# ICGC ARGO Data Breach Policy

## 1. Introduction

This policy describes the principles for responding to a breach of ICGC data including managing a data breach and notification of persons whose privacy may be affected by the breach. For good privacy practice purposes, this policy also covers any instances of unauthorised use, modification or interference with personal or sensitive information held by ICGC or its users. Effective breach management assists ICGC in avoiding or reducing possible harm to both the affected individuals and the data sharing community broadly and may assist in preventing future breaches. The policy also describes the principles relating to documentation, appropriate reporting internally and externally, and communication to meet legislative requirements. It establishes responsibility and accountability for all steps in the process of addressing information security incidents that result in data breaches and describ1/4/2021es clear roles and responsibilities with the aim of ensuring a comprehensive information governance program.

This policy is composed of two main components:

- Reporting of data breaches to ICGC, including ICGC's response plan, and
- Notification and communication of data breaches.

ICGC ARGO has established robust breach detection, investigation and reporting procedures, and key aspects of this policy are:

- We have team protocols in place to recognise a potential personal data breach and escalate a security incident to the appropriate individuals to initiate a follow up investigation.
- The Data Access Agreement agreed to by all users of ICGC controlled-tier data obligates the users to recognise and report data breaches
- We have prepared a response plan for addressing any personal data breaches that occur that meet ICGC's obligations under the EU General Data Protection Regulation (GDPR: https://gdpr-info.eu/) and maximises protection of the personal or sensitive information of ICGC donors and research participants.
- The roles and responsibilities of teams and persons responsible for breach response are well described.

- We have a process in place to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- We document all breaches, even if they don't all need to be reported.

This Data Breach Policy is consistent with the ICGC Data Management Policy and ICGC Security Best Practices for Controlled-Access Data.

This document does not intend to replace existing data breach responses within individual institutions and will not attempt to outline or advise the responses that are required by all international regulatory bodies.

## 2. Data Breach Definition

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data (Recital 85, GDPR). In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. A personal data breach isn't only about loss or theft of personal data and can be broadly defined in two categories: cyber security incidents (brute force, hardware/software misconfiguration, malware infection, failed or successful attempts to gain unauthorised access to ICGC information or information systems) and non-cyber security incidents (incorrect disposal or loss or theft of hardware e.g. (laptop, USB stick) or paperwork containing sensitive or personal information, data posted, faxed or emailed to incorrect recipient or personal data posted onto a website without consent).

## 3. Preparation and Proactive Management of Data Breaches

ICGC through its data management policies and frameworks ensures secure processing by means of appropriate technical and organisational measures. These measures include but are not limited to:

- Appropriate governance frameworks established for authorised access to controlled data
- Policies and Guidelines for data management, ethics and informed consent and data security. These policies are reviewed annually.

- Security policies, processes and procedures that meet international best practices in place within the Data Coordination Centre (DCC), Regional Data Processing Centres (RDPC's) and Data Mirroring Centres (DMC).
- We have in place a process to assess the likely risk to individuals as a result of a breach through an annual Data Protection Impact Assessment (DPIA).

These measures ensure the confidentiality, integrity and availability of ICGC systems and services and the personal data we process within them.

Users of ICGC data are required to have established security policies and technical, organizational and procedural processes in place prior to accessing ICGC data as described in the Data Access Agreement.

## 4. Reporting Breaches to ICGC ARGO

All individuals with access to ICGC controlled-tier data are required to report all security incidents related to ICGC data whether they result in a data breach or not. Incidents should be reported as follows:

1. Possible breaches reported to the Data Coordination Centre (DCC) Helpdesk through the contact form found at https://platform.icgc-argo.org/contact upon discovery. Incidents should be reported as soon as they are detected even if not all the information about the event is yet available.
2. Incidents should be reported using the ICGC ARGO Data Breach Report Form even if all details are not yet available.
3. Institutions or organisations reporting data breaches should identify an accountable point of contact (such as the program or project Principal Investigator) who will coordinate with the DCC and appropriate organisations and affected individuals throughout the incident response process. The contact should have the authority to direct actions required in all phases of the incident response.
4. Upon receipt of the report the DCC Helpdesk alerts the Data Access Officer and the DCC Principal investigator- who acts as the Forensics Lead.
5. The Data Access Officer logs the initial contact in the breach logbook maintained at the Data Access Compliance Office.

## 5. ICGC ARGO Response and Investigation Plan

1. Forensics Lead assigns a DCC staff member to liaise with the accountable point of contact to collect information about the breach for the incident report.
2. Preliminary incident report is reviewed by the Forensics Lead and filed with the Data Access Officer and Secretariat within 48 hours (counting only business days) of the initial report.
3. In the case of a personal data breach, the Data Access Officer will assess the likelihood of a risk to rights and freedoms. The assessment will be based on the incident's potential to result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned (GDPR Recital 85).
4. If a risk is determined, the Data Access Officer shall without undue delay and, not later than 72 hours after having become aware of it, notify the personal data breach to:
    i. The data controller (University of Glasgow Data Protection Office- through secretariat@icgc-argo.org) (even if all the details are not yet available).
    ii. The supervisory authority: The University of Glasgow Data Protection Office (DPO). The DPO may then advise on further action, including if warranted, a report to the supervisory authority for the UK, the Information Commissioner's Office (ICO). Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay (GDPR Article 33).
    iii. The notification can be through the Data Breach Report Form, or if not available shall at least:
        a. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned.

b. communicate the name and contact details of the contact point where more information can be obtained.
c. describe the likely consequences of the personal data breach.
d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

iv. The report is required to be submitted to the supervisory authority for review of compliance with Article 33.

5. Project lead for each ICGC project that may have been compromised.
    a. If a risk to rights and freedoms of participants is determined by Step 3 as *Likely* or *highly likely* project leads are responsible for notifying participants whose personal data may have been disclosed. The DCC team can provide applicable information to assist the notification at this step.
    b. Project leads should proceed to notify in accordance with applicable breach notification laws in their jurisdiction and organisational security policies.
    c. Project leads are responsible for notifying external organisations or centers such as funding agencies if contractually obligated to do so.
    d. Project leads must indicate what actions they have taken within 72 hours of receiving an incident report.
6. Final incident report with a description of measures taken for containment, investigation, mitigation and reporting must be completed by the forensics lead and submitted to the privacy officer when investigation is complete, but no later than 1 month following the initial report.

## 6. Communication of Data breach to Participants

1. Communication of the breach to the participants is required without delay where a *likely* or *highly likely* risk of harm or where consequences have been identified as per Step 5.3 of this policy (GDPR Article 34).
2. If the data breach has not already been communicated to participants, the supervisory authority upon review may require this to be done. The supervisory authority may:

a. Conclude that likelihood of the personal data breach resulting in a high risk and require participants to be notified without delay.
b. Decide that significant measures have taken place to mitigate risk and consequence, and high risk to rights and freedom of patients (*as described above*) are no longer likely.
c. Determine in consultation with relevant personnel that communicating the breach would involve disproportionate effort and a public notice or similar needs to occur to notify the breach.

3. It is the responsibility of the organisational contact or project led to communicate the incident details to participants.
4. The communication to the participant shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in the Data Breach Report.

**7. External Notification and Communication**

1. Outside of the mandatory notification and communication aspects described in Points 5 and 6, other external parties may need to be notified depending on the individual nature and circumstances of the incident. Any required external notifications (such as internet service providers, vendors or data centers) should be documented on the Data Breach Report Form accordingly.
2. Organizational contacts or project leads should coordinate response activities with external parties as appropriate (such as funding bodies, law enforcement, Internet Service Providers, Information Sharing and Analysis Organizations, participant groups etc).
3. Annually a Data Access Compliance Office Report is issued containing a summary of data access statistics, data usage and security incidents or breaches. An appropriate public version of this is published on our website to facilitate transparency and public engagement.