Kyron Medical Privacy Policy

Effective Date: June 1, 2025

Kyron Medical, Inc. (“Kyron Medical,” “we,” “us,” or “our”) is committed to protecting the privacy and security of the information we handle. This Privacy Policy pertains to our websites, software, AI-powered tools, and other online services (collectively, the “Services”).

This Privacy Policy describes how Kyron Medical collects, uses, and discloses information in its capacity as a Business Associate to our healthcare provider clients (“Clients”). This Policy should be read in conjunction with our **Terms of Service** and the **Business Associate Agreement (BAA)** executed between Kyron Medical and our Clients. In the event of a conflict regarding Protected Health Information (PHI), the BAA will govern.

By using our Services, you are agreeing to the practices described in this Privacy Policy.

What Types of Information Does Kyron Medical Collect?

Kyron Medical collects information necessary to provide and improve our Services and to maintain our business relationship with you.

- **Client-Provided Information:** We collect information that you, our Client, provide to us. This includes:
    - **Account Information:** Business contact details such as name, email address, phone number, and mailing address for your authorized users.
    - **Data for Processing:** To perform our Services, you will provide us with data, which may include Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA). This data is processed transiently to generate outputs (e.g., appeal letters, payer interaction scripts) and is handled strictly in accordance with our BAA and internal security policies.
- **Automatically Collected Information:** When you use our Services, we automatically collect certain technical information to ensure the operational integrity, security, and performance of our platforms. This may include:
    - **Log and Usage Data:** Information such as your IP address, browser type, operating system, system activity, API call metadata, and the dates and times of your requests. These logs are essential for security monitoring, auditing, and troubleshooting.
    - **Device Information:** We may collect information about the device you use to access our Services.

- **Information from Cookies and Similar Technologies:** We use “cookies” and similar technologies to help us operate and analyze our Services. These technologies can help us recognize you, store your preferences, and collect statistical information about the use of our Services. You may be able to refuse the use of cookies by selecting the appropriate settings on your browser; however, doing so may affect the functionality of our Services.

How Does Kyron Medical Use My Information?

Kyron Medical uses the information we handle for legitimate business purposes, governed by our agreements with you and by applicable law. These purposes include:

- **To Provide and Operate Our Services:** Our primary use of information, including any PHI provided, is to perform the revenue cycle management services you have contracted for. This includes processing data through our Voice AI and Letter of Appeal Generation AI to create the required outputs.
- **To Maintain and Improve Our Services:** We use technical and usage data to monitor the performance of our systems, improve user experience, and develop new features.
- **To Secure Our Services:** We use information for security purposes, such as monitoring for unauthorized access, preventing breaches, and investigating potential security incidents.
- **To Communicate With You:** We use your account information to send you service-related communications, respond to your inquiries, provide support, and inform you of updates.
- **For Compliance and Auditing:** We maintain records as required by law and our contractual obligations, including generating audit trails for security and HIPAA compliance.
- **AI Model Training:** Our AI models are trained on de-identified or synthetic data. We will not use your PHI to train our AI models without your explicit, prior written opt-in consent. Any such opt-in process is subject to stringent internal controls, as detailed in our AI Security and Responsible Use Policy.

When Will Kyron Medical Disclose My Information?

Kyron Medical discloses information only as necessary to provide our Services and as permitted by law and our BAA. We do not sell your personal information or Protected Health Information.

- **With Our Subcontractors and Service Providers:** We engage trusted third-party subcontractors (such as Amazon Web Services and OpenAI) to provide the underlying infrastructure and technology for our Services. These subcontractors are bound by BAAs and other contractual obligations to maintain the confidentiality and security of the data they process on our behalf, with many adhering to a Zero Data Retention standard.

- **At Your Direction:** We provide the outputs generated by our Services (e.g., draft appeal letters) directly to you, our Client, for your use.
- **For Legal Reasons:** We may disclose information if required to do so by law, subpoena, or other legal process, or if we believe in good faith that disclosure is necessary to protect our rights, your safety, or the safety of others.
- **In Connection with a Business Transfer:** If Kyron Medical is involved in a merger, acquisition, or sale of all or a portion of its assets, information may be transferred as part of that transaction, subject to confidentiality and security commitments.
- **With Your Consent:** We may share information for other purposes with your express consent.

Security and Information Retention

Kyron Medical implements and maintains robust administrative, technical, and physical security measures designed to protect the information we handle. These measures include:

- **Encryption:** Data is encrypted in transit (TLS 1.2+) and at rest (AES-256).
- **Access Controls:** We use role-based access controls (RBAC) and multi-factor authentication (MFA) to limit access to systems and data.
- **Transient Processing:** PHI is processed in memory transiently (typically for less than 5 seconds) and is not persistently stored in model weights or logs.
- **Retention and Destruction:** AI-generated outputs are retained for 30 days for quality control and audit purposes, after which they are securely deleted according to NIST 800-88 standards. System and audit logs are retained for 90 days. All retention and destruction activities are logged and auditable.

International Visitors

Our Services are designed for and hosted exclusively within the United States. All data processing, storage, and transmission occurs on Amazon Web Services (AWS) infrastructure located in the `us-east-1` region within the continental USA. No data is stored, processed, accessed, or destroyed outside the United States.

Children's Privacy

Our Services are intended for use by healthcare organizations and not for direct use by children under the age of 16. We do not knowingly collect personal information directly from children. While our Services may process PHI related to minors on behalf of our Clients, all such processing is done under the terms of our BAA with the healthcare provider.

State Privacy Rights

Certain state privacy laws (such as in California, Colorado, and Virginia) provide residents with specific rights regarding their personal information.

As a Business Associate, Kyron Medical acts as a **Service Provider** to our Clients (the Covered Entities). We collect and process personal information, including PHI, on their behalf and at their direction. Therefore:

- **Requests from Individuals (Patients):** If you are a patient whose information may have been processed by our Services and you wish to exercise your privacy rights (such as the right to access, correct, or delete your data), you must direct your request to your healthcare provider. Your provider is the entity responsible for managing your data and responding to your request.
- **Our Role:** We will assist our Clients in responding to such requests as required by our BAA and applicable law.

We do not “sell” personal information or “share” it for cross-context behavioral advertising as those terms are defined under applicable state privacy laws. We only use and disclose information for the specific business purposes outlined in our agreements.

Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. If we make material changes, we will notify you by updating the date of this Privacy Policy and posting it on our Services.