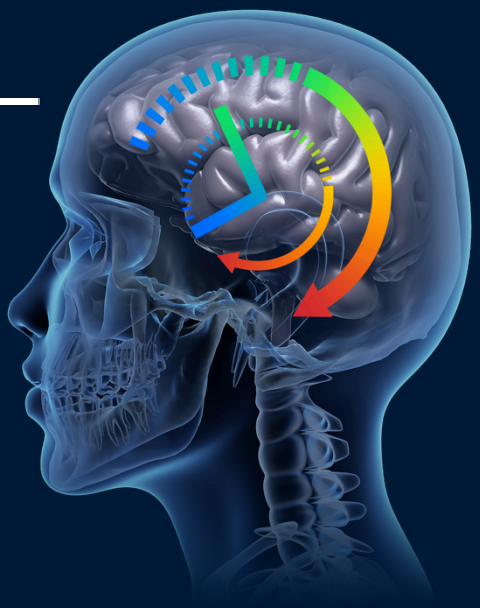
stroke | viewer

it's about time



StrokeViewer Security White Paper

English

StrokeViewer is a product of **Nicolab**
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

NICOLAB

Table of Contents

StrokeViewer is a product of **Nicolab**
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

NICOLAB

Glossary

ACSC – The Australian Cyber Security Centre is a hub for private and public sector collaboration and information-sharing on cyber security, to prevent and combat threats and minimize harm to Australians.

ADFS - Active Directory File Server provides secure, backed up data file storage.

AI – Artificial intelligence is intelligence demonstrated by computers or machines, in contrast to the natural intelligence displayed by animals including humans.

APPs – The Australian Privacy Principles are the cornerstone of the privacy protection framework in the Privacy Act 1988.

CT - Computed Tomography scan is a medical imaging technique used in radiology to obtain detailed internal images of the body noninvasively for diagnostic purposes.

DICOM - Digital Imaging and Communications in Medicine is the standard for the communication and management of medical imaging information and related data.

EEA - The European Economic Area consists of the Member States of the European Union and three countries of the European Free Trade Association (Iceland, Liechtenstein and Norway; excluding Switzerland).

EU - The European Union is an economic and political union of European countries that was established on 1 November 1993 by the Treaty on European Union (Maastricht Treaty).

GCSB - The Government Communications Security Bureau contributes to New Zealand's national security by providing information assurance and cyber security to the New Zealand Government and critical infrastructure organizations, collecting and analyzing intelligence in accordance with the Government's priorities, and providing cooperation and assistance to other New Zealand government agencies.

GDPR - The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852
NICOLAB

HTTPS - Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol which is used for secure communication over a computer network, and is widely used on the Internet.

IEC - The International Electrotechnical Commission is an international standards organization that prepares and publishes international standards for all electrical, electronic and related technologies.

IRAP - The Infosec Registered Assessors Program ensures entities can access high-quality security assessment services.

ISO - The International Organization for Standardization is an international standard development organization composed of representatives from the national standards organizations of member countries.

MDD - The Medical Device Directive is intended to harmonize the laws relating to medical devices within the European Union.

MDR - Managed Detection and Response is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring, and response.

NHS - The National Health Service is the publicly funded healthcare system in England, and one of the four National Health Service systems in the United Kingdom.

NZISM - The New Zealand Information Security Manual is the New Zealand Government's manual on information assurance and information systems security.

OS - Operating System is system software that manages computer hardware, software resources, and provides common services for computer programs.

OWASP - The Open Web Application Security Project is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

PACS - Picture Archiving and Communication System is a medical imaging technology which provides economical storage and convenient access to images from multiple modalities.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852
NICOLAB

TLS - Transport Layer Security the successor of the now-deprecated Secure Sockets Layer, is a cryptographic protocol designed to provide communications security over a computer network.

UK – United Kingdom of Great Britain and Northern Ireland is an island country that sits north-west of mainland Europe.

US – United States of America is a country of 50 states covering a vast swath of North America, with Alaska in the northwest and Hawaii extending the nation's presence into the Pacific Ocean.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

StrokeViewer Security

This white paper summarizes all information security measures implemented in StrokeViewer to ensure the proper handling of patient and user data. Nicolab designed StrokeViewer for sharing and analyzing radiological images of suspected stroke patients. StrokeViewer will not store patient data other than the necessary radiological images (DICOM files) or the metadata extracted from these radiological images. StrokeViewer automatically deletes these DICOM files according to the terms specified in the processing agreement. Nicolab treats patient data with the utmost privacy requirements. Several layers of security have been implemented in StrokeViewer to ensure that patient data is protected both during transfers, storage, and processing. On top of that, Nicolab internal procedures ensure that no Nicolab personnel is authorized to access patient data unless explicitly specified by the healthcare provider as part of support ticket.

Nicolab is ISO/IEC 27001 certified. The ISO/IEC 27001 is an international standard that determines how to establish and improve management systems for information security. On top of ISO/IEC 27001 audits, Nicolab is also regularly audited by notified bodies and other third-party companies. In addition, StrokeViewer undergoes thorough penetration tests regularly. The results of these independent tests confirm that the secure design used to build StrokeViewer is solid.

Secure by design

Nicolab designed StrokeViewer to be secure from its foundations. Industries standards related to security, such as the OWASP Application Security Verification Standard, were adopted from the beginning of StrokeViewer development. Security is a main requirement implemented into each component of StrokeViewer architecture.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

Patient data in the cloud

The only patient data uploaded to StrokeViewer are the DICOM images analyzed by the AI algorithms, including their metadata. The patient's name, gender, and date of birth are extracted from this metadata and shown in StrokeViewer's user interface. This way, healthcare professionals can identify which AI result and medical image belong to each patient. No identifiable patient information is included in the email notifications.

Healthcare professionals are allowed to share patient data with other healthcare professionals as long as that data sharing is done in the context of diagnosis, medical treatment, or any other activity necessary for protecting the vital interests of the patient.

In the European Union, according to Article 6(1)(d) of the GDPR, no consent is required to process data to protect the vital interest of a patient. In addition to this, Article 9(2)(h) states that medical data can be processed with the purpose of medical diagnosis or supporting medical treatment. In Australia and New Zealand, similar rules are in place to allow the lawful collection and processing of patient data for providing a health service. For Australia, these rules are specified in the section 16B of the Privacy Amendment Act. For New Zealand, these rules are specified throughout the Privacy Act 2020. In the United Kingdom, the usage of cloud services like StrokeViewer is recommended by the government in the Health and Care 2020 framework. NHS and social care organizations in the UK are allowed to collect, transfer, store, and process patient data within the UK, European Union, or in the US. For more detailed information on a country specific situation, please check the dedicated session of each country at the end of this white paper.

Can Nicolab use patient data for training of AI algorithms?

The AI algorithms available in StrokeViewer are only trained with de-identified data acquired via research collaborations. The AI algorithms are not being fine-tuned or trained with the patient data that is uploaded to StrokeViewer.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

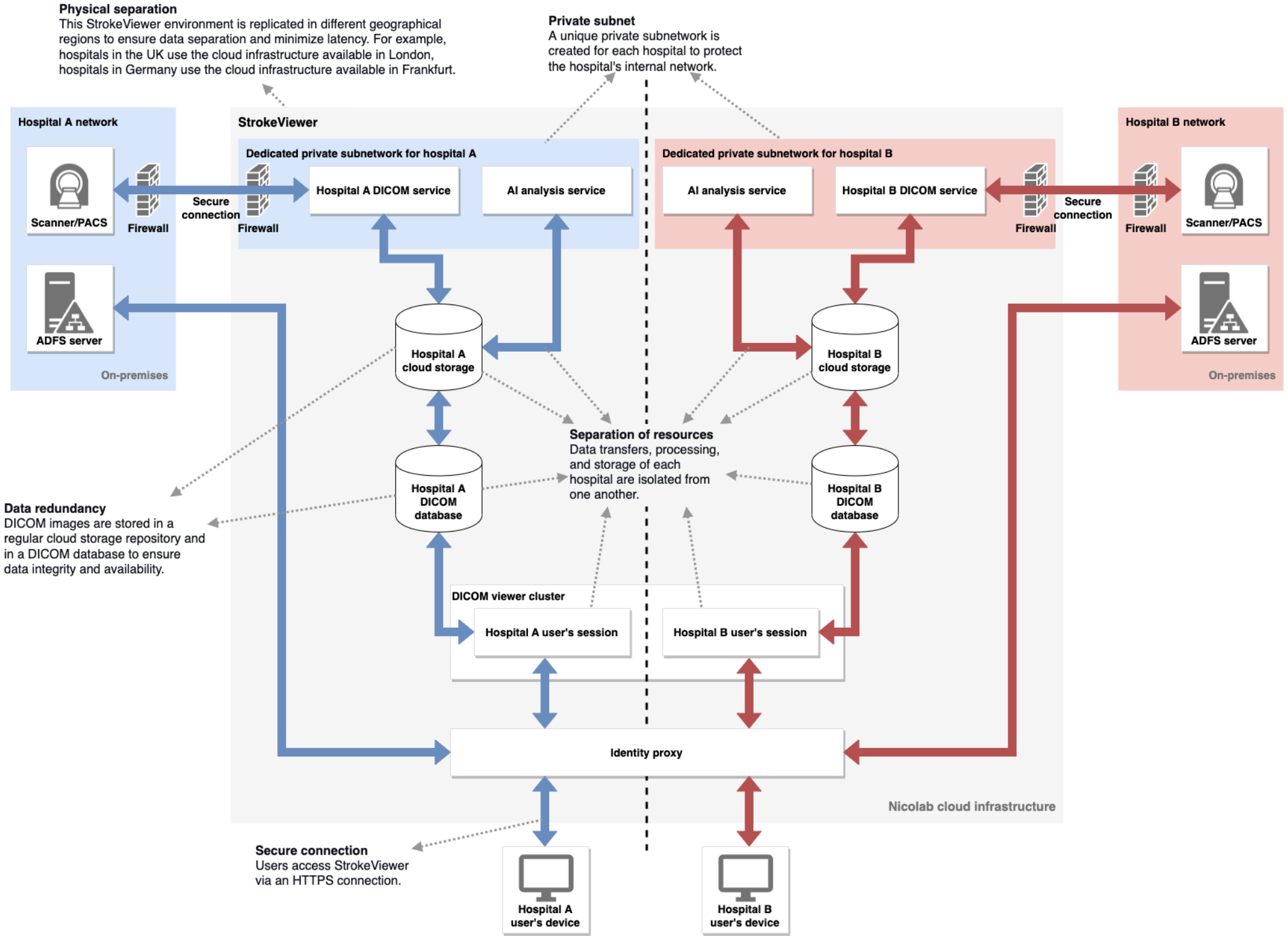
Can Nicolab personnel have access to patient data?

Nicolab employees are not authorized to access patient data unless it is required to solve a customer support request. Nicolab implements the principle of least privilege. This way, the permissions to access patient data are given only to an employee when strictly required. Furthermore, audit logs regarding access to patient data are kept and regularly checked. This is done to ensure that all data accessed by an employee is done appropriately.

What is safer? Cloud or on-premises? What about ransomware attacks?

Most national government agencies acknowledge the importance of using cloud-based services to help to make healthcare more accessible and efficient. Furthermore, it is well-known in the industry that the IT departments of hospitals are overwhelmed with work related to maintaining and securing on-premises services and systems. This creates a situation where it is challenging for hospital IT professionals to deliver the same high-quality service for all the systems they maintain. For example, the majority of the CT scanners currently in operation do not use encrypted DICOM transfers when sending DICOM files to PACS. This means that any malicious actor with access to the hospital network can easily access DICOM files with personal information by monitoring the network traffic. Encryption in transit is a common practice adopted by cloud providers that prevent this type of vulnerability.
Between 2018 and 2020, 235 general hospitals and psychiatric facilities in the USA, in addition to dozens of other healthcare facilities have been victims of ransomware attacks. Ransomware attacks explore simple cybersecurity vulnerabilities that could be easily mitigated by following, for instance, the OWASP recommendations or other industry standards. Nicolab follows the OWASP recommendations and the correct implementation of these recommendations is regularly verified by independent institutions. Nicolab cloud infrastructure is built on top of the most sophisticated security practices. Nicolab is a cloud-native company, and its primary purpose is the development of cloud-based services for the processing of medical data. Therefore, remaining on top of the industry standards related to cybersecurity is a fundamental aspect of Nicolab business.
In short, it is hard to say whether cloud is safer than on-premises because people on both sides can make mistakes and compromise security. Nevertheless, the primary goal of a hospital is to provide high-quality care to patients; the primary purpose of a cloud-native company such as Nicolab is to deliver secure and effective cloud-based services such as StrokeViewer.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852


Physical separation
This StrokeViewer environment is replicated in different geographical regions to ensure data separation and minimize latency. For example, hospitals in the UK use the cloud infrastructure available in London, hospitals in Germany use the cloud infrastructure available in Frankfurt.
Private subnet
A unique private subnetwork is created for each hospital to protect the hospital's internal network.
Hospital A network
Scanner/PACS
Firewall
ADFS server
On-premises
Secure connection
StrokeViewer
Firewall
Dedicated private subnetwork for hospital A
Hospital A DICOM service
AI analysis service
Dedicated private subnetwork for hospital B
AI analysis service
Hospital B DICOM service
Firewall
Secure connection
Firewall
Hospital B network
Scanner/PACS
ADFS server
On-premises
Hospital A cloud storage
Hospital B cloud storage
Separation of resources
Data transfers, processing, and storage of each hospital are isolated from one another.
Hospital A DICOM database
Hospital B DICOM database
Data redundancy
DICOM images are stored in a regular cloud storage repository and in a DICOM database to ensure data integrity and availability.
DICOM viewer cluster
Hospital A user's session
Hospital B user's session
Identity proxy
Nicolab cloud infrastructure
Secure connection
Users access StrokeViewer via an HTTPS connection.
Hospital A user's device
Hospital B user's device

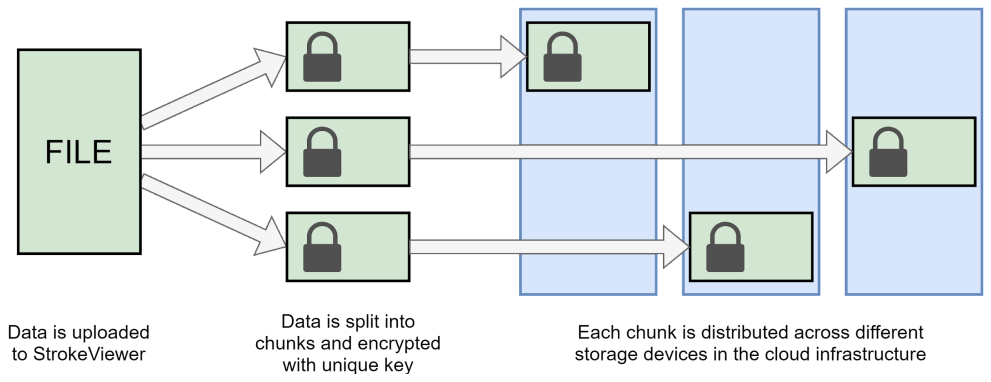
Securing data transfers

Nicolab employs several security measures to ensure the authenticity, integrity, and privacy of data transfers between StrokeViewer components. All component-to-component traffic in StrokeViewer architecture is encrypted. In addition, all data communication to StrokeViewer frontend is authenticated and encrypted. For example, communication between the user device and StrokeViewer frontend is secured using TLS. Upload of patient data is done via a dedicated secure connection for each hospital. Firewalls are configured in these connections to ensure that only the necessary network devices are reachable.

Securing stored data

StrokeViewer stores the patient data of each hospital in a unique cloud repository. For redundancy, StrokeViewer keeps an additional copy of all patient data also in a unique DICOM database. This way, StrokeViewer ensures data availability and prevents a hospital from accessing another hospital's data.

All data stored in StrokeViewer is encrypted at rest using the Advanced Encryption Standard (AES256). For additional security, all stored data is also divided into chunks, and each chunk is encrypted with a unique encryption key. All encryption keys are stored in a key management service. This service is redundant and distributed across servers located in different physical locations.



StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

NICOLAB

No patient data leaves the secure environment defined by StrokeViewer's architecture. All image data presented to users is processed on the server-side. No scans are downloaded to the user's browser or mobile devices. When a user sees an image in the online DICOM viewer or the mobile app, that image is merely being streamed, not downloaded. Therefore, no image data ever leaves StrokeViewer.

Data retention period

All patient data uploaded to StrokeViewer is stored only temporarily. Each hospital is free to choose a retention period that suits their needs. Once the retention period of a DICOM file expires, all copies of that file are permanently deleted together with any AI result linked to it. This operation cannot be reversed.

How can it be made sure that Nicolab deletes the uploaded patient data?
Third-party companies constantly audit Nicolab's information security processes and systems. Nicolab is also audited as part of the ISO/IEC 27001 and the ISO 13485 certifications. These independent audits ensure that Nicolab complies with regulatory, legal, and contractual requirements. If a client requires deletion of uploaded patient data following a retention period, any deviation from such requirement can lead to non-conformities during these audits. All non-conformities must be immediately addressed. Furthemore, Nicolab must implement preventive measures to avoid any reoccurrence of such non-conformities.

User authentication

The authentication of 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 users have access to StrokeViewer, enforcing multi-factor authentication, etc. Thus, when a user attempts to access StrokeViewer, this 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.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852
NICOLAB

Can users access patient data in StrokeViewer outside the hospital network?
When dealing with acute stroke patients, the goal is to determine the best treatment option as soon as possible. Delays in the management of stroke patients have a severe negative impact on patient outcomes. Because of that, radiologists, neurologists, and other caregivers must be able to access StrokeViewer where it is most convenient. StrokeViewer has several layers of security to enable access to patient data in any network over the internet:

1. No patient data is ever downloaded to the devices accessing StrokeViewer. All patient data remains on the Nicolab cloud infrastructure.
2. All data transfers in StrokeViewer are encrypted.
3. Access to StrokeViewer requires two-factor authentication.
4. The mobile app requires the user to provide an additional pin or biometrics for authentication.
5. Email notifications do not include identifiable patient information.
6. Automatic log-off is implemented on both the mobile app and the web-based DICOM viewer to prevent unauthorized access to unattended sessions.

In exceptional situations, such as when the hospitals' internal authentication systems are malfunctioning, StrokeViewer can be configured to allow access to patient data only from inside the hospital network.

Security of the mobile app

StrokeViewer mobile app allows users quick access to AI results, uploaded images, and push notifications. The mobile app was developed by following secure by design principles. Thus, several layers of security are embedded in the mobile app to protect patient and user data:

1. The mobile app does not download any patient scans from StrokeViewer cloud.
2. All data transfers between the mobile app and StrokeViewer cloud are encrypted.
3. The mobile app has an automatic lock mechanism to prevent unauthorized access to devices with no lock screen enabled.
4. Users need to provide valid user credentials to access StrokeViewer data in the app. After that, users can enable the use of a pin code or biometrics to access the StrokeViewer app.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

5. Authentication tokens are securely stored in the respective OS's encrypted storage. On iOS we use Keychain, on Android we use the Keystore. As soon as the app goes into the background, we remove the authentication tokens from memory. Upon a next valid unlock of the app, we retrieve them again from the Keychain and Keystore respectively before the app can interact with our backend APIs.

The StrokeViewer mobile app must be downloaded directly from the official Android and iOS app stores. App stores representatives review all apps registered at these stores to ensure they comply with the legal and security requirements before publishing. More details regarding the iOS legal requirements related to privacy can be found at https://developer.apple.com/app-store/review/guidelines/. For Android devices, this information can be found at https://support.google.com/googleplay/android-developer/answer/10787469?hl=en. The following policies have also been followed when developing the Android version of StrokeViewer app: https://play.google.com/about/developer-content-policy/. Furthermore, both the iOS App Store and Android Play Store require that all apps and updates are digitally signed with a certificate. This guarantees the app's integrity and assures that the app originates from Nicolab and has not been modified since it was signed, thus safe to download and install by a user.

Protecting user data

The only user data stored in StrokeViewer is the user login information. StrokeViewer sends email notifications to general mailing lists, which are managed by the hospital. Thus, if the hospital is configured to have users logging in with a de-identified user ID, no personally identifiable user information, such as email or username, is saved in StrokeViewer. It is the responsibility of the hospitals to configure their identity provider system to use just de-identified user IDs for authentication instead of a user email or username. Nevertheless, Nicolab complies with GDPR. Therefore, Nicolab can remove any personally identifiable information such as user email or username from StrokeViewer upon request.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

Certifications and standards

Nicolab is ISO/IEC 27001 (Information security management), NEN 7510-1 (Health informatics - Information security management in healthcare) and ISO 13485 (Medical devices - Quality Management System) certified, having regular yearly surveillance audits ensuring continuous compliance to standards. Next to the above standards, Nicolab uses ISO 14971, IEC 62304, and IEC 82304 standards in its daily practice. Nicolab is also GDPR compliant.

ISO/IEC 27001

ISO/IEC 27001 specifies requirements for defining an information security management system (ISMS). The ISMS is used as a framework for establishing information security risk management processes. Nicolab is ISO/IEC 27001 certified. Nicolab is audited at least two times each year in relation to the ISO/IEC 27001. One of these audits is performance by an 3rd party company and the other audit is performed by a notified body.

NEN 7510-1

NEN 7510-1 provides guidelines for determining, establishing, and maintaining measures to secure patient information. A NEN 7510-1 certificate provides evidence that an organization can handle patient data securely and responsibly. Nicolab is NEN 7510-1 certified. Nicolab undergoes at least two NEN 7510-1 audits each year. One of these audits is performance by an 3rd party company and the other audit is performed by a notified body.

ISO 13485

The ISO 13485 determines the requirements for a comprehensive quality management system for designing and production of medical devices. ISO 13485 is the medical device industry's most widely used international standard for quality management. ISO 13485 provides a practical foundation for addressing the EU Medical Device Directive (MDD) and the EU Medical Device Regulation (MDR). Nicolab is ISO 13485 certified.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

Additional standards

IEC 62304

IEC 62304 defines a set of processes, activities, and tasks for the development of medical device software. Nicolab followed the IEC 62304 standard when developing StrokeViewer.

ISO 14971

ISO 14971 defines requirements for risk management activities that determine the safety of a medical device during the development life cycle. In addition, other standards, such as ISO 13485 and IEC 62304, require risk management activities. Nicolab followed the ISO 14971 standard when developing StrokeViewer.

IEC 82304

IEC 82304 defines requirements for the safety and security of medical software designed to operate on general computing platforms without dedicated hardware. It covers the entire software development lifecycle, including design, development, validation, installation, and maintenance. Nicolab followed the IEC 82304 standard when developing StrokeViewer.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

NICOLAB

Situation in The Netherlands

A healthcare provider does not need patient consent to place patient data in the cloud. The Algemene Verordening Persoonsgegevens (AVG) allows a hospital to have patient data processed by a 3rd party without the patient's consent. Medical professional secrecy does not prescribe that a healthcare provider must request permission to upload patient data to the cloud. Article 7:457 of the Dutch Civil Code (BW) stipulates that those directly involved in implementing the treatment agreement may use patient data without the patient's consent. A cloud provider that processes patient data for the healthcare provider is considered as directly involved in the execution of the treatment agreement.

There are no special restrictions for transfer of patient data within the EU. Thus, the cloud infrastructure storing and processing patient data collected in the Netherlands is not required to be located within the borders of The Netherlands. At the moment, the data uploaded from Dutch hospitals is processed in Servers in the Netherlands. In case there are not enough computing resources in the Netherlands servers, there is a possibility that the data is processed in our servers located in Belgium or Germany. Nicolab is improving StrokeViewer cloud infrastructure to ensure that all data processed by Dutch hospitals do not leave the Netherlands.

For more information please consult the Praktijkgids - Patiëntgegevens in de cloud by the Autoriteit Persoonsgegevens.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

Situation in Germany

In Germany, the digitalization of healthcare is currently an issue of utmost importance. The recently passed Hospital Future Act (KHZG) explicitly lists cloud-based systems to digitalize processes. In addition, Germany's federal government is investing €4.3 billion for "a better digital infrastructure" in the nation's hospitals. However, given the highly sensitive nature of health data and the principle of medical confidentiality, Germany established strict data security and privacy requirements for health data in cloud environments. These strict requirements have historically led to some reluctance in using specific cloud computing solutions. Nevertheless, StrokeViewer fulfills all German requirements for processing patient data in the cloud.

Under the German Federal Data Protection Act and the EU General Data Protection Regulation, health data qualifies as a special category of personal data. In this context, German regulators have historically implemented more strict requirements for patient data regarding the international transfer of patient data. All data uploaded to the German StrokeViewer environment (https://de.strokeviewer.com/) is never transferred to other countries. All storage, transfers, and processing are performed in servers located in Frankfurt.

The German Federal Office for Information Security has published a White Paper entitled Security Recommendations for Cloud Computing Providers and a Cloud Computing Compliance Controls Catalog about data security. These documents define which requirements providers of cloud services should implement. Among these requirements, the Federal Office emphasizes the importance of the ISO/IEC 27001 standard. Nicolab services comply with ISO 27001 regarding information security management.

In German law, healthcare providers must maintain the secrecy of patient information following the principle of medical confidentiality. In 2017, the German legislature amended the Criminal Code, Section 203, to facilitate the use of cloud services. The amended law allows for the disclosure of confidential information to other people involved in

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852
NICOLAB

professional activities, provided that this confidential information is required for the execution of such professional activities. In other words, doctors can, for example, disclose confidential patient information to an IT service provider to the extent that this information is required to make use of their services. StrokeViewer only needs to receive DICOM images from the patients and no other patient data. Personal information stored in these DICOM images is displayed in the user interface of StrokeViewer to allow healthcare professionals to identify which image corresponds to each patient.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

NICOLAB

Situation in the United Kingdom

The UK Government introduced the 'cloud first' policy in 2013. The usage of cloud services like StrokeViewer is also endorsed in the National Information Board's Personalised Health and Care 2020 framework. This framework is compliant with the National Data Guardian's recommendations. NHS and social care organizations are allowed to collect, transfer, store, and process patient data within the UK, European Economic Area (EEA), a country deemed adequate by the European Commission, or in the US where covered by Privacy Shield. In addition, Nicolab has also passed the NHS Data Security and Protection Toolkit assessment, which can be downloaded at https://www.dsptoolkit.nhs.uk/.

All data uploaded to the UK StrokeViewer environment (https://uk.strokeviewer.com/) is never transferred to other countries. All storage, transfers, and processing are performed in servers located in London. There are no restrictions on where in the UK the data may remain. For instance, data from the NHS in England may be stored in Scotland and vice versa.

A national guidance has been published setting clear expectations for healthcare organizations who want to use cloud services or data offshoring to store patient information. This guidance is called "NHS and social care data: off-shoring and the use of public cloud services" and it can be consulted for more detailed information.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

Situation in Australia

The Australian privacy law has strict rules regarding the way a health service provider can collect and use patient data. The Chapter D of the Australian Privacy Principles guidelines (APPs) set out in the Australian Privacy Act 1988 impose requirements for collecting, managing, dealing with, using, disclosing, and handling personal information related to health situations. More specifically, the Section 16B of the Privacy Amendment Act determines that collecting and managing health information is permitted if done to provide a health service. Nicolab classifies as health service provider and therefore is allowed to collect and process patient data in its cloud.

Nicolab implements and maintains technical and organizational security measures in accordance to globally recognized security frameworks and certifications including OWASP Application Security Verification Standard and ISO/IEC 27001. Furthermore, the cloud infrastructure used by StrokeViewer is physically located within the Australian borders. This cloud infrastructure was evaluated by an independent third-party in regards to the Cloud Security Guidance package. The conclusion of this evaluation was that this cloud infrastructure is strongly aligned with PROTECTED level control requirements. Such requirements contain guidelines for stablishing cybersecurity roles, detecting and managing cybersecurity incidents, physical and personnel security procedures, securing networking, usage of cryptography, among other information security practices. This evaluation was performed based on the ACSC's updated IRAP framework, which is outlined in the Cloud Security Guidance package.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852

Situation in New Zealand

In New Zealand, the Privacy Act 2020 determines how organizations and businesses can collect, store, use, and share personal information. The Privacy Act 2020 replaces the Privacy Act 1933 and it strengthens the privacy protection rules in New Zealand. The Privacy Act 2020 advocates for early intervention and stricter risk management measures related to protection of personal information.

In the context of health information, principle 2 of the Privacy Act 2020 establishes exceptions for handling of information that is used to "to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual", which is the case when using StrokeViewer. In addition, principle 12 determines that personal information can be sent overseas provided that it complies with the Privacy Act 2020. Nicolab is "conducting business in New Zealand" and it is therefore allowed to send patient data overseas subject to New Zealand's Privacy Act. At this moment, the data processed and stored by StrokeViewer is located in Australia. StrokeViewer requires special cloud infrastructure with high performance computing capabilities to deliver the timely results which are needed when managing acute stroke patients. Nicolab has plans to deploy StrokeViewer services physically in New Zealand as soon as such high-performance cloud infrastructures are available in New Zealand.

Additionally, the Government Communications Security Bureau (GCSB) has published the New Zealand Information Security Manual (NZISM) which is the official government manual for information security. The NZISM is consistent with several internationally recognized standards including the ISO/IEC 27001. Nicolab is ISO/IEC 27001 certified. This standard establishes requirements for setting up an information security management system. As part of these requirements, it also includes well established industry practices related to information security risk management.

StrokeViewer is a product of Nicolab
Paasheuvelweg 25 | 1105 BP Amsterdam | info@nicolab.com | +31 20 244 0852