices, please contact:

Chief Privacy Officer

680 South Fourth Street
Louisville, KY 40202

Phone: 1-833-326-8724

Email: Courage@ScionHealth.com