

Acceptable Use Policy

Coris Frontiers, Inc.

Last Updated: October 14, 2026

This Acceptable Use Policy (the “Policy”) describes how the Coris Match platform and our other Services may and may not be used. Coris Frontiers, Inc. (“Coris,” “we,” “us,” or “our”) built Coris Match to help qualified research teams identify patients who may be eligible for clinical research studies. Because the Services work with sensitive health information inside our customers’ environments, we ask everyone who uses them to do so responsibly, lawfully, and in a way that protects patients and research participants.

1. Scope and Relationship to Other Terms

1.1 Who This Policy Applies To. This Policy applies to every customer organization that uses the Services (“you” or “your”) and to every individual who accesses the Services on a customer’s behalf, including employees, investigators, research coordinators, and contractors (“Authorized Users,” as defined in the Terms). It also applies to visitors to our website at www.corisfrontiers.com (the “Website”).

1.2 Part of Your Agreement With Us. This Policy is part of, and supplements, our Terms of Service (the “Terms”), including Section 9 (Acceptable Use). It works together with any Order Form, Business Associate Agreement (“BAA”), Data Use Agreement (“DUA”), Data Processing Agreement (“DPA”), and AI Terms between you and Coris. If this Policy conflicts with one of those agreements, the order of precedence in Section 19.1 of the Terms applies. Our Privacy Policy explains how we handle personal information.

1.3 Defined Terms. Capitalized terms used but not defined in this Policy, such as “Customer Data,” “Equipment,” “Output,” “PHI,” and “Services,” have the meanings given in the Terms.

1.4 Examples, Not a Complete List. The rules in this Policy are examples of conduct we do not permit. They are not exhaustive. If you are unsure whether a particular use is permitted, please contact us before proceeding.

2. Permitted Use

2.1 Intended Purpose. The Services may be used only for their intended purpose: helping qualified research personnel identify, prescreen, and review individuals who may be eligible for clinical research studies, under an approved study protocol, as described in Section 3 of the Terms and in the Documentation.

2.2 Authorized Access Only. Only Authorized Users whom you have approved, and who have a legitimate research or operational need, may access the Services. Each Authorized User must use the Services through their own individually assigned account and only within the roles and permissions their organization has assigned.

2.3 Minimum Necessary. Authorized Users should access, view, and use only the Customer Data reasonably necessary for their assigned research tasks, consistent with HIPAA's minimum necessary standard and your institution's policies.

2.4 Compliance With Your Obligations. All use of the Services must comply with applicable law, your institutional policies, any applicable institutional review board ("IRB") approval or waiver, your study protocols, and your agreements with Coris.

3. Prohibited Uses

You may not use the Services, and you may not allow or help anyone else to use the Services, in any of the following ways.

3.1 Unlawful or Harmful Activity. Do not use the Services to:

- violate any applicable law or regulation, including HIPAA, the HITECH Act, the Common Rule, FDA human subject protection regulations, state health privacy and consumer protection laws, anti-discrimination laws, and export control and sanctions laws;
- infringe, misappropriate, or violate the intellectual property, privacy, publicity, or other rights of any person;
- engage in fraud, deception, or misrepresentation, including misrepresenting your identity, credentials, or affiliation, or the source or nature of any Output;
- harass, threaten, intimidate, or harm any person; or
- facilitate any activity that would violate the healthcare compliance commitments in Section 19.2 of the Terms, including offering or receiving anything of value in exchange for patient referrals or study enrollment.

3.2 Misuse of Customer Data and Patient Information. Do not use the Services to:

- access, view, or use patient information for any purpose other than an authorized research purpose, including out of personal curiosity or for matters involving yourself, family members, friends, coworkers, or public figures;
- sell, license, rent, or trade patient information or Output, or use it for marketing, advertising, or any commercial purpose unrelated to the approved study;
- profile, score, or make decisions about individuals for insurance underwriting, eligibility for benefits, employment, credit, housing, law enforcement, immigration, or any other non-research purpose;
- attempt to re-identify any individual from de-identified data, a limited data set, or aggregate results, except as expressly permitted by your agreements and applicable law; or
- combine Customer Data with other data sources in a manner not authorized by your IRB approval, your study protocol, and your agreements with Coris.

3.3 Misuse of the Platform. Do not:

- copy, modify, or create derivative works of the Services, except as the Terms expressly permit;

- reverse engineer, decompile, disassemble, or attempt to discover the source code, model weights, model parameters, training data, or underlying algorithms of the Software, except to the extent applicable law expressly permits despite this restriction;
- use the Services, the Output, or any information about how the Services perform to build, train, benchmark for publication, or improve a competing product or service, without our prior written consent;
- sell, resell, rent, lease, sublicense, time-share, or otherwise make the Services available to anyone other than your Authorized Users;
- remove, obscure, or alter any proprietary notices, labels, or markings on the Services, Documentation, or Equipment; or
- use automated means to scrape, crawl, or collect content from the Website or the Services, other than ordinary search engine indexing of the Website.

4. Responsible Use of AI and Output

Coris Match uses artificial intelligence to support, not replace, the judgment of qualified research professionals. To keep its use safe and appropriate:

4.1 Human Review Is Required. A qualified individual, such as the principal investigator or a delegated member of the study team, must review each recommendation and the supporting information the Services display before anyone relies on it, including before any individual is contacted about, enrolled in, or excluded from a study. You may not configure, integrate, or use the Services so that Output triggers patient contact, enrollment, exclusion, or any other action without that review.

4.2 Not for Clinical Care. Do not use the Services or Output to diagnose, treat, cure, mitigate, or prevent any disease or condition; to make or support clinical care decisions; to triage patients; or in any emergency. Output, including image classifications and lesion measurements, is not a substitute for a clinical evaluation and must not be entered into or relied upon in the medical record as a clinical finding.

4.3 No Misrepresentation of Output. Do not present Output as a diagnosis, as a clinical determination, or as the decision of a clinician, and do not represent that the Services have been cleared, approved, or certified by the U.S. Food and Drug Administration or any other regulatory authority unless we have stated so in writing.

4.4 Use Within Validated Conditions. Use the Services only within their Validated Conditions, as defined in the AI Terms: the data types, imaging modalities, imaging devices, patient populations, and study criteria described in the Documentation or Model Documentation or agreed with us in writing. AI performance can vary across patient populations, data sources, and imaging equipment. Before applying the Services to a new study, patient population, imaging modality, imaging device, or data source, please consult us.

4.5 No Discriminatory Use. Do not use the Services or Output to unlawfully discriminate against, or to systematically exclude, individuals on the basis of race, color, ethnicity, national origin, sex, gender identity, sexual orientation, age, disability, religion, or any other characteristic protected by law, except where a criterion is required by an approved study protocol.

4.6 No Manipulation of the Models. Do not attempt to manipulate, bypass, or interfere with the AI features of the Services, including by submitting inputs designed to cause inaccurate Output, extracting model behavior or parameters through systematic querying, or disabling the display of supporting evidence that accompanies Output.

4.7 Publication and Performance Claims. If you publish or present research that describes the performance of the Services, please describe the Services accurately, and do not attribute to Coris any claim or result that we have not made or verified. Nothing in this Policy restricts accurate reporting of research results as required by your institution, a journal, or applicable law.

5. Security and System Integrity

5.1 Account Security. Authorized Users must keep their login credentials confidential and must not share accounts, credentials, or active sessions with anyone, including other members of the study team. Do not use another person's account, and do not create or use generic or shared accounts unless we and your organization have approved them in writing for a specific operational purpose.

5.2 No Circumvention. Do not circumvent, disable, or interfere with any security, authentication, access control, encryption, logging, or audit feature of the Services, and do not access or attempt to access any part of the Services, Equipment, or Customer Data, or any Coris computing hardware brought into your environment, that you are not authorized to access.

5.3 No Malicious Activity. Do not introduce viruses, malware, ransomware, or other malicious code into the Services or Equipment, and do not interfere with or disrupt the integrity, performance, or availability of the Services, including through denial-of-service activity or by placing an unreasonable load on the Services.

5.4 Security Testing. Your organization may include the Equipment in its routine security monitoring and vulnerability scanning, and may run its own endpoint detection and response agent on it, as described in Section 6.5 of the Terms. Penetration testing, red-team exercises, or other active testing of the Services or Equipment beyond routine scanning require our prior written approval so that we can coordinate scope and timing with you.

5.5 Care of Equipment. Equipment provided by Coris must be kept in a secure location with suitable environmental conditions. Do not open, modify, relocate, re-image, or connect unauthorized devices or storage media to the Equipment; do not install software on it (other than an endpoint detection and response agent your organization runs under Section 5.4); and do not use it for any purpose other than the Services, except as reasonably necessary in an emergency or as we approve in writing.

5.6 No Unauthorized Data Movement. Do not configure, connect, or use the Services or Equipment to transmit Customer Data outside your environment, including to cloud services, personal devices, personal email, or third-party AI services, except as your organization has authorized under its policies and your agreements with Coris.

6. Handling Customer Data

6.1 Agreements Before PHI. Do not make PHI available to the Services until a BAA and, where applicable, a DUA are in place between your organization and Coris, as Section 5.3 of the Terms requires.

6.2 Authority to Use Data. Make available to the Services only Customer Data that you have the right, consents, authorizations, and approvals to use for the relevant study, including any required IRB approval or waiver of authorization.

6.3 Exports and Copies. Export, download, print, photograph, or copy Customer Data or Output only as necessary for an authorized research purpose and only to locations approved by your organization. Any copies must be protected under your organization's security policies and disposed of securely when no longer needed.

6.4 Patient Outreach. Any contact with patients or prospective participants identified through the Services must be made by your study team, in accordance with your IRB-approved recruitment procedures, applicable law, and the individual's documented communication preferences. Do not use the Services to send unsolicited communications, and do not state or imply to a patient that Coris or an AI system has determined their eligibility or medical condition.

6.5 Sharing With Coris. Please share Customer Data with Coris personnel only as needed for support and only on site, during a supervised support visit, so that it stays within your environment. Please do not send Customer Data to Coris by email, chat, text message, or support ticket. When you report an issue, include the minimum Customer Data needed to resolve it. Coris personnel will handle any Customer Data they receive as described in the Terms, the BAA, and our Privacy Policy.

6.6 Sensitive Categories. Take particular care with information subject to heightened legal protection, such as substance use disorder records governed by 42 C.F.R. Part 2, genetic information, mental health records, and information about minors. Do not make such information available to the Services unless your study and agreements specifically permit it.

7. Your Responsibilities for Authorized Users

As the customer, you are responsible for how your Authorized Users use the Services. In particular, you agree to:

- grant access only to individuals who need it for an approved research activity and who have completed any training your institution requires, such as HIPAA and human subjects protection training;
- assign roles and permissions consistent with each Authorized User's responsibilities, and promptly remove or adjust access when someone changes roles, leaves your organization, or no longer needs access;
- make this Policy available to your Authorized Users and ensure they comply with it;
- review the audit and activity records the Services maintain within your environment as part of your normal compliance and security programs; and

- remain responsible for any violation of this Policy by your Authorized Users, as if you had committed it yourself.

8. Reporting Concerns

8.1 Violations and Misuse. If you become aware of any actual or suspected violation of this Policy, please notify us promptly using the contact information in Section 11.

8.2 Security Incidents. Report any actual or suspected security incident involving the Services or Equipment, including compromised credentials, unauthorized access to Customer Data, or lost, stolen, or tampered Equipment, to Coris without unreasonable delay. Please also follow your own incident response procedures and any notification obligations in your BAA.

8.3 Concerns About Output. If you believe any Output is inaccurate, biased, or otherwise concerning, please record it in the review interface, which we review with you when we are on site, or contact us, as described in Section 4.4 of the Terms. We review each report in good faith.

8.4 Vulnerabilities. If you believe you have found a security vulnerability in the Services, please report it to us privately at security@corisfrontiers.com and give us a reasonable opportunity to address it before disclosing it to anyone else. We appreciate good-faith reports and will not pursue action against anyone who reports a vulnerability in good faith and in accordance with this Section.

8.5 No Retaliation. Coris will not retaliate against anyone for reporting a concern in good faith, and we encourage customers to extend the same protection to their Authorized Users.

9. Investigation and Enforcement

9.1 Investigation. When Coris Match is deployed within your environment, we do not remotely monitor how Authorized Users use the Services. We may investigate suspected violations of this Policy based on reports we receive, information we observe while providing on-site support, or information you share with us. We will coordinate any investigation with you, and we will access Customer Data, systems, and Equipment only as you authorize and as our agreements permit.

9.2 Cooperation. You agree to reasonably cooperate with any investigation of a suspected violation, including by reviewing relevant audit records and sharing information about the circumstances, subject to your legal and confidentiality obligations.

9.3 Remedies. If we reasonably determine that this Policy has been violated, we may, depending on the nature and severity of the violation, work with you to correct it, require you to suspend or remove an Authorized User's access, or suspend all or part of the Services. Where reasonably practicable, we will give you notice and an opportunity to cure before suspending the Services. We may act immediately, with notice as soon as practicable afterward, where necessary to prevent harm to patients, research participants, Customer Data, the Services, or others, or to comply with law. We will restore access once the issue has been resolved.

9.4 Other Rights. Serious or repeated violations may constitute a material breach of the Terms, allowing us to exercise our rights under Section 16 of the Terms. Where required by law or where we believe in good faith that it is necessary to protect the safety of any person, we may report a violation to

appropriate authorities. Our rights under this Policy are in addition to any other rights or remedies available under our agreements or applicable law.

10. Changes to This Policy

We may update this Policy from time to time to reflect changes in the Services, the law, or industry practice. When we do, we will post the updated Policy on the Website and revise the “Last Updated” date above. If a change is material, we will give reasonable advance notice to customers with active accounts, for example by email. Updated versions apply going forward and will not change the terms of an Order Form during its current term unless you agree in writing. Your continued use of the Services after the update takes effect means you accept it.

11. Contact Us

If you have questions about this Policy, need to report a concern, or are unsure whether a particular use is permitted, please contact us:

Coris Frontiers, Inc.

720 Garfield St.

Denver, CO 80206

Email: legal@corisfrontiers.com, security@corisfrontiers.com, privacy@corisfrontiers.com,
support@corisfrontiers.com

Website: www.corisfrontiers.com