

# Fulton County Health Center JOB APPLICANT PRIVACY NOTICE

**Last Updated: 6/23/25**

This Job Applicant Privacy Notice (the “Notice”) explains, in plain language, how Fulton County Health Center (“FCHC”) collects, uses, shares, and protects the individually identifiable information (“Personal Information” or “Personal Data”) we collect from and about you when you apply for jobs with us. It also describes the choices and rights you have. We are committed to protecting the privacy and security of the Personal Information we collect during the application process. Please read this Notice carefully. If you have questions, reach out using the contact details at the end of this Notice.

This Notice reflects FCHC’s practices related to the application and recruitment process and how it is used. Other data may be collected about you during this process, including data collected automatically by our website, that is not used by FCHC during the recruitment process. As a result, this Notice does not address the collection or use of such information. Please review FCHC’s Privacy Notice for information about how we collect, use, and disclose such information.

Additionally, in the event that FCHC extends you an offer of employment, additional Personal Information will be collected from or about you. Such information is collected, used, and disclosed pursuant to our Employee Privacy Policy, a copy of which will be provided to you should an offer of employment be extended.

## **I. WHAT INFORMATION DO WE COLLECT?**

When you apply for a position at FCHC, we may collect a range of Personal Information, as listed below:

<b>Category</b>	<b>Examples</b>
Contact Details	Name, mailing address, email address, phone number
Identification & Eligibility	Social Security number, government-issued ID, work-authorization documents, driver’s license, passport number
Application Materials	Résumé/CV, cover letter, employment history, education, professional licenses, references (and any information obtained from references with your consent), salary expectations, work preferences, previous applications
Assessments & Interviews	Interview notes, screening question responses, video/audio recordings (if you choose), contents of communications (including emails and online chats) with FCHC representatives
Background Information	Background check results, credential verification, drug-screen results, criminal history (where permitted by law)
Equal Opportunity Data	Race/ethnicity, gender, veteran status, disability status (all voluntary)

Category	Examples
Health-Related Data	Information needed for reasonable accommodations, vaccination status (where required)
Automated Screening Data	Scores or categories generated by automated tools to match your qualifications to job requirements

We collect this information directly from you, from your use of our online systems, and, where applicable, from third parties such as background check providers or references.

## II. HOW DO WE USE YOUR PERSONAL INFORMATION?

FCHC may use Personal Information as permitted by law, for the following business purposes:

- **Processing your application:**
  - Reviewing your qualifications;
  - Scheduling and conducting interviews;
  - Administering assessments and tests;
  - Making hiring decisions; and
  - Demonstrating agreement to, or acceptance of, applicable documentation.
- **Communicating with you:**
  - Sending updates on your application status;
  - Requesting additional information; and
  - Notifying you of future job opportunities.
- **Verifying your information:**
  - Confirming your identity and work eligibility; and
  - Checking credentials, background, and references.
- **Legal and regulatory compliance:**
  - Meeting federal, state, and local requirements (e.g., equal employment, immigration, health, and safety laws).
- **Improving our processes:**
  - Measuring the effectiveness of recruiting campaigns; and
  - Enhancing our hiring processes.
- **Protecting FCHC:**
  - Preventing fraud;
  - Detecting security threats; and
  - Defending against legal claims.

***Disclosure of Personal Information:*** To the extent permitted by law, your Personal Information may be disclosed with the following categories of third parties:

- **Internal Staff and Departments:**
  - Human Resources personnel involved in recruitment, hiring, and onboarding;
  - Hiring managers and designated interviewers for the position you applied for;

- IT administrators and support staff responsible for maintaining and securing our systems;
- Compliance, privacy, and legal personnel, if required for regulatory or legal purposes;
- Security staff, only as necessary to investigate or respond to security incidents;
- Senior management and executives, if necessary for oversight or decision-making; and
- Internal audit and risk management teams .
- **External Service Providers\* and Vendors:**
  - Background-check and credential verification companies;
  - Drug-screening vendors;
  - Skills and assessment testing services;
  - Applicant tracking system (ATS) and recruitment software providers;
  - Video interview and virtual meeting platforms;
  - IT infrastructure and cloud hosting providers;
  - Data analytics and reporting service providers; and
  - Payroll, benefits, and onboarding service providers (if you are hired).
- **Government Agencies, Law Enforcement, or Courts:**
  - When required to comply with federal, state, or local law, regulation, subpoena, court order, or other legal process; and
  - To respond to requests from regulatory authorities or law enforcement.
- **Professional Advisors:**
  - External lawyers, legal counsel, and consultants;
  - Auditors and accountants; and
  - Insurers and risk management consultants (to protect our legal or regulatory interests).
- **Parties Involved in Corporate Transactions:**
  - In the event of a merger, acquisition, reorganization, sale, joint venture, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock, your data may be shared with the new owner or successor entity, subject to continued protection and confidentiality obligations.
- **Other Third Parties (as required or permitted by law):**
  - References and former employers (for verification purposes, with your authorization);
  - Accrediting, licensing, or certification bodies (if relevant to the position);
  - Unions or works councils, if required by applicable law or collective bargaining agreements; and
  - Any other third party with your explicit consent.

\* All service providers are contractually required to keep your data confidential and use it only as instructed by FCHC.

The following chart summarizes who may receive your data:

Recipient	Purpose
Internal staff and departments	Application review, hiring, IT support, compliance, management
Service providers and vendors	Background checks, testing, system management, IT infrastructure
Government/courts/agencies	Legal and regulatory compliance
Professional advisors	Legal, audit, insurance, and risk management matters
Corporate transaction parties	Mergers, acquisitions, reorganizations, or asset transfers
Other third parties	References, licensing bodies, unions, with consent or as required

***Legal Basis for Processing:*** FCHC processes applicant data only when permitted by applicable law. This includes taking pre-contractual steps necessary to evaluate and potentially hire you, pursuing FCHC's legitimate business interests such as efficient recruitment, workforce planning, and protection against fraud, and fulfilling legal obligations related to employment, tax, immigration, equal opportunity, and public health laws.

In some cases, FCHC may request your express consent, for example, when asking for sensitive information such as disability status for accommodations or when required for background checks. You may withdraw your consent at any time.

***How Long FCHC Keeps Your Data:*** If you are hired, your data becomes part of your employment record and is retained according to FCHC's data retention schedule. For unsuccessful applicants, we normally keep your data for up to three (3) years after the hiring decision. This retention period allows FCHC to demonstrate that it conducted a fair hiring process, comply with record-keeping laws, and consider you for future openings unless you request otherwise. After the retention period, FCHC securely deletes or de-identifies your data.

### III. YOUR RIGHTS RELATED TO YOUR PERSONAL INFORMATION

FCHC provides several ways for you to exercise certain privacy choices regarding your Personal Information processed by FCHC. FCHC is committed to respecting your privacy rights under all applicable privacy laws. These rights are designed to give you greater transparency and control over your information. Depending on your circumstances, you may be able to exercise one or more of the following rights:

- **Access:** You may have the right to request and receive a copy of the personal data FCHC holds about you. This includes information you have provided to us, as well as data generated during the application process (such as interview notes, assessment results, and communications). You may request a summary of the categories of data collected about you, the purposes for which it is used, and the parties with whom it has been shared.
- **Correction (Rectification):** If you believe that any Personal Information FCHC holds about you is inaccurate, incomplete, or outdated, you may request that FCHC correct

or update it. FCHC will promptly investigate and make corrections as appropriate. You may also supplement your data with additional information if you believe it is necessary for accuracy.

- **Deletion (Erasure):** You may request that FCHC delete your personal data when it is no longer necessary for the purposes for which it was collected, if you withdraw your application, or if you believe FCHC is processing it unlawfully. Please note that certain data may need to be retained for legal, regulatory, or record-keeping purposes, but FCHC will inform you if this is the case.
- **Restriction of Processing:** You may request that FCHC restrict the processing of your personal data in certain circumstances, such as if you contest the accuracy of the data, if you believe the processing is unlawful, or if you need FCHC to retain the data for legal claims. If we restrict processing of your data, FCHC will continue to store your data but not use it for other purposes.
- **Objection to Processing:** You may have the right to object to certain types of processing, such as automated screening or processing based on FCHC's legitimate interests. If you object, FCHC will review your request and, where required by law, cease or limit the processing unless FCHC has compelling legitimate grounds to continue.
- **Data Portability:** You may request to receive a copy of the personal data you have provided to FCHC in a structured, commonly used, and machine-readable format. Where feasible, you may also request that FCHC transmit this data directly to another organization of your choice.
- **Withdraw Consent:** Where FCHC relies on your consent to process specific types of data (such as sensitive information or background checks), you have the right to withdraw your consent at any time. Withdrawing consent will not affect the lawfulness of processing carried out before your withdrawal but may impact FCHC's ability to consider you for certain positions.
- **Human Review of Automated Decisions:** If you are subject to automated screening or decision-making, you may request a human review of the outcome and provide additional information for consideration.
- **Explanation and Information:** You may request further information about how your data is processed, including the categories of data collected, the purposes of processing, the recipients of your data, and the criteria used to determine retention periods.

FCHC will process any request in accordance with – and where required by – applicable law with respect to your Personal Information. FCHC will take steps to verify your identity before implementing your request. FCHC does not charge a fee to process or respond to your verifiable consumer request unless it is excessive, repetitive, manifestly unfounded, otherwise creates a burden or workload in excess of standard requests or is prohibited by law. If it is determined that a fee is warranted by the request, you will be informed of the determination and provided both a written justification for the fee, as well as a cost estimate, prior to completing your request.

Although our active systems and databases will reflect updates that have been requested and processed, FCHC may retain all Personal Information for backups, archiving, prevention of

fraud and abuse, analytics, and satisfaction of other legal obligations we reasonably believe applicable.

#### Time for Changes to Take Effect

FCHC aims to complete requests as soon as reasonably practicable and consistent with any applicable laws. Requests made on behalf of another, and thus requiring confirmation of the authority of the agent and the authenticity of the requestor, will likely take more time to complete.

FCHC may need to retain certain information for recordkeeping purposes and/or to complete any actions that you began prior to requesting a change or deletion. There may also be residual information that will remain within FCHC databases and other records, which will not be removed. FCHC may not always be able to fully address your request, for example if it would impact the duty of confidentiality owed to others, or if FCHC is legally entitled to deal with the request in a different way.

#### IV. HOW WE PROTECT YOUR INFORMATION

FCHC is committed to maintaining the security of your Personal Information. FCHC implements a comprehensive set of technical, organizational, and administrative safeguards designed to protect your data against loss, misuse, unauthorized access, disclosure, alteration, or destruction.

***Who Has Access:*** Access to your Personal Information is strictly limited to specific personnel who require it to perform their job duties. This includes:

- Human Resources staff involved in recruitment and hiring;
- Hiring managers and designated interviewers for the position you applied for;
- IT administrators responsible for maintaining and securing our systems;
- Compliance, privacy, and legal personnel, if required for regulatory or legal purposes;
- Security staff, only as necessary to investigate or respond to security incidents;
- Senior management and executives, if necessary for oversight or decision-making;
- Internal audit and risk management team;s
- Service providers and vendors who support our recruitment, background checks, drug screening, skills testing, applicant tracking systems, video interview platforms, and IT infrastructure (all contractually required to protect your data and use it only as instructed);
- Professional advisors, such as external lawyers, auditors, and insurers, for legal, audit, or insurance matters;
- Government agencies, courts, or law enforcement, when required to comply with law, regulation, subpoena, or court order; and
- Parties involved in corporate transactions, such as a merger, acquisition, reorganization, or transfer of assets, subject to continued protection of your data All

personnel and third parties with access to applicant data are required to follow strict confidentiality obligations and receive training on data privacy and security.

All personnel with access to applicant data are required to follow strict confidentiality obligations and receive training on data privacy and security.

***Security Measures:*** Your Personal Information is protected by industry-standard security measures and processes. To maintain that security FCHC employs the following:

- We use role-based access controls to ensure only authorized individuals can view or process your data.
- Applicant data is stored in secure, access-controlled systems and databases, with encryption applied both in transit and at rest.
- Physical access to servers and offices where data is stored is restricted to authorized staff only.
- We regularly review and update our security policies and conduct audits to monitor compliance.
- Our systems are protected by firewalls, intrusion detection systems, and anti-malware tools.
- We require strong authentication (such as unique user IDs and passwords) for all personnel accessing applicant data.
- Regular security awareness training is provided to all staff with access to Personal Information.

While FCHC strives to use reasonable and appropriate security measures, no system can be guaranteed to be 100% secure. If you have reason to believe that your Personal Information has been compromised or accessed in an unauthorized manner, please contact us immediately using the details provided below.

## **V. AGE RESTRICTIONS**

FCHC does not knowingly collect any Personal Information from children under the age of 13. Parents and legal guardians are encouraged to monitor their children's Internet usage and to help enforce this Privacy Notice by instructing their children never to provide Personal Information without parental permission. If a parent or guardian believes that FCHC has Personal Information of a child under the age of 13 in its database, please contact us immediately at [employment@fulhealth.org](mailto:employment@fulhealth.org) and we will use our best efforts to promptly remove such information from our records.

## **VI. AUTOMATED DECISION-MAKING**

We or our third-party vendor (currently Paylocity) may use computer-based tools to help screen résumés and match applicants to job requirements. These tools may assign scores based on objective factors such as education, certifications, and years of experience. **No final hiring decisions are made solely by automated means; a human reviewer is always involved.**

You have the right to request a human review of any automated screening result. You may also provide additional information that you believe is relevant to your qualifications. If you object to our use of automated tools, you may do so without harming your application, although it may slow the review process.

## **VII. CHANGES TO THIS NOTICE**

We may periodically update this Job Applicant Privacy Notice. Please reference the “LAST UPDATED” legend at the top of this page to see when this Notice was last revised. Any changes to this Notice will become effective when we post the revised Notice online.

In the event that any changes to this Privacy Notice could potentially require you to provide renewed or additional consent for the use of your Personal Information, notice of the requirement, as well as information we are required to disclose related to your renewed or additional consent, will be sent to you directly via email, text message, and/or any other acceptable means of contact under applicable law.

## **VIII. RESERVATION OF RIGHTS**

Regardless of any other provision in this Privacy Notice, we reserve the right to disclose any personally identifiable or non-personally identifiable information about you to: (a) fulfill a government request; (b) conform with the requirements of the law or legal process; (c) protect or defend our legal rights or property, our Website, or other users; or (d) protect, in an emergency, the health and safety of our customers or the general public. This includes exchanging information with third parties and organizations in connection with credit risk reduction and fraud protection.

## **IX. HOW TO CONTACT US**

**Contact: Rachel Geckle**  
Fulton County Health Center  
725 S. Shoop Avenue  
Wauseon, OH 43867  
Email: [employment@fulhealth.org](mailto:employment@fulhealth.org)  
Phone: (419) 335-2015