Privacy Policy

Cairn Surgical
Operate Precisely

1. Purpose

Cairn Surgical, Inc. ("CairnSurgical," "we," "us," or "our") is committed to protecting the privacy of our clients and customers and the security of the personal information you provide through the CairnSurgical Portal ("Portal") and all other systems. This Privacy Policy describes our privacy and security practices. By accessing, submitting information through, and using the Portal, or providing personal information by any other means, you agree to the terms of this Privacy Policy, and you consent to the use and processing of your personal data as set forth in this Privacy Policy.

2. Scope of this Privacy Policy

This Privacy Policy applies to all Personal Data as defined in Article 4 of the General Data Protection Regulation (GDPR) and all Protected Health Information (PHI) as defined in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule that is collected, processed and/or maintained by CairnSurgical.

3. What Personal Data Do We Collect?

- Personal information that is identifiable to you. This includes your name and title, email address, phone numbers, and names and contact information of associates.
- Name, phone number, and address of the organization(s) you are associated with.
- Personally identifiable information, health, and diagnostic information including medical imaging and clinical reports you provide for patients in your care.

4. What Do We Do with the Personal Data We Collect?

- Your information is primarily used to create unique user accounts and to associate your account with your organization and other users you are associated with.
- Patients' personal information including identifiers and image and diagnostic data is used for the creation of patient-specific medical devices.
- We may use your information to communicate directly with you concerning a specific case, with changes to the function of the Portal or other systems, to provide support, alert you to developments in our products, or to request feedback on our product offerings.
- We transfer your personal data only to our contracted partners for ordering, image management, storage, and manufacturing.
- We may use aggregated data without personally identifiable information for research and development purposes.

- We may share your personal data to comply with laws or respond to lawful requests and legal processes. Your personal data may be subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission, or any other U.S. authorized statutory body.
- We do not sell, trade, or otherwise transfer any personal data you provide to third parties that are not contracted business partners.
- We do not use your personal data for any purpose other than necessary to provide products and services as contractually defined.

5. How long to we retain your personal data?

- Personal data will be kept for no longer than is necessary for the purposes for which the personal data are processed.
- When applicable national, federal, state or local regulation applies to information retention, CairnSurgical will retain data according to that applicable law.

6. How Do We Secure Your Personal Data?

- All users' demographic personal data and patient's demographic personal data are stored in a database hosted by Amazon Web Services (AWS), a fully secure HIPAA and GDPR compliant system. Find the AWS Privacy Notice at https://aws.amazon.com/privacy/
- All Image data and diagnostic reports are stored on Ambra Health, a fully secure HIPAA and GDPR compliant system accessed through the Portal. Find the Ambra Health Privacy Policy at https://access.ambrahealth.com/privacy.
- All personal data is encrypted during transfer and at rest.

7. CairnSurgical's Compliance with the Data Privacy Framework Principles

CairnSurgical, Inc. complies with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the U.S. Department of Commerce. CairnSurgical has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("EU-U.S. DPF Principles") with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF ("UK-U.S. DPF Principles"). CairnSurgical, has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles ("Swiss-U.S. DPF Principles") with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the UK-U.S.

DPF Principles, and/or the Swiss-U.S. DPF Principles (collectively, the "Principles"), the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit Data Privacy Framework website.

The Federal Trade Commission within the U.S Department of Commerce has jurisdiction over CairnSurgical's compliance with the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF. This Privacy Policy describes the types of Personal Data we collect, the purposes for which we collect and use your Personal Data, and the purposes for which we disclose your Personal Data to certain types of third parties in the sections above. Pursuant to the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF, EU, UK, and Swiss individuals have the right to obtain our confirmation of whether we maintain Personal Data relating to them in the U.S. Upon request, we will provide EU, UK, and Swiss individuals with access to the Personal Data that we hold about them. EU, UK, and Swiss individuals may also correct, amend, or delete the Personal Data we hold about them where it is inaccurate, or has been processed in violation of the EU-U.S. DPF Principles, the UK-U.S. DPF Principles, and the Swiss-U.S. DPF Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. An EU, UK, or Swiss individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the U.S. under the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF, should direct their query to privacy@cairnsurgical.com. If requested to remove data, we will respond within a reasonable timeframe. For more information about rights afforded to EU, UK, and Swiss individuals, please see the "Your Rights" section of this Privacy Policy.

In addition, under the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF, we will provide EU, UK, and Swiss individuals with the choice to opt-out from the sharing of their Personal Data with any third parties (other than our agents or those that act on our behalf or under our instruction), or before we use it for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized.

We will provide EU, UK, and Swiss individuals with the choice to opt-in to sharing their sensitive Personal Data with any third parties or if we plan to process their Personal Data for a purpose other than those for which it was originally collected or subsequently authorized. EU, UK, and Swiss individuals may request to limit the use and disclosure of your Personal Data by submitting a written request to privacy@cairnsurgical.com.

In addition to any other disclosures described in our Privacy Policy, in certain situations, we may be required to disclose Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

CairnSurgical's accountability for Personal Data that it receives in the U.S. under the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF and subsequently transfers to a third party acting as an agent on our behalf is described in the EU-U.S. DPF Principles, the UK-U.S. DPF Principles, and the Swiss-U.S. DPF Principles. In particular, CairnSurgical remains liable under the EU-U.S. DPF Principles, the UK-U.S. DPF Principles, and the Swiss-U.S. DPF Principles, if our agents process Personal Data in a manner inconsistent with the EU-U.S. DPF Principles, the UK-U.S. DPF Principles, and the Swiss-U.S. DPF Principles, unless CairnSurgical proves that we are not responsible for the event giving rise to the damage.

In compliance with the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF, CairnSurgical commits to resolve EU-U.S. DPF Principles, UK-U.S. DPF Principles, and Swiss-U.S. DPF Principles -related complaints about our collection and use of your Personal Data. EU, UK, and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the DPF should first contact CairnSurgical at privacy@cairnsurgical.com.

CairnSurgical has further committed to refer unresolved complaints under the EU-U.S. DPF, the UK-U.S. DPF, and the Swiss-U.S. DPF program to an independent dispute resolution mechanism, Data Privacy Framework Services, operated by BBB National Programs. If you are an EU, UK, or Swiss individual and you do not receive timely acknowledgment of your EU-U.S. DPF Principles, UK-U.S. DPF Principles, or Swiss-U.S. DPF Principles-related complaint, or if your complaint is not satisfactorily addressed, please visit BBB National Programs DPF Services Dispute Resolution Process at www.bbbprograms.org/dpf-complaints.
for more information and to file a complaint. This service is provided free of charge to you.

If your EU-U.S. DPF, UK-U.S. DPF, or Swiss-U.S. DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Annex 1 of the Data Privacy Framework Principles at the following link:

https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

8. Your Rights

- Right to access
  You have the right to request details of your personal information, including a copy of the data being processed.
- Right to rectification
  You have the right to request that incorrect personal information be edited or updated.
- Right to erasure
  You have the right to request that your personal information be deleted if it is no longer necessary or if you object to processing.
- Right to data portability
  You have the right to request a copy of your personal information in a machine-readable format.
- Right to object
  You have the right to object to the processing of your personal information.
- Right not to be subject to automated processing
  You have the right to prevent decisions from being made solely based on automated processing.
- You may also have the right to make a GDPR complaint to the relevant Supervisory Authority. A list of Supervisory Authorities is available here: https://edpb.europa.eu/about-edpb/board/members_en.

9. Questions, Complaints, or Concerns Regarding Your Personal Data

You may contact CairnSurgical via mail:

CairnSurgical, Inc.
16 Cavendish Court
Lebanon, NH 03766, USA

You may contact CairnSurgical via email:
privacy@cairnsurgical.com

Please check this policy for updates prior to providing your personal data to CairnSurgical through the Portal or any other means. CairnSurgical will update this Privacy Policy as required.

The last update was released on January 14, 2025