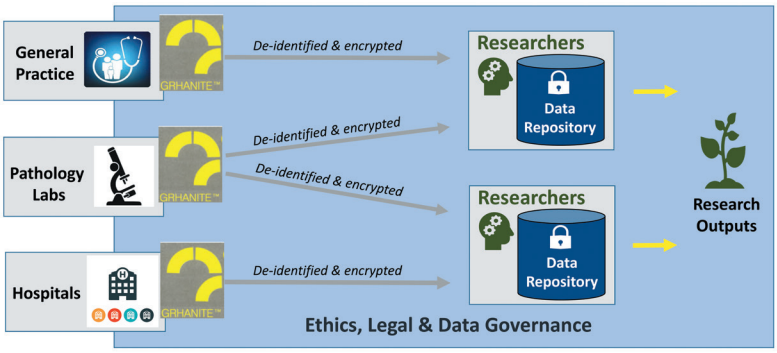
THE UNIVERSITY OF MELBOURNE

Faculty of Medicine, Dentistry and Health Sciences

Introduction to GRHANITE®

GRHANITE® A tool enabling de-identified data transfer and linkage



Our motivation

The University of Melbourne supports the ethical advancement of health-related research to improve population health, by enabling controlled, 'secondary' use of data that has previously been collected for other purposes.

Enabling research

Since inception, GRHANITE® has been used for research projects across a range of subjects, including cancer management, mental health, chronic disease management, Indigenous wellbeing and intimate partner violence. GRHANITE's privacy-protected record linkage enables investigation of the onset and progression of disease, care pathways, and patient outcomes.

How it works

With data custodian permission, and subject to ethics committee approval and legal agreement, GRHANITE® extracts and curates the delivery of sensitive data to secure research data storage facilities.

With security and privacy at its heart, data is de-identified and encrypted at source, with decryption keys held only by the authorised recipient organisation. Person identifiers are removed from the data in all but ethically-approved and exceptional circumstances.

Where data comes from

GRHANITE® can extract from most data repositories, for example, in hospitals, pathology laboratories, general practices, community health centres, Council administrative systems, birth registries and other administrative sources.

Non-exclusive data collection

GRHANITE® is independent of other health-related software. It is not an audit tool and it does not interfere or impact in-house clinical software, GP audit or workflow tools.

Principles

GRHANITE® is based on principles of contributing to public good and ensuring privacy protection.

History

Since its development in 2007 GRHANITE® has been installed in well over 1,000 general practices and other organisations. It has enabled research to improve public health, health services and patient journeys of care.

HaBIC R²

The team at HaBIC R², the Department of General Practice, The University of Melbourne, oversee the installation of GRHANITE® across Australia and work with researchers and various organisations to deliver data.

A/Prof Douglas Boyle,
Director, Health and Biomedical Informatics Centre, Research Information Technology Unit (HaBIC R²)

Department of General Practice
The University of Melbourne
Victoria, Australia, 3010

www.grhanite.com

Frequently Asked Questions

Why is GRHANITE® needed?

Many data collection tools are designed for audit, not research. For audit, data is often summarised or transformed before use. Researchers normally require data to be in as close to its original state as possible, including all historic changes to the data. GRHANITE® is designed specifically for this purpose with an ability to collect data from health and social services while enabling management of consent and privacy-preserving data linkage.

What data fields are collected by GRHANITE®?

GRHANITE® is configured on a program by program basis to collect particular data fields. The fields collected depend on a program's ethics committee approval. GRHANITE® is configured with the aim to not collect names, addresses, full dates of birth, Medicare numbers or other identifying fields – except in exceptional circumstances with prior agreement and ethics approval. Data minimisation means that only fields necessary to meet program objectives are collected.

How does GRHANITE® de-identify data?

Person identifiable data fields are systematically excluded from data extracts. Data de-identification also depends, to some extent, on computer system operators using the correct fields for data capture in their own computer systems (e.g. clinical software systems). Additional privacy filters are employed by GRHANITE® in fields where user error is known to occur.

Can personally identifying information be collected?

GRHANITE® supports opt-in consent research studies where direct consumer involvement and identification are required. Identifying information is only collected with strict compliance to ethical approvals and the law.

Is record linkage possible with GRHANITE®?

GRHANITE® enables privacy-protected record linkage, for example, linking GP, pathology, hospital and registry data, so more can be learned about onset and progression of disease, care pathways and patient outcomes. This creates a powerful tool for generating new knowledge to improve the health of Australians.

How are records linked using GRHANITE®?

GRHANITE® generates 'hashes' or 'signatures' from person-identifiable information before the data leaves the computer. These 'signatures' are irreversible, meaning that unlike statistical linkage keys, there is no way to retrieve person identifiable information from the signature. When information is extracted using GRHANITE® from multiple organisations, the signatures provide a mechanism to link records.

How safe or secure is the data during transmission?

GRHANITE® uses a number of internationally recognised encryption mechanisms to protect data in transit, providing many layers of security. Each instance of GRHANITE® has a unique password and license, and site-specific encryption keys that are themselves encrypted. GRHANITE® exhibits 'end-to-end' encryption with endpoint authentication.

Does the University of Melbourne access the data?

Some data repositories are hosted at the University of Melbourne; in these cases, the University can only access held data in accordance with the relevant project's ethics approvals and agreements. Data from different projects are not pooled.

Does GRHANITE® slow down computer processing?

No it does not. GRHANITE® software is normally installed on a networked computer not on a server. Data extractions / transmissions normally occur overnight and do not impact on the speed of the computer or the internet.

Core features

- ✓ Not for profit.
- ✓ Helps foster knowledge discovery.
- ✓ Supports opt-in, opt-out and waiver of patient consent models.
- ✓ Enables privacy-protected record linkage.
- ✓ De-identified data can be re-identified within the setting where it was generated.
- ✓ Public identification of organisations sponsoring use of the GRHANITE tool increases the social acceptability and trust related to data sharing.
- ✓ Multiple layers of encryption help to keep data safe during transmission.
- ✓ A data preview mode enables holders of the software to view the data.

Can GRHANITE® be installed in businesses that also share data with other institutions?

YES! For example, many general practices share data with multiple organisations using a variety of tools such as GRHANITE®, Pen CS and POLAR. Using one tool would normally NOT prevent other tools from also being used.

Who uses GRHANITE®?

GRHANITE® is used by a variety of organisations around Australia. The software is installed at general practices and other institutions throughout the country.

How can I find out more information?

Contact: HaBIC R^2 | Email: support@grhanite.com.au | Phone: +61 3 9035 4111
HaBIC R^2 = Health and Biomedical Informatics Centre, Research Information Technology Unit
Department of General Practice, The University of Melbourne, Victoria, Australia 3010