INFORMATION SECURITY SERVICES
INFORMATION TECHNOLOGY
The University of Oklahoma Health Sciences Center

Insight™ Platform Rules of Behavior

January 17, 2019
1.0 Version
February 29,2019
2.0 Version
September 2, 2020
3.0 Version
December 1, 2021
4.0 Version
February 22, 2023
5.0 Version

1. Revision History

1.1 Version

Version	Date	Updates Made By	Updates Made
1.0	1/17/2019	Michela Aguirre	Creation of document
2.0	2/29/2019	Michela Aguirre and Ashley Mathews	Insight Platform Data and Security
3.0	09/02/2020	Jason Heckard	Updated User Password requirements
4.0	12/01/2021	Jason Heckard	Revised system diagrams
5.0	02/22/2023	Jason Heckard	Document Review

2. Overview

Rules of Behavior describe security controls associated with user understanding of Insight data and security protocols as well as responsibilities and certain expectations of behavior for following security policies, standards, and procedures. The Insight Platform used to create web and mobile applications is for Individuals who are authorized to use the OU Health Science Center (OUHSC) Insight Platform must comply with the specific Rules of Behavior (RoB) listed below.

All new users of the OUHSC Insight Platform must read the OUHSC Insight Platform Rules of Behavior (RoB) and sign the accompanying acknowledgement before accessing the Service. This acknowledgement must be completed annually thereafter. By signing the form, users reaffirm their knowledge of, and agreement to adhere to, the OUHSC Insight Platform RoB. The OUHSC Insight Platform RoB may be presented to the user in hardcopy or electronically. The user's acknowledgement may only be obtained by written signature.

The OUHSC Insight Platform RoB cannot account for every possible situation. Therefore, where the OUHSC Insight Platform RoB does not provide explicit guidance, users must use their best judgment to apply the principles set forth in the RoB for ethical conduct to guide their actions.

Non-compliance with the OUHSC Insight Platform RoB may be cause for immediate suspension of access privileges.

3. Data and Security

All data collected by the Insight Platform is encrypted during storage and in transit. Users of the OUHSC Insight Platform should confer with their institution's policies regarding restrictions associated with data collection and transfer between the Insight mobile application, Microsoft Azure servers, and users' institutional servers. Data collected and stored by users is intended to be de-identified. Any data classified as PHI will require users' institution to enter into an appropriate Business Associate Agreement.

Architecture of the Insight Platform is shown below (see Fig. 1):

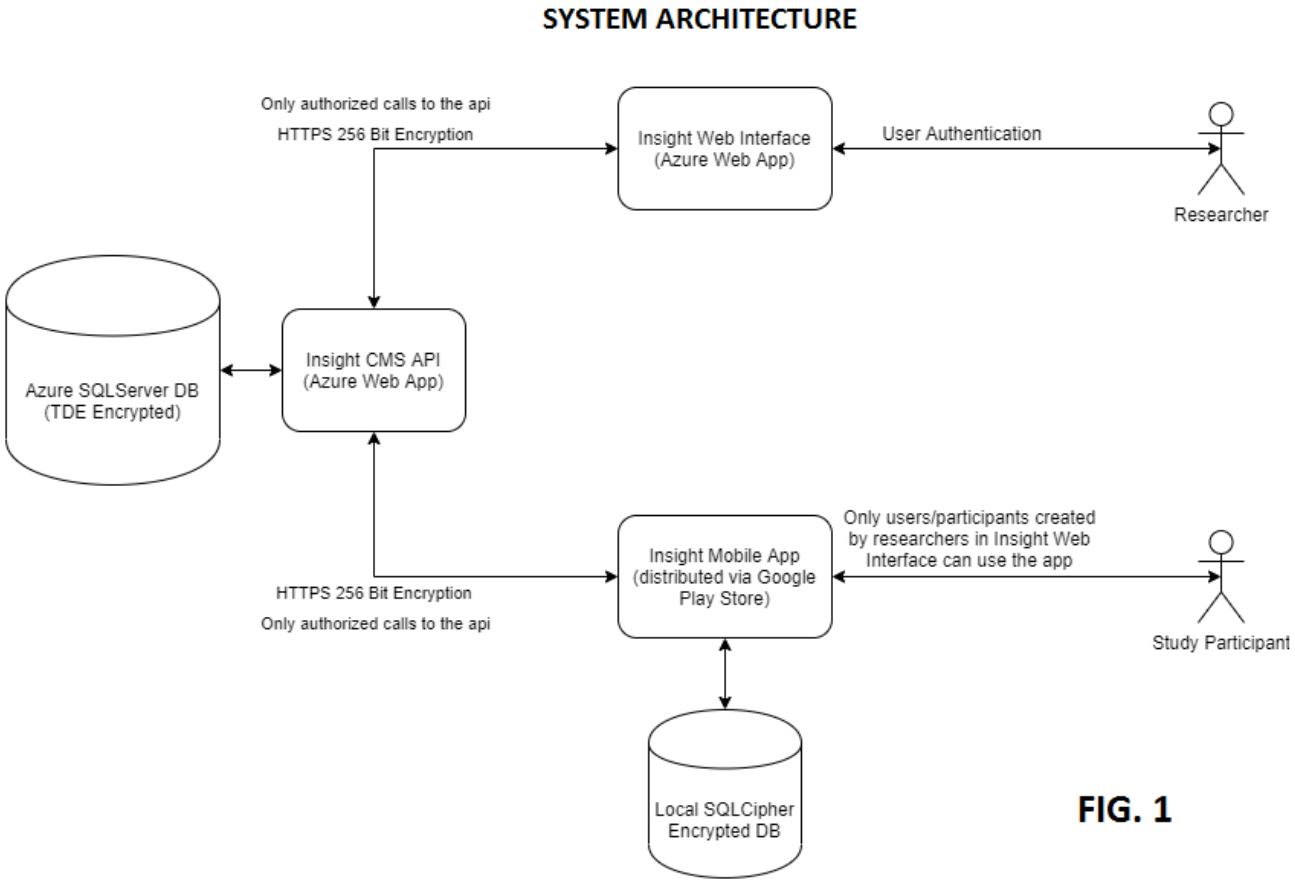

FIG. 1

The following describes the processes associated with data security:

3.1 Phone Data

Database: SQLite

Encryption: SQLCipher

- encryption algorithm is 256-bit AES in CBC mode
- OpenSSL libcrypto, LibTomCrypt, and CommonCrypto for cryptographic functions

https://www.zetetic.net/sqlcipher/design/

https://www.zetetic.net/sqlcipher/sqlcipher-for-dotnet/

3.2 Data in Transit

All data in transit is encrypted utilizing a COMODO SSL Certificate for 256-bit encryption.

The data transfer and storage process is shown below (see Fig. 2):

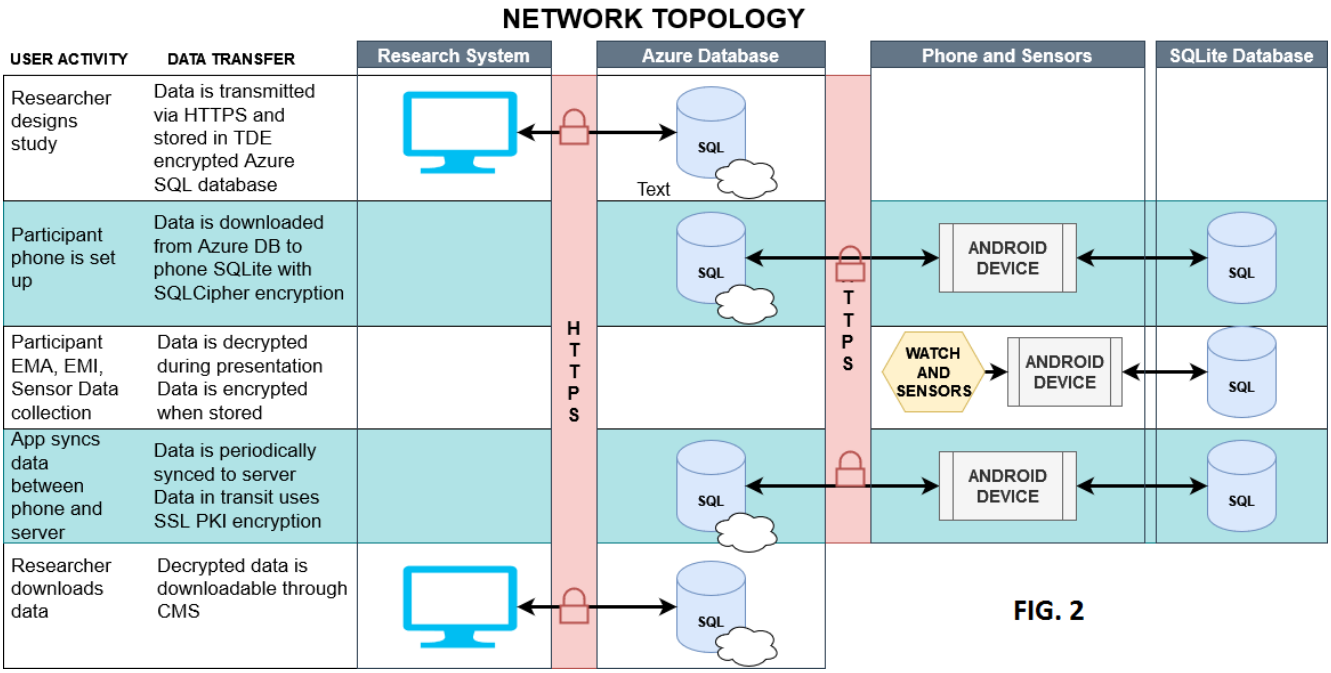

FIG. 2

3.3 Server Data – MS Azure Web Application and Database Hosting

- App resources are secured from the other customers' Azure resources.
- VM instances and runtime software are regularly updated to address newly discovered vulnerabilities.
- Communication of secrets (such as connection strings) between the app and other Azure resources (such as SQL Database) stays within Azure and doesn't cross any network boundaries. Secrets are always encrypted when stored.
- All communication over the App Service features is encrypted.
- Connections with remote management tools like Azure SDKs, REST APIs, are all encrypted.
- Transparent Data Encryption: real-time encryption and decryption of the database, associated backups, and transaction log files at rest
- 24-hour threat management protects the infrastructure and platform against malware, distributed denial-of-service (DDoS), man-in-the-middle (MITM), and other threats.

https://docs.microsoft.com/en-us/azure/app-service/overview-security

3.4 MS Azure Compliance

Microsoft enterprise cloud services are also covered by FedRAMP assessments. Microsoft Azure and Microsoft Azure Government received a Provisional Authority to Operate from the FedRAMP Joint Authorization Board; Microsoft Dynamics 365 U.S. Government received an Agency Authority to Operate from the US Department of Housing and Urban Development, as did Microsoft Office 365 U.S. Government from the US Department of Health and Human Services."

https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)
- Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0
- HIPAA Privacy and Security Rules
- ISO/IEC 9001, 27001, 27017, 27018
- FDA CFR Title 21 Part 11
- FedRAMP Moderate

https://azure.microsoft.com/en-us/industries/healthcare/

4. End User Responsibilities

A. Accountability

- Users of the Insight Platform are accountable for their actions and may be held liable for any unauthorized actions. Any failure to comply with the Rules of Behavior shall be considered an Information Security Incident.
- Any Human Participant Research Data uses of < Insight Platform > must comply with the Rules of Behavior and shall include in the submitted IRB Protocol, any risks identified during the Information Security Risk Assessment (ISRA) in order to remain in compliance with IRB submission criteria.

B. Acceptable Use

- The Insight Platform is owned by the University of Oklahoma Health Sciences Center and data collected by the Insight Platform can only be used with user authorization. All users with an approved Sevice Agreement with the University of Oklahoma Health Sciences Center will have access to agreed upon services specified in the Service Agreement.

C. Passwords

User passwords must meet OUHSC minimum standards for:

- Complexity – all four character types must be used (upper case, lower case, numeric, and special character)
- Length – a minimum of 12 characters must be used

Users are responsible for:

- Maintaining the secrecy of their password, which means that a user's password may not be written down, stored electronically, or revealed to anyone, regardless of position, either inside or outside of the organization;
- Notify the mHealth Shared resource at 405-271-3150 immediately if a user of the Insight Platform needs to change their password, if they suspect the password has been compromised, or if a password and access should be removed;
- Not utilize another individual's password and User ID or allow others to utilize their password and User ID.
- Not use the same home institutuional user ID and\or password for access into Insight Platform.

D. Data Storage

- Users are responsible for encrypting data while at rest at their home institutional servers.

5. Signature

I have read the *OUHSC Insight Platform Rules of Behavior* and understand and agree to comply with its provisions. I understand that violation of the OUHSC Insight Platform RoB may lead to immediate suspension of access privileges.

User's Name: _____

(Print Name)

User's Signature: _____ Date: _____