NHS
Surrey Downs
Clinical Commissioning Group

Information Governance and Cyber Security Incident Management and Reporting Procedures

Policy ID	IG10
Version	3.0
Owner	Justin Dix, Governing Body Secretary
Approving Committee	Executive Committee
Date agreed	27th October 2015
Next review date	27th October 2017

Improving care together across Surrey Downs

Summary

This document sets out how Information Governance (IG) and Cyber Security Serious Incidents will be identified, investigated and reported 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.

Version History

Version	Review Date	Name of Reviewer	Ratification Process	Notes
0.1	01/10/2013	NHS South CSU IG Team	Draft	New document
1.0	21/3/2014	NHS South CSU IG Team	Final	Approved by Executive Committee
1.1	31/07/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect recent HSCIC incident reporting guidelines
1.2	28/08/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Minor addition, reference to SE CSU Serious Incident Management Policy and Procedures
2.0	16/09/2015	Interim Information Governance Manager – Surrey Downs CCG	Final	Approved by IG Steering Group
2.1	23/10/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect new CCG SIRO
3.0	27/10/2015	Interim Information Governance Manager – Surrey Downs CCG	Final	SIRO changes approved by Executive Committee
Contributors		Governing Body Secretary, Head of Planning & Performance and, South East CSU Information Governance Principle Associate.		
Audience		All CCG officers, Governing Body members and staff (which includes temporary staff, contractors and seconded staff) and CCG members in their capacity as commissioners.		

Equality Statement

Surrey Downs Clinical Commissioning Group (Surrey Downs CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties or difficulty in understanding this policy, the use of an interpreter will be considered.

Surrey Downs CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Equality Analysis

This policy has been subject to an Equality Analysis, the outcome of which is recorded below.

1. Does the document/guidance affect one group less or more favourably than another on the basis of:			
		Yes, No or N/A	Comments
	Race		
	Ethnic origins (including gypsies and travellers)	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation including lesbian, gay and bisexual people	No	
	Age	No	
	Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the document/guidance likely to be negative?	N/A	
5	If so, can the impact be avoided?	N/A	
6	What alternative is there to achieving the document/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

Contents

1. Introduction

Surrey Downs Clinical Commissioning Group (the CCG) recognises the importance of reporting all incidents as an integral part of its risk identification and risk management strategy. The CCG is committed to improving the quality of service to patients/service users and the safety of staff and members of the public, through the consistent monitoring and review of incidents that result, or had the potential to result in confidentiality breach, damage or other loss.

This document sets out how Information Governance (IG) and Cyber Security Serious Incidents will be identified, investigated and reported 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.

2. Aims and Objectives

This document is designed to achieve the following aims and objectives:

- a standardised approach to the management of IG and cyber security incidents in the CCG;
- to ensure that learning from incidents is an integral part of the organisation's culture;
- analysis of trends which may identify the further need for intervention;
- to improve staff patient/servicer users safety by addressing systematic errors;
- to promote a culture of accountability without 'blame'.

The CCG will investigate and manage all IG and cyber security incidents including Serious Incident Requiring Investigation (SIRI) and provide staff with guidelines on identifying and reporting information incidents including near-misses. In doing so, the aim of the CCG is to promote a positive and non-punitive approach towards incident reporting, as long as there has been no flagrant disregard of the CCG's policies, fraud or gross misconduct.

This document ensures CCG that Caldicott 2 recommendations are addressed and contractual obligations are adhered to with regards to managing, investigating and reporting SIRIs in a standardised and consistent manner.

All IG and Cyber Security Incidents will be investigated, assessed, categorised and reported using the Health and Social Care Information Centre (HSCIC) Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

3. Definition of Terms Used

3.1 Incident

An Incident is defined as an event which has happened to, or occurred with, a patient(s), service-users, staff or visitor(s), the result of which might be harmful or potentially harmful, or which does cause or lead to injury/harm.

3.2 Serious Incident Requiring Investigations (SIRIs)

Serious Incident Requiring Investigations (SIRIs) are incidents which involve actual or potential failure to meet the requirements of the Data Protection Act 1998 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.

3.3 Adverse Event

Any untoward occurrence which can be unfavorable and an unintended outcome associated with an incident.

3.4 A Near Miss

A near miss is an incident that had the potential to cause harm but was prevented. These include cyber, 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.

4. Roles and Responsibilities

4.1 Senior Information Risk Owner (SIRO)

The role of Senior Information Risk Owner (SIRO) is assigned to the Chief Finance Officer (SIRO). The SIRO takes ownership of the organisation's information risks and act as advocate for information risk to the CCG's Governing Body and Audit Committee by providing written advice on the organisation's information security incident reporting and response arrangements.

4.2 Caldicott Guardian

The CCG's Caldicott Guardian is a member of the Governing Body with responsibility for reflecting patients' interests regarding the use of Personal Confidential Data (PCD). The Caldicott Guardian will ensure that they are aware of all incidents including unauthorised disclosure of confidential information and promptly reported to the SIRO for consideration of any necessary actions.

4.3 NHS South East Commissioning Support Unit

In line with the existing contract/Service Level Agreement/s (SLAs) the Information Communication Technology (ICT) department/directorate within South East Commissioning Support Unit (the CSU) is responsible for managing ICT services on

behalf of the CCG and would inform the CCG of any cyber security serious incident 24 hours of become aware.

The CSU Principle Associate for IG is responsible for investigating all incidents 24 hours of becoming aware and informing the SIRO and Caldicott Guardian.

4.4 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are senior members of staff at manager level responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.

4.5 Data Custodians

Data Custodians should ensure that:

- All IG and cyber security incidents are reported to the CSU Principle Associate for IG, their IAO/line manager within 24 hours of becoming aware;
- they consult with their IAOs on incident management procedures;
- they familiarise themselves with the Health and Social Care Information Centre (HSCIC) Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation;
- recognise actual/potential IG or cyber security incidents and take steps to mitigate the risks;
- staff in their directorate/departments follow the CCG's procedures and guidance documents.

Staff Guideline on Identifying and Reporting IG or Cyber Security Incidents can be found in Appendix A

4.6 Information Governance Steering Group (IGSG)

The Information Governance Steering Group (IGSG) is responsible for bringing to the attention of the CCG's Executive and Audit Committees any IG or cyber issues that present a significant risk to the CCG's system or asset.

5. Possible Causes of Incidents

An Incident can be caused by a number of factors such as:

- Negligence or human error.
- Unauthorised or inappropriate access, including processing confidential personal data without a legal basis.
- Loss or theft of information or equipment on which information is stored.
- Systems or equipment failure.
- Accidents.
- Unforeseen circumstances such as fire, flood and other environmental factors

- Inappropriate access, viewing information for purposes other than specified/authorised e.g. an individual browsing record about an ex-partner to find their current address.
- Unauthorised access, using other people's user IDs and passwords.
- Poor physical security.
- Inappropriate access controls allowing unauthorised use.
- Lack of training and awareness.
- Hacking attacks.
- 'Blagging' offences where information is obtained by deception.

5.1 Possible Consequences of an IG Incident including Cyber

The negative impact of an IG incident can vary, for instance it may lead to:

- Embarrassment, damage and harm or distress for individuals.
- Loss or denial of service - this could be a physical service e.g. part of the business, or access to certain information necessary for the organisation to function.
- Possible damage to the integrity of information assets
- Litigation.
- Fraud and financial loss.
- Monetary Penalties of up to £500,000 by the Information Commissioners Office.
- Criminal liability.
- Reputational damage.

Incidents can be categorised by their effect on data subjects:

- confidentiality e.g. unauthorised access, data loss or theft causing an actual or potential breach of confidentiality;
- integrity, e.g. records have been altered without authorisation and are therefore no longer a reliable source of information;
- availability, e.g. records are missing, misfiled, or have been stolen compromising or delaying patient care.

6. Reporting, Managing and Investigating IG and Cyber Incident

On becoming aware of an IG and cyber security incident or potential incident, it should be reported within 24 hours of becoming aware to the CSU Principle Associate for IG using the Incident Reporting Form which can be found in Appendix B.

As part of an initial assessment of an incident, the CSU Principle Associate for IG will liaise with the directorate/department's IAO, Data Custodian and the CCG's SIRO to ensure incidents are correctly investigated, reviewed, graded and reported. The purpose for an incident investigation is to determine the facts concerning the incident and:

- To identify whether any deficiencies in the application of the CCG's policies or procedures and/or the CCG's arrangements for confidentiality and data protection contributed to the incident or;
- Determine whether a human error has occurred, but not to allocate blame;
- Establish what actually happened and what actions need to be taken to prevent reoccurrence.
- Carry out root cause analysis in order to ascertain the cause and to make recommendations

The CSU Principle Associate for IG, responsible IAO and Data Custodian will establish a process so that all facts are looked at and the investigation are be based on establishing what actually happened and what actions need to be taken to prevent reoccurrence, **but not to allocate blame;** However, in some cases the investigation may identify whether any disciplinary processes may need to be invoked.

The decision to notify a data subject will be made by CCG SIRO and the Caldicott Guardian on the grounds of disclosure, including transparency and the ability to protect against harm. This may include theft or blackmail; weighed against the potential harm that may be caused to the subject if notified of the incident.

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.

Please see Appendix C in this document which outlines process for reporting and managing incidents (Flowchart).

6.1 Assessing the severity of IG incidents (IG SIRI)

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

- The numbers of individual data subjects affected;
- sensitivity factors selected;
- the potential for media interest;
- the potential for reputational damage;

Other factors may indicate that a higher rating is necessary, for example the potential for litigation or significant distress or damage to the data subject and other personal data breaches of the Data Protection Act. As more information becomes available, the IG SIRI level will be re-assessed by the CSU Principle Associate for IG or the investigating team

Where the numbers of individuals that are potentially impacted by an incident are unknown, a sensible view of the likely worst case will inform the assessment of the SIRI level. When more accurate information is determined the level will be revised as quickly as possible.

Conversely, when lost data is protected e.g. by appropriate encryption, so that no individual's data can be accessed, then there is no data breach (though there may be clinical safety implications that require the incident to be reported down a different route). When the data is protected but risk of individuals being identified remains an incident and should be reported. The sensitivity factors will reflect that the risk is low.

6.2 Assessing the severity of a Cyber incident (IG SIRI)

The primary factors for assessing the severity level of incidents will be 'criticality and scale' of the incident, for example the potential for impact on confidentiality, integrity or availability. As more information becomes available, post incident investigation the Cyber SIRI level will be re-assessed. Conversely, when targeted systems are protected e.g. by an Intrusion Prevention System, so that no services are affected. The sensitivity factors will reflect that the risk is low.

6.3 Categorising Information Governance incidents including SIRIs

The categorisation of IG incidents including SIRI is determined by the context, scale and sensitivity. An initial assessment of the incident will be made using the Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

6.4 IG and Cyber SIRI Categorisation Review

Incidents which have been categorised as potential level 2 or higher (SIRI) will be investigated and considered in greater detail among members of the IGSG (the group includes SIRO and the Caldicott Guardian) and findings will be reported to the CCG Executive and Audit Committees.

The decision to report a level 2 incident is the responsibility of the SIRO together with the Caldicott Guardian. Once agreed the CSU Principle Associate for IG will ensure that they are reported to the Department of Health (DH), Information Commissioners Office (ICO) and other regulators through the use of the Information Governance Toolkit Incident Reporting Tool. Details of the findings will be recorded by the CSU Principle Associate for IG within 24 hours of becoming aware of the incident.

All parties including DH and ICO whom may have been notified of the incident previously will be updated on the investigation outcome and lessons learnt.

6.5 Reporting to third parties

Where it is suspected that an IG or Cyber security incident has taken place, staff should ensure that the CSU Principle Associate for IG and other key staff are immediately informed as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'.

6.6 Internal Reporting

Any IG or cyber security incidents that takes place that is not recorded as a SIRI will be included in IG reports circulated to the IGSG. These are primarily for awareness and to identify trends in minor incidents.

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

All IG and Cyber Security Incidents will be investigated, assessed, categorised and reported using the Health and Social Care Information Centre (HSCIC) Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

7. Duty of Care and Statutory Obligations

The CCG has in place adequate technical and organisational safeguards, to prevent incidents and have a common law, 'duty of care' and statutory obligation to protect confidential information against such events. Technical safeguards is thought of as physical protection ranging from ICT passwords and firewalls to building security, whilst organisational safeguards are aimed at employees such as ensuring adequate training, policies and procedures are in place.

8. Freedom of Information Requests (FoI)

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

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

9. Action Plans and Audit

The CCG will ensure that:

- There is continuous improvement in confidentiality and data protection and learning outcomes;
- all incidents are audited to ensure any recommendation made have been implemented;
- learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring;

This will ensure that the CCG fully embeds improvements to its information governance structure and demonstrate it is proactive in assessing and preventing information risk.

10. Record keeping

A record of all decisions, actions, and recommendations (e.g. evidence, incident forms and reports) will be kept throughout the investigation and final report. The department's IAO, Data Custodian and the CSU Principle Associate for IG will ensure that:

- All records and documentation are kept in a secure location;
- any Personal Confidential Data (PCD) including medical records, photos or other; evidence is secured at the start of the investigation;
- records are kept in a logical order;
- file notes with dates are kept of all discussions; minutes of all meetings are produced.

11. Procedure Review

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.

12. Training

The CCG recognise the importance of an effective training structure and programme to deliver compliant awareness of confidentiality and data protection and its integration into the day-to-day work and procedures.

All permanent/contract staff will complete the online mandatory training modules within first week of employment, with further training required for managers / team leaders, staff who process personal confidential data, and staff with specific information roles.

13. Dissemination and implementation

This document will be published on the internet/intranet. IAOs and other senior managers are required to ensure that their staff understand its application to their practice.

Awareness of any new content or change in process will be through electronic channels e.g. through email, in staff bulletins etc. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the IGSG.

This document should be read in conjunction with other CCG's related policies. The document applies to incidents that impact on the security and confidentiality of personal information.

14. Related documents policies and procedures

The following documentation relates to the management of information and together underpins the CCGs' Information Governance Assurance Framework. This procedure should be read in conjunction other policies:

- Information Governance Policy
- Confidentiality Policy - Data Protection
- Records Management Policy
- Information Security Policy
- Freedom of Information Policy
- Remote Working and Portable Devices Policy
- HSCIC Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.
- South East CSU Serious Incident Management Policy and Procedures

Appendix A: Staff Guideline on Identifying and Reporting IG or Cyber Security Incidents

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

All incidents (IG or cyber security) must be reported to the CSU Principle Associate for IG, your line manager, Information Asset Owner/Data Custodian within 24 hours of becoming aware. The Information Governance Incident Form must also be completed and forwarded to the CSU Principle Associate for IG.

Examples of what should you report?

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

- Finding a computer printout of Personal Confidential Data (PCD) details laying around;
- Identifying that a fax that was thought to have been sent to a recipient had been received by an unknown recipient or organisation;
- Finding confidential waste in a 'normal' waste bin;
- Losing a mobile computing device with personal information on it;
- Giving information to someone who should not have access to it – verbally, in writing or electronically;
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password;
- Trying to access a secure area using someone else's swipe card or pin number when not authorised to access that area;
- Finding your PC and/or programmes aren't working correctly – potentially because you may have a virus;
- Sending a sensitive e-mail to an unintended recipient or 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to the organisation.

What happens next?

The CSU Principle Associate for IG and your line manager/IAO will investigate the incident and may wish to speak to you directly as things progress.

Appendix B - IG Incident Reporting Form

INFORMATION GOVERNANCE INCIDENT REPORTING FORM

Section 1 – Incident Details to be completed by person reporting			
Date of incident		**Incident Number** *(completed by IG)*	
Date became aware of incident		**Person reporting the incident**	
Date reported to CSU Principle Associate for IG, manager or IAO		**Responsible Information Asset Owner (IAO)**	
Incident Details			
Number of records/patients involved		**Types of Personal Confidential Data involved (e.g. name, NHS Number)**	
Initial Actions taken			

Section 2 – Incident Grading *to be completed by CSU Principle Associate for IG*				
Initial SIRI grading		**Date reported to CG/SIRO**		**Date reported to DH/ICO**
Date reported to CG/SIRO				
Date reported to DH/ICO				

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

Section 4 – Actions/Learning *to be completed by investigating manager*			
Action	**Responsible person**	**Date for completion**	**Completed date**
1.			
2.			
3.			
Date RCA Investigation Report Completed (Level 2 SIRI only)			
Date incident closed by CG/SIRO			

Once completed, this form should be given or sent (NHSmail to NHSmail) to the CSU Principle Associate for IG to assist in investigation.

Appendix C: Incident Management and Reporting Flowchart