Information Governance Incident Management and Reporting Procedure

Document control

Title of Document:	Information Governance Incident Management and Reporting Procedure		
Document Reference:	IG05		
Supersedes:	CSESCA - Information Governance Incident Management and Reporting Procedure H&R / EHS - New policy (previously was covered by general Incident Reporting Policy) CWS – Information Incident Management and Reporting Procedure		
Placement in Organisation:	Covers Sussex Clinical Commissioning Groups		
Consultation / Stakeholders			
Author(s) Name:	Policy originally created by SCW CSU Amended and adapted by CCG IG Managers		
Department / Team:	Information Governance		
Approved By:	Strategic Information Governance Group – East and West		
Approval Date:	28/01/2020	**Review Date:**	Three years from date of approval
Implementation Date:	28/01/2020		
Implementation Method:	Policy will be shared on the CCGs' intranet pages and via the staff bulletin		
Version Control	*PLEASE NOTE: the most recent version of this document is available on the CCGs' websites. Printed copies (or saved electronic copies) must be checked to ensure they match the most recent version.* 1.0 - Initial Draft 1.1 – Reformatted for Sussex Clinical Commissioning Groups		

Contents

Introduction

1.1	The General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018, introduces a duty on all data controllers to report certain types of personal data breaches to the relevant supervisory authority, previously this duty applied only to the NHS. In the UK, a data controller must report a notifiable breach of personal data to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.
1.2	The Sussex CCGs will ensure robust breach detection, investigation, and internal reporting procedures are in place which comply with legislative timescales for reporting.
1.3	The Sussex CCGs will also keep a record of any personal data breaches, regardless of whether they are required to notify externally.
1.4	The Sussex CCGs will use the NHS Digital Data Security and Protection Incident Reporting tool for the purposes of notifying breaches on one form, which will be shared across several regulatory agencies. These include personal data breaches of the GDPR to the Information Commissioner, cyber security incidents to NHS Digital and NIS notifiable incidents will be forwarded to the Department of Health and Social Care (DHSC) where appropriate.
1.5	The Sussex CCGs will comply with the National Data Guardian Data Security Standard six to provide evidence of their compliance in the Data Security and Protection Toolkit.
1.6	The Sussex CCGs will maintain a local file system and incident log or use an incident management system to fully record the particulars of all incidents, investigations and remedial actions

Purpose

2.1	The Sussex CCGs recognise the importance of reporting all incidents as an integral part of their 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. 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.
2.2	This document sets out how all information governance incidents, including Serious Incidents Requiring Investigations (SIRIs), will be identified, reported by staff, and managed in the Sussex CCGs. 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 Sussex CCGs are committed to identifying, evaluating and mitigating all risks to data subjects; these include patient / service users, permanent and temporary staff.

Responsibilities

3.1	**Accountable Officer** Has overall responsibility for Information Governance within the organisations. As Accountable Officer, they are responsible for the management of the organisations and for ensuring appropriate mechanisms are in place to support service delivery and continuity.
3.2	**Senior Information Risk Owner (SIRO)** The Senior Information Risk Owner (SIRO) for the Sussex CCGs is an executive board member with allocated lead responsibility for the organisations' information risks and provides the focus for management of information risk at Governing Body level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisations and for any services contracted by the organisations. They will oversee IG related Serious Incidents Requiring Investigation (SIRIs).
3.3	**Caldicott Guardian** The Caldicott Guardian is the person within the Sussex CCGs with overall responsibility for protecting the confidentiality of personal data and special categories 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 Sussex CCGs' Governing Body and relevant committees on confidentiality issues. They will support the SIRO in overseeing IG related Serious Incidents Requiring Investigation (SIRIs).
3.4	**Data Protection Officer** The Data Protection Officer (DPO) is the person that has been assigned the responsibilities set out in the GDPR, such as monitoring and assuring CCG compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments (DPIAs), giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the 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.
3.5	**Information Governance Team** The Information Governance Team will support the organisation in investigating incidents, offer advice and ensure the organisation complies with legislation, policies and protocols.
3.6	**Cyber Security Manager** The Cyber Security Manager will ensure breaches of policy and recommended actions are reported in line with organisations' procedures.
3.7	**Information Asset Owners (IAO)** The Information Asset Owners (IAOs) will support the organisations in investigating incidents.
3.8	**Information Asset Administrators (IAA)** Information Asset Owners (IAAs) will support the organisations in investigating incidents.
3.9	**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.
3.10	**Strategic Information Governance Groups** The Strategic Information Governance Groups East (SIGG-E) and West (SIGG-W) are responsible for overseeing day to day information governance issues and provide a reporting mechanism and forum for discussing incidents, other types of IG breach and also near misses.

Definitions

4.1

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 it is possible to 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 attempts at anonymisation the data continues to be personal data. It should be noted that when personal data is anonymised, it is being processed 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 Sussex CCGs 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.
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.
Data controller	A data controller determines the purposes and means of processing personal data.
Data processor	A processor is responsible for processing personal data on behalf of a controller.

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 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.
Pseudonymised data	The 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…"
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 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 data	Special categories data is personal data 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 GDPR.

Procedure

5.1 The procedure for reporting incidents, breaches and near misses is included as Appendix A. The IG incident reporting form can be found separately on the intranet. (https://www.sussexccgs.nhs.uk/ccg-team/tools-for-your-work/information-governance/reporting-ig-incidents/)

Process for Approval and Ratification

6.1 Approval of the policy is obtained from the Strategic Information Governance Group (SIGG), following which it will be ratified by the relevant Audit Committee(s).

Dissemination, Training and Advice

7.1 The Sussex CCGs recognise 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.

7.2	The identification of breaches is included in the online IG Training module provided by NHS Digital.
7.3	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.
7.4	This policy and procedure will be made available to staff on relevant pages of the intranet and will be signposted to in staff communications regularly.

Review, Monitoring and Compliance

8.1	The Sussex CCGs will ensure that they fully embed improvements to their Information Governance structure and they are 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.
8.2	In line with the organisations' key documents, this document will be reviewed no later than three years from the date of original circulation unless new, revised legislation or national guidance necessitates an earlier review. .

References

9.1	NHS Digital Data Security and Protection Incident Reporting Guidance: https://www.dsptoolkit.nhs.uk/Help/Attachment/148
9.2	Information Commissioners Office guidance on data breaches: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Public Sector Equality Duty- Equality Impact Assessment

9.3	An Equality Impact Assessment on this policy has been conducted by SCW CSU. No adverse impact or other significant issues were found.

Appendix A – Procedure

Internal incidents procedure

The flow chart below details the Sussex CCGs' internal IG incident reporting and management procedure:

Internal Report

- Staff member makes initial report to line manager or IAO / IAA immediately upon becoming aware of the incident
- Staff Member completes IG Incident reporting form and emails to SXCCG.IG@nhs.net
- 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.

Initial assessment

- Relevant IG Manager reviews the form and completes initial grading asessment based on the NHS Digital guidance, develops investigation / action plan and logs incident or near miss on incident recording spreadsheet
- IG Manager identifies where immediate actions may be required to mitigate impact, these are undertaken by the appropriate individual
- DPO is made aware of the incident and intial grading and provides input / approves grading.

External reporting

- Incidents which are graded at a level (see matrix) indicating external reporting is required are logged on the relevant CCG's incident reporting tool (which is part of the DSP Toolkit). This tool automatically shares the report with the relevant organisation.

Investigation

- Investigation is conducted by IG Manager in liaison with DPOs / IAOs / IAAs / Line Managers / Directors as required
- Actions are agreed and undertaken, including case by case decsions on whether data subjects need to be informed
- Lesson learned are identified
- CCG complies with instructions from external bodies where they are involved.

Review

- All incidents and near misses are discusssed at the next available SIGG-E or SIGG-W meeting depending on the CCG where the incident or near miss occurred.

External incidents

Incidents of data processors or data sharing partners:
Where an incident involves data or information that is processed by an organisation on behalf of the Sussex CCGs, the DPO 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 partner's forms part of each organisations' obligations under that agreement.

Received information:
Where any staff member identifies that they have received data inappropriately from another organisation, they will immediately notify the sender of the breach and delete any copies of the data received. They should also notify the relevant IG Manager so that a log can be kept and senders contacted separately in certain cases (e.g. repeat offenders). While a log of these incidents is kept, they are not considered in Sussex CCGs incident statistics unless the breach has occurred due to CCG staff error in some form.

Classification of incidents and near misses

There are three types of breaches defined in the NHS Digital Data Security and Protection Incident Reporting Guidance:

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 is 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.

Assessing the severity of an incident

Grading of the severity of incidents will be made using the grading system detailed in the NHS Digital Data Security and Protection Incident Reporting Guidance. This grading system identifies which incidents are notifiable to external organisations.

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

Within the grading system the factors for assessing the severity level of incidents are impact and likelihood these are detailed below.

Impact: The potential significance of the adverse effect on individuals
This is graded from 1 (lowest) to 5 (highest) with details as follows:

No.	Impact	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

Likelihood: The likelihood that adverse effect has occurred
This is graded from 1 (non-occurrence) to 5 (occurred) with details as follows:

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.

Once Impact and Likelihood have been assessed the incident grading is found using the matrix below:

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

Reportable to the ICO **and** Reportable to the DHSC
Reportable to the ICO
An impact is unlikely (not externally reportable)
No impact has occurred (not externally reportable)

Sensitivity Factors
Sensitivity factors have been incorporated into the grading scores and where a non-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:

- 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 data (this includes health data)

Containment factors
There are also some containment factors to consider which may affect the grading of the incident, these are:

- 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 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 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

Investigations

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 Sussex CCGs' policies or procedures and/or Sussex CCGs' 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 may need to be invoked.

Internal Reporting

Any information incident that takes place that is not reportable will still be included in reports circulated to the Strategic Information Governance Steering Groups. 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 in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.