FRIMLEY
INTEGRATED CARE BOARD

Information Governance and Cyber Incident Management and reporting Procedure

Version	Version 1.3
Adopted by	ICB Board
Document Author	South Central West CSU
Date of adoption	May 2024
Next due for review	May 2026

Version	Date	Author	Status	Comment
1.0	5/5/2022	SCW CSU	Final	Version adapted from CCG version.
1.1	24/8/2023	SCW CSU	Final	Updates on Root Cause Analysis.
1.2	27/1/2023	SCW CSU	Final	Minor commentary updated
1.3	09/01/2024	SCW CSU	Final	Adoption of NIS Procedures and other commentary from latest CSU document

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.

The Security of Network and Information Systems Regulations 2018 ("NIS Regulations") seek to ensure that essential services, including healthcare, have adequate data and cyber security measures in place to deal with the increasing volume of cyber threats. They require 'operators of essential services' to report any network and information systems incident which has a 'significant impact' on the continuity of the essential service that they provide to the relevant 'competent authority'.

NIS Regulation also requires reporting of relevant incidents to the Department of Health and Social Care (DHSC) as the competent authority where organisations are subject to NIS Regulation.

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.

The ICB will ensure robust breach detection and internal reporting procedures are in place that complies with legislative timescales for reporting and enables the ICB to fulfil its responsibilities when acting as a Processor under a relevant contract or other legal agreement with a Controller so They can be notified immediately that a breach or potential breach has occurred.

The ICB will use Datix to report breaches and other information incidents including Cyber Security Incidents. The ICB will keep a record of all personal data breaches and near misses, regardless of whether it is required to notify external bodies.

When a breach is identified as requiring escalation, the ICB will use the NHS England Data Security and Protection Incident Reporting tool as guidance. Controllers can use the tool which is linked to Their own Data Security and Protection toolkit for the purposes of notifying breaches on one form which may Then be shared across several regulatory agencies. These include personal data breaches under the Data Protection Legislation to the Information Commissioner and cyber security incidents to NHS England.

The ICB 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 ICB will maintain a local file and use an incident management system (Datix) to fully record the particulars of any investigation and remedial action.

The ICB 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 confidentiality breach, damage or other loss which may.

Research has shown that the more incidents that are reported combined with the use of root cause analysis to understand why an incident has occurred, the more information will be available about any problems. It should be noted that root cause analysis would only normally be undertaken on more serious incidents and would not be an appropriate approach for minor incidents.

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 will be identified, reported, and managed in the ICB. 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, potential harm from Them is minimised and lessons are learnt. This policy applies to all staff employed to undertake any work under contract to the ICB.

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 ICB 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 UK GDPR. They are responsible for reporting breaches to the relevant body.
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 its 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, 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.
Pseudonymised data	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 have 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…"
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under UK GDPR. They are responsible under contract, for informing the Controller of any potential or actual breach without delay and at all times, to assist the Controller to meet Their legal obligations.
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. Serious Incident Requiring Investigations (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 UK GDPR.

4. ROLES AND RESPONSIBILITIES

The ICB Managing Director

The ICB Managing Director has overall responsibility for Information Governance within the organisation. As 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 ICB Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner for the ICB is an executive management team member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at executive management level. The SIRO must provide the Accountable Officer 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 Serious Incidents Requiring Investigation (SIRIs).

The ICB Caldicott Guardian

The Caldicott Guardian is the person within the ICB with overall responsibility for protecting the confidentiality of information that includes personal data and special categories of personal data, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the ICB Executive Management Team on confidentiality issues. They will support the SIRO in overseeing Serious Incidents Requiring Investigation (SIRIs).

The ICB Data Protection Officer

The Data Protection Officer (DDPO) is the person within the ICB that has been identified to support the role of Data Protection Officer (DPO) in NHS England. This role has the responsibilities as set out in UK GDPR guidance and is responsible to feedback any Information Governance issues to the ICB Executive Management Team and the DPO at NHS England. 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 (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident.

The ICB Corporate Information Governance Team

The Information Governance Team will support the organisation in investigating information breaches, incidents and near misses, offer advice and ensure the organisation complies with legislation, policies and protocols.

The ICB Cyber Security Manager

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

The ICB Information Asset Owners (IAO)

The Information Asset Owners (IAOs) are responsible for the assets within Their team and as such, will support the organisation in detecting and investigating information breaches, incidents and near misses.

The ICB Information Asset Administrators (IAA)

IAA's will support Their IAO and the Information Governance team in investigating information breaches, incidents and near misses.

All the ICB Staff

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

The ICB Information Governance Steering Group

The ICB Information Governance Steering Group is responsible for overseeing day to day Information Governance issues and provides a reporting mechanism and forum for discussing Serious Incidents Requiring Investigation (SIRIs), other types of IG breach.

5. PROCEDURES

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

6. TRAINING

The ICB 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 Theon-line Data Security Awareness Level 1 IG Training modules accessed NHS England through the ESR portal. Further tailored training will be provided where it is deemed necessary due to high levels of confidential data being handled, recurrent breaches are being reported or as identified as part of a lessons learned report.

7. MONITORING AND REVIEW

The ICB will ensure that it fully embeds improvements to its information governance 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 NHS England 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 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.

This procedure will be reviewed on every two years but will be monitored by Audit and Risk Assurance Committee to ensure any legislative changes that occur before the review date are incorporated.

8. REFERENCES AND ASSOCIATED DOCUMENTS

The ICB Confidentiality and Safe Haven Policy
The ICB IG Staff Handbook
The ICB IG Policy
The ICB DPIA Guidance Framework
The ICB IG Framework and Strategy
The ICB Information Risk Management Programme
The ICB Records Management Policy
The ICB Data Quality Policy
IT Incident Management Policy
NHSE Guide to TheNotification of Data Security and Protection Incidents

The link to the NHS England Data Security and Protection Incident Reporting Guidance can be found here Toolkit.

The link to the Information Commissioners Office guidance on data breaches can be found here ICO breach guidance.

9. FREEDOM OF INFORMATION REQUESTS (FOI)

The ICB 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 ICB, 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 ICB will follow established procedures to deal with queries from members of the public.

10. PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT

An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found. A copy of the EIA is attached at Appendix C.

APPENDIX A: STAFF GUIDANCE ON IDENTIFYING AND REPORTING AN INFORMATION INCIDENT

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

All incidents must be reported to your line manager and Information Asset Owner/Information Asset Administrator immediately you become aware of the incident. The ICB Information Governance team should as a minimum be informed within 24 hours or 1 working day of you becoming aware of the incident at scwcsu.igenquiries@nhs.net. **Incidents must be reported on the ICB Datix system.**

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.

Where further information is required by the reporter to complete an investigation, timely responses are required from the reporter to ensure the official timescales are adhered to.

What should you report?

There are three types of breaches defined by 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 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 the 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 an email 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 aren't 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 experienced a defacement

What happens next?

Where an incident involves data or information that the ICB is not the Controller for, Information Governance Consultancy Lead, System & Digital Transformation acting as the NHS England Deputy DPO will inform the Controller's Data Protection Officer of the potential breach and in addition to providing support for any necessary notification to third parties, agree an appropriate investigation plan.

The incident will be investigated by the controller, but the ICB will assist in anyway it can. The controller retains the legal obligation to report and investigate incidents.

The purpose of an incident investigation is to:

- Carry out a root cause analysis where appropriate to establish what happened and what actions and recommendations are needed to be taken to prevent reoccurrence (it should be noted that root cause analysis is only normally undertaken on more serious incidents);
- To identify whether any deficiencies in the application of the ICB policies or procedures and/or the ICB arrangements for confidentiality and data protection contributed to the incident;
- Determine whether a human error has occurred, but not to allocate blame;
- All incidents that are considered a serious incident or are assessed as requiring reporting to the ICO will be reported immediately to the NHS England Corporate IG Team whilst simultaneously reported directly to the NHS England CSU Transition Team. The NHS England DPO in conjunction with the NHS England Corporate IG Team will lead on the oversight of the risk on the grounds of disclosure, including transparency and the ability to protect against harm;
- Decide whether to notify the data subject. This decision will be made by the ICB SIRO and the Caldicott Guardian on the recommendation of the Data Protection Officer but only after appropriate advice and guidance has been sought from NHS England in line with their Risk Management Procedure Framework;
- 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 England 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:

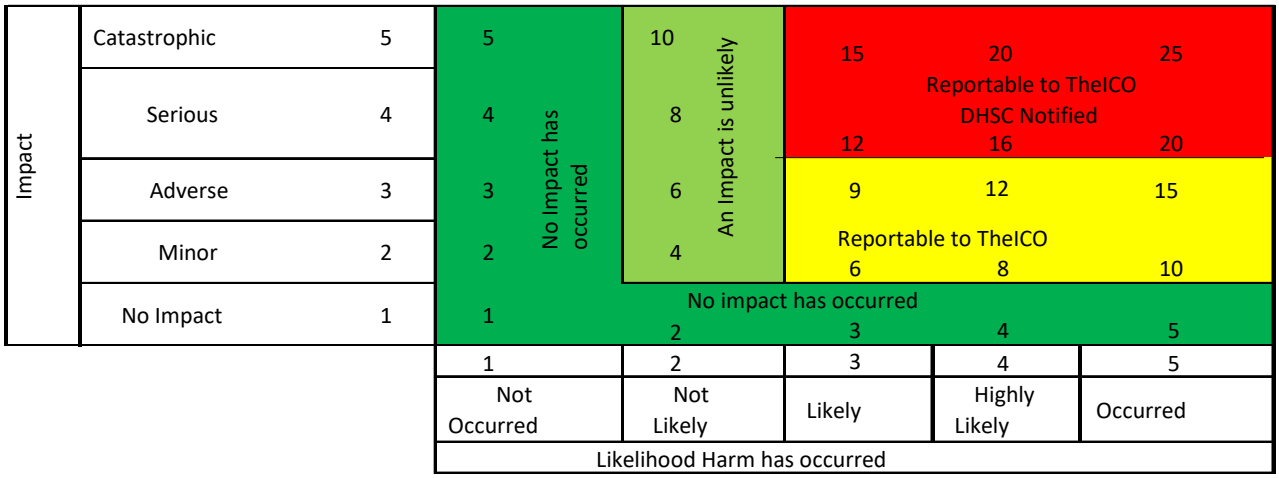
- The potential significance of the adverse **effect** on individuals graded from 1 (lowest) to 5 (highest);

No.	Effect	Description	Example
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach	Spreadsheet of anonymous data sent to the wrong team in an NHS organisation
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.	Email containing PCD from the ICB regarding the non-funding of a procedure sent to the incorrect GP practice
3	Potentially Some adverse effect	An adverse effect may be 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.	Email containing PCD sent from the ICB to incorrect member of the public via email regarding funding for potential treatment for a patient.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or There has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.	Email sent from trust to incorrect GP practice regarding the new diagnosis of a patient which delays treatment, and which may increase suffering. Or Bank details of employee being sent to member of the public by HR causing loss of funds from bank account
5	Death/catastrophic event.	A person dies or suffers a catastrophic occurrence	Urgent change in treatment for warfarin patient sent to wrong GP practice, delays treatment and contributes to death of patient.

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

No.	Likelihood	Description	Example

1	Not occurred	There is absolute certainty that There can be no adverse effect. This may involve a reputable audit trail or forensic evidence	No harm can be felt from this breach
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.	Minor adverse effect but no harm is reported due to nature of breach e.g. not funding of non-urgent treatment is not going to incur harm to the patient, any other harm is nulled due to mitigation as GP practice is a trusted partner.
3	Likely	It is likely that There will be an occurrence of an adverse effect arising from the breach.	Person **likely** to suffer an adverse effect – e.g. CHC patient assessment sent to the wrong family or HR disciplinary report sent to the wrong staff member for validation. Could cause distress to person now or in the future.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.	Significant harm recorded e.g. HR sent staff bank details sent to an incorrect member of the public resulting in loss of funds
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.	Severe harm recorded – death



Sensitivity factors have been incorporated into Thegrading 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

Any breach graded at 4 or above should be discussed with the DPO as soon as possible.

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 case-by-case basis. Nevertheless, the controller still must keep information concerning the breach as part of the general duty to maintain records of breaches. Examples of trusted partners – other NHS organisations, departments within your own organisation, organisations that you current work with providing a DPIA has been undertaken and the contract clearly states that any information sent to the recipient in error should be reported back to the sender immediately and double deleted from Their system e.g. BI provided by Deloitte for a certain project who are sent information collected for another project.
- Cancel the effect of a breach - where the controller can null the effect of any personal data breach.

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

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

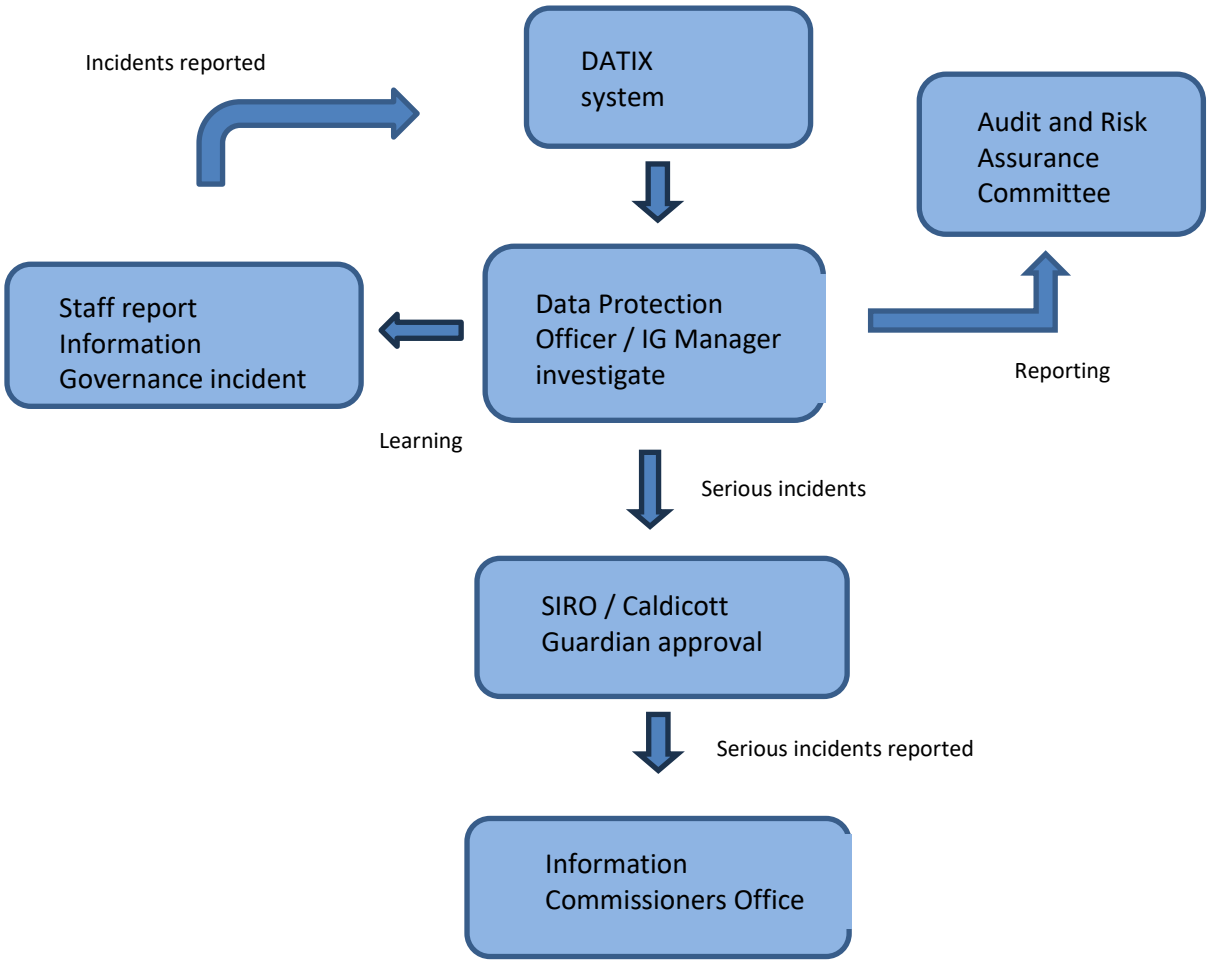
Internal Reporting

Any information incident that takes place that is not reportable will still be included in reports circulated to the Audit and Risk Assurance Committee. These are primarily for staff awareness and to identify trends in minor incidents.

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

Incidents are also reported into individual teams/directorate for learning purposes and to prevent/reduce the re-occurrence.

APPENDIX B: INFORMATION GOVERNANCE INCIDENTS FLOW CHART



APPENDIX D: EQUALITY IMPACT ASSESSMENT

1 What is it about?	***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Incident Management and Reporting Procedure details how the ICB will meet its legal obligations and NHS requirements concerning the identification, reporting and investigation of personal data breaches and the arrangements in place to support this.	
b) Who is it for? All staff	
c) How will the proposal/policy meet the equality duties? The procedure will have no adverse effect on equality duties.	
d) What are the barriers to meeting this potential? There are no barriers currently identified.	
2 Who is using it?	***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The procedure is applicable to all.	
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the procedure as this is an operational procedure in response to legislative requirements.	
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.	
3 Impact	***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created.	
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified? Not applicable	
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This procedure is equal across all groups.	
d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.	
4 So what (outcome of this EIA)?	***Link to the business planning process***
a) What changes have you made during this EIA? None	
b) What will you do now and what will be included in future planning? Nothing	
c) When will this EIA be reviewed? At procedure review.	

d) How will success be measured?

No equality issues are created.