NHS
Bury
Clinical Commissioning Group

Information Governance Incident Reporting Policy

Version:	5.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Steering Group
Date ratified:	18 June 2021
Name of originator /author (s):	GMSS IG Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	July 2021
Review date:	March 2023
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.020.5.0
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 Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 3100
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
4.1 = Review	NHS Bury Clinical Commissioning Group IG Team	15th June 2021
5.0 = policy once ratified	NHS Bury Clinical Commissioning Group Information Governance Operational Group	18th June 2021

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
- Data protection and Security 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 The following definitions apply in respect to this policy:

- Information Governance Related Incident

2.2 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.

2.3 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

2.4 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**

2.5 A breach of security can be :

- 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**

2.6 A breach of confidentiality could include

- 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 locations and / or 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;
- An e-mail being received by the incorrect recipient.

- **Information Governance Serious Incident Requiring Investigation (SIRI)**

2.7 There is no simple definition of a serious IG incident as 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:

- A breach one of the principles within the Data Protection Act 2018 and Article 6 of the UK General Data Protection Regulation (UK 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;
- A Personal data breaches which could lead to identity fraud or have other significant impact on individuals;
- Any incident, irrespective of the media involved, which could include both electronic media and paper records relating to staff and service users.

- **Information Governance Cyber Serious Incident Reporting Investigation (SIRI)**

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

2.9 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 The following roles and responsibilities apply in respect to this policy:

- **Accountable Officer (AO)**

3.2 The AO 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.

- **Data Protection Officer (DPO)**

3.3 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. The DPO monitors 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.

3.4 In addition, the DPO is required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

- **Caldicott Guardian**

3.5 The Caldicott Guardian reviews and provides feedback regarding all incidents reported relating 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.

- **Senior Information Risk Owner (SIRO)**

3.6 The SIRO reviews IG incidents and reports IG and Information Security issues to the Executive Team. They also ensure that any external reporting of the incident if required is undertaken

- **Information Governance manager**

3.7 The IG manager is responsible for:

- co-ordinating and investigating reported IG incidents, ensuring all reported incidents are fully updated on Datix and making recommendations to act on lessons learnt;
- liaising with the DPO, SIRO, CCG Head of IT and Greater Manchester Shared Services (GMSS) IT Services / Information Security Lead as

appropriate pertaining to cyber security incidents;
- escalating incidents to the DPO in order to inform the SIRO, and / or Caldicott Guardian as appropriate;
- preparing a monthly IG breach report for the Information Governance Steering Group; and
- grading the incident and report it where necessary on the Data protection and Security Toolkit Incident Reporting Tool.

- **Head of IT**

3.8 The Head of IT is required to:

- work with GMSS IT to investigate all Cyber Security incidents, making recommendations and act on lessons learnt;
- liaising with the IG Manager as appropriate especially regarding reporting;
- informing the Senior Information Risk Owner and/or Caldicott Guardian of any cyber security incidents as appropriate; and
- supporting the grading of cyber security incidents, ensuring that where necessary it is reported on the Data Protection and Security Incident Reporting Tool (Cyber Security section) in collaboration with the IG Manager.

- **GMSS IT Services**

3.9 Bury CCG commissioning IT and IT security from Greater Manchester Shared Service (GMSS). Under this arrangements, the GMSS IT service and IT security manager are responsible for the following actions in relation to incident reporting:

- On receipt of any notification from CCG staff of an incident, advising of the need to report the incident to the CCG IG Manager;
- Alerting the CCG Head of IT and the CCG IG Manager when a potential or actual cyber security incident is reported;

- **GMSS Information Security Manager**

3.10 The Information Security manager is required to

- work with IT Service Team and CCG Head of IT to investigate cyber security incidents, make recommendations and act on lessons learnt;
- liaising with the CCG IG Manager as appropriate especially regarding reporting and onward escalation to the Senior Information Risk Owner and / or Caldicott Guardian of any cyber security incidents as appropriate.

- **All staff**

3.11 All staff are required to report incidents that they are aware of, whether it has arisen from their actions or they have become aware of the incident in the operation of their day-to-day activities.

4. Information Governance Reporting and Management Process

4.1 The CCG recognisies that it can only improve its information governance practice if it understands when things go wrong.

4.2 It is important that all incidents are reported whether considered minor in nature or impact or whether this is a ‘near miss’.

4.3 To support proactive incident reporting, the CCG supports a culture of fair blame, recognising that when things go wrong, this is often due to poor systems and processes rather than by the person or persons involved.

4.4 The CCG will use Datix as the system of choice for the recording and management of incidents.

4.5 All incidents, including 'near misses', must be recorded at the earliest opportunity, and as a minimum within 24 hours, onto the Datix system and notified to the IG Manager who will assess the information provided to determine the grading of the incident, using the NHS Digital "Checklist for Reporting, Managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation" as set out at Appendix 1 to determine the grading, based on the severity and sensitivity of an incident.

4.6 All incidents, irrespective of grading will be investigated to support continuous improvement through the identification and dissemination of any 'lessons learnt' as set out in the flowchart at Appendix 2.

- **Incidents Graded Level 1 or Below**

4.7 For all incidents graded as a Level 1 or below, the CCG will follow an internal reporting procedure as set out in the Figure 1 for IG Incident Reporting Process Flowchart.

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

4.8 All 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.

4.9 Once approval has been received from the SIRO, the CCG IG Manager will report Level 2 incidents on the Data Protection and Security Toolkit Incident Reporting Tool. The IG Manager will liaise with the incident reported to ensure all the relevant information has been provided in Datix within 24 hours of the incident being reported.

5. Cyber Security Incident Reporting and Management Process

5.1 Incident reporting for cyber security incidents is set out at Appendix 3.

5.2 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. GMSS IT will advise CCG colleagues to also report the incident through the CCG's Incident Reporting arrangements.

5.3 The GMSS IG Team will link with IT services and the GMSS IT Security Manager to capture such recorded incidents and will ensure any and all relevant information is notified to the CCG IG Manager.

5.4 Once a cyber security incident is confirmed, notification will be forwarded to the GMSS IG Team who will then liaise with IT Security Manager, Information Security Lead and CCG IT Manager to assess its severity and sensitivity and will grade the incident as per the NHS Digital checklist. The incident will be updated through the GMSS arrangements and also on Datix throughout the investigation process.

5.2 Incidents may also be captured via the CCG's Datix system for incident reporting. In these cases, the IG manager will liaise with the CCG's Head of IT and the GMSS IT Security 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 Data Protection and Security 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**.

6. Reporting

6.1 All incidents reported will be notified to the Information Governance steering Group on a monthly basis.

6.2 In addition, the CCG is required to report the Annual report and Annual Governance Statement the number of data breaches in the reporting period and of those, the number of Incidents classified as IG SIRI's level 2

6.4 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.

6.5 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**

<table>
<tr><td colspan="5">SUMMARY OF SERIOUS UNTOWARD INCIDENTS INVOLVING PERSONAL DATA AS REPORTED TO THE INFORMATION COMMISSIONERS OFFICE [from year to year]</td></tr>
<tr><td>Date of Incident (month)</td><td>Nature of Incident</td><td>Nature of data involved</td><td>Number of people potentially affected</td><td>Notification Steps</td></tr>
<tr><td><i>Jan 2017</i></td><td><i>Loss of inadequately protected electronic storage device</i></td><td><i>Forename, Surname, address, NHS number,</i></td><td><i>1,500</i></td><td><i>Individuals notified by letter / post</i></td></tr>
</table>

		Medical Details		
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 will also be published in the annual reports / governance statement following the format as set out below, subject to any changed in the Group Accounting manual (GAM)

- **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	

6.3 Incidents designated as “pure cyber” incidents are not required to be included in the annual report, however cyber incidents that are also IG SIRI’s will be included.

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, following investigation and review through the IGSG, be notified to colleagues in respect to any associated lessons learned. This may be communicated via email / staff briefings / team meetings.

7.2 Part of the lessons learned will consider any additional training that is required, whether on an individual, team or organisational level. Additional training and further information can be gained from NHS Digital Information Governance Training Package. For further information, please speak to the IG Manager or contact the corporate office for further information at **buccg.corporateoffice@nhs.net**

8. Training and Awareness

8.1 All staff will be supported to ensure adherence to this policy through advice, guidance and training on the Datix system.

9. Monitoring and review

9.1 This procedure will be reviewed on a two-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

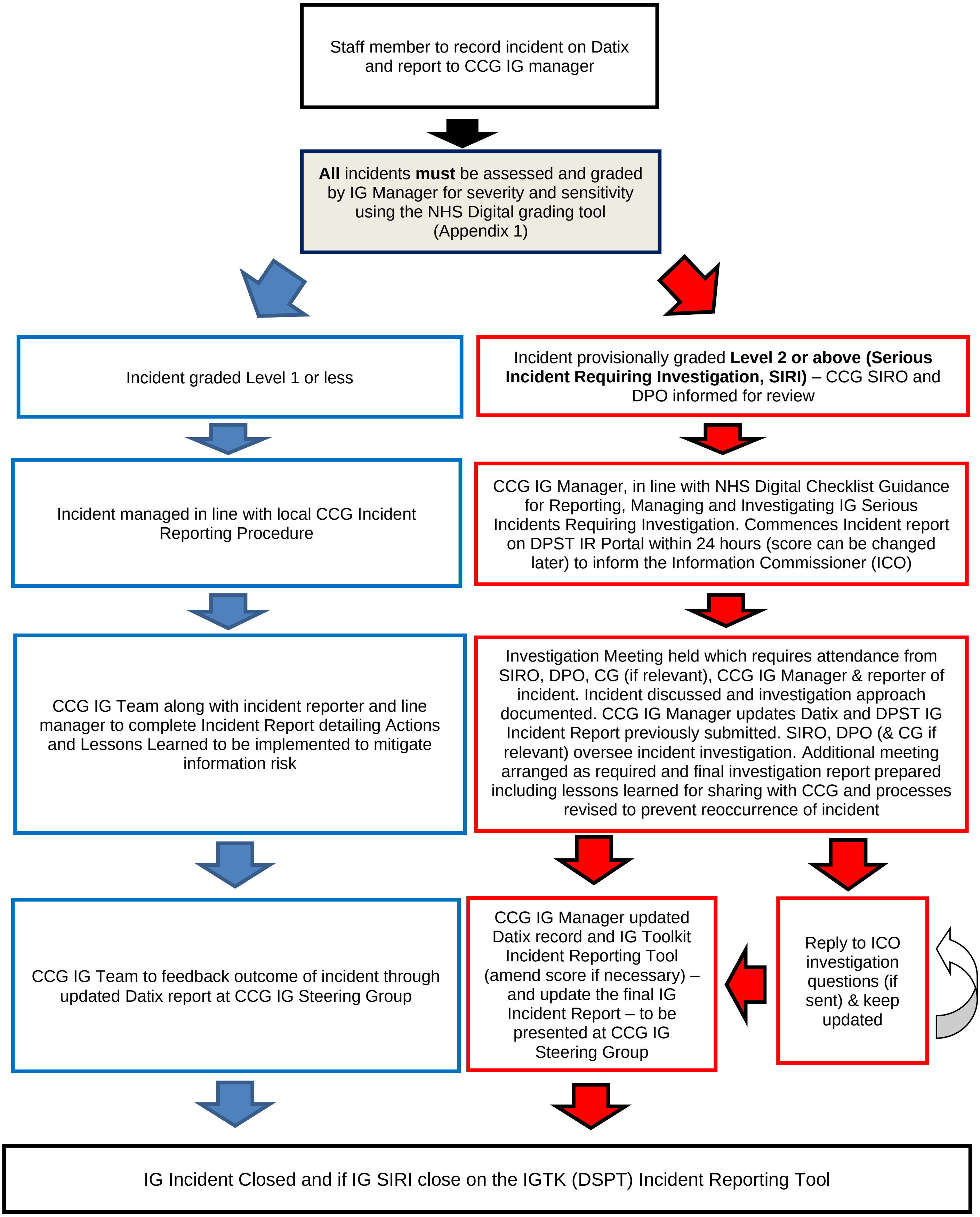
- UK General Data Protection Regulation
- Data Protection Act 1998

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

Appendix 2 : IG Incident Reporting Flowchart



Staff member to record incident on Datix and report to CCG IG manager

All incidents **must** be assessed and graded by IG Manager for severity and sensitivity using the NHS Digital grading tool (Appendix 1)

Incident graded Level 1 or less

Incident managed in line with local CCG Incident Reporting Procedure

CCG IG Team along with incident reporter and line manager to complete Incident Report detailing Actions and Lessons Learned to be implemented to mitigate information risk

CCG IG Team to feedback outcome of incident through updated Datix report at CCG IG Steering Group

Incident provisionally graded **Level 2 or above (Serious Incident Requiring Investigation, SIRI)** – CCG SIRO and DPO informed for review

CCG IG Manager, in line with NHS Digital Checklist Guidance for Reporting, Managing and Investigating IG Serious Incidents Requiring Investigation. Commences Incident report on DPST IR Portal within 24 hours (score can be changed later) to inform the Information Commissioner (ICO)

Investigation Meeting held which requires attendance from SIRO, DPO, CG (if relevant), CCG IG Manager & reporter of incident. Incident discussed and investigation approach documented. CCG IG Manager updates Datix and DPST IG Incident Report previously submitted. SIRO, DPO (& CG if relevant) oversee incident investigation. Additional meeting arranged as required and final investigation report prepared including lessons learned for sharing with CCG and processes revised to prevent reoccurrence of incident

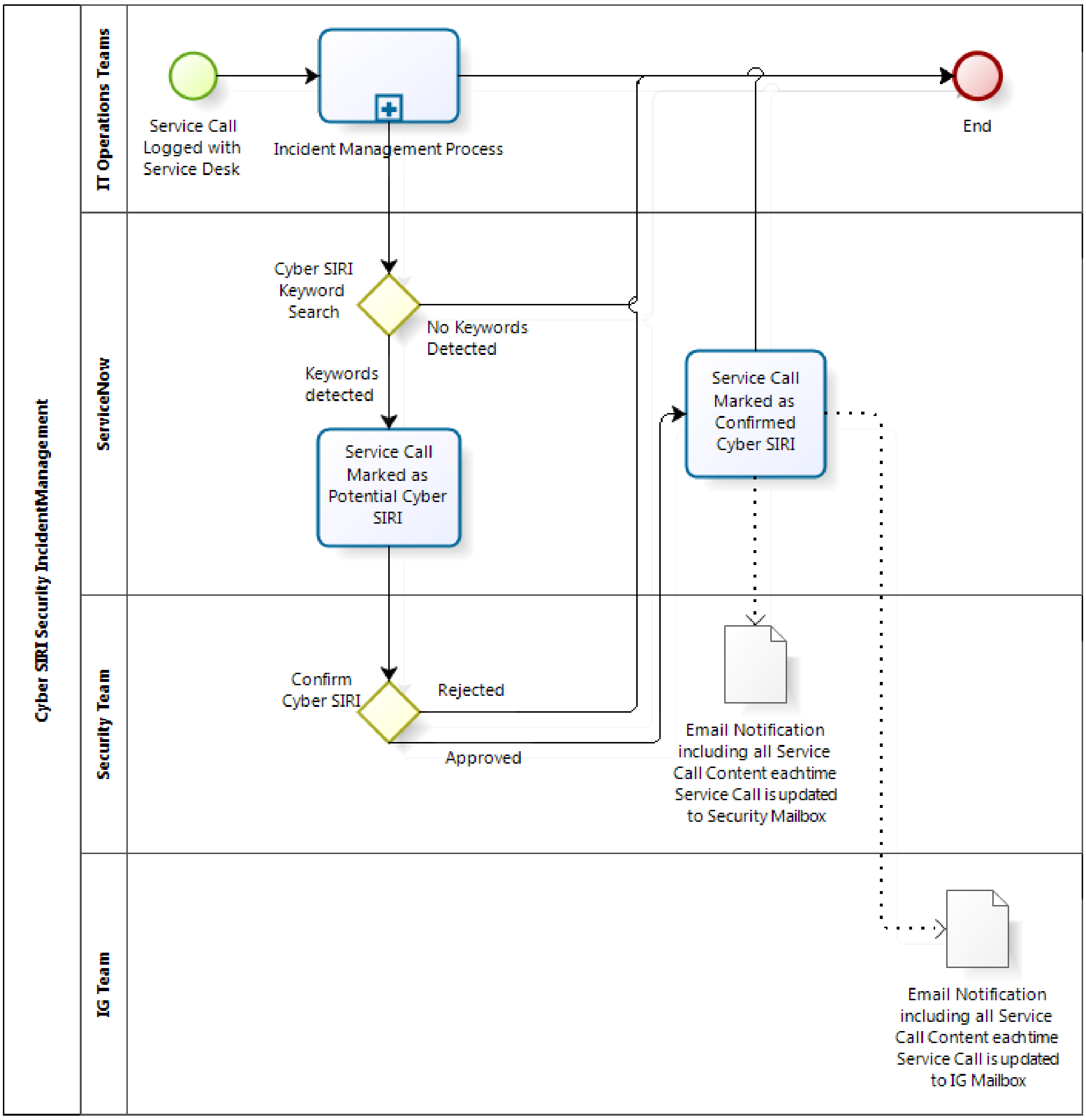
CCG IG Manager updated Datix record and IG Toolkit Incident Reporting Tool (amend score if necessary) – and update the final IG Incident Report – to be presented at CCG IG Steering Group

Reply to ICO investigation questions (if sent) & keep updated

IG Incident Closed and if IG SIRI close on the IGTK (DSPT) Incident Reporting Tool

Appendix 3 : Cyber Security Incident Reporting Process

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


Cyber SIRI Security IncidentManagement
IT Operations Teams
ServiceNow
Security Team
IG Team
Service Call Logged with Service Desk
Incident Management Process
End
Cyber SIRI Keyword Search
No Keywords Detected
Keywords detected
Service Call Marked as Potential Cyber SIRI
Service Call Marked as Confirmed Cyber SIRI
Confirm Cyber SIRI
Rejected
Approved
Email Notification including all Service Call Content eachtime Service Call is updated to Security Mailbox
Email Notification including all Service Call Content eachtime Service Call is updated to IG Mailbox

- **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