BioMedIT

General Security Concept

1 Introduction to BioMedIT

The BioMedIT Network Project was funded by the Swiss federal government for the period of 2017-2020 within the framework of the Swiss Personalized Health Network Initiative (SPHN) and in close collaboration with the strategic focus area Personalized Health and Related Technologies (PHRT) of the Swiss Federal Institutes of Technology (ETH) domain (second funding period 2021-2024). The goal of the BioMedIT Network Project is to create a national, secure IT infrastructure to support computational biomedical research and clinical bioinformatics using confidential (i.e. sensitive personal) data. The BioMedIT Network can jointly be used by all Swiss Universities, research institutions, hospitals and other interested partners.

The BioMedIT Network encompasses:

1. the local technical and procedural high-security BioMedIT Node infrastructures (BioMedIT Nodes)
2. the connection and collaboration between the BioMedIT Nodes (BioMedIT Network), and
3. the central infrastructure components and procedural solutions provided as a central service.

The BioMedIT Network builds on three legally independent scientific IT competence centers and respective platforms: sciCORE in Basel, operated by the University of Basel, Core-IT in Lausanne, operated by the SIB Swiss Institute of Bioinformatics, and SIS in Zurich, operated by ETH Zurich). Under the umbrella of the BioMedIT Network Project, all three engaged institutions committed to build a high performance computing infrastructure (in addition to their already existing scientific compute clusters) especially designed for sensitive data for Personalized Health and data-driven research: sciCOREmed in Basel, SENSA (Secure sENSitive data processing plAtform) in Lausanne, and Leonhard Med in Zurich – the BioMedIT Nodes. A BioMedIT Node is a local or regional node that provides a secure compute and storage infrastructure for handling (securely storing, managing and processing) sensitive research data, whether clear text, pseudonymized or coded personal data. Each Nodes is an integral part of the BioMedIT Network and performs its function within a ‘snowflake’ architecture (see figure below) - receiving and routing data, warranting interoperability, interfacing and collaborating with the other existing BioMedIT Nodes. The BioMedIT Network is specifically designed for collaborative research projects on sensitive data that is brought together from federated data sources and analyzed by multidisciplinary research teams from different institutions (called “project clients”). The computational service infrastructure of individual BioMedIT Nodes can also be used by organizational clients (Swiss universities, research institutes, hospitals, service providers and other interested partners) requiring a secured workspace (institutional tenant) with enhanced security to securely store, manage and process confidential research data.

SIB Swiss Institute of Bioinformatics
Personalized Health Informatics Group (PHI)
Elisabethenstrasse 43
CH-4051 Basel

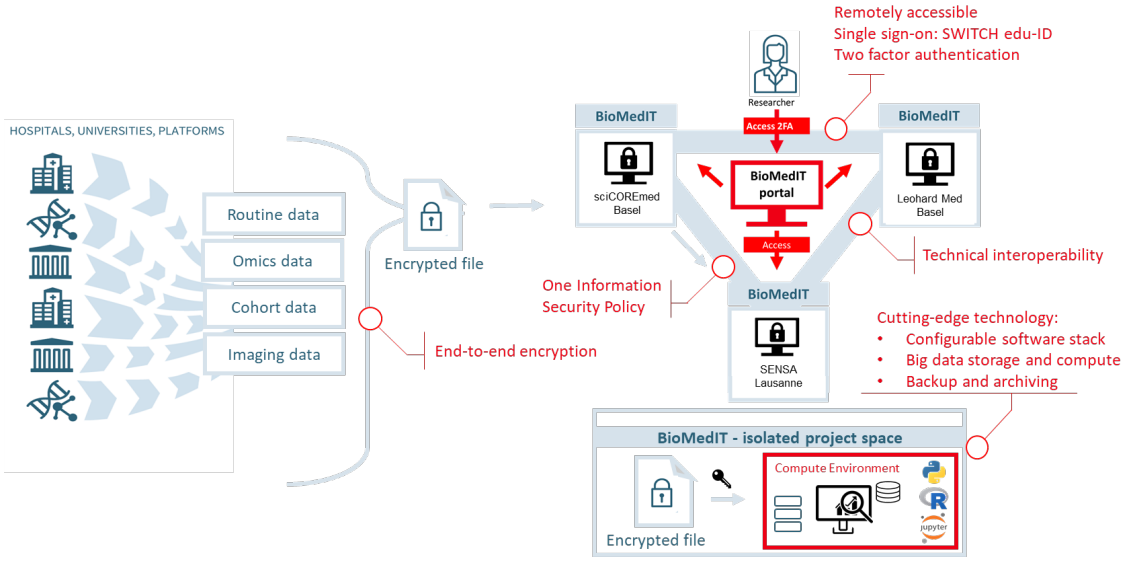

Figure 1: The components, organization, characteristics and context of the BioMedIT Network

Central infrastructure components (such as tools, platforms, etc.) and procedural solutions are under the responsibility of SIB's Personalized Health Informatics (PHI) Group. PHI operates a central service layer and is responsible for the coordination of the BioMedIT Network Project.

2 BioMedIT security aspects

2.1 SPHN Information security policy

An Information Security Policy, applicable across the entire BioMedIT network, defines the necessary organizational and technical measures to allow researchers to process sensitive data in a secure way. This policy sets out how confidentiality, integrity, and availability of information are to be handled thereby preventing misuse and malicious damage. The Policy is underpinned with a range of Standard Operating Procedures (SOPs), Work Instructions and Guidelines to support both users and administrators.

2.2 Secure data transfer

The network follows a hub-and-spoke organizational design. Transfer of data within the network is carried out in a "snowflake" manner - one BioMedIT Node serves as the main (destination) node, on which the data is gathered and processed, and the other two nodes receive the data from Data Providers in their proximity and route the data to the destination node. Data providing institutions are securely connected to the network to enable secured sharing of sensitive research data over the BioMedIT infrastructure. Each Data Provider has one landing zone to where encrypted and signed data packages are sent, generally via Secure File Transfer Protocol (SFTP) from whitelisted IP addresses; the same method is used for data transfers which take place internally between the BioMedIT Nodes. To facilitate end-to-end encrypted and standardized data transfers throughout the whole network, the BioMedIT Interoperability Working Group (BIWG) developed and maintains sett (Secure Encryption and Transfer Tool), a tool to support the full process of

secure data transfer with both a graphical user interface (GUI) and a command line interface (CLI). sett has the following four modules: PGP key management, data packaging and encryption, data transfer, as well as decryption and unpacking.

2.3 Users

BioMedIT users are trained in “data privacy and IT security”, BioMedIT offers the “Data Privacy and IT Security Training” as on-line training or class-room course hosted regularly in different cities in Switzerland. Users must pass a mandatory on-line exam. It is in the responsibility of the Project Lead to grant access to the project space. An authorized user can then access the project spaces via the BioMedIT Portal using a SWITCH edu-ID account with two factor authentication. Additionally, the BioMedIT network can only be accessed from within trusted IT environments (e.g. from within a Swiss university or university hospital network or via VPN).

2.4 Project Spaces

Data security in the BioMedIT Nodes is principally based on allocation of project-specific IT resources within an access-controlled, private, virtual environment offering network isolation, data isolation and computational resources isolation (private tenant). Shared tenants are only permitted in those cases where there is a specific authorization. A private tenant ensures that data stored in one project space cannot be shared – intentionally or by accident - with another project. Users can then connect to project spaces for which they are specifically authorized via a virtual desktop with a graphical interface or a virtual terminal session. Access to the Internet from the BioMedIT project space is strictly controlled, limited to trusted and explicitly white-listed web resources. Encrypted backups of the data are done on a regular basis. By default, direct Secure Shell (SSH) access is not permitted but can be enabled in exceptional, authorized cases and to specific project spaces.

The security concepts of the individual nodes are available upon request (dcc@sib.swiss).