Personal Data Breach Flowchart

In line with the General Data Protection Directive (GDPR) in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (Information Commissioner) unless following review of severity the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

This flowchart below outlines how incidents involving personal data breaches must be handled in line with severity and the relevant timescales which should be adhered to.

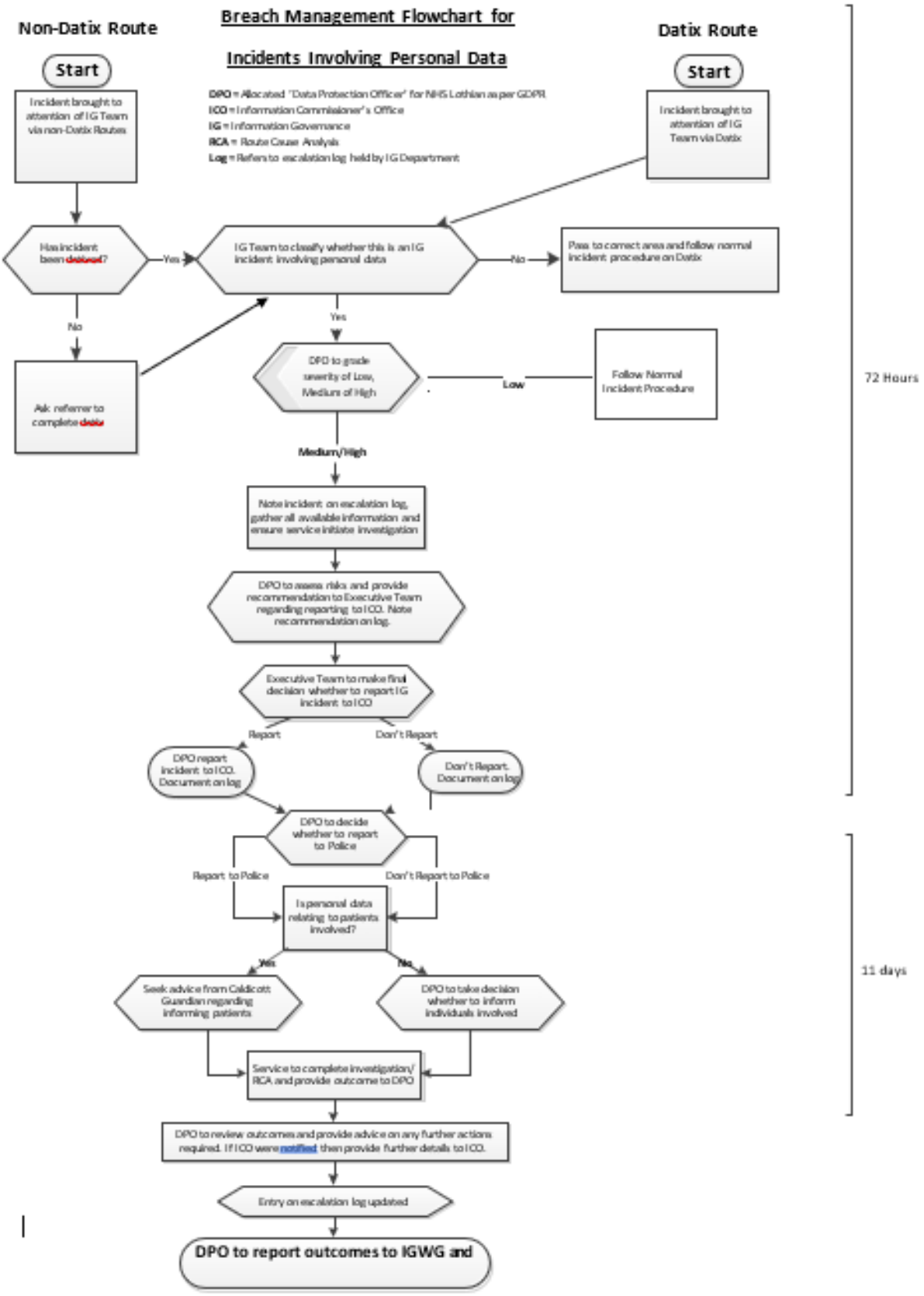
All breaches of personal data should be reported to the Information Governance Department. Breaches can be reported in many ways which includes by patients, relatives, members of the public, the Information Commissioner's Office, third sector organisations and the internal reporting system DATIX.

Incidents will be graded in order of severity within 48 hours of being reported. As per legislation, any reporting to the Information Commissioner's Office must take place within 72 hours of the organisation becoming aware of the breach. The Data Protection Office will as appropriately liaise with a Health Board Executive prior to reporting.

Severity Grading

The following table provides a guide when grading the severity of any personal data breaches:

		Number of Individuals Affected		
		Less than 10 individuals	Between 10 and 100	Over 100 individuals
Type of Information Involved	Minimum amount of personal data	Low	Medium	High
	Sensitive Personal Data breached or in the public domain	Medium	High	High
	Highly Sensitive Data breached or in the public domain	High	High	High


Breach Management Flowchart for
Incidents Involving Personal Data
DPO = Allocated "Data Protection Officer" for NHS Lothian as per GDPR
ICO = Information Commissioner's Office
IG = Information Governance
RCA = Route Cause Analysis
Log = Refers to escalation log held by IG Department
Non-Datix Route
Start
Incident brought to attention of IG Team via non-Datix Routes
Has incident been delayed?
Yes
No
Ask referrer to complete datix
Datix Route
Start
Incident brought to attention of IG Team via Datix
IG Team to classify whether this is an IG incident involving personal data
No
Pass to correct area and follow normal incident procedure on Datix
Yes
DPO to grade severity of Low, Medium of High
Low
Follow Normal Incident Procedure
Medium/High
Note incident on escalation log, gather all available information and ensure service initiate investigation
DPO to assess risks and provide recommendation to Executive Team regarding reporting to ICO. Note recommendation on log.
Executive Team to make final decision whether to report IG incident to ICO
Report
Don't Report
DPO report incident to ICO. Document on log
Don't Report. Document on log
DPO to decide whether to report to Police
Report to Police
Don't Report to Police
Is personal data relating to patients involved?
Yes
No
Seek advice from Caldicott Guardian regarding informing patients
DPO to take decision whether to inform individuals involved
Service to complete investigation/ RCA and provide outcome to DPO
DPO to review outcomes and provide advice on any further actions required. If ICO were notified then provide further details to ICO.
Entry on escalation log updated
DPO to report outcomes to IGWG and
72 Hours
11 days