navify®

FAQ

navify Decision Support portfolio

Data Security, Privacy and Compliance

Table of Contents

Introduction

navify® Decision Support portfolio is a suite of interoperable, scalable workflows and apps that empower personalized healthcare. By aggregating patient-specific detail with relevant, curated scientific and medical data from an ever-expanding knowledge base, clinicians can confidently make better decisions across the care continuum. Roche takes the safeguarding of sensitive data* seriously. The **navify** portfolio of cloud-based Software as a Service (SaaS) solutions achieves multi-layer security through state-of-the-art security controls to ensure sensitive data remains secure and compliant with jurisdictional privacy regulations, such as HIPAA (US) and GDPR (EU). This Frequently Asked Questions (FAQ) document provides answers to common queries and concerns in relation to the protection of sensitive data in **navify** portfolio. Further information in relation to the security and privacy controls implemented by Roche and its technology partners to protect the confidentiality, integrity and availability of sensitive data can be provided on request.

Where does navify Decision Support portfolio host patient data?

navify portfolio is securely hosted in the Amazon Web Services (AWS) Cloud. As of January 2020, AWS spans more than 20 geographic regions and around 70 Availability Zones. An AWS region is an independent cluster of AWS data centers built in a specific geographic location (country). A region can be thought of as a data residency zone. Each AWS Region consists of between 2 to 6 AWS Availability Zones, which are discrete data centers with redundant power, networking and connectivity, housed in separate facilities. Availability Zones offer the ability to operate production applications and databases that are more highly available, fault tolerant and scalable than would be possible from a single data center. Roche has deployed **navify** portfolio instances in multiple AWS regions which allows us to optimize network latency and ensure high availability while maintaining compliance with data residency requirements. Roche controls the location in which each customer's data is processed and stored. Data is replicated between availability zones but never leaves the region in which the tenant has been deployed. For example, tenants belonging to customers based in mainland Europe and the Republic of Ireland are deployed in the "eu-central-1" AWS region, located in Frankfurt, Germany. AWS will not move content without Roche's consent.

*This document uses the term "sensitive data" to refer to the following: US: Personally Identifiable Information (PII) and Protected Health Information (PHI) EU: Personal data and sensitive personal data

Is it safe to store patient data in the cloud?

The software deployment model (on-premise versus cloud-hosted) is just one of many factors that contribute to the security of sensitive data at rest. Roche has developed a robust security strategy which combines the built-in security of the AWS cloud infrastructure with our product security measures to protect sensitive data and the integrity of the application as a whole. AWS cloud security is built to meet the requirements of the most security sensitive organizations. The AWS infrastructure has been designed to provide high availability, while putting strong safeguards in place to protect sensitive information. Roche and its partners for sub-contracted services have implemented a security architecture which focuses on safeguarding sensitive data through industry-leading encryption and key management, identity and access management, infrastructure security, logging and monitoring and incident response. As part of Roche's commitment to data security, controls are implemented in alignment with industry-leading security frameworks, including HITRUST CSF and ISO/IEC 27001*, 27017** and 27018***.

How is data segregation ensured?

navify® Tumor Board utilizes a multi-tenant architecture, which stores all data in a single physical database. Data access is strictly managed and the product restricts the access of a tenant's data to users belonging only to that tenant. This separation of each customer's data is controlled through a combination of a logical authorization layer and a data model which logically segregates data from each facility. The data model links all patient data to a patient and a patient to a facility. The authorization layer enforces role-based access control policies to further restrict the data each user has permissions to.

How are new users created?

Roche provisions a privileged account known as the "Customer Administrator" account as part of the initial tenant setup which is assigned to a customer designated user within the customer's institution. A tenant or facility is a logically isolated **navify** Tumor Board instance dedicated to an individual customer. A user with Customer Administrator privileges can create additional users for their tenant from within **navify** Tumor Board. Alternatively, Roche can create non-administrative user accounts upon customer request. Newly provisioned users receive an email from Okta (**navify** Tumor Board's identity and access management service provider) containing their user ID and a link to set up an initial password and security question/answer used for password recovery. Once the setup is complete, users can close the Okta page, enter the **navify** Tumor Board URL and authenticate to the application with their newly-created credentials.

How do we ensure that data access is restricted to the appropriate users?

navify Tumor Board utilizes role-based access control to enforce restrictions on the creation of users, the scope of patient access (all patients within a facility or only patients associated with a particular tumor board) and the type of actions that can be performed on patient profiles (read, write, update and delete). **navify** Tumor Board also enforces "Parent/Child" authorization logic for sites that collaborate on tumor board meetings i.e., a parent institution can view all patients from all sites that are connected to it whereas a child institution can only see patients that are associated to their site.

What is available in navify Tumor Board with respect to traceability and audit logging?

navify Tumor Board has an integrated audit log that can be accessed via the Administration page by users with the Customer Administrator role. The audit log captures all actions performed by **navify** Tumor Board users, including but not limited to login and logout attempts and actions (create/view/change) performed on data within the application. Each log entry includes the following information: date/time stamp, user's Okta ID, Organization universally unique identifier (UUID), browser type and HTTP REST API call.

*27001: Information security management systems - Requirements.
**27017: Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
***27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

When can patient data in navify Tumor Board be deleted?

navify® Tumor Board users can delete patient profiles from within the application. Deleting a patient profile removes all data, reports and attachments about the patient. Deleted patient profiles cannot be recovered. It is important to note that **navify** Tumor Board is not intended for use as an electronic medical record system, or to substitute a customer's primary data sources. The customer maintains full responsibility for the retention of patient data in accordance with regulatory or organizational requirements, although Roche may support the customer in fulfilling data subject requests and meeting data retention requirements where necessary.

How does navify portfolio encrypt sensitive data?

navify portfolio employs bulk encryption of sensitive data both in transit and at rest using the de facto Advanced Encryption Standard (AES) symmetric encryption algorithm. Data in transit (that flows between the client's browser, application front-end, back-end services and AWS data stores) is encrypted using AES as part of Transport Layer Security (TLS) version 1.2.TLS1.2 supports AES encryption with a key length of up to 256 bits*. Encryption at rest is implemented whenever sensitive data is stored, using AES with 256 bit keys.

How does navify portfolio protect the cryptographic keys used to encrypt sensitive data?

The security of encrypted data is dependent on the key management infrastructure that protects the cryptographic keys used to perform encryption and decryption operations. **navify** portfolio employs the AWS Key Management Service (KMS) to securely manage cryptographic keys throughout the duration of their lifecycle. KMS provides a highly available key generation, storage, management and auditing solution for the encryption of data across AWS services. KMS is based on the concept of envelope encryption whereby the data keys used to encrypt sensitive information are themselves encrypted by a master key. Envelope encryption allows data keys to be securely distributed and stored in encrypted form while reducing the scope of the key management problem of the secrecy of the master key. AWS KMS stores master keys in FIPS 140-2 (a U.S. government computer security standard used to approve cryptographic modules). KMS is designed so that no one, including AWS employees, can retrieve plaintext master keys from the HSMs. Plaintext master keys are never written to disk and are only ever used in the volatile memory of the HSMs for the time needed to perform a specific cryptographic operation. Updates to software on the HSM firmware are controlled by multi-party access control that is audited and reviewed by an independent group within AWS as well as a NIST-certified lab in compliance with FIPS 140-2. Access to KMS resources, such as requests from AWS services for the generation, encryption or decryption of data keys, is controlled by a strict identity and access management policy. *Key lengths are negotiated as part of the TLS handshake protocol.

How is the data protected in the interface between the hospital EMR and navify Tumor Board?

navify Tumor Board supports the Health Level 7 version 2 (HL7v2) Minimum Lower Layer Protocol (MLLP) and Fast Healthcare Interoperability Resources (FHIR) healthcare information exchange standards as part of our data integration platform services. Since HL7 transports data using MLLP and data encryption was not considered as part of the MLLP specification, confidentiality and entity authentication is provided by the exchange of MLLP messages over an IPSec encrypted tunnel. The FHIR specification is based on a RESTful framework where transactions are performed using request/response as part of the HTTP protocol. This allows for the use of Transport Layer Security (TLS) for the exchange of messages over an encrypted and mutually authenticated channel.

Does Roche have access to sensitive data?

Roche and its subcontractors do not have intelligible (unencrypted) access to patient data. Temporary access to patient data may be granted by the customer if so required under specific circumstances (e.g., to troubleshoot and resolve production issues). Details of the circumstances in which Roche or its subcontractors may require temporary access to patient data are outlined in our data processing agreement or equivalent (as applicable, by location).

What services does Roche outsource to third parties (and do third-party service providers have access to sensitive data)?

Roche employs the services of the following third-parties in relation to the provision of **navify**® Tumor Board:

Accenture

Accenture is responsible for the provision of services in relation to the integration of customer data to Roche's **navify** Tumor Board solution via the digital data integration platform. Accenture also provides support and maintenance services specifically related to data integration (e.g., incident and problem management). Subject to the customer's approval, Accenture may require temporary access to patient data to troubleshoot and resolve production digital integration platform-related issues. Such activities would be visible to, and under the direct control of the customer.

Okta UK Ltd, Okta, Inc.

Okta is a provider of managed authentication services. Okta stores user data, such as system login IDs, in encrypted form.

What is Amazon Web Services (AWS) responsible for?

navify Tumor Board is a Software as a Service (SaaS) solution hosted in the AWS Cloud. AWS is responsible for the provision of a reliable and scalable cloud computing infrastructure, the physical security of the infrastructure and the security of the core compute, storage and networking services.

What security certifications does navify Tumor Board have?

navify Tumor Board has achieved multiple security and privacy certifications and has been designed to operate in accordance with the laws and regulations of the jurisdiction in which it is commercially available, including HIPAA (US) and GDPR (EU). **navify** Tumor Board falls under the scope of Roche ISO/IEC 27001, 27017 and 27018 certifications. ISO 27001, the most well known in the 27000 series of international standards for information security management, specifies a comprehensive set of information security management system requirements. Conformance to 27001 demonstrates the implementation, maintenance and continual improvement of a framework of policies, procedures, technical controls and overall governance for the protection of sensitive data in line with industry best practice. ISO 27017 and 27018 compliment 27001 by specifying additional cloud-specific control requirements. ISO 27017 details controls related to the provision of cloud-based services while 27018 focuses on the protection of sensitive information stored and processed in the cloud.

How does navify Tumor Board maintain compliance with data protection regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the EU General Data Protection Regulation (GDPR)?

Roche recognizes the importance of incorporating privacy and security principles in our product development process and has designed **navify**® Tumor Board to adapt to changing data privacy needs and requirements for data storage locations while upholding the rights of data subjects. We track the flow of data in transit and in storage in the cloud, provide safeguards at every stage of the data's life cycle, and map policies, procedures and technical measures to regulations in each geography. Robust attention to compliance responsibilities ensures changing security and privacy needs are continuously met.

Has navify Tumor Board been cleared by the FDA? by European Authorities?

navify Tumor Board is a software product that is intended to optimize the workflow of a multidisciplinary care team meeting (known as a tumor board). It is a patient data aggregation and visualization tool for care management. It is not intended for use as an active patient monitoring device, nor does it intercept or analyze clinical laboratory tests or other device data, results or findings. Based on its stated intended purpose and functionality, **navify** Tumor Board does not fulfill the definition of "medical device" outlined in the Medical Devices Directive (Directive 93/42/ECC), Medical Devices Regulation (Regulation EU 2017/745) or Section 201(h) of the Federal Food, Drug, and Cosmetic Act. As such, **navify** Tumor Board is not subject to FDA regulation or CE marking.

Who owns the data that is transferred to navify Tumor Board?

Personal data of users (patients or customers) is always owned by such users. Any potential analytics Roche may create with non-personal and/or technical data would be owned by Roche, though exceptions are possible and likely depending on the nature of the data.

MC--03631 (June 2023)