# Nicolab Services Privacy Policy

***Last modified 06-Mar-2024***

## 1. Introduction

At Nicolab, we respect your privacy regarding any information we may collect while operating our services. Personal Data means information that can directly or indirectly identify you or other individuals ("Personal Data"), for example first name, last name, or email address.

We do not disclose your Personal Data to any third party except to our affiliates and to data processors that assist us with providing our services or to authorities if we are required to adhere to laws or court order(s). With your consent we use cookies for marketing, performance and statistical purposes.

You always have the right to request information about your stored Personal Data, its origin, its recipients, and the purpose of its collection at no charge. You also have the right to request that it be corrected, blocked, or deleted. You can contact us at any time using the address given of our Data Protection Officer below if you have further questions about the issue of privacy and data protection. You may also, of course, file a complaint with the competent regulatory authorities.

## 2. General provisions

This Nicolab Services Privacy Policy applies to Personal Data processed by Nicolab (hereinafter, "us", "we") in connection with the operation and services we offer to you through our subscription services, the StrokeViewer app and the website (nicolab.com) (collectively referred to as "Services"). This Nicolab Services Privacy Policy explains what Personal Data may be collected, how we use it, how you may exercise your rights, and under what circumstances we may disclose this Personal Data to third parties. We also process patient data on behalf of your organization, for which we have a separate data processing agreement in place with your organization.

Personal Data is administered by NICo-Lab B.V., registered with the trade register of the Chamber of Commerce in Amsterdam under registration number (KvK): 64531775, with principal place of business and address for service at Paasheuvelweg 25, 1105 BP, Amsterdam, The Netherlands.

Nicolab has appointed a Data Protection Officer who can be contacted at the following address: infosec@nicolab.com.

We process your Personal Data to be able to provide you with the Services[1], including but not limited to:

- Automatic analysis of DICOM images using StrokeViewer Algorithms
- Web DICOM viewer
- Mobile DICOM viewer

[1] The full list of Services is provided in the Principal Agreement and can be different for each party.

- Network-wide image sharing
- Instant messaging
- Technical support in case of malfunctions or in other cases when deemed necessary
- Training services

Personal Data submitted through the Services will be processed in accordance with applicable data protection laws.

By using our Services, you agree that we are processing your Personal Data in accordance with the terms set out in this Nicolab Services Privacy Policy.

In addition, a separate agreement between us and our customer governs delivery, access and use of the Services (the "Principal Agreement"), including the processing of any Personal Data, files or other content submitted through use of the Services (collectively, "Customer Data"). The organization (e.g., your employer or another entity or person) that entered into the Principal Agreement ("Customer") controls certain aspects of their use of the Services (their "Deployment") and associated Customer Data, for example, how long Nicolab will retain Customer Data.

To the extent processing of your Personal Data is based on your consent, we will not change the scope of such processing, unless you have given additional consent to the changed scope of such processing.

If you are employed by a Customer, this Nicolab Services Privacy Policy together with the Principal Agreement sets forth the provisions and policies governing your use of our Services.

**3. Scope of Personal Data collected and processed**

We may process the following Personal Data as a result of our Principal Agreement or Nicolab granting access to individuals to a Deployment ("Authorized Users"). In addition, we may collect data on in-application settings such as notification preferences and preferred method of logging in.

Personal Data of Authorized Users collected to enable Authorized Users to use the Services:

1. Data collected within service provision:
    - Full Name
    - Job Title
    - Employer
    - E-mail address
    - Mobile phone number (optionally)
    - IP Address
    - Session cookies

2. Data collected in case of mobile access to the Services:

- Mobile device profile[2]
- Application preferences[3]
- Application pin code (optionally)

3. Data collected within instant messaging Service:
    - Text and media forwarded

StrokeViewer can be accessed through a browser or mobile application with the country specific domain of strokeviewer.com (e.g., in the Netherlands nl.strokeviewer.com).

Authorized Users must first undergo training before using the Services. Training content may differ depending on the job description of the Authorized User and information on training will be communicated via email.

Nicolab offers support with technical issues regarding use of the Services. When the support desk is contacted the following details may be collected to better assist with the issue.

Additional data:

- Log data: As with most technology services delivered over the internet, our servers automatically collect information when you access or use our Services and record it in log files.
- Customer Data: Deployments are configured to send Customer Data to Nicolab for using the Services, for example digital computed tomography (CT) studies may be sent to Nicolab through the Services in order for an artificial intelligence algorithm to detect suspected conditions such as a large vessel occlusion. Customer Data may include data concerning health. Such sensitive data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. Such sensitive data is governed by the Principal Agreement and the data processing agreement between the Customer and Nicolab and not by this Nicolab Services Privacy Policy.

We may also use your e-mail address to send you post market surveys on the basis of our legitimate interest. If you do not want your e-mail address to be used for this purpose, you can always object to this processing.

## 4. Purpose of Personal Data collected & legal basis

[2] Mobile device profile is the collection of a variety of data about an Authorized User's device and the way that device is used, including but not limited to: IP Address, Country and Carrier, Device Brand and Model, Device Operation System Version, Language preference.

[3] Application preferences are the settings in the mobile application configured by an Authorized User individually, including but not limited to: Preference for pin code or Biometric Fast Login, Push notifications (on/off), push tokens (a token whereby the mobile phone of the Authorized User can be targeted for push notifications).

Applicable data protection legislation allows Nicolab to process your Personal Data for the purpose of performance of the Services, as defined in the relevant Principal Agreement (your employer) or on the basis of your consent.

## 5. Retention period of Personal Data

The Personal Data is stored for the time needed for the performance, termination, or expiration of a Principal Agreement and once our statutory obligations to preserve records have expired. Additional provisions on duration of data storage are made under the Principal Agreement.

## 6. Sub-Processing

### 6.1. Service providers (processors)

To ensure the proper functioning of the Services, including the performance of the Principal Agreement, Nicolab uses external services (such as third-party software). We use only services provided by such data processors who can properly guarantee that appropriate technical and organizational measures are implemented to ensure the compliance of Personal Data processing with the requirements of the applicable data protection laws and protect the rights of the persons the data pertains to. Before we disclose Personal Data to third parties, we will enter into a (sub-)processing agreement imposing appropriate security standards on them.

Nicolab discloses Personal Data only if it is necessary to pursue a specific purpose of data processing and only insofar as it is necessary to achieve such a purpose. Personal Data of the Authorized User of our Services may be disclosed to the service providers in order to supply us with the technical, IT, and organizational solutions needed by Nicolab to carry on its business activity. We disclose the Authorized User's Personal Data to a contracted supplier only if and insofar it is necessary to achieve a specific purpose of the data processing hereunder.

### 6.2. Other recipients (controllers)

We may share your Personal Data with the following controllers (i.e. third parties that process your Personal Data for their own purposes):

- law enforcement or other agencies if we are required to do so by law, or by a warrant, subpoena or court order to disclose your Personal Data.

## 7. Cross border data transfer

The transfer of Personal Data provided under the Services complies with national and international legislation.

## 8. Rights of the person the Personal Data pertains to

You have the rights to your Personal Data that are described below.

- Right to access, rectify, limit, delete, or move Personal Data – the person the Personal Data pertains to has the right to request us to provide him or her with access to his or her Personal Data, to rectify or delete such Personal Data ("the right to be forgotten"), to limit or object the processing thereof, as well as to have his or her Personal Data moved.
- Right to withdraw the consent at any time – the person whose Personal Data is processed by Nicolab based on such a person's consent is entitled at any time to withdraw his or her consent, this not affecting the right to process such Personal Data based on the consent before it was withdrawn.
- Right to lodge a complaint – the person whose Personal Data is processed by Nicolab is entitled to lodge a complaint with the Autoriteit Persoonsgegevens, the Dutch supervisory authority.
- Right to make an objection – the person whose Personal Data is processed is entitled to raise at any time an objection against his or her Personal Data being processed.

You can exercise your rights by contacting us at infosec@nicolab.com so that we may consider your request in accordance with applicable law. When we receive your rights request via email, you accept that we may take steps to verify your identity before complying with the request to protect your privacy and security, for example by contacting you or your employer in order to establish your identity and your qualification as an Authorized User.

## 9. Security

Considering the nature, scope, context, and purposes of data processing and the risk, however likely and imminent, of violating any right or freedom of natural persons, Nicolab implements appropriate technical and organizational measures to make data processing compliant with applicable data protection laws and be able to prove it. Our security measures are being improved continuously as technology develops.

### 9.1. Technical measures

Nicolab takes technical measures to prevent unauthorized persons from intercepting or altering any Personal Data that is transmitted electronically. Nicolab is ISO 27001 and ISO 13485 certified.

### 9.2. Links to external sites

Our Services may contain hyperlinks to external websites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. Once you have left our Services, we cannot be responsible for the protection and privacy of any information which you provide. We strongly advise you to review the Nicolab Services Privacy Policy and terms and conditions of every website you visit. We have no control over, and assume no responsibility for the content, privacy policies or practices of any third party sites, products or services.

### 9.3. Authentication and authorization of Authorized Users

The authentication of Authorized Users is completely managed by the hospital's identity provider system, such as an Active Directory File Server (ADFS). This way, the hospital has complete control to determine password policies, which Authorized Users have access to StrokeViewer, enforcing multi-factor authentication, etc. Thus, when an Authorized User attempts to access StrokeViewer, this Authorized User is redirected to the hospital identity provider system. If the identity provider system used by the hospital does not support two-factor authentication, the hospital can use the StrokeViewer app to provide two-factor authentication.

Once authenticated, an Authorized User is authorized for:

- 1 hour of web access to the product;
- 336 hours (14 days) of mobile access to the product.

After expiring this period, the Authorized User is requested to authenticate themselves again. The extra security measures are also applied:

- if the Authorized User account is suspended or revoked by the Customer's identity provider their access to the product is automatically terminated not later than in 1 hour;
- the mobile app requires Authorized User to provide an additional pin or biometrics for authentication;
- web access is automatically locked after 20 minutes of inactivity to prevent unauthorized access to unattended sessions, to unlock it the Authorized User has to authenticate themselves again;
- if Authorized User switched to another tab in the browser or to another window and does not return to the product's web page for 10 minutes their web access is locked even if Authorized User keeps working with the other applications and/or browser tabs, to unlock it the Authorized User has to authenticate themselves again;
- mobile access is automatically locked after 1 minute of inactivity to prevent unauthorized access to unattended sessions, to unlock it the Authorized User has to provide an additional pin or biometrics.

## 10. Personal Data breach and notification obligation

In the event of a Personal Data breach concerning the Services provided by Nicolab, Nicolab will promptly notify affected Authorized Users and, if applicable, relevant supervisory authorities, in the event of a Personal Data breach that poses a risk to the rights and freedoms of the affected Authorized Users. The notification will be made without undue delay after becoming aware of the breach, but within 72 hours at the latest. In the event of a Personal Data breach, Nicolab will take all reasonable measures to limit the consequences of the Personal Data breach and/or prevent a new one, against payment of the reasonable costs by you.

## 11. Nicolab Services Privacy Policy changes

Nicolab reserves the right to modify, amend or change this Nicolab Services Privacy Policy at any time and at its sole discretion. Such changes may be implemented by Nicolab without prior notice. Nicolab encourages visitors to frequently check this page for the latest information on our privacy practices and for any updates or revisions. Your continued use of this site after any change in this Nicolab Services Privacy Policy will constitute your acceptance of such change.

**Personal Data details**

| | |
|---|---|
| Description of services | StrokeViewer is a Software as a Service (SaaS) image processing application. StrokeViewer automatically analyzes scans received from patients with symptoms of stroke. After the analysis, a report is generated that includes relevant features of the images for stroke. These features can be used by the physician as a supporting tool for further diagnostics.<br>1. Automatic analysis of DICOM images using StrokeViewer Algorithms<br>2. Web DICOM viewer,<br>3. Mobile DICOM viewer<br>4. Network-wide image sharing<br>5. Instant messaging<br>6. Technical support in case of malfunctions or in other cases when deemed necessary<br>7. Training services |
| Type of Personal Data | 1. Personal Data of Authorized Users excluding special categories of Personal Data (GDPR Art.4,9) |
| Categories of those involved | 1. Authorized Users |
| Purposes of Processing | Processing will only take place in the context of and for the duration of the Principal Agreement for the purposes of:<br>- Service Provision<br>- Communication<br>- Diagnostics and Troubleshooting<br>- Personalization and Customization<br>- Analytics and Research<br>- Legal Compliance |
| Approved Processors | Google Cloud, Stream.io, Mixpanel |
| Retention period | 1. The log record is kept as long as the contract with Customer is valid but not longer than 5 years |