Generic Health Network Information Technology for the Enterprise (GRHANITE™)

GRHANITE™ Data, Messaging and Security Provisions, July 2016

Background

The University of Melbourne GRHANITE™ tool provides ethical and secure mechanisms for the provision of data for audit, health surveillance and research applications. GRHANITE™ is developed and maintained by the University of Melbourne Health and Biomedical Informatics Centre, Research Technology Unit (HaBIC R²). HaBIC R² trustworthy status relies on it continuously achieving operational performance that aligns to University of Melbourne values. This document provides technical guidance on the data, messaging and security provisions built into the tool and our University processes.

Data Extracted by GRHANITE™

GRHANITE™ is designed to extract data in a de-identified manner. Patient names, dates of birth, address or other identifying information are not extracted except under exceptional circumstances by prior agreement (see below). The number of fields and the types of data extracted for a client project are reviewed by medical ethics committees and GRHANITE™ strictly conforms to what is approved by these ethics committees. Non-research uses of the technology (for example regional population health planning) do not require ethics approval although similar strict governance mechanisms still apply.

- The HaBIC R² unit have over nine years’ experience in data acquisition and we advise our customers on the best approaches to obtaining the required data including aggregating data as much as possible and minimising what is extracted.
  - The HaBIC R² unit undertake a process of certification with our clients aimed at ensuring that interface data extracted conforms to ethics.
  - Control mechanisms are adopted throughout a project’s lifecycle to further minimise any prospect of a data breach arising or impacting on individuals.
  - The HaBIC R² unit will not permit data extracts that do not have appropriate approvals.
- GRHANITE™ has a data preview mode that allows a clinic to view the data GRHANITE™ is intending to transmit. This allows a final review by the data custodian before any data is released from the practice or clinic.
- GRHANITE™ has a privacy-protecting record linkage capability. This mechanism utilises hashes (signatures) that are generated from person-identifiable information. These signatures are generated within the practice or clinic. The signature process is irreversible (i.e. there is no way to retrieve person identifiable information from the signatures).
- Exceptional circumstances: GRHANITE™ supports an opt-in consent model where direct patient involvement and hence person identification is required. Projects of this nature or direct clinical care projects may involve the extraction of person identifiers. This is always done by prior agreement in strict compliance with applicable legislation and policy frameworks. For avoidance of doubt, no identifying information is ever extracted for out-of-consenting research projects or for population health planning applications.
GRHANITE Messaging and Security Provisions

GRHANITE employs a number of internationally-recognised encryption mechanisms to protect data in transit. GRHANITE applications employ RSA and AES key cycling mechanisms. These mechanisms have been designed to provide many layers of security.

- All GRHANITE messaging is via IP Port 80 and is always encrypted.
- GRHANITE communications are never initiated from the Web Server – the communications always initiate from within the practice to avoid opening a practice to in-bound attacks.
- The same mechanism applies to GRHANITE client databanks where the data ultimately resides. These communicate with the Web Server but not the other way around.
- GRHANITE has a remote XML definition update mechanism that allows a data extract to be modified remotely should the database schema change.

GRHANITE uses similar encryption protocols to the NEHTA Secure Message Delivery system (SMD) as utilised by services such as Argus and Healthlink. GRHANITE does not use SMD as SMD is designed for secure small clinical message communication for direct clinical care between care providers. As such, GRHANITE cannot fit within this framework as extractions can be bulk-oriented and destined for secure servers rather than health provider organisations.

GRHANITE Site Installation

To determine the identity of individual GRHANITE sites utilising GRHANITE software, a unique password and license is required during software installation that results in an RSA key pair exchange with the GRHANITE Web Server. During this process further key pairs are exchanged so that key pairs used during the installation process are not utilised in subsequent communications.

- Subsequent communications within a messaging session use cycling 256-bit AES encryption keys with RSA keys used to initiate and authenticate the session.
- EVERY RSA-encrypted message transmitted by GRHANITE is 256-bit AES encrypted first.
- Should an RSA message be cracked, the AES encryption must also be cracked.
- Each GRHANITE site utilises its own site-specific encryption keys that are themselves encrypted.
- GRHANITE software will not operate if copied or moved from one computer to another. All installations require a unique authorising license.
- The GRHANITE software is activated during installation tying it to the physical hardware present. By design this device can, if deemed necessary, be isolated from the local network.
Transmission of Clinical Data

To protect data during transmission, the following security mechanisms have been built into GRHANITE:

Each GRHANITE Databank where GRHANITE de-identified data will reside generates 10,000 RSA key pairs. When a GRHANITE Client requests data, one of these 10,000 keys is randomly assigned to the data transmission session.

- The data is additionally encrypted using 256-bit AES encryption.
- The only location in the world with the RSA private key is the client databank server. (Meaning this is the only place in the world where data can be decrypted).
- Only authorised users can login to the GRHANITE software on a GRHANITE databank server to perform a data extract.

Obfuscation

- All GRHANITE code libraries are obfuscated and utilise string encryption.

GRHANITE Encryption libraries

GRHANITE utilises RSA encryption RFC 2315 PKCS #7 Cryptographic Message Syntax v1.5 with a 1024 bit key length.

All message contents are additionally encrypted prior to RSA encryption using the Microsoft Cryptography library implementation AES Encryption (rijndaeleenhanced) with a 256-bit key.

i.e. even if the RSA encryption is cracked, the 256-bit AES encryption must also be cracked. Randomly-generated 100-character initialisation passphases are used in all 256-bit AES encryptions.

- GRHANITE is regularly released and reflects the latest incarnation of the Microsoft libraries.

Summary

The University and HaBIC R² work hard to provide systems and services that provide data for audit, health surveillance and research whilst giving the best possible reassurances to stakeholders in relation to data security and privacy. We are always working to improve our systems and services and value feedback and requests for further information.

Kind regards,

Dr Douglas Boyle Ph.D., FACHI | Director
Tel: +61 (3) 5823 4521 I Mob: +61 458 220 820 I Email: dboyle@unimelb.edu.au