

Biometric Screening and Privacy Policy

Policy No. 6-06

Policy Owner: IT and HR

Original Effective Date: 7/17/2026

Revision Effective Date:

PURPOSE

This policy governs the collection, use, storage, disclosure, retention, and destruction of biometric identifiers and biometric information, including facial geometry/faceprint/image along with ID capture that can include name ,address ,DOB, ID type, sex ,height ,weight, eye and hair color, and ID number (“RP” and/or the “Practice”). The Practice contracts a vendor to provide the above data collection services in connection with the interview (when permissible by state law) and pre-employment process. This policy is intended to advise candidates and teammates of the nature of collection and their rights under any and all state applicable laws.

SCOPE

This policy applies to all teammates, contractors, and job applicants whose biometric data may be collected and/or processed by the practice.

POLICY

Definitions:

- **“Biometric Identifier”** includes retina or iris scans, fingerprints, voiceprints, or scans of hand/face geometry.
- **“Biometric Information”** means any information used to identify an individual based on their biometric identifier.
- **“Confidential and Sensitive Personal Information”** means personal information that can be used to uniquely identify an individual or an individual’s account or property.
- **“Electronic Signature”** means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
- **“Private Entity”** means an individual, partnership, corporation, limited liability company, association, or other group, however organized. This does not include any state or local government agency.
- **“Written Release”** means informed written consent, electronic signature, or, in the context of employment, a release executed by an employee as a condition of employment.

Collection of Biometric Data

The Practice’s 3rd party vendor, Incode Technologies, Inc. will collect data only where reasonably necessary for legitimate business purposes, such as:

- Identity verification processes

Prior to collecting any biometric data, the Practice will:

- Provide written notices to the teammate and/or candidate
- Obtain prior, informed written consent from the teammate and/or candidate

Notice Requirements

Before collecting biometric data, the Practice will provide written notice that includes the following:

- The specific biometric data being collected
- The purpose of the collection and use
- The length of time the data will be retained
- How the data will be stored, used, and destroyed
- The teammates and/or candidates rights under applicable law

Use Limitations

The Practice and its 3rd party vendor will use biometric data solely for the purposes disclosed at the time of the collection. The data will not be sold, leased, traded or otherwise profited from. Biometric data will not be used for any undisclosed or unauthorized purpose.

Disclosure and Sharing

The Practice will not disclose or disseminate biometric data unless:

- The teammate and/or candidate provides prior consent
- Disclosure is required by law, subpoena, or court order
- Disclosure is necessary to complete a transaction requested by the individual
- Data is shared with authorized vendors providing services on behalf of the Practice

All 3rd party vendors must:

- Enter into a written agreement
- Use biometric data only for contracted services
- Maintain appropriate security safeguards
- Comply with applicable laws and this Policy

Data Security

The Practice in conjunction with their 3rd party vendor, will implement reasonable safeguards designed to protect biometric data including:

- Encryption and secure storage methods
- Access controls limiting data access to authorized personnel only
- Regular monitoring and risk assessments
- Protections equivalent to or greater than those used for other sensitive personal data

Individual Rights

Where required by law, individuals may have the right to:

- Request access to their biometric data
- Request deletion of their biometric data
- Withdraw previously provided consent
- Restrict or object to certain uses of biometric data

Requests may be submitted to HR@radpartners.com

Alternative Methods

The Practice recognizes that certain individuals may be unable to provide biometric data due to medical conditions, disabilities, religious beliefs, or other legally protected reasons.

Accordingly, the Practice will provide reasonable accommodations and/or alternative identification methods consistent with applicable federal and state law.

Requests should be submitted to HR@radpartners.com

The Practice will engage in an interactive process, where required by law, to determine if an appropriate accommodation can be provided.

Prohibition on Retaliation

The Practice prohibits retaliation against any individual who:

- Refuses to provide biometric data where alternatives are available
- Exercises rights under applicable privacy laws
- Raises concerns regarding the use of biometric data

Vendor Management

All vendors or service providers handling biometric data must:

- Maintain confidentiality and security of the data
- Use the data for authorized purposes only
- Not sell or disclose the data unlawfully
- Delete or return the data upon request or termination of services

Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment or contract.