Information Governance Incident Reporting Policy

Version:	4.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Date ratified:	29th November 2017
Name of originator /author (s):	GMSS IG Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	January 2018
Review date:	December 2019
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Information Governance Incident Reporting Policy CCG.GOV.020.4.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS IG Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff; Safe Transfer of Information Policy (safe haven).
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Information Governance Operational Group
Published by	NHS Bury Clinical Commissioning Group 21 Silver Street Bury BL9 0EN Main Telephone Number: 0161 762 5000
Copies of this document are available from	CCG Corporate Office CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	15th February 2016
3.1 = policy once reviewed	GMSS IG Team	8th November 2017
4.0 = policy once ratified	NHS Bury Clinical Commissioning Group Information Governance Operational Group	29th November 2017

Information Governance Incident Reporting Policy

Table of Contents

1. Introduction

1.1 NHS Bury Clinical Commissioning Group (hereafter referred to as the CCG) is committed to a programme of effective risk and incident management. The CCG has a responsibility to monitor all Information Governance (IG) related incidents that occur that may breach security and / or confidentiality of personal information.

1.2 Due to the increase in IG and Cyber Security incidents, NHS Digital have introduced documentation called the "Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" and on-line reporting via the IG Toolkit. The guidance covers reporting arrangements and actions that need to be taken when an IG / cyber security and / or IG Serious Incident Requiring Investigation (SIRI) occurs. It also contains guidance regarding scoring an incident based on numbers of individuals affected together with other sensitivity factors. It is important as it defines when an incident becomes an IG SIRI. For a reported IG incident to become an IG SIRI, a level 2 score has been attained. This then has an effect on how the incident is reported which the NHS Digital checklist outlines and the CCG must therefore ensure the correct process is followed.

1.3 This document details the IG Incident Reporting process that brings together the various tools that have to be completed when reporting an IG incident, and / or a Cyber Security incident, including when either such incidents are graded as a SIRI. These reporting processes include the following:

- Local CCG reporting
- Information Governance Toolkit IG Incident Reporting Tool (for IG SIRI's and Cyber Security SIRI's)

1.4 The IG Incident Reporting Policy and enclosed Procedure is required in order for the CCG to meet its full responsibilities for reporting and managing IG and Cyber Security incidents.

1.5 This procedure applies to all staff who work for or on behalf of the CCG. Third party contractors and others (e.g. business partners, including other public sector bodies, volunteers, commercial service providers) who may potentially use the CCG's facilities must be aware of the importance of reporting perceived or actual events.

2. Definitions

2.1 Information Governance Related Incident

An IG or Information Security related incident relates to breaches of security and / or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street.

It could also be any event that has resulted or could result in:

- The integrity of an information system or data being put at risk
- The availability of an information system or information being put at risk
- An adverse impact, for example, embarrassment to the NHS, threat to personal safety or privacy, legal obligation or penalty, financial loss and / or disruption of activities

Some more common areas of incidents are listed below but this list is not exhaustive and should be used as guidance only. If there is any doubt as to what you have found being an incident it is best to report it to the relevant personnel for this decision.

Breach of security

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media, for example, cd's, memory sticks / USB sticks due to crime or an individual's carelessness
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident

Breach of confidentiality

- Finding a computer printout with personal identifiable data on it in a public area
- Finding any paper records about a patient / member of staff or business of the organisation in any location outside secured CCG premises
- Being able to view patient records in an employee's car
- Discussing patient and / or staff personal information with someone else in an open area where the conversation can be overheard
- A fax being received by the incorrect recipient

2.2 Information Governance Serious Incident Requiring Investigation (SIRI)

There is no simple definition of a serious IG incident. What may at first appear to be of minor importance may, on further investigation, be found to be serious or vice versa. As a general guide, the scope of an IG SIRI is as follows:

- The type of incident which will typically breach one of the principles within the Data Protection Act 1998 and Article 6 of the General Data Protection Reform (GDPR) and / or one of the principles of the Common Law Duty of Confidence;
- Incidents of unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy;
- Personal data breaches which could lead to identity fraud or have other significant impact on individuals;
- Incidents irrespective of the media involved, which could include both electronic media and paper records relating to staff and service users.

2.3 Information Governance Cyber Serious Incident Reporting Investigation (SIR)

There are many possible definitions of what a Cyber incident is. For the purposes of reporting a Cyber-related incident, it is defined as anything that could (or has) compromised information assets within Cyberspace. 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.

3. Roles and Responsibilities

3.1 Chief Operating Officer

Has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support incident reporting for IG and cyber security incidents.

3.2 Data Protection Officer (DPO)

This is a new role required as per the General Data Protection Regulations (GDPR). The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other current data protection laws. They are required to monitor compliance with the GDPR and current data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

3.3 Caldicott Guardian

To review and provide feedback regarding an incident where this relates to patient data. This may involve decision making about informing patients regarding an incident or not if this would deem to cause them harm / distress.

3.4 Senior Information Risk Owner (SIRO)

To review IG incidents and report IG and Information Security issues to the Senior Management Team and ensure that any external reporting of the incident if required is undertaken

3.5 Greater Manchester Shared Services (GMSS) Information Governance Team

- To co-ordinate and investigate reported IG incidents, maintain the CCG IG Incident Logbook, make recommendations and act on lessons learnt.

- To liaise with the CCG IG Lead, CCG SIRO and Greater Manchester Shared Services (GMSS) IT Services / Information Security Lead and CCG IT Manager as appropriate pertaining to cyber security incidents.
- To escalate incidents to the CCG IG Lead in order to inform the SIRO, and / or Caldicott Guardian as appropriate.

- To grade the incident and report it where necessary on the IG Toolkit Incident Reporting Tool and local CCG IG Incident Logbook.

3.6 CCG IT Manager

- To work with IT to investigate the Cyber Security incident, make recommendations and act on lessons learnt.
- To liaise with IG Teams as appropriate especially regarding reporting.
- To inform the Senior Information Risk Owner, and/or Caldicott Guardian as appropriate.
- To grade the incident, and ensure that where necessary it is reported on the IG Incident Reporting Tool – Cyber Security section (through the IG Team).

3.7 GMSS IT Services / IT Security Manager

- For IG Incidents, advise CCG staff to report the incident to their CCG IG Lead and GMSS IG Team.
- To alert Information Security Lead and CCG IT Manager when a potential or actual cyber security incident is reported.
- To alert the GMSS IG Team when a potential or actual cyber security incident is reported.

3.8 Information Security Lead

- To work with IT Service Team / IT Security Manager / CCG IT Manager to investigate cyber security incidents, make recommendations and act on lessons learnt.
- To liaise with the GMSS IG Team as appropriate especially regarding reporting.
- To inform the Senior Information Risk Owner / deputy and / or Caldicott Guardian / deputy as appropriate.
- To grade the incident, and ensure that where necessary it is reported on the IG Incident Reporting Tool – Cyber Section, local IG / IG Cyber Security Incident Logbook.

4. Information Governance Reporting and Management Process

4.1 The CCG will continue to utilise its own internal incident reporting procedure for the management of incidents. All incidents must be reported initially to the CCG IG Lead and GMSS IG Team. If this is identified as an IG incident the GMSS IG Team will log this on the CCG IG Incident Logbook and assess the incident in the light of GDPR and according to the NHS Digital checklist to grade it (Level 1 or below or Level 2 IG SIRI).

4.2 The NHS Digital "Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" is at Appendix 1. This sets out how to grade the severity and sensitivity of an incident.

4.3 All staff are encouraged to report IG 'near misses' as well as actual incidents, so that we can take the opportunity to identify and disseminate any 'lessons learnt'.

4.4 **Incidents Graded Level 1 or Below**

4.4.1 The CCG utilises its own internal incident reporting procedure for the management of Information Governance incidents graded Level 1 or below – refer to Figure 1 for IG Incident Reporting Process Flowchart.

4.4.2 The incident is graded using the NHS Digital grading tool in the "Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" – refer to Appendix 1.

4.5 **Incidents Graded Level 2 or Above (IG SIRI)**

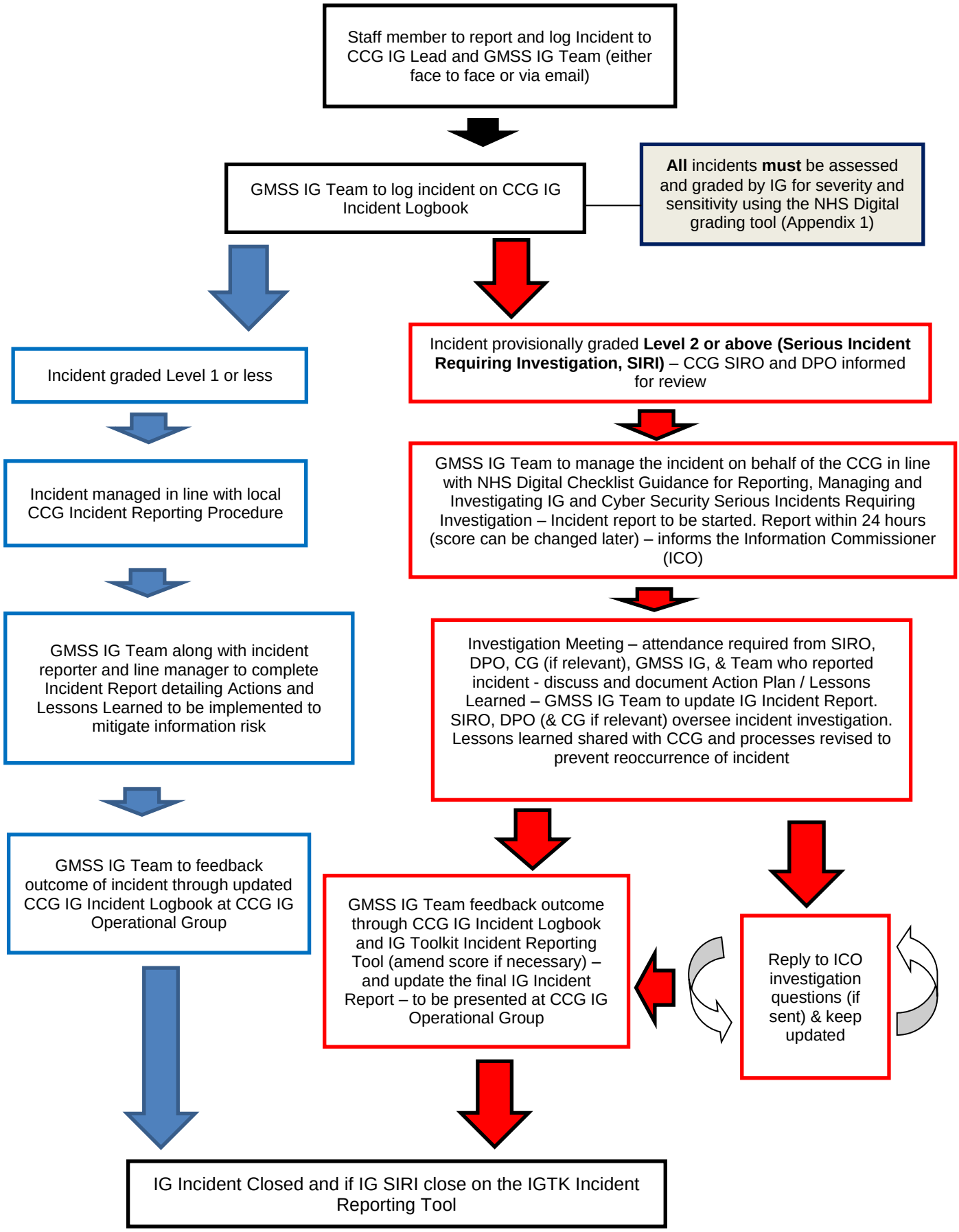
4.5.1 GMSS IG Team will grade the incident utilising the CCG's internal incident reporting procedure as stated above in 4.4.1 and 4.4.2.

4.5.2 Incidents initially graded at Level 2 or above (IG SIRI) are immediately notified to the CCG's SIRO, Data Protection Officer / or if appropriate the Caldicott Guardian with a view to them confirming the score.

4.5.3 Once approval has been received from the SIRO, the GMSS IG Team will report Level 2 incidents on the IG Toolkit Incident Reporting Tool on behalf of the CCG. In order to do this GMSS IG Team will complete Information Governance Incident Form for IG SIRIs and use this to report on to the IG Toolkit. This must be sent within 24 hours of the incident being reported.

4.6 The flowchart (Figure 1) sets out the overall process for reporting, managing and investigating Information Governance incidents for the CCG for incidents scored level 1 and below and level 2 and above (IG SIRI's).

Figure 1 - IG Incident Reporting Flowchart



5. Cyber Security Incident Reporting and Management Process

5.1 Figure 2 outlines the incident reporting process for cyber security incidents. In most cases, staff will report such incidents via the GMSS IT helpdesk as they will tend to be IT related such as PC / laptop not working correctly, phishing emails or denial of access to a system or webpage. Due to this, the GMSS IG Team are linking with IT services and the GMSS IT Security Manager to capture such recorded incidents. They will be identified through the use of key words and confirmed whether they are cyber security incidents. The notification of this will be forwarded to the IG Team who will then liaise with IT Security Manager, Information Security Lead and CCG IT Manager to assess its severity and sensitivity and graded as per the NHS Digital checklist. The incident is logged on the Cyber Security Incident Logbook and updated throughout the investigation process.

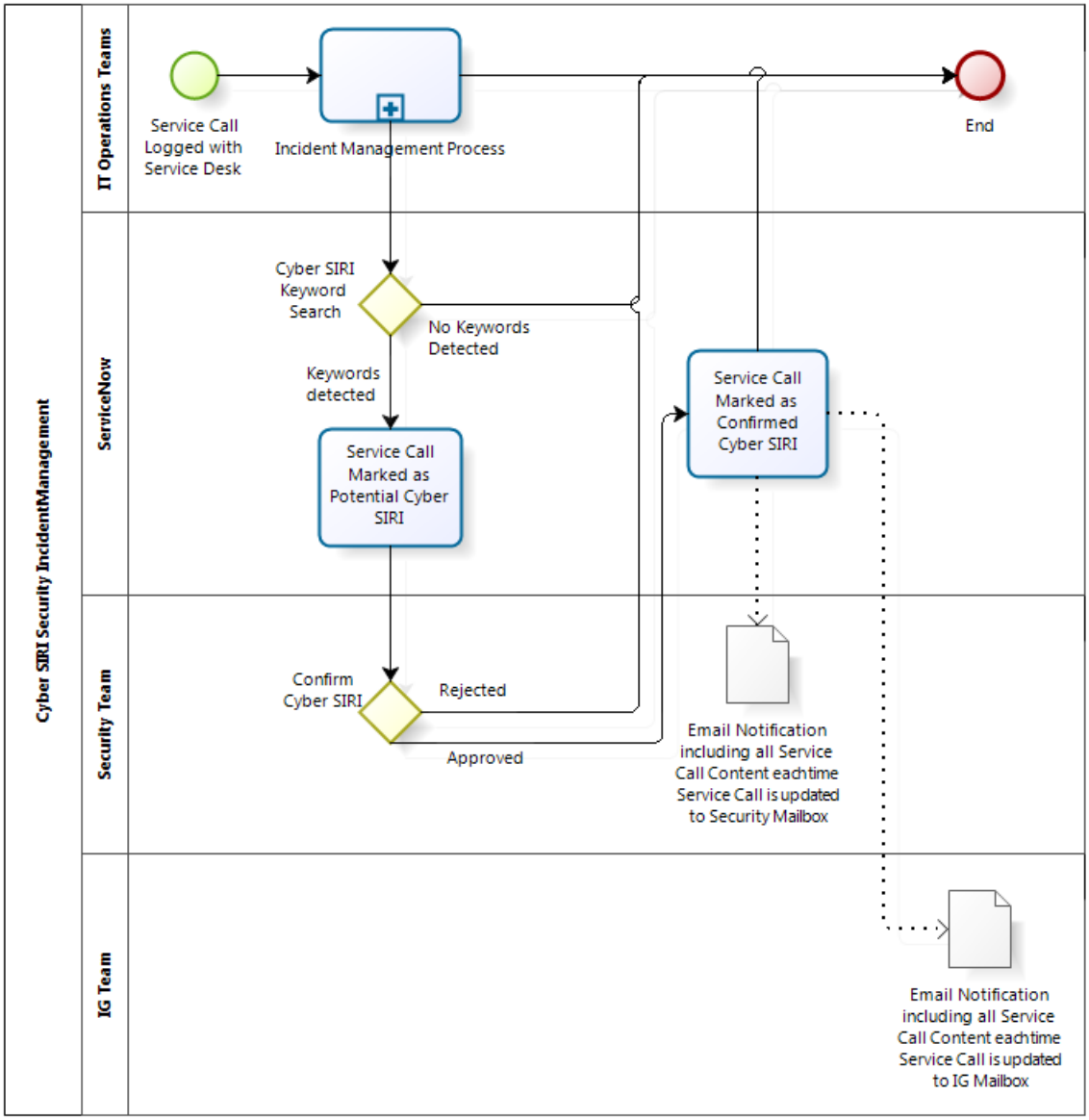
5.2 Incidents may also be captured via the CCG's incident policy and procedure. In these cases, the GMSS IG Team will liaise with IT Security Manager, Information Security Lead and CCG IT Manager to inform them and follow the same process as above.

5.3 For Cyber Security incidents, it is vital that the person responsible for any operational response, typically the CCG IT Manager is notified and the SIRO kept up to date.

5.4 Cyber security incidents scored Level 2 and above must be logged on the IG Toolkit Incident Reporting Tool. This then triggers an automated notification email to the Department of Health and NHS Digital. **Please note the ICO are not informed of cyber incidents scored level 2 and above**.

Figure 2: Cyber Security Incident Reporting Process

Step One – Notification from IT Services / GMSS IT Security Manager



Step Two – Investigation of Cyber Security Incidents

GMSS IT Team will forward email notification to GMSS IG Team who log incident on CCG Cyber Security Incident Logbook & inform the Information Security Lead, CCG IT Manager and IT Tech Support

Follow IG incident investigation process as per Figure 1 liaising with GMSS IT Security Manager / Information Security Lead / CCG IT Manager – note the ICO notification and response is excluded

6. Reporting

6.1 Reporting in the Annual Governance Statement / Statement of Internal Control

6.1.1 Incidents classified as IG SIRI's level 2 and above will trigger an automated notification email to the Department of Health, NHS Digital and the Information Commissioner's Office, in the first instance, and to other regulators as appropriate.

6.1.2 These incidents need to be detailed individually in the annual report / governance statement / Statement of Internal Control as per Table 1 below. Notes to assist in completion of the table can be found in the NHS Digital checklist (Appendix 1).

Table 1 – Summary Table of IG SIRI's

SUMMARY OF SERIOUS UNTOWARD INCIDENTS INVOLVING PERSONAL DATA AS REPORTED TO THE INFORMATION COMMISSIONERS OFFICE [from year to year]				
Date of Incident (month)	**Nature of Incident**	**Nature of data involved**	**Number of people potentially affected**	**Notification Steps**
Jan 2017	*Loss of inadequately protected electronic storage device*	*Forename, Surname, address, NHS number, Medical Details*	*1,500*	*Individuals notified by letter / post*
Further action on information risk	*The CCG will continue to monitor and assess its information risks, in lights of the events noted above, in order to identify and address any weaknesses and ensure continuous improvement of its systems.* *The member of staff responsible for this incident has been dismissed.*			

6.2 A summary of IG incidents can also be published, if the CCG wish to, in annual reports / governance statement using the summary table as highlighted in Table 2:

Table 2 – Annual Summary of IG reported incidents below Level 1

SUMMARY OF OTHER PERSONAL DATA RELATED INCIDENTS IN [insert year to year]		
Category	**Nature of Incident**	**Total**
A	Corruption or inability to recover electronic data	
B	Disclosed in Error	
C	Lost in Transit	
D	Lost or stolen hardware	
E	Lost or stolen paperwork	
F	Non-secure Disposal – hardware	
G	Non-secure Disposal – paperwork	
H	Uploaded to website in error	
I	Technical security failing (including hacking)	
J	Unauthorised access / disclosure	
K	Other	

Please note incidents designated as “pure cyber” are not required to be included in the annual reports and Statement of Internal Control at this time. However cyber incidents that are also IG SIRI’s should be included.

6.3 Reporting to the CCG’s Senior Management Team

6.3.1 IG incidents are reported routinely at the CCG’s IG Operational Group Meeting who report to the CCG’s Audit Committee via the IG Key Statistics Report. Lessons learned are discussed and actioned when necessary.

7. Closure and Lessons Learned from the IG Incident

7.1 It is essential that action is taken to help to minimise the risk of IG incidents re-occurring in the future. Therefore, all IG incidents that are reported will be logged and any associated lessons learned will be fed back to staff. This may be communicated via email / staff briefings / team meetings.

7.2 Staff involved with an IG incident should consider with their line manager if additional training and support is needed. Additional training and further information can be gained from NHS Digital Information Governance Training Package, speak contact the GMSS IG Team for further information at **gmcsu.ig@nhs.net**.

8. Training and Awareness

8.1 Line managers are responsible for ensuring that all staff, particularly new staff, temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information. They are also responsible for monitoring compliance with this guideline e.g. undertake ad hoc audits to check for inappropriate disclosures, records left out, abuse of passwords etc.

8.2 Staff are responsible for maintaining the confidentiality of all personal and corporate information gained during their employment with the CCG and this extends after they have left the employ of the CCG.

8.3 Individual staff members are personally responsible for any decision to pass on information that they may make.

8.4 All staff are responsible for adhering to the Caldicott Principles, the Data Protection Act, General Data Protection Regulation and the Confidentiality Code of Conduct.

8.5 Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy /strategy and procedure manuals; line manager;
- specific training course;
- other communication methods (e.g. team brief/team meetings); staff Intranet;

8.6 All staff are mandated to undertake Information Governance training on an annual basis. This training should be provided within the first year of employment and then updated as appropriate in accordance with the Information Governance policy.

9. Monitoring and review

9.1 This procedure will be reviewed on a yearly basis, and in accordance with the following on an as and when required basis:

- legislative changes; good practice guidance; case law;
- significant incidents reported; new vulnerabilities; and
- changes to organisational infrastructure.

10. Legislation and related documents

10.1 A set of procedural document manuals will be available via the CCG's website.

10.2 Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff Intranet.

10.3 A number of other policies are related to this policy and all employees should be aware of the full range below:

- Information Governance Framework
- Information Governance Policy
- Data Protection and Confidentiality Policy
- Information Security Policy
- Acceptable Use Policy
- Records Management Policy
- Information Risk Policy
- Confidentiality Audit Policy
- Information Security Policy

10.4 Acts Covered Under Policy

- General Data Protection Regulation
- Data Protection Act 1998

Appendix 1 - Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Please click on the link below to view:

https://www.igt. - NHS Digital.gov.uk/resources/ - NHS DIGITAL%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf