Australian Genomics Data Breach Policy

Scope:

This data breach policy defines what is considered a data breach and sets out procedures to follow in the event that the Australian Genomics Health Alliance (Australian Genomics) experiences (or is suspecting) such a data breach is occurring, or has occurred. It presents a framework nominating roles and responsibilities for the management of a data breach, depending on which Australian Genomics data tool(s) is being, or has been affected. The aim of this policy and the response process it describes is to mitigate potential harm to affected individuals, by facilitating an efficient and comprehensive response to a suspected or confirmed data breach.

This policy covers all data created, managed and shared by Australian Genomics; whether it be on paper or electronic format; identifiable, de-identified or aggregated data; irrespective of the purpose and use of collected data.

Background and definitions:

What is a data breach?

The Office of the Australian Information Commissioner (OAIC)[i] defines a data breach occurring when "personal information that an entity holds is subject to unauthorised access or disclosure, or is lost."

The following are examples of data breaches:

- Loss or theft of a physical device (such as a laptop or mobile storage device) or paper records containing personal, identifiable or re-identifiable information;
- Disposal of digital hardware data storage without prior permanent deletion of all content on the device;
- Inadvertent disclosure of personal or identifiable information due to human error, such as an email with identified or re-identifiable data sent to the wrong recipient;
- Unauthorised access to personal, identifiable or re-identifiable data by an employee;
- A database being illegally accessed by contractor or an individual outside of Australian Genomics;
- An Australian Genomics employee or investigator affiliated with a partner of Australian Genomics accessing data beyond their approved scope of work.

What is considered personal information?

Personal information is defined in the Privacy Act as[ii]: "Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not."

The definition of personal Information is not limited to an individual's family and private life, but also extends to opinions about the individual from which they can reasonably be identified. This definition is also technology neutral and encompasses changes in information-handling practices over time.

The following list gives examples of recognised personal information under the Privacy Act:

- Sensitive information (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information);
- Health information;
- Employee record information;
- Credit information;
- Tax file number information;

What is considered serious harm?

In the case of a data breach, serious harm can impact upon the individual whose personal information is involved in the data breach. Serious harm to the individual might manifest itself in various forms: it may affect the physical or mental and emotional well-being of an affected individual; it could also, for example, result in financial loss, damage to their reputation or identity theft.

Serious harm could also impact upon the institution(s) holding and/or handling the data involved in the data breach by way of reputational damage. This can however be mitigated by the institution(s) demonstrating accountability, effectiveness and transparency in their data breach response and in the handling of the personal information in their care.

How do breaches occur?

Data breaches can have many origins, not all of which are malicious.

A data breach can:

- occur when information is mishandled by poorly-trained staff;
- be due to an organisation not having appropriate data handling and management policies and procedures in place;
- be caused by human error, for example by emailing information to an incorrect recipient;
- be of malicious intent, presenting as an information technology or service attack, or an attempt to access data protected by a firewall.

These are only some examples of how a data breach can originate: this list is by no means complete or exhaustive. There are many other ways data can be lost, accessed and/or disclosed without authorisation.

Data breach response process:

Should you suspect or are made aware of a data breach occurring, or that has occurred, please immediately notify: security@australiangenomics.org.au irrespective of the severity of the breach. This email box is monitored and will alert the core Data Breach Response Team (see below for the configuration of the team).

In this email, include all information you have regarding the data breach, including but not limited to:

- the type of data is affected;
- the individual or cohort of individuals affected;
- the time the breach first occurred;
- the type of breach (see above);
- your contact details.

The data breach response team will then contact you for further details, and/or to advise you of progress or resolution of the breach.

Each data breach will be considered on a case-by-case basis. Not all steps described in the framework below will be required, depending on the severity of the data breach. Evaluation and management of the breach is the responsibility of the Data Breach Response Team, who will determine the actions required.

Upon notification, the response team (as listed in Figure 2 and Appendix 1) will follow the four key points strategy as described here, summarised in Figure 1 and listed in the checklist in Appendix 2:

1) ***Contain*** *the breach (immediately)*
    a. This can be by limiting, or entirely removing, access to the affected data system; or
    b. By physically switching off the hardware supporting the affected system;
    c. Making sure to preserve evidence that may be valuable in assessing the breach and risks associated with it.

To help the core team identify the most suitable strategy to contain the breach, the core team must address the following questions:

- How did the data breach occur?
- Is the data affected by the breach still being shared or disclosed without authorisation? Or is it still lost?
- Who currently has access to the affected data?
- What can be done to secure the information, restrict access to it and stop unauthorised access and potential harm to the affected individual(s)?

2) ***Assess*** *the risks associated with the breach (within the first 48 hours)*
    a. Conduct an internal investigation to collect information about the breach, including:
        i. Date, time, duration and location of the breach;
        ii. Type of personal information involved in the breach;
        iii. Who discovered the breach and how;
        iv. A list of all affected individuals and the risk of resulting serious harm to them.
    b. Establish the cause, circumstances and extent of the breach.
    c. Establish which parties have gained unauthorised access to the personal information.
    d. Assess risks and priorities based on the collected facts and information.
    e. Keep a record of all steps actioned, as well as the reasoning behind those steps, since the discovery of the breach.

3) ***Notify*** *(within 7 days of the breach being discovered)*

In order to decide who is to be notified and how, the core response team should consider the following:

- The risk of harm to the individual(s) whose data is being breached;
- The risk to the wider community;
- If notification to the affected individual(s) would create more unnecessary harm than benefits, such as stress and anxiety;
- The number of individuals affected;
- If the data breach indicates a systematic problem with respect to data handling;
- The risk to the reputation of MCRI and / or Australian Genomics.

The core team must consider notifying the following parties:

a. The affected individual: the relevant breach response team members are to determine whether notification is required and identify the notification list, depending on the severity of the breach; the type of personal data affected; the risk of serious harm to the individual and the wider community; and the practicality of contacting the individual(s). If notification is required, it will fall into one of the following three categories in order to be able to take steps to reduce their own risk of harm:
   i. Only those individuals at risk of serious harm, by phone or email;
   ii. All individuals involved in Australian Genomics, including participants, staff and partner entities, by either phones or email depending on practicality;
   iii. Do a public notification (if i. or ii. are not practicable) via an email newsletter and/or announcement on the Australian Genomics website. An example is presented in Appendix 3.

b. If necessary, escalate and notify the Murdoch Children's Research Institute (MCRI) Data Breach Response Team (**DBRT**) team[iii]; Australian Genomics partners' breach response team in case of jointly held information being affected; MCRI legal health department; and MCRI HR department where the breach is due to malicious or involuntary but negligent behaviour from an employee of Australian Genomics or MCRI.

c. As the data breach affects a Global Alliance for Genomics Health (GA4GH) driver project, notify SECURITY-NOTIFICATION@GA4GH.ORG. Include in this email a brief summary of the data breach, ensuring no details of the breach are shared via this channel creating a further chance of breach. Also include a list of the actions already taken and the plan for further actions.

d. The relevant authorities, if required. This includes law enforcement agencies and the Office of the Australian Information Commissioner (OAIC) in the case of a notifiable breach. For a breach to qualify for the Notifiable Data Breach scheme, it has to involve jointly held information and/or serious harm to individuals is likely to occur. The phrase "likely to occur" means the risk of serious harm to an individual is more probable than not (rather than possible)[i].

e. For more details, please read Notifiable Data Breaches Scheme[iv]. The report must be communicated to the OAIC either by email to enquiries@oaic.gov.au, by phone: 1300 363 992 or via the web form[v]. The notification and reporting to the OAIC has to be performed within 30 days of breach discovery.

4) ***Review*** *the incident, the response and take action to prevent future breaches (within 30 days of breach discovery)*
    a. Implement strategies to address any weaknesses identified during the assessment process;
    b. Update security and the data breach response if necessary;
    c. Change policy and procedures if required.

Within 30 days of the data breach being discovered, a meeting with all major stakeholders and Australian Genomics partners must be held to review and improve data management processes and policies.

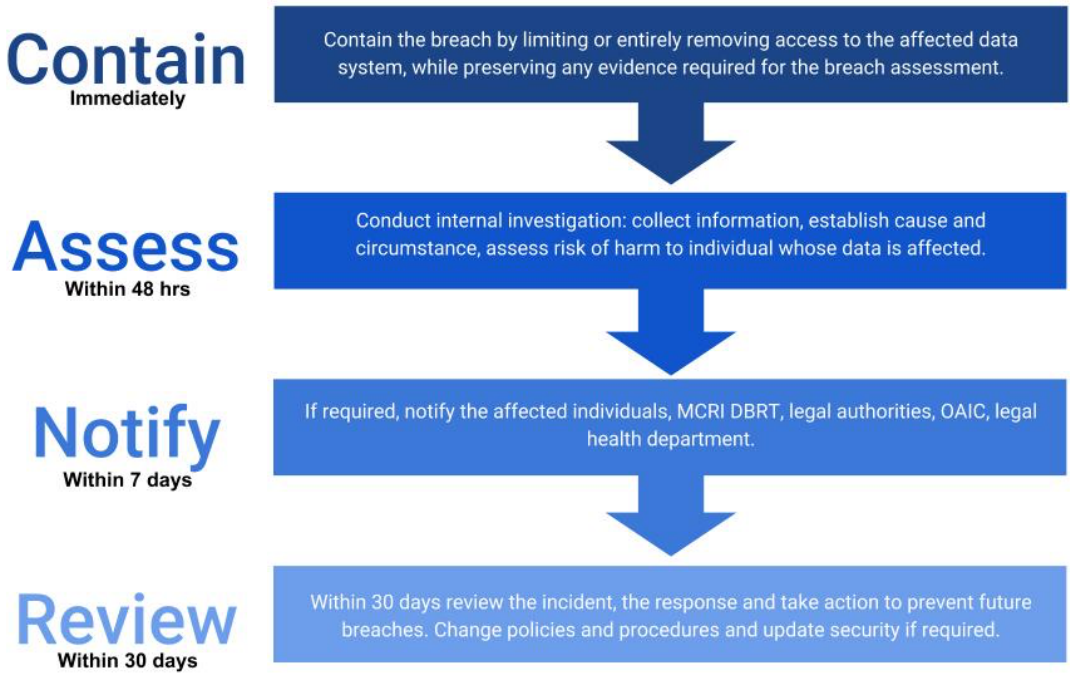
In case of a severe data breach, steps one to three might need to be performed simultaneously or in rapid succession, in order to efficiently mitigate the potential harm to the individual(s) whose data is affected.

Irrespective of the severity of the data breach, a copy of the notification email, as well as a record of all steps undertaken and their justification are to be kept for the same time period as all other data collected within the frame of Australian Genomics and will be stored on the internal server.

Keeping records of a data breach will enable a full assessment of weaknesses in the data access and storage systems as well as providing accountability and transparency for participating individuals and stakeholders.

To ensure this data breach policy remains adequate and fit-for-purpose, it will be reviewed on an annual basis or at the launch of any new major data tool.

Figure 1: Data Breach Response Process

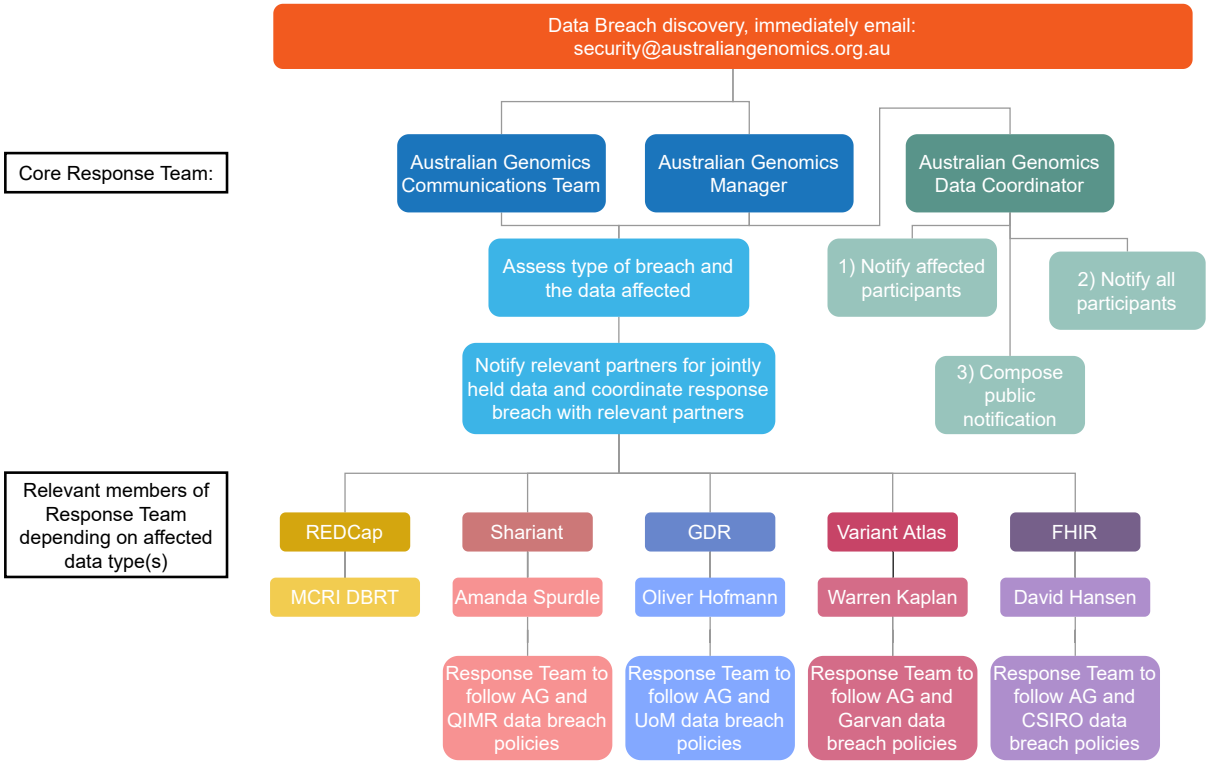


Data Breach Response Team:

The core response team will comprise the Australian Genomics Manager, the Data Program Manager, Data Governance Officer and the Media and Communications Manager. Depending on the Australian Genomics data tool(s) affected by the data breach, a different configuration of specialist members and partners will be informed by the core response team at the time of the incident. See Figure 2 for a diagram of the expected data breach response team configuration(s). According to the severity of the data breach, services external to Australian Genomics, but within the MCRI entity, might be contacted for advice, such as legal, information technologies and/or human resources departments.

In the appendix a primary and secondary contact for each position on the data breach team is listed and must be kept up to date at all times.

Figure 2: Data Breach Response Team



Appendix 1: List of primary and secondary contact for each Australian Genomics Data tool

Data tool	*Primary contact*	*Secondary contact*
Management	Tiffany Boughtwood tiffany.boughtwood@mcri.edu.au	Marie-Jo Brion Marie-Jo.Brion@qimrberghofer.edu.au
Coordination	Marie-Jo Brion Marie-Jo.Brion@qimrberghofer.edu.au	Tessa Mattiske tessa.mattiske@mcri.edu.au
Shariant	Amanda Spurdle Amanda.Spurdle@qimrberghofer.edu.au	Emma Tudini Emma.Tudini@qimrberghofer.edu.au
Genomic Data Repository	Oliver Hofmann oliver.hofmann@unimelb.edu.au	Lavinia Gordon gordonl@unimelb.edu.au
Variant Atlas	Warren Kaplan w.kaplan@garvan.org.au	Dmitry Degrave d.degrave@garvan.org.au
FHIR Server	David Hansen david.hansen@csiro.au	Alejandro Metke Alejandro.Metke@csiro.au
Communications Team	Dorothy Illing dorothy.illing@mcri.edu.au	Merryn Pearce merryn.pearce@mcri.edu.au
Spokesperson	Dorothy Illing Tiffany Boughtwood	John Christodoulou Kathryn North

Appendix 2: Data breach response plan quick checklist

Step 1: Contain the breach

- ❑ Notify security@australiangenomics.org.au
- ❑ Limit or entirely remove access to the affected data tool
- ❑ Preserve evidence for breach assessment
- ❑ Determine best strategy to contain the breach by answering following:

Issue	Comment
How did the data breach occur?	
Is the data affected by the breach still being shared or disclosed without authorisation? Or is it still lost?	
Who currently has access to the affected data?	
What can be done to secure the information, restrict access to it and stop unauthorised access and potential harm to the affected individual(s)?	

Step 2: Assess the risk associated with the breach

- ❑ Conduct an internal investigation to collect the following information
    - ❑ Date, time, duration and location of the breach
    - ❑ Type of personal information accessed during the breach
    - ❑ Who discovered the breach and how
    - ❑ A list of all affected individuals and the risk of resulting serious harm to them
- ❑ Establish the cause, circumstance and extent of the breach
- ❑ Establish what parties have gained unauthorised access to the personal information
- ❑ Assess risks and priorities from what is known
- ❑ Keep a record of all steps actioned since the discovery of the breach

Step 3: Notify

- ❑ The core team, including the communications team, should decide who needs to be made aware of the breach (internally, individuals affected, Australian genomics partners, GA4GH, external authorities) by answering the following:

Issue	Comment
What is the risk of harm to the individuals whose data is being breached?	
What is the risk to the wider community?	
Would a notification create more unnecessary harm (like stress or anxiety) than benefit?	
What is the number of affected individuals?	
Does the data breach indicate a systematic problem?	
What is the risk to the reputation of Australian Genomics and MCRI?	

- ❑ How are individuals to be notified?
    - Via phone or email if practicable
    - Via a newsletter or general email to all Australian Genomics participants and/or partners and staff.
    - Via a public notification by means of an email or announcement on the website.
- ❑ Example of email or announcement of a data breach in Appendix 3
- ❑ Notification to outside relevant authorities (Federal Police, OAIC, or other relevant authorities depending on the type and severity of the data breach.)

Step 4: Review the incident

Within 30 days of discovery of the breach, the core team is to organise a meeting with the relevant Australia Genomics partners and stakeholders to review the incident, address any weaknesses identified during the assessment and update all necessary policies and documents.

Issue	Comment
Date of review meeting	
Weaknesses to be addressed	
Policies and documents to be updated	

Appendix 3: Template for communication to individuals whose data is affected

Dear *(insert name)*

- We are writing to let you know that an incident occurred with our computer systems *(when)* that *(may affect you/reassure that it won't affect them and what this means for them)*
- *(describe incident in plain language and its impact on the person you are addressing)*
- *(Describe how we are responding to the incident)*
- We apologise sincerely for any (*concerns/inconvenience)* this may have caused you.
- *(Reassure them that everything is being done to ensure it does not recur etc.)*
- *(Provide options for them to pursue from here/what they might want to do)*
- *(Provide contact person and details for further queries)*

While writing the data breach notification letter, please ensure that you:

- ❑ Take responsibility and apologise sincerely
- ❑ Be clear and express yourself in simple yet factual manner for everyone to understand
- ❑ Explain the possible options for the participants, without instilling fear in them
- ❑ Reassure the participants by explaining what has been done thus far and what actions will be undertaken to prevent a similar incident to occur in the future

Policy Revision History

Policy Version	Date effective	Summary of Revision
V 1.0	February 2019	Original Document
V 1.1	August 2020	Contact details updated Addition of Shariant to flow chart
V 1.2	November 2020	Formatting Updating AGHA acronym to AG Removing contact details for public version of policy

References and Bibliography:

[i] Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth): https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

[ii] Section 6 of the Privacy Act: https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information#how-does-the-privacy-act-define-personal-information

[iii] Murdoch Children's Research Institute (MCRI) Data Breach Response Team (DBRT): https://intranet.mcri.edu.au/sites/policies/Pages/Data-Breach-Response-Plan.aspx

[iv] Notifiable Data Breaches Scheme from the Office of the Australian Information Commissioner (OAIC): https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#overview

[v] Notifiable Data Breaches Scheme reporting online form: https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB