Buckinghamshire, Oxfordshire and Berkshire West Integrated Care Board

BUCKINGHAMSHIRE, OXFORDSHIRE AND BERKSHIRE WEST INTEGRATED CARE BOARD (BOB ICB)

Policy	**Information Governance Incident Management and Reporting Procedure**
Version Number	1.0
Version Date	November 2022
Review Date	November 2024
Responsible Owner	Governance Manager
Approving Body	Audit and Risk Committee
Target Audience	All staff

Document Control

Reviewers and Approvals

This document requires the following reviews and approvals:

Name	Version Approved	Date Approved
Information Governance Steering Group	1.0	22/11/2022
Audit and Risk Committee	1.0	03/01/2023

Revision History

Version	Revision Date	Details of Changes	Author
0.1	08/09/22	Changes to comply with requirements of DSPT	SCW CSU IT Consultant

Links or Overlaps with Other Key Documents and Policies

Document Title	Version and Issue Date	Link
Confidentiality and Safe Haven Policy	V1.0; September 2022	https://www.bucksoxonberksw.icb.nhs.uk/media/2244/bob-icb-confidentiality-and-safe-haven-policy-v10-final.pdf
IG Staff Handbook	V1.0; September 2022	https://www.bucksoxonberksw.icb.nhs.uk/media/2238/bob-icb-ig-staff-handbook-v10-final.pdf
IG Management Framework, Strategy and Policy	V1.0; September 2022	https://www.bucksoxonberksw.icb.nhs.uk/media/2240/bob-icb-information-

		governance-policy-management-framework-strategy-v10-final.pdf
DPIA Guidance Framework DPIA Template	Oct 2020	https://www.bucksoxonberksw.icb.nhs.uk/media/2001/08-dpia-template-guidance-v6-20201006.pdf https://www.bucksoxonberksw.icb.nhs.uk/media/2002/09-dpia-template-v6-20201006.pdf
Records Management Policy	V1.0; September 2022	https://www.bucksoxonberksw.icb.nhs.uk/media/2241/bob-icb-records-management-policy-with-retention-schedule-v10-final.pdf

The link to the NHS Digital Data Security and Protection Incident Reporting Guidance can be found here.
https://www.dsptoolkit.nhs.uk/Help/29

Acknowledgement of External Sources

Title / Author	Institution	Link

Freedom of Information

If requested, this document may be made available to the public and persons outside the healthcare community as part of BOB ICB's commitment to transparency and compliance with the Freedom of Information Act.

Equality Analysis

BOB ICBG aims to design and implement services, policies and measures that are fair and equitable. As part of the development of this policy its impact on staff, patients and the public have been reviewed in line with BOB ICB's legal equality duties.

Contents

1. INTRODUCTION AND PURPOSE

The UK General Data Protection Regulation (UK GDPR) as implemented by the UK Data Protection Act 2018 introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours of discovery. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

The BOB ICB will ensure robust breach detection; investigation and internal reporting procedures are in place that complies with legislative timescales for reporting.

The BOB ICB will also keep a record of other personal data breaches, regardless of whether it is required to notify externally.

In line with NHS policy, BOB ICB will use the Incident Reporting tool situated within the NHS Digital Data Security and Protection Toolkit (DSPT) to report a notifiable breach. and which informs relevant regulatory agencies, e.g. personal data breaches of the UK GDPR to the Information Commissioner and cyber security incidents to NHS Digital.

The BOB ICB will maintain a local file or use an incident management system to record the particulars of any investigation and remedial action.

The BOB ICB recognises the importance of recording 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.

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.

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 individual mistakes. Incident reporting needs an open and fair culture, so 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 personal confidential information

remains secure and therefore, it is important to ensure that when incidents occur, damage from them is minimised and lessons are learnt from them.

The BOB ICB 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.
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 BOB 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 sharing of, 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 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, 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.
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 the UK GDPR.

4. ROLES AND RESPONSIBILITIES

The Accountable Officer
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.

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner for the BOB ICB 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 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 SIRO is responsible, in line with the BOB ICB Board agreed Scheme of Reservation and Delegation (SORD), for reporting to the Audit and Risk Committee all incidents that are reported to the supervisory authority, including the results of the investigation undertaken by the Data Protection Officer (DPO) and for providing the Audit and Risk Committee with an action plan that outlines clear steps for mitigating risk and/or service improvement for such data security and personal data breaches, including responsibility and timescales for completing the work.

Caldicott Guardian
The Caldicott Guardian is the person within the BOB ICB 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 BOB ICB Board and relevant committees on confidentiality issues. They will support the SIRO in overseeing Serious Incidents Requiring Investigation (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 BOB ICB compliance with IG legislation, providing advice and recommendations to staff on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the Information Commissioner's Office (ICO). At BOB ICB the DPO is responsible for overseeing an investigation into all incidents reported (including directing actions both to contain the incident and prevent a repeat) and is responsible for assessing the seriousness of any incident and in so doing, for deciding if the breach is reportable to the supervisory authority. As part of the investigation into a data security and protection incident, when appropriate they shall conduct root cause analysis and where the incident requires, include support from a multi-disciplinary team.

When the DPO concludes an incident is likely to result in a risk to the rights and freedoms of Data Subjects, they are responsible for reporting the incident (via the DSPT reporting tool) no later than 72 hours after the organisation became aware of the incident. The DPO should inform the SIRO and Caldicott Guardian of the incident and of their decision to report. The DPO is the designated point of contact with the relevant supervisory authority and is responsible for co-ordinating and responding to any ICO investigation at BOB ICB.

SCW CSU Information Governance Team
The Information Governance Team will support the DPO's investigation of all reported incidents and will provide advice and recommendations to help ensure the organisation complies with relevant legislation, policies, and protocols.

SCW Cyber Security Manager
The SCW's Cyber Security Manager will advise on cyber related incidents and breaches of policy and recommended actions in line with organisation's procedures.

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

Information Asset Administrators (IAAs)
Information Asset Administrators will support the DPO 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. Not only are all staff responsible for reporting when a breach, they must follow guidance and policies and take reasonable steps to prevent a breach from occurring in the first place. Everyone working in or for the NHS has the responsibility to use personal data in a secure and confidential way.

Information Governance Steering Group
The Information Governance Steering Group provides executive oversight and leadership to the BOB ICB to ensure it meets its statutory duties and assurance to the Audit and Risk Committee on matters relating to IG and information security.

5. PROCEDURES

The procedure for reporting incidents, breaches and near misses is included as Annex A.

6. TRAINING

The BOB 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 the on-line IG Training modules provided to staff.

7. MONITORING AND REVIEW

The BOB 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. All incidents are audited to ensure any recommendations made have been implemented
c. Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring
d. Records of all decisions, actions, and recommendations (e.g. evidence, incident forms and reports) will be kept throughout the investigation and final report
e. All records and documentation will be kept in a secure location
f. Any Personal Confidential Data (PCD) including medical records, photos or other evidence will be secured at the start of the investigation
g. File notes with dates will be kept of all discussions
h. Minutes of all related meetings will be produced.

In line with the organisation's key documents, this document will be reviewed no later than 2 years from the date of original circulation unless new, revised legislation or national guidance necessitates an earlier review.

The link to the Information Commissioners Office guidance on data breaches can be found here.
https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

ANNEX 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 your Information Asset Owner **immediately** you become aware of the incident. The Data Protection Officer **must**, as a minimum, be informed within 24 hours or one working day of you becoming aware of the incident. The BOB ICB's incident reporting tool, Blueteq, should be used to report IG breaches as soon as possible after becoming aware of an incident. The Blueteq tool is available on the BOB ICB's website Information Governance page through the following link.

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.

Staff should consult with their IAO or with the DPO if they suspect a breach

Types of Breach

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

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

- Integrity breach - unauthorised or accidental alteration of personal data

Here are some examples of the types of information incidents that occur:

- A confidential or sensitive e-mail has been sent to an unintended recipient or 'all staff' by mistake
- Information has been given to someone who should not have access to it – verbally, in writing or electronically
- You lose or temporarily misplace a mobile computing device or mobile phone that may have personal information on it
- A computer database has been accessed using someone else's authorisation e.g. someone else's user id and password
- You find a computer printout containing Confidential Data laying around
- You find confidential waste in a 'normal' waste bin
- 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 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.

Where an incident involves data or information that a Controller has asked another organisation to process for them, the Controller DPO should be informed by the Processor'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 same must apply where a Data Sharing Agreement has been put in place and notification of potential breaches to each party forms part of the organisations' obligations.

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

The purpose of the 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 BOB ICB policies or procedures and/or the BOB ICB 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 Data Protection Officer
- In some cases, the investigation may identify whether any disciplinary processes need to be invoked.

Assessing the severity of an incident

An initial assessment of the incident will be made by the DPO, applying the evidence gathered to the scoring matrix used by the DSPT reporting tool that has been designed to identify those breaches that meet the threshold for notification.

Notifiable breaches are those that are likely to result in a high risk to the rights of freedoms of the individual (data subject).

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 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 there has been some financial detriment 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.

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 should 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 can null the effect of any personal data breach.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor and the decision is taken to report the incident by the DPO, full details will be automatically emailed to the Information Commissioners Office and the NHS Digital Data Security Centre.

Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following it must still be reported as a level 2 and as such notifiable to the ICO:

- 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

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 Information Governance Steering (IGSG) Group. These are primarily for staff awareness and to identify trends in minor incidents to allow for actions to prevent future similar incidents from occurring.

IG incident reports will also be presented to the Governing Body in line with the BOB ICB Board agreed SORD via the Audit and Risk Committee by the SIRO, in order to provide awareness and assurance that appropriate controls are in place and that IG risks and incidents are being managed effectively.