NHS
Hampshire, Southampton and
Isle of Wight
Clinical Commissioning Group

Information Governance Incident Management and Reporting Procedure

Document number	IG/008/V1.2
Version	Version 1.2
Approved by	Policy Sub Group
Document author	Information Governance Consultant, South Central & West Commissioning Support Unit
Executive lead	Chief Finance Officer (Senior Information Risk Owner)
Date of approval	12 August 2021
Next due for review	April 2023

Version control sheet

Version	Date	Author	Comment
V1.0	15/02/21	Hayley Matthews	Review and update in line with planned merger of HIOW Partnership of CCGs, West Hampshire CCG and Southampton CCG to form NHS Hampshire, Southampton and Isle of Wight CCG on 1st April 2021. Update includes removal of EU GDPR, replaced with UK GDPR.
V1.1	11/05/21	IG Transition Group	Amendments recommended by IG Transition Group
V1.2	23/08/21	Governance Manager	Minor amendments recommended by Policy Sub Group of 12/08/21 and reformat into CCG approved template

Contents

1. Introduction and purpose

The UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018, introduces a duty on Controllers to report certain types of personal data breaches to the relevant supervisory authority. In the UK, a Controller must report a notifiable breach of personal data to the Information Commissioners Office within 72 hours of becoming aware of it. A Controller can be an organisation or an individual, however in the CCG's case they are the Controller of the data for which they determine the purposes and means of processing personal data.

The CCG will ensure robust breach detection, investigation and internal reporting procedures are in place that comply with legislative timescales for reporting.

The CCG will use Datix as the incident management system, to fully record the particulars of all incidents, investigations and remedial actions regardless of whether it is required to be notified externally.

The CCG will use the NHS Digital Data Security and Protection Toolkit Incident Reporting tool for the purposes of notifying breaches, which will be shared across several regulatory agencies. These include personal data breaches of the Data Protection Legislation to the Information Commissioner, cyber security incidents to NHS Digital and Network & Information Systems (NIS) and notifiable incidents will be forwarded to the Department of Health and Social Care (DHSC) where appropriate.

The CCG will comply with the National Data Guardian Data Security Standard 6 to provide evidence of their compliance in the Data Security and Protection Toolkit.

The CCG recognises the importance of reporting all incidents as an integral part of its risk identification and information risk management programme through the consistent monitoring and review of incidents that result, or have the potential to result in a confidentiality breach, damage or other loss.

The benefits of incident and near miss reporting include:

- ✓ Identifying trends across the organisation
- ✓ Pre-empting complaints
- ✓ Making sure areas of concern are acted upon
- ✓ Targeting resources more effectively

- ✓ Increasing awareness and responsiveness

Most information incidents relate to system failure and disclosure in error due to human error. Incident reporting needs an open and fair culture so that staff feel able to report problems without fear of reprisal and know how to resolve and learn from incidents.

2. Scope

This document sets out how all information incidents, including Serious Incidents Requiring Investigations (SIRIs), will be identified, reported by staff, and managed in the CCG. It is the responsibility of all staff to ensure that information remains secure where this is required and therefore, it is important to ensure that when incidents occur, damage from them is minimised and lessons are learnt from them.

The CCG is committed to identifying, evaluating and mitigating all risks to data subjects; these include patient/service users, permanent and temporary staff.

3. Definitions

Adverse Event	Any untoward occurrence which can be unfavourable and an unintended outcome associated with an incident.
Anonymous data	Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. If you could at any point use any reasonably available means to re-identify the individuals to which the data refers, that data will not have been effectively anonymised but will have merely been pseudonymised. This means that despite your attempt at anonymisation you will continue to be processing personal data. You should also note that when you do anonymise personal data, you are still processing the data at that point.
Availability Breach	Unauthorised or accidental loss of access to, or destruction of, personal data.
Citizen	Any person or group of people. This would include patients, service users, the public, staff or in the context of incident reporting, anyone impacted by the incident.

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Confidentiality Breach	Unauthorised or accidental disclosure of or access to personal data.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the UK GDPR.
Cyber Incident	There are many possible definitions of what a Cyber incident is. For the purposes of reporting, a Cyber incident is defined as anything that could (or has) compromised information assets within Cyberspace. “Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.” It is expected that the type of incidents reported would be of a serious enough nature to require investigation by the organisation. These types of incidents could include, denial of service attacks, phishing emails, social media disclosures, web site defacement, malicious internal damage, spoof website, cyber bullying.
Damage	This is where personal data has been altered, corrupted, or is no longer complete.
Destruction	This is where the data no longer exists, or no longer exists in a form that is of any use to the controller.
Incident	An Incident is defined as an event which has happened to, or occurred with, a patient(s), staff or visitor(s), the result of which might be harmful or potentially harmful, or which does cause or lead to injury/harm.
Integrity Breach	Unauthorised or accidental alteration of personal data.
Loss	The data may still exist, but the controller has lost control or access to it, or no longer has it in their possession.
Near Miss	A near miss is an incident that had the potential to cause harm but was prevented. These include clinical and non-clinical incidents that did not lead to harm or injury, disclosure or misuse of confidential data but had the potential to do so.

Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Personal data breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the UK GDPR.
Pseudonymised data	The UK GDPR defines pseudonymisation as: "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Pseudonymisation may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Whilst you can tie that reference number back to the individual if you have access to the relevant information, you put technical and organisational measures in place to ensure that this additional information is held separately. Pseudonymising personal data can reduce the risks to the data subjects and help you meet your data protection obligations. However, pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data.

	"…Personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person…"
Serious Incident Requiring Investigation (SIRI)	There is no simple definition of a serious incident. What may first appear to be of minor importance may, on further investigation, be found to be serious or vice versa. SIRIs are incidents which involve actual or potential failure to meet the requirements of the Data Protection Legislation and/or the Common Law Duty of Confidentiality. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy. This definition applies irrespective of the media involved and includes both electronic media and paper records. When lost data is protected e.g. by appropriate encryption, so that individuals data cannot be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported via a different route).
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Unauthorised Processing	Unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the UK GDPR.

4. Roles and responsibilities

The Accountable Officer

Has overall responsibility for Information Governance (IG) within the organisation. As the Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The Managing Director

Has lead responsibility for the CCG who will work closely with the Clinical Chair/s ensuring that the services delivered provide the most effective use of resources to meet local needs.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) for the CCG is an executive board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the Chief Executive with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. They will oversee SIRIs.

Caldicott Guardian

The Caldicott Guardian is the person within the CCG with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the CCG Board and relevant committees on confidentiality issues. They will support the SIRO in overseeing SIRIs.

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been assigned the responsibilities set out in the UK GDPR, such as monitoring and assuring CCG compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments (DPIA), giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the and Information Commissioner's Office (ICO). The DPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO is informed no later than 72 hours after the organisation becomes aware of the incident.

South Central & West Commissioning Support Unit (SCW) Information Governance Team

The IG Team will support the organisation in investigating incidents, offer advice to staff and will report notifiable breaches to the ICO. Support will be given to the DPO as required. This will ensure the organisation complies with legislation, policies and protocols.

SCW Cyber Security Manager and IoW NHS Trust Cyber Security Manager

The Cyber Security Managers will ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

Information Asset Owners

The Information Asset Owners (IAOs) will support the organisation in investigating incidents.

Data Custodians

Data Custodians (DCs) will support the organisation in investigating incidents.

All Staff

All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of and comply with the requirements of this procedure.

Information Governance Working Group *(to be confirmed if required)*

The IG Working Group is responsible for overseeing day to day IG issues and provides a reporting mechanism and forum for discussing incidents, other types of IG breach and also near misses.

Audit and Risk Committee

The Audit and Risk Committee has oversight and accountability for IG ensuring that the CCG complies with their statutory responsibilities and fulfils the requirements of administrative law, Data Protection Act 2018, General Data Protection Regulation 2016, the Common Law Duty of Confidentiality and The Records Management Code of Practice for Health and Social Care 2016.

5. Procedures

The procedure for reporting incidents, breaches and near misses is included as Appendix A. The incident reporting form can be found at Appendix B.

6. Freedom of Information Requests (FOI)

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management of incidents. Incidents will be defined and where appropriate kept confidential, underpinning the Caldicott principles and the regulations outlined in the Data Protection Legislation and Freedom of Information Acts.

Non-confidential incidents relating to the CCG and its services will be available to the public through a variety of means including reports, minutes and the procedures established to meet requirements in the Freedom of Information Act 2000. The CCG will follow established procedures to deal with queries from members of the public.

7. Equality analysis

The CCG is committed to equality, diversity and inclusion for all, as well as to meeting the Public Sector Equality Duty (Equality Act 2010).

Both new policies / procedures, and existing policies / procedures when reviewed, come within the Public Sector Equality Duty. This means that authors must consider whether the policy will be effective for all patients and/ or staff. This process is called Equality Impact Assessment.

These procedures have been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full EIA is not required.

However, the CCG Datix system which is used to record all incidents has a number of fields that can be selected to record equality aspects of incidents, which enables the CCG to capture data regarding equality incidents, address individual cases and analyse trends; this will include any related to IG breaches / incidents.

8. Training

The CCG recognises the importance of an effective training structure and programme to deliver compliance and awareness of confidentiality and data protection and its integration into day-to-day work and procedures. The identification of breaches is included in the on-line IG Training modules provided by NHS Digital that can be accessed through the Consult OD learning and development portal. All staff are required to complete mandatory IG training on an annual basis and the SIRO, Caldicott Guardian, DPO, IAOs and DCs undertake additional training in accordance with their key role. Further tailored training will be provided where it is deemed necessary due to high levels of confidential data being handled, recurrent breaches being reported or as identified as part of the root cause analysis or lessons learned report.

9. Dissemination

This document will be made available to staff on the IG page of the CCG website, with a link to the appropriate page also available on the staff intranet / StayConnected portal.

10. Monitoring compliance and effectiveness

The CCG will ensure that it fully embeds improvements to its IG structure and demonstrate it is proactive in assessing and preventing information risks by evidencing that:

a. There is continuous improvement in confidentiality and data protection and learning outcomes

b. Any changes to the Data Security and Protection Incident Reporting Tool or guidance is reflected in this policy

c. All incidents are audited to ensure any recommendations made have been implemented

d. Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring

e. Records of all decisions, actions, and recommendations (e.g. evidence, incident forms and reports) will be kept throughout the investigation and final report

f. All records and documentation will be kept in a secure location

g. Any Personal Confidential Data (PCD) including medical records, photos or other evidence will be secured at the start of the investigation

h. File notes with dates will be kept of all discussions

i. Minutes of all related meetings will be produced.

11. Review

This policy will be reviewed annually or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from NHS England, NHS Digital and the Information Commissioner or any relevant case law.

12. Stakeholder / consultation information

This policy was already in place in the HIOW Partnership of CCGs, West Hampshire CCG and Southampton City CCG prior to the merger to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021.

It has been through an internal process and reviewed by the Information Governance Team, South Central & West Commissioning Support Unit, with input from the IG Transition Group, DPO, Governance Managers and reviewed by the SIRO.

13. References and associated documents

- Confidentiality and Safe Haven Policy
- IG Staff Handbook
- IAO & DC Staff Handbook
- IG Policy
- DPIA Guidance Framework
- IG Framework and Strategy
- Information Risk Management Programme
- Records Management Policy
- SCW / IoW NHS Trust IT Services Security Incident Handling Policies

The link to the NHS Digital Data Security and Protection Incident Reporting Guidance can be found here. The link to the Information Commissioners Office guidance on data breaches can be found here.

Appendix A: Staff Guidance on Identifying and Reporting an Information Incident

This guidance applies to all staff including permanent, temporary and contracted staff.

All incidents must be reported to your line manager and Information Asset Owner/Data Custodian immediately you become aware of the incident. The SCW IG Consultants should as a minimum be informed within 24 hours or 1 working day of you becoming aware of the incident. The SCW IG Consultant will escalate notifiable incidents to the CCG DPO, SIRO and Caldicott Guardian as appropriate.

Where an incident occurs out of business hours, the designated on-call officer will ensure that action is taken to inform the appropriate contacts within 24 hours of becoming aware of the incident.

The Incident reporting form at Appendix B must be completed and forwarded to the SCW IG Team at scwcsu.igenquiries@nhs.net, the CCG Information Asset Owner and Data Protection Officer (DPO). Please refer the flow chart at appendix C. (***To be removed on implementation of Datix***)

What should you report?

There are three types of breaches defined under the Article 29 Working Party which informed the drafting of the UK General Data Protection Regulation (UK GDPR):

- Confidentiality breach - unauthorised or accidental disclosure of, or access to personal data

  Example - Infection by ransomware (malicious software which encrypts the controller’s data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as a confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. If the attacker has not accessed personal data the breach would still represent an availability breach and require notification if there is potential for a serious impact on the rights and freedoms of the individual.

- Availability breach- unauthorised or accidental loss of access to, or destruction of, personal data

  Example - In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals’ rights and freedoms; for example, operations may be cancelled. This is to be classified as an availability breach.

- Integrity breach - unauthorised or accidental alteration of personal data

  Example - Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach. For example, a ‘do not resuscitate’ notice on the wrong patient record may have the significant consequence of death whilst an entry recording the patient blood pressure may not have the same significant result.

Here are some more examples of information incidents that should be reported:

- You find a computer printout containing Confidential Data laying around
- You identify or are informed that a fax that was thought to have been sent to an intended recipient had been received by an unknown recipient or organisation
- You find confidential waste in a ‘normal’ waste bin
- You lose or temporarily misplace a mobile computing device or mobile phone that may have personal information on it
- Information has been given to someone who should not have access to it – verbally, in writing or electronically
- A computer database has been accessed using someone else’s authorisation e.g. someone else’s user id and password
- A secure area has been accessed using someone else’s swipe card or pin number when not authorised to access that area
- A PC and/or programmes are not working correctly – potentially because the device may have a virus
- A confidential or sensitive e-mail has been sent to an unintended recipient or ‘all staff’ by mistake
- A colleague’s password has been written down on a ‘post-it’ note and found by someone else
- A physical security breach (‘break in’) to the organisation is discovered
- A phishing email has been received
- A Website has suffered from defacement

What happens next?

The incident will be investigated by the Controller but they can be supported to do this by other organisations. The Controller retains the legal obligation to report and investigate incidents.

Where an incident involves data or information that is processed by an organisation on behalf of the Controller, the DPO for the Controller should be informed by the Processor of the potential breach and in addition to providing support for any necessary notification to third parties, agree an appropriate investigation plan. The same must apply where Data Sharing Agreements are in place and notification of potential breaches to agreement partners forms part of each organisation's obligations under that agreement.

The purpose of an incident investigation is to:

- Carry out a root cause analysis in order to establish what actually happened and what actions and recommendations are needed to be taken to prevent reoccurrence;
- To identify whether any deficiencies in the application of CCG policies or procedures and/or the CCG arrangements for confidentiality and data protection contributed to the incident;
- Determine whether a human error has occurred, but not to allocate blame;
- Decide whether to notify the data subject. This decision will be made by SIRO and the Caldicott Guardian on the recommendation of the DPO
- In some cases the investigation may identify whether any disciplinary processes may need to be invoked.

Assessing the severity of an incident

An initial assessment of the incident will be made using the NHS Digital Data Security and Protection Incident Reporting tool.

Notifiable breaches are those that are likely to result in a high risk to the rights of freedoms of the individual (data subject). The scoring matrix used in the reporting tool has been designed to identify those breaches that meet the threshold for notification.

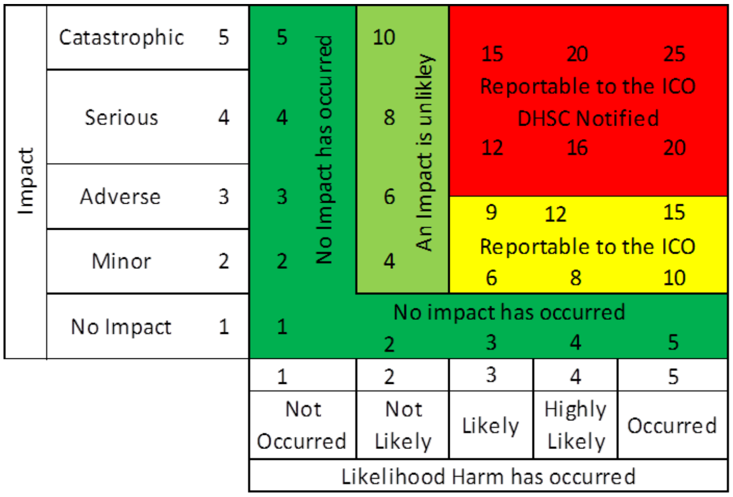
The factors for assessing the severity level of incidents are determined by:

- the potential significance of the adverse **effect** on individuals graded from 1 (lowest) to 5 (highest);

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be the release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or some financial detriment has occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event	A person dies or suffers a catastrophic occurrence.

- the **likelihood** that adverse effect has occurred graded from 1 (non-occurrence) to 5 (occurred);

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence.
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.



Impact	Catastrophic	5	5 No Impact has occurred	10 An Impact is unlikley	15 Reportable to the ICO DHSC Notified	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9 Reportable to the ICO	12	15
	Minor	2	2	4	6	8	10
	No Impact	1	1	2 No impact has occurred	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood Harm has occurred				

Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following categories of data, the breach assessment must start at ‘minor impact’ and ‘harm not likely’ scoring it at 2 x 2 = 4. It will only be reportable to the ICO where further assessment increases along the likelihood of harm axis i.e. scores of 6 and above:

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information including the alleged commission of offences by the data subject or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health
- Special Categories of personal data

Under the following circumstances notification may not be necessary;

- Encryption – Where the personal data is protected by means of encryption.
- ‘Trusted’ partner - where the personal data is recovered from a trusted partner organisation. The controller may have a level of assurance already in place with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take

any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on a case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches.

- Cancel the effect of a breach - where the controller is able to null the effect of any personal data breach.

Assessing the risk to the rights and freedoms of a data subject

The UK GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following;

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Internal Reporting

Any information incident that takes place that is not reportable will still be included in reports circulated to the appropriate group / committee. These are primarily for staff awareness and to identify trends in minor incidents.

IG incident reports will also be presented to the appropriate group / committee and the relevant committees through the SIRO and or DPO in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.

Appendix B: Information Governance Incident Reporting Form *(to be removed on implementation of Datix)*

Please discuss the incident with the CCG IG Manager and complete/submit this form **electronically** (NHSMail to NHSMail) using the relevant question set to SCWCSU.IGEnquiries@nhs.net.

Name:-	Date & time of reporting:-	

For Internal IG incidents *Data sent by the CCG in error*	**For External IG Incidents** *Data sent to the CCG in error*	**Details**
Date and time of incident	Date and time of Incident	
Directorate	Type of Organisation *NHS Provider, Contractor etc.*	
Team	Sender *Organisation & senders name*	
Location	Location	
Category *Post, Memory stick, email etc.*	Category *Post, Memory stick, email etc.*	
Description *Include what and how the data was sent, no. of records etc.*	Description *Include what and how the data was sent, no. of records etc.*	
Actions Taken	Actions Taken	

Please ensure all information pertaining to the incident is securely stored until advised by the assigned IG Manager.

Internal SCW use only

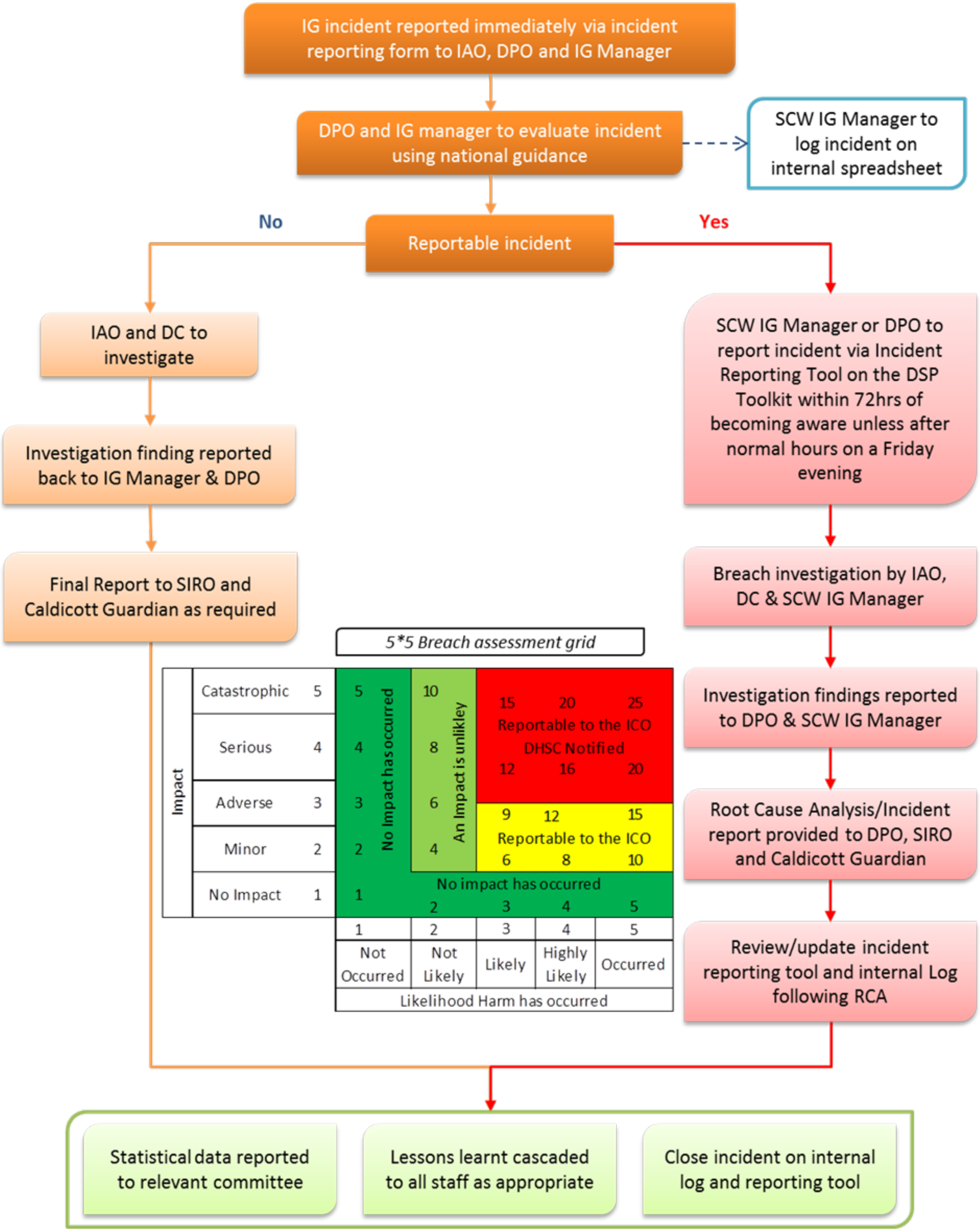
IG Manager		Incident Number		Matrix Score	
Recommendation and actions taken					
Incident reportable					

Section 2 – Incident Grading *to be completed by xxxxxxxxxxxxxx*			
Incident Number		Date Received and logged	
Date reported to the Data Protection Officer		Date reported to CG/SIRO	
Date reported on the DSP toolkit			
Detail any other stakeholders (Controllers/Processors) and when they have been notified *add extra lines if necessary	**Controller**		**Date notified**
Initial Incident grading and reasoning			
What further information has been gathered since notification and when?			
Final Incident grading and reasoning			

Section 3 – Investigation Details *to be completed by investigating manager*	
Causes and contributory Factors	
Process issues raised	
Lessons learnt & recommendations	

Section 4 – Actions/Learning *to be completed by investigating manager*			
Action	**Responsible**	**Date for completion**	**Completed date**
1.			
2.			
3.			
Date Investigation Report Completed			
Date reported to IGSG			
Date incident closed by CG/SIRO			

Appendix C: Information Governance Incident Flow Chart *(to be amended on implementation of Datix)*


IG incident reported immediately via incident reporting form to IAO, DPO and IG Manager
DPO and IG manager to evaluate incident using national guidance
SCW IG Manager to log incident on internal spreadsheet
No
Reportable incident
Yes
IAO and DC to investigate
Investigation finding reported back to IG Manager & DPO
Final Report to SIRO and Caldicott Guardian as required
SCW IG Manager or DPO to report incident via Incident Reporting Tool on the DSP Toolkit within 72hrs of becoming aware unless after normal hours on a Friday evening
Breach investigation by IAO, DC & SCW IG Manager
Investigation findings reported to DPO & SCW IG Manager
Root Cause Analysis/Incident report provided to DPO, SIRO and Caldicott Guardian
Review/update incident reporting tool and internal Log following RCA
Statistical data reported to relevant committee
Lessons learnt cascaded to all staff as appropriate
Close incident on internal log and reporting tool

*5*5 Breach assessment grid*

Impact						
Catastrophic	5	5	10	15	20	25
Serious	4	4	8	12	16	20
Adverse	3	3	6	9	12	15
Minor	2	2	4	6	8	10
No Impact	1	1	2	3	4	5
		1	2	3	4	5
		Not Occurred	Not Likely	Likely	Highly Likely	Occurred

Likelihood Harm has occurred

No Impact has occurred

An impact is unlikley

Reportable to the ICO DHSC Notified

Reportable to the ICO

No impact has occurred