NHS
West Hampshire
Clinical Commissioning Group

INFORMATION INCIDENT MANAGEMENT AND REPORTING PROCEDURES

Version 3.2

Subject and version number of document:	Information Incident Management and Reporting Procedures Version 3.2
Serial number:	WHCCG/002/V3.02
Operative date:	1 August 2019
Author:	NHS South, Central & West Commissioning Support Unit (SCW CSU) Information Governance Team
CCG owner:	Chief Finance Officer (Senior Information Risk Owner)
Links to other (CCG) policies	• Confidentiality and Safe Haven Policy • Information Governance Staff Handbook • Information Governance Policy • Data Protection Impact Assessment (DPIA) Guidance Framework • Information Governance Framework and Strategy • Information Risk Management Programme • Records Management Policy • SCW IT-Services Security Incident Handling Policy
Review date:	July 2021
For action by:	All staff
Document statement:	This document identifies the measures taken to ensure that the CCG manages information incidents in a way that meets organisational, NHS and regulatory body requirements.
Responsibility for dissemination to new staff:	Line Managers
Mechanisms for dissemination:	All new and revised policies, procedures and guidelines are published on the CCG website and promoted through the CCG staff newsletter.
Training implications:	All staff at induction and annual information governance training, plus specific training related to IG role e.g. SIRO, Data Custodian/Information Asset Administrator etc.
Resource implications:	There are no resource implications in relation to these procedures.
Further details and additional copies available from:	Information Governance Team, NHS South, Central and West CSU Website: https://westhampshireccg.nhs.uk/document-tag/ig-

	and-security-policies/
Equality analysis completed?	Yes
Consultation process	CSU IG team Policy Sub Group
Approved by:	Policy Sub Group
Date approved:	17 July 2019

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	July 2015	9, 10 and appendices 1,3,5 + new appendix 4	HSCIC guidance, reporting process (v2.)	July 2015
2	June 2016	2	Review date amended in line with 3 year review cycle as agreed by policy sub group Update hyperlinks Update references to Corporate Governance Committee to Finance & Assurance Committee Amend references to Data Custodians to include Information Asset Administrators	14 Jun 16
3	Oct 2016	Pg 15 Throughout	To also inform IT Service Desk if an information security breach is suspected / has occurred Amend references to HSCIC to NHS Digital	Oct 2016
4	Sept 18	Throughout	Complete rewrite (v3)	Sept 18
5	28 Dec 18	Pg 11	Update DPO role (v3.01)	28 Dec 18
6	Jul 19	Pg 13	Full review. No changes apart from changing review period from annual to biennial.	8 Jul 19

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Reviewer	Ratification Process	Notes
2	July 2015	IG Manager, NHS South, Central & West CSU	Policy Sub Group & Corporate Governance Committee July 2015	As amend 1 above
3	Sept 18	IG Manager, SCW CSU	Policy sub Group	As amend 4 above
3.2	Jul 19	IG Manager, SCW CSU	Policy Sub Group	As amend 6 above.

INFORMATION INCIDENT MANAGEMENT & REPORTING PROCEDURES

CONTENTS

INFORMATION INCIDENT MANAGEMENT & REPORTING PROCEDURES

1. INTRODUCTION AND PURPOSE

1.1 The General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018 introduces a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority.

1.2 An organisation must notify a breach of personal data within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

1.3 The CCG will ensure robust breach detection; investigation and internal reporting procedures are in place that comply with legislative timescales for reporting.

1.4 The CCG will also keep a record of any personal data breaches, regardless of whether it is required to notify externally. An incident register is managed by the South Central & West Commissioning Support Unit (SCW CSU) Information Governance Manager on which all incidents are recorded.

1.5 The CCG will use the NHS Digital Data Security and Protection Incident Reporting Tool, which can be used for the purposes of notifying breaches on one form, which may then be shared across several regulatory agencies. These include personal data breaches of the GDPR to the Information Commissioner and cyber security incidents to NHS Digital.

1.6 The CCG will comply with the Data Security Standard 6 and provide evidence of this in the Data Security and Protection Toolkit

1.7 The CCG will maintain a local file or use an incident management system to fully record the particulars of any investigation and remedial action.

1.8 The CCG recognises the importance of reporting all incidents as an integral part of its risk identification and information risk management programme through the consistent monitoring and review of incidents that result, or have the potential to result in a confidentiality breach, damage or other loss.

1.9 Research has shown that the more incidents that are reported, combined with the use of root cause analysis to understand why an incident has occurred, the more information will be available about any problems.

1.10 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

1.11 Most information incidents relate to system failure and individual mistakes. Incident reporting needs an open and fair culture so staff feel able to report problems without fear of reprisal and know how to resolve and learn from incidents.

2. SCOPE AND DEFINITIONS

Scope

2.1 This document sets out how all information incidents, including Serious Incidents Requiring Investigations (SIRIs), will be identified, reported by staff, 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.

2.2 The CCG is committed to identifying, evaluating and mitigating all risks to data subjects; these include patient/service users, permanent and temporary staff.

Definitions

Adverse Event	Any untoward occurrence which can be unfavourable and an unintended outcome associated with an incident.
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 CCG 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.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR.
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.
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 of Personal 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.
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR.
Serious Incident Requiring	There is no simple definition of a serious incident. What may first appear to be of minor importance may, on further

Investigation (SIRI)	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 the 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' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information 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.

3. ROLES AND RESPONSIBILITIES

3.1 Chief Officer

The chief officer, as accountable officer, has overall responsibility for information governance within the organisation. As accountable officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

3.2 Senior Information Risk Owner (SIRO)

The SIRO for the CCG is the chief finance officer, with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the chief officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services

contracted by the organisation. They will oversee Serious Incidents Requiring Investigation (SIRIs).

3.3 **Caldicott Guardian**
The Caldicott guardian is the director of quality and nursing, with overall responsibility for protecting the confidentiality of personal data and special categories of personal 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 CCG Board and relevant committees on confidentiality issues. They will support the SIRO in overseeing SIRIs.

3.4 **Data Protection Officer (DPO)**
The DPO is the CCG director of strategy and service developoment who 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 Information Commissioner's Office (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 **South Central & West Commissioning Support Unit (SCW CSU) Information Governance Team**
The information governance team will support the CCG in investigating incidents, offer advice and ensure the organisation complies with legislation, policies and protocols. The SCW IG lead will report incidents likely to result in a risk to the rights and freedoms of Data Subjects to the CCG DPO offering guidance regarding informing the ICO.

3.6 **SCW Cyber Security Manager**
The SCW cyber security manager will ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

3.7 **Information Asset Owners (IAO)**
IAOs will support the organisation in investigating incidents.

3.8 **Data Custodians (DC's) / Information Asset Administrators (IAAs)**
DCs / IAAs will support the organisation 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 **West Hampshire CCG IG Group**
The Information Governance Group is responsible for overseeing day to day information governance issues and provides a reporting mechanism and forum for discussing incidents, other types of IG breach and also near misses.

4. PROCEDURES

4.1 The procedure for reporting incidents, breaches and near misses is included as Appendix 1.

5. FREEDOM OF INFORMATION REQUESTS (FOI)

5.1 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 Legislation and Freedom of Information Act.

5.2 Non-confidential incidents relating to the CCG and their services will be available to the public through a variety of means including reports, 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

6. TRAINING

6.1 The CCG recognises 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. The identification of breaches is included in the on-line IG Training modules provided by NHS Digital that can be accessed through the ConsultOD learning and development portal.

6.2 All staff are required to complete IG training on an annual basis. The SIRO, Caldicott guardian, DPO, IAOs and IAAs are required to undertake additional training in accordance with their roles.

7. EQUALITY ANALYSIS

7.1 The CCG is committed to equality, diversity and inclusion for all, as well as to meeting the Public Sector Equality Duty (Equality Act 2010).

7.2 Both new policies / procedures, and existing policies / procedures when reviewed, come within the Public Sector Equality Duty. This means that authors must consider whether the policy will be effective for all patients and/ or staff. This process is called equality impact assessment.

7.3 These procedures have been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full equality impact assessment is not required.

7.4 However, the CCG Datix system which is used to record all incidents has a number of fields that can be selected to record equality aspects of incidents, which enables the CCG to capture data regarding equality incidents, address individual cases and analyse trends; this will include any related to information governance breaches / incidents. Please refer to the CCGs overarching Incident Management Policy & Guidance, for which a full Equality Impact Assessment has been completed.

8. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

8.1 The CCG will ensure that it fully embeds improvements to its information governance structure and demonstrates it is proactive in assessing and preventing information risks by evidencing that:

a. There is continuous improvement in confidentiality and data protection and learning outcomes
b. All incidents are audited to ensure any recommendations made have been implemented
c. Learning outcomes will be shared with other directorates/departments in order to prevent similar incidents from reoccurring
d. Records of all decisions, actions, and recommendations (e.g. evidence, incident forms and reports) will be kept throughout the investigation and final report
e. All records and documentation will be kept in a secure location
f. Any Personal Confidential Data (PCD) including medical records, photos or other evidence will be secured at the start of the investigation
g. File notes with dates will be kept of all discussions
h. Minutes of all related meetings will be produced.

9. REVIEW

9.1 This document may be reviewed at any time at the request of either the staff forum or management, or in the response to changes in legislation, but will automatically be reviewed on a biennial basis.

10. REFERENCES AND LINKS TO OTHER DOCUMENTS

- Confidentiality and Safe Haven Policy
- Information Governance Staff Handbook
- Information Governance Policy

- Data Protection Impact Assessment (DPIA) Guidance Framework
- Information Governance Framework and Strategy
- Information Risk Management Programme
- Records Management Policy
- SCW IT-Services Security Incident Handling Policy

NHS Digital Data Security and Protection Incident Reporting Guidance
https://www.dsptoolkit.nhs.uk/Help/29?AspxAutoDetectCookieSupport=1

Information Commissioners Office guidance on data breaches
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

APPENDIX 1: STAFF GUIDANCE ON IDENTIFYING AND REPORTING AN INFORMATION INCIDENT

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

All incidents must be reported to the Information Asset Owner and SCW IG Team as soon as staff become aware of the incident. The Data Protection Officer should as a minimum be informed within 24 hours or 1 working day of staff becoming aware 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.

The IAO will consider whether the incident needs to be logged on Datix.

What should be reported?

There are three types of breaches defined under the Article 29 Working Party which informed the drafting of the General Data Protection Regulation (GDPR):

- **Confidentiality breach**- unauthorised or accidental disclosure of, or access to personal data

  Example - Infection by ransomware (malicious software which encrypts the CCG'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 are 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.

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

- Finding a computer printout containing Confidential Data laying around;
- Identifying or informed that a fax that was thought to have been sent to an intended recipient had been received by an unknown recipient or organisation;
- Finding confidential waste in a 'normal' waste bin;
- Loss or temporarily misplacement of a mobile computing device or mobile phone that may have personal information on it;
- Information has been given to someone who should not have access to it – verbally, in writing or electronically;
- A computer database has been accessed using someone else's authorisation e.g. someone else's user id and password;
- A secure area has been accessed using someone else's swipe card or pin number when not authorised to access that area;
- A PC and/or programmes aren't working correctly – potentially because the device may have a virus;
- A confidential or sensitive e-mail has been sent to an unintended recipient or 'all staff' by mistake;
- A colleague's password has been written down on a 'post-it' note and found by someone else;
- A physical security breach ('break in') to the organisation is discovered;
- A phishing email has been received;
- A Website has suffered from defacement.

What happens next?

Where an incident involves data or information that the Controller has asked another organisation to process for them, the DPO should be informed by the Processor's Data Protection Officer 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 a Data Sharing Agreement has been put in place and notification of potential breaches to each party forms part of the organisations' obligations.

The incident will be investigated by the Controller but can be supported to do this by other organisations. The Controller retains the legal obligation to report and investigate incidents.

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;

- Identify whether any deficiencies in the application of CCG policies or procedures and/or the CCG 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;
- Please refer to the CCGs overarching Incident Management Policy & Guidance for further details of investigation processes.

Assessing the severity of an incident

An initial assessment of the incident will be made using the NHS Digital Data Security and Protection Incident Reporting tool.

Notifiable breaches are those that are likely to result in a high risk to the rights or freedoms of the individual (data subject). The scoring matrix used in the reporting tool has been designed to identify those breaches that meet the threshold for notification.

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

- the potential significance of the adverse **effect** on individuals graded from 1 (lowest) to 5 (highest);

No.	Effect	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 the 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

- the **likelihood** that adverse effect has occurred graded from 1 (non-occurrence) to 5 (occurred);

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.

Under the following circumstances notification may not be necessary;

- 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.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor and the decision is taken to report the incident), full details will be automatically emailed to the Information Commissioners Office and the NHS Digital Data Security Centre.

Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following it must still be reported to the ICO:

- 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 of personal data

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

Internal Reporting

Any information incident that takes place that is not reportable will still be included in reports circulated to the West Hants IG Group and to the SIRO, Caldicott Guardian and DPO at monthly meetings. These are primarily for staff awareness and to identify trends in minor incidents.

IG incident reports will also be presented to the Audit Committee through the SIRO in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.

Information Governance Incident Reporting and Investigation: Flow Chart