DATA BREACH POLICY

Lead Manager	**Data Protection Officer**
Responsible Director	**Director of eHealth**
Approved by	**Area Partnership Forum**
Date approved	**May 2018**
Date for Review	**May 2021**
Version	**2.5**
Replaces previous version	**2.4**

Consultation and Distribution Record

Contributing Authors	Data Protection Officer IT Compliance Manager Data Protection Adviser
Consultation Process / Stakeholders	Information Governance Steering Group Area Partnership Forum
Distribution	All Staff

Change Record

Date	Author	Change	Version No
Jun 16	I Brown	Definition of data breach and examples of data breaches added at appendix B as agreed at IGSG	2.2
Aug 16	I Brown	Data Flow Chart update to add 'yes' to one of the boxes and change IT Security Manager to Compliance Manager	2.3
Dec 16	APF	Minor Changes	2.4
Feb 18	J Henderson	Reviewed in line with requirements under GDPR	2.5

Contents

1.0 Introduction

The policy describes how NHS Greater Glasgow and Clyde (NHSGGC) aims to address Information Governance (IG) related data breaches, also known as IG incidents. NHSGGC is committed to reducing such occurrences.

Information Governance type breaches include actual, suspected or near- misses. A Flow Diagram showing the incident reporting process can be found at Appendix A. The definition of a data breach and some examples of these can be found at Appendix B.

2.0 Scope

This policy applies to all staff employed by NHSGGC. It also applies to contractors, partnership organisations and visitors not employed by NHSGGC but engaged to work with, or who have access to, information systems, applications and paper records.

3.0 Roles and Responsibilities

3.1 Role of Chief Executive

The Chief Executive has overall responsibility for ensuring all IG related data breaches are reported and investigated and, where applicable, are reported to the Information Commissioner's Office. This responsibility has been delegated to the Data Protection Officer.

3.2 Role of Director of eHealth

The Director of eHealth has delegated responsibility for ensuring organisational compliance with the General Data Protection Regulation (GDPR). The Director of eHealth is supported by the Boards Medical Director, Data Protection Officer, Caldicott Guardian and Senior Information Risk Officer (SIRO).

3.3 Data Protection Officer

The Data Protection Officer (DPO) is a senior member of staff responsible for ensuring that NHSGGC Board and its staff are informed and given advice about how it can meet its obligations under the GDPR and other data protection laws. The DPO is responsible for monitoring compliance of the Regulation in how it relates to the personal information NHSGGC processes, including managing internal data protection activities, providing advice on data protection impact assessments; train staff and conduct internal audits. The DPO is the first point of contact for the Information Commissioners Office and for individuals whose personal information is processed (employees, patients etc).

The appointment of a DPO is a mandatory requirement for NHSGGC under the General Data Protection Regulation, Regulation (EU) 2016/679 (GDPR).

3.4 Role of Information Governance Steering Group

The Information Governance Steering Group will receive regular reports on all IG related data breaches. The Steering Group will consider the breaches and subsequent actions taken to determine if any further actions/recommendations are required or if any changes in practice are necessary to reduce the risk of a similar breach occurring. The IG Steering Group is chaired by the SIRO and meets four times per annum.

3.5 Role of Directors and Heads of Departments

Directors and Heads of Departments are responsible for ensuring good security practices are implemented and maintained within their area of responsibility by:

- Ensuring that staff know what is expected of them and that they act in a sensible way to protect information (whether manual or electronic);
- Ensuring that policies, standards and procedures are followed at all times;
- Reporting all breaches, whether actual or suspected, using the On-Line Incident Management System (Datix) and, if appropriate, to the IT Service Desk;
- Where this involves the actual or suspected loss of personal data this must be reported to the Data Protection Officer as soon as it is identified;
- Setting a good example to staff by applying good security principles to their own work;
- Ensuring departments and staff share information only on 'need to know' principles.

3.6 Role of Staff

It is the responsibility of all staff to ensure they have read and understood this Policy and to ensure it is adhered to. Staff should safeguard and maintain the confidentiality of information they access, create, receive, control or destroy at all times.

4.0 Incident Reporting Process

4.1 The loss or theft of personal identifiable data, whether held on paper or electronic form must immediately be reported to the member of staff's Line Manager/Director and notified to the Information Governance Department (0141 355 2059) in the first instance.

4.2 The breach must be reported through the On-Line Incident Management System (Datix) by the person reporting the incident.

4.3 The loss/theft of IT equipment, including mobile devices, should be reported:

- to the IT Service Desk (using the icon on the computer desktop or by telephoning 0345 612 5000 or #650 if in Glasgow area);
  AND
- to the Information Governance Department (0141 355 2059);
  AND
- on Datix;
  AND
- to the Police.

4.4 The Line / Department Manager is required to conduct an investigation to establish the circumstances surrounding the loss/theft.

4.5 As part of the investigation, it may be necessary to suspend an employee's access to the network and any electronic information system. Authorisation will be sought from the appropriate People and Change Manager before this is carried out.

4.6 Where there is evidence that a criminal act has been committed e.g. audit of internet logs reveals viewing/downloading of Child Pornography, these **must** be reported to the Police, the Data Protection Officer and the IT Compliance Manager immediately.

5 Investigating a Breach

5.1 The relevant Line/Department Manager will be responsible for arranging an investigation into the incident and for a Report to be produced. They will consult with their directorate management as appropriate. The Report will include actions already taken and any recommendations. A report template for investigation is attached at Appendix C.

5.2 The relevant Director will liaise with the Information Governance Department at this stage of the process which will provide guidance as required.

5.3 A copy of the final report, including all actions taken and recommendations will be sent to the Data Protection Officer.

5.4 Where an individual has been suspended and/or the investigation leads to disciplinary action under the Board's disciplinary, policy, the outcome should be recorded using the form at Appendix D and a copy sent to the Data Protection Officer.

6 Information Governance Department

Information Governance will liaise with Line/Departmental Manager for the investigation and report findings back to the Caldicott Guardian, Data Protection Officer, Information Governance Steering Group and the Board.

6.4 Information Governance will liaise with the relevant Manager to ensure the under noted parties have been notified, as appropriate, and that regular updates of the investigation are provided:

- Chief Executive
- Caldicott Guardian
- SIRO
- Data Protection Officer
- Director for eHealth
- Director, General Manager, Clinical Nurse Manager or Line Manager of Directorate involved in data breach
- Communications Team
- People and Change Manager
- Police
- Counter Fraud Services

6.3 Information Governance will provide guidance to senior management as to whether the data breach is required to be notified to the Information Commissioner's Office. Where this is required it should be done without undue delay and at least within 72 hours. Advice will be based on the ICO's Guidance.

6.4 We are required by GDPR to notify any patients or staff who are the subject of a data breach, unless to do so would cause serious harm to the physical or mental wellbeing of the individual. The notification should be carried out by a senior manager and the Information Governance Department can be contacted for assistance if required.

6.5 Any correspondence with the Information Commissioner's Office will be handled by the Data Protection Officer on behalf of the SIRO.

6.6 All data breaches will be reported, on a quarterly basis, to the Information Governance Steering Group and the Board.

6.7 In the absence of the Data Protection Officer, the Data Protection Advisor has delegated authority to carry out these actions.

7.0 Associated Legislation / Policies / Standards

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988
- General Data Protection Regulation, Regulation (EU) 2016/679
- Freedom of Information Act (Scotland) Act 2002
- Human Rights Act 2000
- NHSiS IT Security Manual
- NHSScotland Caldicott Guardian"s Principles into Practice – November 2010
- NHSScotland Code of Practice: Protecting Patient Confidentiality
- Privacy and Electronic Communication Regulations 2003
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Other relevant Data Protection laws

8.0 Policy Review

This policy will be reviewed every three years, unless the introduction of any new or amended relevant legislation warrants an earlier review.

9.0 Communication and Implementation

This Policy will be communicated through the Information Governance Framework.

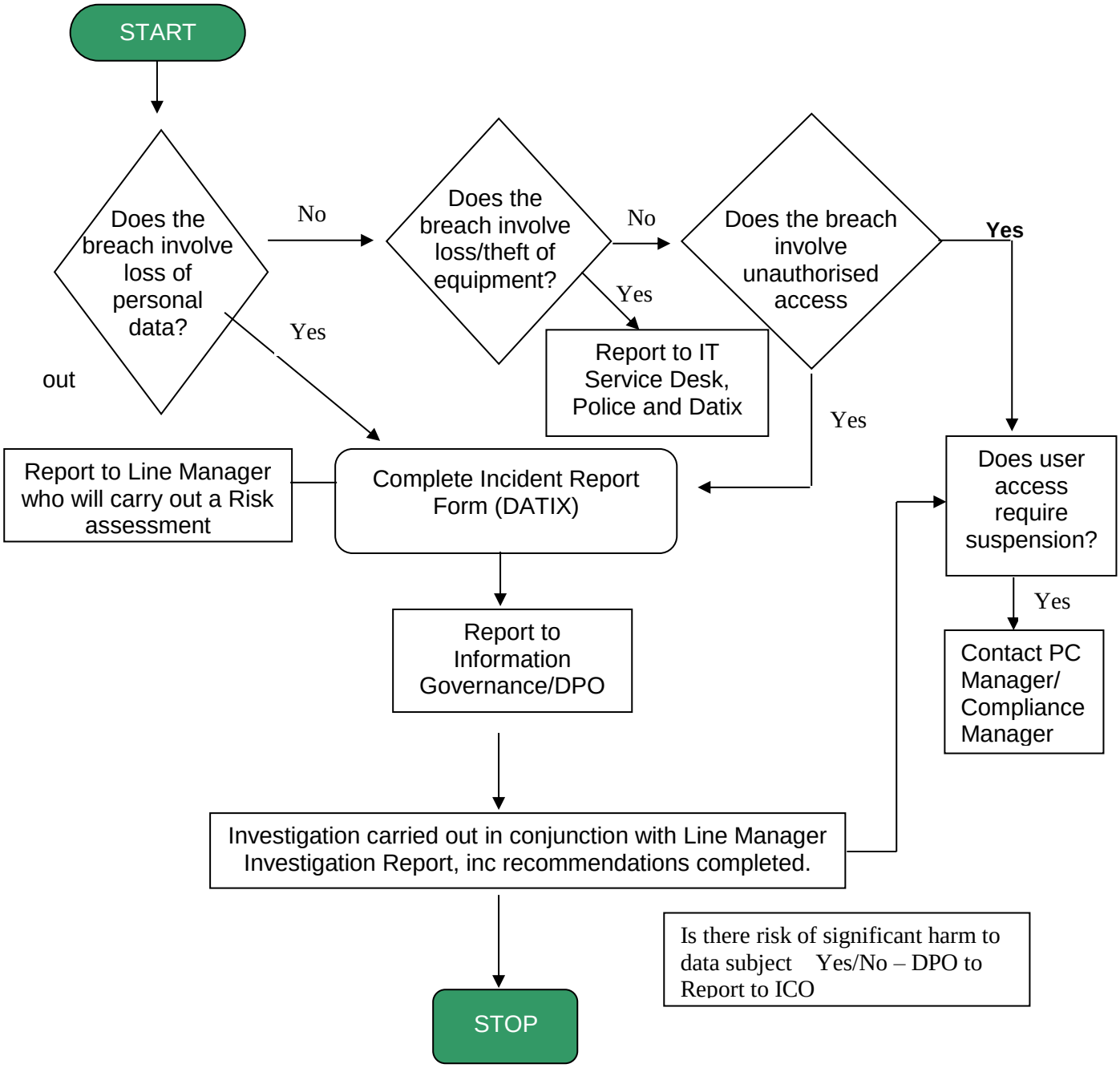
10.0 Further Advice

For further advice on this Policy please contact the Information Governance Department.

Tel: 0141 355 2059 or Email: data.protection@ggc.scot.nhs.uk

APPENDIX A

Flow Diagram to show Data Breach/Incident reporting process



APPENDIX B

Data Breach Definition

The Information Commissioner's Office describes a breach of personal data as:

> *"*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.*"*

Data Breach Examples

The following are examples of data breaches and should be reported on Datix. Please note this list is not exhaustive.

1. Staff member looking up their own information on our clinical systems;
2. Staff member looking up information of family, friends or colleagues on our clinical systems;
3. Leaving log on and password details visible or easily found such as taped to the office / ward computer where anyone can see or access this;
4. Leaving passwords and/or encryption keys kept with your mobile device;
5. Failure to log off when leaving a computer unattended;
6. Leaving any personal identifiable data in a public place, such as on a bus, in a taxi;
7. Leaving personal identifiable data overnight in the boot of your car;
8. Losing personal identifiable data in the public domain;
9. Stolen/lost IT equipment / device which holds patient identifiable data – even if the device is encrypted;
10. Incorrectly addressing a letter containing personal identifiable data which is subsequently received by the wrong person;
11. Emailing/Faxing information to the wrong recipient or copying the wrong recipient in;
12. Posting information about patients, colleagues or your employer on social network sites;
13. Discussing confidential information in a public place – being overheard.

APPENDIX C

DATA BREACH OUTCOME FORM

This form must be completed and signed by Senior Manager/ People and Change Manager conducting the investigation and a copy returned to the Data Protection Officer. Please refer to the Data Breach Policy or contact Information Governance Department if further guidance is required.

DATE OF INCIDENT…….....

SUMMARY OF INCIDENT

- IMPORTANT Please refer to Appendix D for the type of information required.

SUMMARY OF INVESTIGATION UNDERTAKEN

OUTCOME OF INVESTIGATION

SUMMARY OF ACTION TAKEN AGAINST INDIVIDUALS (Do not list the names of staff)

Signed…… Dated ……

APPENDIX D

The General Data Protection Regulation (GDPR) requires organisations to report significant breaches within 72 hours of being identified. It also requires the inclusion of specific information when the breach report is submitted.

In order to ensure Regulatory requirements are met please provide as much information as possible and ensure that all mandatory (*) fields within the Breach Outcome Form are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please provide information to this effect and details as to when this information will be available. This needs to be relied to the ICO.

Following a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps being taken to achieve this should be included on the form.

Please provide the following information:

- A description of the incident in as much detail as possible;
- When the incident happened and when it was identified if different;
- How it happened;
- An explanation if, for any reason, there was a delay in reporting the breach;
- Any measures we had in place that should have prevented this type of breach;
- Extracts from any policies and procedures considered relevant and explain which of these were in existence at the time of the incident, and the date of their implementation if known;
- The type of records involved in the breach. Does it include special category data, such as medical records, and provide the details of the level of records involved;
- The number of individuals involved;
- Whether the individuals know about the breach, and any relevant complaints received;
- What the potential consequences and adverse effects on the individuals could be;
- What action has been taken to minimise/mitigate the effect on the individuals concerned;
- Whether the data placed at risk has now been recovered;
- What steps have/will be taken to prevent a recurrence of this incident;
- If we have notified any other third parties about the incident – eg overseas data protection authority; police; regulatory bodies; and
- If there has been, or is expected to be any media coverage, and details of this.