Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents (IG SIRI)	
Standard Operating Procedure (SOP) – Version 2	
Prepared by: Helen Thorn	
Presented to: Management of Information Group	**Date:** 7 September 2015
Ratified by: Management of Information Group	**Date:** 9 September 2015
Due for review:	September 2016
Relating to policies: Incident Policy Information Management Policy Data Protection Policy	

1. Purpose of this document:

1.1 The document outlines the reporting arrangements and describes the actions that need to be taken in terms of communication and follow up when a breach of confidentiality (IG SIRI or Cyber SIRI) occurs.

1.2 This document applies to all staff, contractors and volunteers working within the Trust. The document should be read in conjunction with the Data Protection Policy, Incident Reporting Policy and guidance for the use of Datix.

2. Scope of this SOP: - *Who does it relate too and who it is aimed at.*

This document relates to all staff, contractors and volunteers working within Torbay and Southern Devon Health and Care NHS Trust.

3. Competencies required

None identified

4. Roles and Responsibilities

4.1 Information Governance is responsible for:

- Scoring all IG SIRIs reporting either directly or through the Datix system;
- Reporting all reportable or potentially reportable IG SIRIs to the Caldicott Guardian and the SIRO;
- To complete the IG SIRIs reporting tool;
- To provide regular reports and feedback to the appropriate bodies;
- To ensure that the appropriate level of investigation is undertaken and the learning and outcomes are shared widely within the Trust.
- To provide collated information for the annual report and annual governance statement.

- To regularly provide information to the Management of Information Group on breaches of confidentiality
- To close down all Datix reports for breaches of confidentiality.

4.2 Service Leads / Managers are responsible to:

- Undertake a local investigation if incident is level 0 (as identified by Datix) and should complete the Datix entry, in particular the learning and outcome section.
- Contact the Information Governance Team if the incident is level 1 or 2 and work with them to carry out a full investigation.

4.3 All Staff should inform their line manager of any incidents as soon as possible and report such events through the Trust's reporting system. All staff must ensure they are up-to-date with all training they are required to undertake and familiarise themselves with the Trust's information Governance policies and procedures available from the public website.

5 Reporting an IG SIRI Incidents

5.1 All breaches of confidentiality/data loss should be logged immediately through the Datix incident reporting system, with the name of a manager that can provide additional information.

5.2 All incidents should be scored within 2 days of entering the Datix System, and confirmed by the Information Governance Team.

5.3 All potential level 2 incidents should be logged through the IG Incident Report Tool within 24 hours and updated within 5 working days by the Information Governance Team. The incident should be closed with the outcome of investigation within 4-6 weeks.

5.4 Incidents will be reported on a regular basis through the Management of Information Group up to Board level.

5.5 For information and advice regarding the reporting of incidents and near misses, please contact the Professional Practice Team directly 01803 210585 / incidentreporting.t-sd@nhs.net.

5.6 For advice and guidance regarding breaches of confidentiality/data loss, please refer to the Information Governance pages on iCare or contact the Information Governance Team directly (01803) 210507 / t-sd.infogov@nhs.net.

6. Investigating an IG SIRI Incidents

6.1 Level 0 incidents

Local investigation to be undertaken by the manager and the outcome and learning put into the Datix system within 5 working days. Appendix 2 provides details of what should be covered in such an incident.

6.2 Level 1 incidents

Information Governance Team will seek further information from the manager to ascertain the level of investigation to be undertaken. Appendix 2 outlines what would be expected to be covered as part of the initial investigation. All level 1 incidents should be completed within 20 working days and Datix incident closed.

6.3 Level 2 incidents

The Information Governance Team will seek further information from the manager to ascertain the level of investigation to be undertaken and if appropriate, jointly commission a formal investigation with the manager into the incident. Appendix 2 outlines what would be expected to be covered in such an investigation.

All level 2 incidents should be completed within 2 months and Datix incident closed unless a disciplinary process is being put in place in line with the Trust's Disciplinary Policy.

Outcome of all investigations will be reported through the Management of Information Group through the Trust's annual report and Annual Governance Statement.

Please Note: When writing an investigation report, please bear in mind that this report or parts of it is likely to shared wider than those involved in the investigation, i.e. data subject, Management of Information Group, Board, external bodies i.e. Information Commissioner Office, HSCIC.

7. Cyber Security Scoring and Reporting

7.1 Cyber SIRI categories are determined by the context, scale and sensitivity.

7.2 Information Governance together with the SIRO will determine the level of severity by using the factors outlined in Appendix 1.

7.3 Cyber SIRI confirmed level 2 incidents will be reported to the HSCIC and Department of Health using the IG SIRI reporting tool.

8. Publishing Details of IG SIRIs

The Trust will publish details of IG SIRIs through its Annual Report and Statement of Internal Control in accordance with the HSCIC *Checklist*

Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigations Annex D.

9. Monitoring, Auditing and Review

9.1 This document will be monitored and audited through the regular Datix Reporting System Reports presented to Management of Information Group. This document will be reviewed in two years or earlier if guidance or good practice from the HSCIC, ICO changes or as a result of internal learning from reporting IG SIRIs.

10 Monitoring tool

Standards:

Item	%	Exceptions
IG Team to score incidents within 2 working days	100	
Level 0 incidents to be completed and closed within 5 working days.	95%	
Level 1 incidents to be completed and closed within 20 working days	90%	
Level 2 incidents to be completed and closed within 2 months	85%	

Equality Statement.

The Trust is committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership.

The Trust is committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy

References:

HSCIC *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation V5.1 – May 2015*

Appendices

Appendix 1	Cyber Security Scoring Matrix
Appendix 2	Reporting Information
Appendix 3	Template letter to send to data subject(s)
Appendix 4	IG SIRI Flow Chart
Appendix 5	Glossary

Amendment History

Issue	Status	Date	Reason for Change	Authorised
V1.1	Draft	04/08/2015	Updated and formatted on correct template.	
v.2	Ratified	09/09/2015	To provide additional information to staff in line which changes made to Datix to meet HSCIC requirements.	MIG

Appendix 1 – IG Cyber Scoring Matrix

Please note that this scoring matrix is not part of the Datix reporting system. This will be completed by the Information Governance in conjunction with the SIRO.

Datix Incident No:	

Low: For each of the following factor reduce the baseline score of 0 by 1	**Score**	**Scored**
(1) A Tertiary system affected which is hosted on infrastructure outside health and social care networks.	1	

High: for each of the following factors increase the baseline score by 1	**Score**	**Scored**
(2) Repeat incident (previous incident within last 3 months)		
(3) Critical business system unavailable for over 4 hours		
(4) Likely to attract media interest		
(5) Confidential information release (non personal)		
(6) Require advice on additional controls to put in place to reduce reoccurrence		
(7) Aware that other organisations have been affected		
(8) Multiple attacks detected and blocked over a period of 1 month.		

Cyber Security Score	
Completed By:	Date:

Further clarification on the factors can be found in Annex F of the HSCIC *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation V5.1 – May 2015*

Appendix 2 –IG SIRI Reporting of Information

Level 0 Investigation

1. Date, time and location of incident
2. Breach Type (Definitions at the bottom of this Appendix)
3. Details of personal or sensitive information i.e. data fields
4. Description of what happened
5. Number of patients/service users/staff involved
6. Number of records involved
7. Format of records i.e. paper, digital
8. If digital, whether encrypted or not
9. Whether there is likely to be media interest
10. Whether the incident could damage the reputation of an individual, team, Trust or sector
11. Whether the data subject has been notified (if not sure whether to, then consult with IG)
12. Is the data subject likely to make or has made a complaint
13. Are the staff members involved up to date with their IG Training, if not when are they planning to undertake the mandatory training
14. What immediate actions have been taken to mitigate the risk
15. Outline details of the learning from the incident and any actions to be taken and by when.

Level 1 Investigation

Should include Points 1-15

16. Has IG Team been notified?

17 Whether the incident is in the public domain

18 Name of manager who can provide additional information

19. Chronology of events, if applicable
20. Are there any legal implications?

21 Are there any other incidents relating to this one?

22. Are there any consequent risks to the data subject ?
23. Produce an action plan with clear timescales and leads to mitigate further risk

24 Outline how the learning from this incident can be shared.

Level 2 Investigation

A full scale investigation will be commissioned by the IG Lead and/or Caldicott Guardian jointly with the line manager. The Term of Reference for such an investigation should include:

- Target timescales for completing investigation and finalising reports
- Who will review the report?
- Who will sign off the report, i.e. IG Lead, Manager, Caldicott Guardian?
- Who will receive the outcome of the report i.e. relevant person, committee?

The final report should include all the above information in points 1-24 and any recommendations to mitigate future risks.

The person who signs of the report will be responsible for putting an action plan into place with clear timescales and leads together with details of who will disseminate any learning from the incident.

Please note

- An incident cannot be closed until all aspects, including any disciplinary action taken against staff, are settled.
- The investigation report or any part of the report may be published by the Trust or through the IG Incident Reporting Tool.

Appendix 3 –Template Letter to Data Subject(s)

Note: *Before sending out such a letter, the manager needs to consider the risks and implications of sending such a letter against the benefits. If the manager is unsure, then they should contact the IG Lead or Caldicott Guardian for advice.*

[Date]

Dear Sir / Madam,

[Subject]
[Datix Reference]

I am writing to you in relation to a recent information breach that has occurred within our Trust.

(Insert summary of incident and how client was affected)

This means [that records will have contained / that another person may have seen] your [demographic / medical information]. [Also detail records NOT accessed/taken]

As a Trust we take our duty of confidentiality extremely seriously and wish to assure you that we place significant importance on the safety of patient/client information. We wish to apologise for our error and any distress this may have caused.

[Can the information be recovered, what steps are being taken? Is there a police contact or reference they need?]

[Are there concerns regarding identity theft, what steps should the individual take / where to seek further advice.]

We have carried out an investigation into this incident and have made changes to our systems to ensure this does not occur in the future.

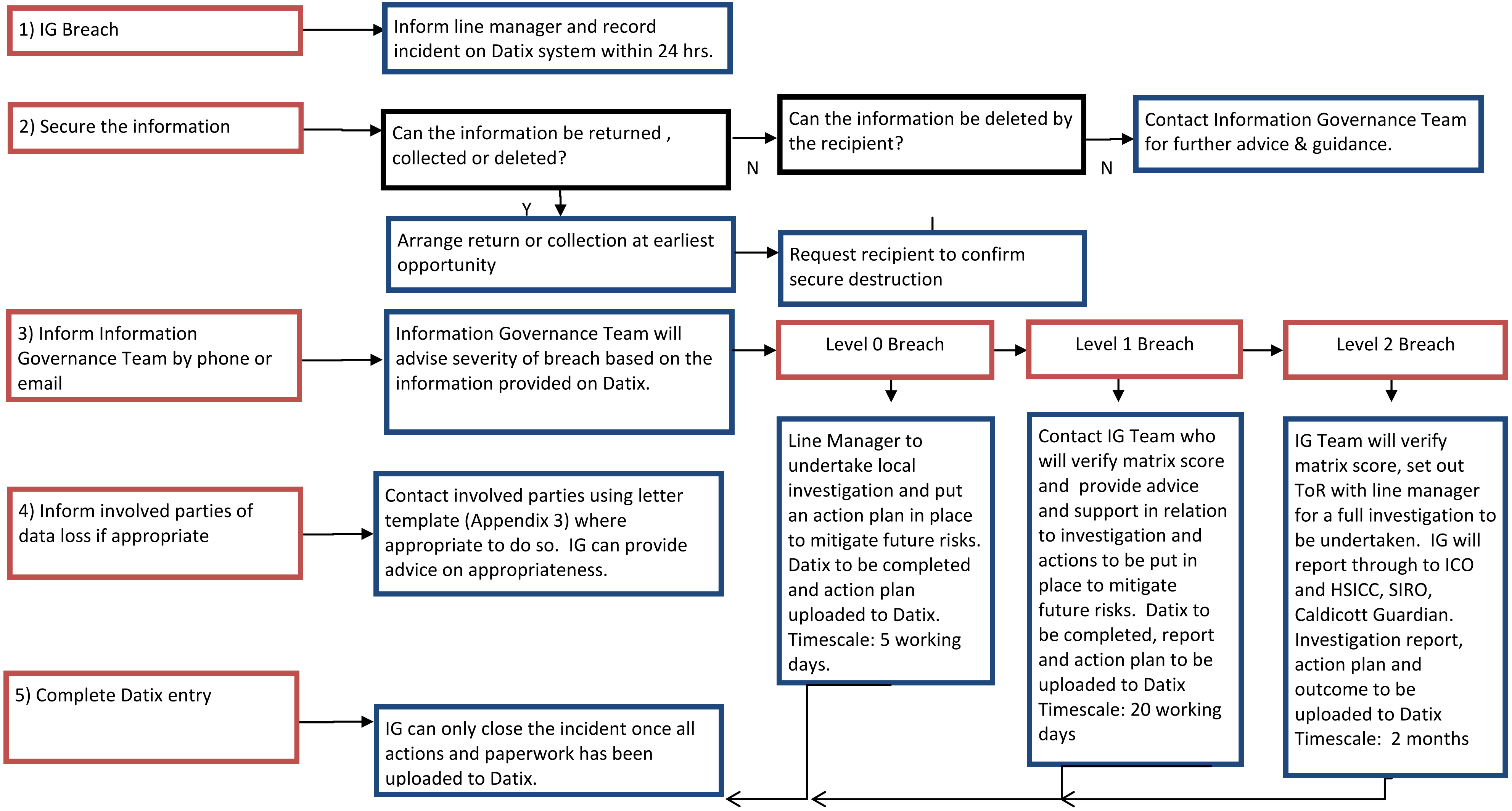
[Insert remedial action taken]

If you have any questions or would like to discuss this matter, please feel free to contact us.

Please be assured that this error has in no way affected your care and/or treatment or your right to complain. If you wish to make a formal complaint, you can write to our Complaints Officer at Torbay and Southern Devon Health and Care NHS Trust, Bay House, Nicholson Road, Torquay, TQ2 7TD or email: feedback.t-sd@nhs.net.

Yours sincerely,

Appendix 4 – IG SIRI Flowchart



1) IG Breach

Inform line manager and record incident on Datix system within 24 hrs.

2) Secure the information

Can the information be returned , collected or deleted?

N

Can the information be deleted by the recipient?

N

Contact Information Governance Team for further advice & guidance.

Y

Arrange return or collection at earliest opportunity

Request recipient to confirm secure destruction

3) Inform Information Governance Team by phone or email

Information Governance Team will advise severity of breach based on the information provided on Datix.

Level 0 Breach

Level 1 Breach

Level 2 Breach

Line Manager to undertake local investigation and put an action plan in place to mitigate future risks. Datix to be completed and action plan uploaded to Datix. Timescale: 5 working days.

Contact IG Team who will verify matrix score and provide advice and support in relation to investigation and actions to be put in place to mitigate future risks. Datix to be completed, report and action plan to be uploaded to Datix Timescale: 20 working days

IG Team will verify matrix score, set out ToR with line manager for a full investigation to be undertaken. IG will report through to ICO and HSICC, SIRO, Caldicott Guardian. Investigation report, action plan and outcome to be uploaded to Datix Timescale: 2 months

4) Inform involved parties of data loss if appropriate

Contact involved parties using letter template (Appendix 3) where appropriate to do so. IG can provide advice on appropriateness.

5) Complete Datix entry

IG can only close the incident once all actions and paperwork has been uploaded to Datix.

Appendix 5 – Glossary

Data Subject is a living individual to whom personal data relates

Datix is the incident reporting system utilised by Torbay and Southern Devon Health and Care NHS Trust. The Datix incident reporting system can be accessed via the home page from the Trust's intranet (iCare).

Health and Social Care Information Centre (HSCIC) is responsible for publishing a set of rules (called a Code of Practice) to set out how the personal confidential information of patients should be managed by health and care staff and organisations in accordance with statutory functions and duties.

Information Governance Serious Incident Requiring Investigation (IG SIRI) is a type of incident that will typically breach one of the principles of the Data Protection Act and/ or Common Law Duty of Confidentiality. It includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy. Further information can be found in the HSCIC *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation – Version 5.1*.

Information Governance Cyber Serious Incident Requiring Investigation (IG Cyber SIRI) is a type of incident is anything that could be (or has) compromised information assets within Cyberspace. "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communication information. It includes the internet, but also the other information systems that support our business, infrastructure and services." (Source UK Cyber Security Strategy, 2011).

Sensitive Personal data includes data subjects racial or ethnic origin; political opinions; religious beliefs or other beliefs; trade union membership; physical or mental health conditions; sexual life; commission or alleged commission of any offence; or any proceedings for any offence committed or alleged to have committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Confidential Information includes clinical records or any data that would enable someone to learn something confidential about someone that they didn't already know.