Policy for Managing Incidents and Serious Incidents

Version	v12.0
Supersedes:	v11.0
Date Ratified by Board:	26.01.2017 (original policy)
Reference Number:	PC24POL32
Title & Department of originator:	Associate Director of Nursing
Title of responsible committee / department:	Quality Workforce Committee
Effective Date:	February 2018
Next Review date:	February 2021 or sooner when there is a change in Policy or national guidance.
Target audience:	All personnel as defined in clause 3.1
Impact Assessment Date:	16.11.2016

Version	Date	Control Reason	Title of Accountable Person for this Version
v7.0	2017	Reviewed and extensively updated to reflect a) Datix implementation, responsibilities, and Incident Management processes. b) Updated in line with the changes to the National SI Reporting. c) Updated to include EIA Screening All previous versions have been archived.	Associate Director of Nursing
v8.0	02/18	Annual review of policy. Additional guidance in the debrief of staff 7.2	ADoN
v9.0	07/18	Updated to include debrief process.	ADoN
v10.0	11/18	Flow chart on p 33 amended to include correct personnel	ADoN
v11.0	02/20	Title of the organisation changed from PC24 to PC24 throughout the document. Responsibilities for manager in Section 5 to incorporate debriefing of staff. Titles of managers added.	ADoN
v12.0	05/20	Changes made to Section14 'Root Cause Analysis', providing more detailed descriptors of the three levels of investigation.	ADoN

Reference Documents	Electronic Locations (Controlled Copy)	Location for Hard Copies
Please refer to section 28	PC24 Intranet/Governance/Risk Policies	**Policy File, Wavertree Headquarters**

Consultation: Committees / Groups / Individual	Date
Original Policy - Leadership Team, SMT, Policy Group, Quality & Workforce Committee (26.01.17). Associate Director of Nursing. Board.	Nov.18

CONTENTS **Page**

Appendices **Page**

1 INTRODUCTION

Primary Care 24 Social Enterprise, hereafter known as PC24, provides integrated Primary Care services across Liverpool, Knowsley, Halton and St Helens. In addition, primary and community services in Knowsley and Sefton.

1.2 The aim of this policy is to support the delivery of the organisational aims and objectives through effective management of risk across all of the PC24's functions and activities through effective incident management processes, measurement, analysis and organisational learning.

1.3 PC24 will promote an open learning culture where incidents, complaints and other learning events are investigated thoroughly to determine root causes and action where appropriate to improve services as a result.

2 Purpose

The purpose of an incident reporting system is to identify problems or potential problems to prevent or minimise a further recurrence. This policy allows concerns to be raised which may have an effect on the safety of patients and the public in general, and/or the safety of their personal data. This document sets out the Serious Incident, incidents, accident and near miss reporting, management, and investigation procedure for Primary Care 24. It details the measures and procedures to be adopted when reporting, managing and investigating accidents, incidents, complaints and near misses. The management and investigation of accidents / incidents/near misses will be based on the severity of their outcome, with the ultimate aim to learn and make changes as a result, in order to improve safety for patients, staff, visitors and contractors. Qualitative and quantitative data analysis will be used to highlight trends and identify any further need for action.

2.1 This policy aims to facilitate learning by promoting a fair, open and just culture and that lessons from incidents are learned and quickly acted upon in a positive and constructive way.

2.2 PC24 will fully support any individual reporting an incident. In many instances, the root cause of incidents lies in the management and organisational systems that support the delivery care.

2.3 The essence of PC24's reporting procedure is to identify and address the underlying causes of incidents. All incidents will be investigated and managed in a sensitive and non-punitive manner.

2.4 Disciplinary procedure will only be considered in the following cases:

- Deliberate failure to report and incident
- Failure to cooperate with an investigation
- Criminal actions
- Actions so far removed from reasonable practice that any competent practitioner/member of staff would have been able to predict the outcome reported.
- Breach of Professional Codes of Conduct
- Repeated error involving the same individual

PC24's approach to investigating and learning from incidents focuses on what went wrong and not who is wrong. However, if staff feel unable to report an incident via the incident reporting system, they should follow the PC24's Raising a Concern (Whistleblowing) Policy, PC24POL102.

2.5 It is PC24's Policy that all incidents are:

- Reported within the Datix Risk Reporting Management system
- Reviewed and the appropriate action taken, including full investigation where indicated

- Reported to external bodies, including Care Quality Commission, NHS Health and Safety Executive, NHS England and Commissioners in the timescales required when necessary.

2.6 This policy should be read in conjunction with Primary Care 24's

• Confidentiality and Data Protection Policy	PC24POL1
• Disciplinary Policy	PC24POL14
• Public Interest Disclosure Policy	PC24POL18
• Safeguarding of Vulnerable Children	PC24POL23
• Safeguarding of Vulnerable Adults	PC24POL74
• Capability Policy	PC24POL37
• Whistleblowing Policy	PC24POL102
• Duty of Candour Policy	PC24POL103
• Complaints, Concerns and Compliments Policy	PC24POL34

3 SCOPE

3.1 This policy applies to all employees, GPs working in any PC24 services, bank and agency staff, visitors and contractors in PC24, hereafter referred to as personnel.

3.2 It is the responsibility of all personnel employed & contracted by PC24 to report incidents and near misses through the organisation's Datix Risk Reporting and management framework. It is their duty to report those incidents in which they are directly involved and those of which they are aware.

4 DEFINITIONS

4.1 **Incident** - An event or circumstance which could have resulted, or did result, in unnecessary damage, loss or harm to patients, staff, visitors or members of the public.

4.2 Clinical Incident - Defined as “any unintended or unexpected incident which could have or did lead to harm for one or more patients receiving NHS care.”(NPSA, 2008).

4.3 Non-Clinical Incident - Defined as any event or circumstance that does not involve a patient’s treatment or care which leads to, or could potentially lead to, unintended or unexpected harm, loss or damage to staff, financial loss or injure the reputation of the Trust.

4.4 Near Miss - Defined as any unexpected or unintended incident which was prevented either by intervention or by luck” (NPSA, 2001).

4.5 Serious incident (SI) - A serious incident will require investigation and is defined as an incident that occurred in relation to NHS funded services and care resulting in one of the following:

- The unexpected or avoidable death of one or more patients, staff, visitors or members of the public
- Permanent harm to one or more patients, staff, visitors or members of the public, or where the outcome requires lifesaving intervention or major surgical / medical intervention, or will shorten life expectancy (this includes incidents graded under the NPSA definition of severe harm (Seven Steps To Patient Safety, Full Reference Guide 2004).
- A scenario that prevents, or threatens to prevent, a provider organisation’s ability to continue to deliver health care services, for example, actual or potential loss or damage to property, reputation or the environment
- Allegations of abuse
- Security incidents
- Adverse media coverage or public concern for the organisation

4.6 Never Events – Never-Events are serious, largely preventable patient safety incidents that should not occur if the available preventative measures have been implemented. These are updated on an annual basis by NHS England. (NHS England

Revised Never Events Policy and Framework March 2015 and NHS England – Never Event List 2015/16). Contact Quality & Patient Safety Team for further information if required, 0151 254 2553.

4.7 'Patient Safety Incident' – Any incident that has involved or could have affected the safety of one or more service users.

4.8 Security Incident – From April 2010 NHS Security Management Service introduced a Security Incident Reporting System (SIRS). This was developed to provide a clearer picture of security incidents across the health service in England, locally and nationally. The following security must be reported using SIRS:

- Any security incident involving physical assault of NHS staff
- Non-physical assault of NHS staff (including verbal abuse, attempted assaults and harassment)
- Theft of or criminal damage (including burglary, arson, and vandalism) to NHS property or equipment (including equipment used by staff)
- Theft of or criminal damage to staff or patient personal property
- Property damage arising from these types of security incidents

4.9 Duty of Candour - In the wake of the Mid-Staffordshire Public Inquiry, the Government have introduced a range of measures to reinforce the value of openness, with sanctions for the most serious failings in candour and honesty.

There is a new statutory Duty of Candour on organisations, supported by strengthened guidance and codes for regulated professionals, which will champion openness and safety across. Primary Care as a Social Enterprise has embraced the principles of Duty of Candour.

4.10 Strategic Executive Information System (StEIS) – A reporting system 'hosted' by NHS England; all Serious Incidents are reported by a member of the Quality & Patient Safety Team externally.

4.11 Unexpected Death – Where natural causes are not suspected, local organisations should investigate these to determine if the incident contributed to the unexpected death.

4.12 Permanent harm - Harm directly related to the incident and not to the natural course of the patient's illness or underlying conditions; defined as permanent lessening of bodily functions, including sensory, motor, physiological, or intellectual.

4.13 Prolonged pain and/or prolonged psychological harm – Pain or harm that a patient has experienced, or is likely to experience, for a continuous period of 28 days.

4.14 Abuse – It should be recognised that the term 'abuse' can be subject to wide interpretation and that, when determining whether adult abuse is taking place, consideration will need to be given to a range of factors.
Abuse is a violation of an individual's human and civil rights by any other person or persons. Abuse may consist of:

- A single act or repeated acts
- It may be physical, psychological or emotional
- An act of abuse neglect or omission to act
- Occur when a person is persuaded to enter into a financial or sexual transaction to which they have not, or cannot consent
- Abuse may be deliberate or unintentional or result from lack of knowledge

4.15 External body / agency - An organisation that has an official advisory or regulatory role that has been mandated to regulate the corporate and professional activities of NHS providers.

4.16 RIDDOR - is the Reporting of Injuries, Diseases, and Dangerous Occurrences Regulations 1995 (as amended). RIDDOR Incident is defined as any incident, disease, or dangerous occurrence reportable under the RIDDOR regulations by the Health and Safety Executive (HSE).

4.17 Information Governance Incident - Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals.

The above definition applies irrespective of the media involved and includes both loss of electronic media and paper records.

All reported information governance incidents attributable to the actions of personnel employed by PC24 are risk rated in accordance with the Checklist guidance for reporting, managing, and investigating information governance serious incident requiring investigation (Department of Health 2013).

4.18 Complaint/Claim - A complaint is defined is an expression of dissatisfaction (written or verbal) about a service provided or which is not provided, which requires a response. Examples of complaints include: Concerns about the quality of service provided, the following of standard procedures and good practice, poor communication and the attitude or behaviour of a member of staff.

4.19 Initial Management Assessment (IMA) – A short report aimed to ensure more serious incidents are investigated promptly and to the appropriate level. The report is used to record further information about an incident to identify any service delivery issues or risks and as a decision making tool as to whether further investigation is required.

4.20 Root Cause Analysis (RCA) - Is defined as the process by which the underlying cause(s) of patient safety and non-clinical incidents are established. The nature and extent of an RCA will be subject to the nature and level of incident. An action plan will be established for all root causes and issues identified which have contributed to/resulted in an incident

4.21 Strategy/Scoping Meeting - A meeting convened at the request of the Line Manager/Senior Manager/Quality and Safety team to: plan the route of the investigation,

appoint an Investigating Officer and agree Terms of Reference and timelines for the investigation.

5 RESPONSIBILITIES

All personnel have a responsibility to adhere to the terms and conditions of this policy.

5.1 Directors, Heads of Service and Clinical/Medical Leads who are specified as the responsible people within the policy must ensure the correct procedure is carried out.

5.2 Any queries on the application or interpretation of this policy must be discussed with the author of the policy prior to any action taking place.

5.3 This policy will be reviewed at least every three years and updated as appropriate.

5.4 Below are the specified duties and roles within Primary Care 24 for the implementation of this policy.

5.5 All personnel are responsible for reporting incidents and complaints appropriately and recording them within the Datix system and assisting in any clinical and non-clinical Incidents investigations, which may require their assistance.

5.6 All personnel must be aware of this policy. They must be familiar with all Primary Care 24 policies and complete induction and training in order to ensure continued competence when carrying out their duties.

5.7 The **Quality and Patient Safety Department** are responsible for:

- Act as custodians for PC24's Policy for Managing Incidents and Serious Incidents and will support the monitoring processes in relation to compliance and implementation.

- Responsible for ensuring that there is good data regularly reported to the relevant committees on all incidents and or serious incidents (SI). They, along with the Director or nominated deputy, will also meet with relatives or carers of those involved in an incident if appropriate and required. This will be both to inform and apologise on behalf of the organisation and provide good communication on the on-going management of an incident or SI.
- Maintain the Datix Risk Management Reporting System and monitor the quality of incident reporting to ensure adequate data quality is maintained
- Ensure that the incident reporting process is maintained (See Appendix 1)
- Provide advice and support to all staff and ensure training, resources and information is available to all staff relating to reporting, managing and investigating incidents.
- Report to external agencies as required in Appendix 2 This includes reporting to the relevant Clinical Commissioning Group via the StEIS system within 2 working days of being made aware of a reportable incident. StEIS will be updated as information becomes available, including uploading reports from serious incidents requiring investigation.
- Keep all accident/incident information for a period of ten years in line with Department of Health guidance for record retention.
- Regularly provide data/reports to different levels within the organisation to enable scrutiny of data, identification of risks and the sharing of learning from all incidents.
- Support Directors, Associate Directors and Heads of Service as appropriate to the nature of the incident, in the grading of incidents, contributing to the development of necessary plans and providing appropriate actions have been taken.
- Support teams to initially review incidents that may require a more detailed investigation and support these staff were necessary in the escalation of the incident.

5.8 Deputy Directors, Heads of Service, Service Managers and Clinical Leads will ensure that reporting process is followed and that all actions to address the issues identified during the investigation process are completed within the agreed timescales. Appendix 1.

5.9 The appropriate Manager will provide help and support to all employees before, during and after an incident report and facilitate provision training where identified. The appropriate manager will provide debrief support to staff following incidents as soon as possible after the event has occurred.

5.10 The investigating officer/manager will identify and raise any trends highlighted within the procedures or through personnel following the incident investigation with the **Quality and Patient Safety Department**. The investigation of all incidents will be completed by the relevant Director/Associate Director/Head of Service, Line Manager or delegated staff member. They will identify the root cause of the incident and work to eliminate, mitigate or accept the risk that this poses to the organisation. (See Appendix 3, Investigation Template).

5.10 Heads of Service/Shift Managers will support staff to ensure that, in the wake of any incident, any patient or personnel is made safe and receives any appropriate care or treatment as a priority. (See Appendix 4, Action Plan Template)

5.11 Heads of service are responsible for ensuring that all action plans are completed within the agreed timescales. These timescales will be monitored by the **Quality and Patient Safety Department** to ensure compliance.

5.12 The Directors have ultimate responsibility to ensure that there is adequate training and support in place for personnel under their supervision in relation to incident reporting, investigating or feeding back. The Chief Executive should be informed of progress and development in the investigation of any SIs or incidents with a risk score of 15+. (See Appendix 5, Risk Scoring Matrix).

5.13 The Directors have a central role in ensuring that all incidents are handled in accordance with the policy and that the lessons learned are fed back to all employees.

5.14 In serious incidents where questions of clinical competence might arise, the Medical Director, or delegated Medical staff or Director of Nursing or delegated Nursing staff will be responsible for overseeing the investigation and managing the outcomes.

5.15 The Chief Executive is the Accountable Officer for the organisation and therefore responsible for all systems, processes, policies and procedures.

5.16 The Director of Nursing is the Board Lead for safeguarding adults and children. This role includes specific responsibilities for overseeing investigations and ensuring recommendations are implemented. The Director of Nursing is directly accountable to the Board for all incident and serious incident reporting and management.

5.17 The Chair and Non-Executive Directors hold the Executive team to account for the management of all incidents. They seek the appropriate assurances from the Chief Executive and Directors that incidents are being identified and managed appropriately and that lessons are being learned and implemented. The PC24 Board is responsible for developing and maintaining an open culture that places safety at the forefront of its priorities at all times.

6 REPORTING INCIDENTS

6.1 The most senior person on duty is responsible for ensuring that incidents are reported by personnel.

6.2 The incident must be reported onto the Datix Risk Management System using the DIF 1 form. A link to the DIF 1 is available on each desktop. See Appendix 6.

6.3 All safeguarding concerns must be reported as incidents on the Risk Management system, Datix and also referred to the PC24 Adult or Child Safeguarding Lead, (Director of Nursing). For further guidance please refer to the Safeguarding Adults Policy (PC24POL24) or the Safeguarding Children's Policy (PC24POL23).

6.4 All incidents where there is any suspicion of fraud, bribery, corruption or a similar offence must also be reported to PC24's Chief Executive Officer.

6.5 PC24 is required to report some incidents to external agencies and stakeholders. This depends on a variety of other criteria, detailed as Appendix 1.

7 IMMEDIATE ACTION AND MANAGEMENT OF INCIDENTS

7.1 The member of personnel who discovers or is informed about the near miss/good call or incident is responsible for informing the most senior member of staff on duty and taking immediate necessary action to ensure the safety of those involved.

7.2 The most senior member of personnel is responsible for assessing the situation and taking appropriate immediate action to:

- Ensure the wellbeing of all those involved and ensure the area is safe.
- Manage the incident and minimise potential adverse effects of the incident.
- Minimise the risk of the incident occurring again in the future.
- Escalate as appropriate request support for debrief of staff in real time if the situation deems it to be appropriate.

7.3 It should be remembered that the potential exists for the location of the incident to be classified as a "scene of crime", if this is the case, or likely to be the case, the immediate location should not be disturbed more than is essential to provide first aid and should not be cleared or cleaned until authorised by police.

8 RECORDING, SCORING AND GRADING INCIDENTS

8.1 The information recorded on the Datix system is to contain factual

information and clinical judgements only, statements of opinion or assumptions must not be included. The incident report should be treated as any professional document and should be recorded the same standard.

Relevant and pertinent information must also be recorded on clinical and/or personnel records as appropriate. A printed copy of the incident from must not be used in patient or staff files as this could contain unnecessary or unrelated third party information.

8.2 The incident is graded to indicate both potential severity and the actual impact which indicates the level of investigation required. Impact influencing the grading must be directly related to the incident. (See Appendix 7, Investigation Types, Levels and Timescales).

8.3 All incidents should be scored and graded using the Risk Scoring Matrix found in Appendix 5 of this policy. The action taken in response to each incident will be determined by this score. The risk assessment should be documented using the risk assessment template in Appendix 8 of this policy.

8.4 Information Governance Incidents follow specific potential severity grading based on Information Commissioner Guidelines. Further information can be found in the PC24's Information Governance Corporate Policy and Strategy PC24POL8.

9 SERIOUS INCIDENTS (SI)

9.1 Serious Incidents in health care are adverse events, where the consequences to patients, families and carers, staff or the organisation are so significant or the potential for learning is so great, that the heightened level of response is justified. The needs of those affected should be the primary concern of those involved in the response to and the investigation of serious incidents.

9.2 Serious incidents can extend beyond incidents which affect patients directly and include incidents which may indirectly impact patient safety or an organisation's ability to deliver ongoing healthcare.

9.3 Serious Incidents must be declared internally as soon as possible and immediate action must be taken to establish the facts, ensure the safety of the patient(s), other service users and staff, and to secure all relevant evidence to support further investigation. (See Appendix 9) Serious Incidents should be disclosed as soon as possible to the patient, the family (including victims' family where applicable) or carers.

9.4 The commissioner must be informed (via StEIS and/or verbally if required) of a Serious Incident within 2 working days of it being discovered. Other regulatory, statutory and advisory bodies, such as CQC, must also be informed as appropriate without delay.

9.5 Discussions should be held with other partners (including the police or local authority for example) if other externally led investigations are being undertaken. This is to ensure investigations are managed appropriately, that the scope and purpose is clearly understood (and those affected informed) and that duplication of effort is minimised wherever possible.

9.6 Where it is not clear whether or not an incident fulfils the definition of a serious incident, PC24 will engage with the service commissioners in open and honest discussions to agree the appropriate and proportionate response.

9.7 If a serious incident is declared but further investigation reveals that the definition of a serious incident is not fulfilled, the incident can be downgraded.

9.8 Primary Care endorses the application of 7 key principles in the management of all serious incidents. (Appendix 10)

Often more than one organisation is involved in the care and service delivery in which a serious incident has occurred. If PC24 identifies the serious incident we will alert other

providers, commissioners and partner organisations as required in order to initiate discussions about subsequent action. (See Appendix 11).

10 INCIDENTS RELATING TO SAFEGUARDING VULNERABLE ADULTS & CHILDREN

10.1 Abuse means the violation of an individual's human or civil rights by another person or persons. Abuse may consist of single or repeated acts. It can be physical, sexual, verbal, psychological, or as a results of an act of neglect or omission to act.

10.2 Abuse may occur when a vulnerable person is persuaded to enter into a financial or sexual transaction to which she/he has not consented or cannot consent. Abuse can occur in any relationship and may result in significant harm or exploitation of the person subjected to it. Reference should be made to PC24's policies on Safeguarding of Vulnerable Children PC24POL23 and Safeguarding of Vulnerable Adults PC24POL74.

10.3 For adults, the national 'No Secrets Policy' defines abuse and is incorporated into local policies and strategies by the Local Authority who have their own multi-agency arrangements for managing allegations of suspected adult abuse. The Care Quality Commission provides guidance to organisations on compliance with the Registration Regulations.

10.4 For children, the statutory guidance is in Working Together to Safeguard Children March 2015. Any incident of suspected child abuse must be reported to the local social services or police safeguarding team. The organisation will be required to participate in the Local Safeguarding Board processes.

10.5 Any incident relating to either suspected or actual abuse of a vulnerable adult or child **must** be reported.

11 INFORMATION SECURITY BREACHES AND LOSS OF DATA

11.1 Any incident relating to the loss of information or data or breach of confidentiality is a serious incident. If the incident related to the loss of Person Identifiable Date (PID) must be reported to the Information Commissioner as well as commissioners via the Serious Incident process detailed in Section 9 of this policy.

11.2 The following sections should be reported under this category of serious incident:

- Breach of confidentiality
- Breach of security
- Information Security Incident

11.3 Cyber Security Incidents

All Organisations processing Health, Public Health and Adult Social Care personal data are expected to use the IG Toolkit Cyber SIRI extended functionality to contribute to health and social response to the UK's Cyber Security Strategy.

11.3.1 Definition of a Cyber Security Incident

There are many possible definitions of what a Cyber incident is, for the purposes of reporting a Cyber incident is defined as:

A Cyber-related incident is 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." Source: UK Cyber Security Strategy, 2011

11.4 Breach of confidentiality includes the following incidents:

- Finding a computer printout with a header and a person's information on it at a location outside the organisation's premises.

- Finding any paper records about a patient/member of staff or business of the organisation in any location outside the organisation's premises
- Being able to view patient records in the back (or front) of an employee's care (e.g. Doctors and Nurses)
- Discussing, in person or on the phone, patient or staff personal information with someone else in an open area where the conversation can be overheard
- A fax, email or letter being received by the incorrect recipient

11.5 Breach of Security includes:

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer medial for example, USB drive, CD due to crime or an individual's carelessness
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident
- Trying to access a secure part of the organisation's system using someone else's PIN number, swipe card
- Finding the doors and/or windows have been broken and forced entry gained to a secure room/building

11.6 Information Security Incident is any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person
- The integrity of the system or data being put at risk
- The availability of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact such as:
    - Threat to personal safety or privacy
    - Legal obligation or penalty
    - Financial loss
    - Disruption of activities
    - Embarrassment to the NHS

The Caldicott Guardian provides advice and support to all employees on matters of confidentiality and handling of patient data.

PC24 expects all personnel to abide by the Six Caldicott principles when handling or considering issues in relation to patient information and records. These can be found at Appendix 12 and are referenced in the PC24's Confidentiality, Data Protection & Caldicott policy, PC24POL1.

12 NEVER EVENTS

12.1 Never events are serious, largely preventable patient safety incidents that should not occur if the available preventative measures have been implemented.
Incidents are considered as 'Never Events' if:

- There is evidence that the never event has occurred in the past and is a known source of risk
- There is existing national guidance or safety recommendations, which if followed, would have prevented this type of never event from occurring
- Occurrence of the never event can be easily identified, defined and measured on an ongoing basis.

12.2 NHS England has a list of 25 types of incident which can be considered as 'Never Events'. These can be found listed at NHS England Never Events.

12.3 All 'Never Events' should be reported as serious incidents immediately.

13 INVESTIGATION AND ACTION PLANNING

13.1 A comprehensive investigation should be initiated for serious incidents.

13.1.1 Any investigation must be objective in its approach. In practice, this means that the investigating officer should not be connected with the people or events that are subject to investigation.

13.2 The Role and Skills of the Investigating Officer

13.2.1 The role of the investigating officer is to establish the facts of a situation or case. This can be completed via a number of means;

- Interviewing employees, patients or other parties connected with the incident
- Reviewing clinical or administrative records, both paper and electronic
- Reviewing other paper based information pertinent to the situation or case, including PC24's policies and procedures.
- Reviewing national evidence of best practice or standards
- Interviewing people with specialist knowledge or information that may be relevant to the case or situation

13.2.2 Investigation officer/teams should be appropriately trained and resourced. For Serious Incidents it is recommended that Investigation Officers/teams are sufficiently removed from the incident to be able to provide an objective view.

13.2.3 Investigating officers should have access to relevant specialists/experts, communications expertise, administrative support and/or additional resources to support investigations where required.

13.3 Appointing and briefing the Investigation Officer

13.3.1 The individual who has commissioned the investigation should appoint the Investigating Officer and provide a brief. The Director initiating the investigation should then provide a brief, including the relevant documents, terms of reference and scope of the investigation.

13.3.2 Sufficient time should be allowed for the investigating officer to interrogate the information and conduct the investigation.

13.3.3 For Serious Incidents or complex incidents, the decision may be taken to appoint an investigation team. In such cases a lead investigator will be identified and will be responsible for external updates from the investigation team.

13.3.4 The investigation process may vary depending on the requirements of the investigation. However, generally the stages are outlined in Appendix 7 and Appendix 9.

13.3.5 In cases of SI's, and following the conclusion of the investigation, the investigating officer must compile a report. (See Appendix 3) The report should:

- Be simple and easy to read
- Have an executive summary, index and contents page and clear headings
- Include the title of the document and state whether it is a draft or the final version
- Include the version date, reference initials, document name, computer file path and age number in the footer
- Disclose only relevant confidential personal information for which consent has been obtained, or if patient confidentiality should be overridden in the public interest. This should however be considered by the Caldicott Guardian and where required confirmed by legal advice
- Include evidence and details of the methodology used for an investigation (for example chronology (See Appendix 13 for chronology template) / cause and effect charts, brainstorming/brain writing nominal group technique, use of contributory factor Framework and fishbone diagrams, five whys and barrier analysis)
- Disclose if the Incident Decision Tree has been used to support the understanding as to whether the incident is attributed to organisational or individual culpability issues and describe and document your conclusion. (See Appendix 14)
- Identify root causes and recommendations
- Ensure that conclusions are evidenced and reasoned, and that recommendations are implementable

- Include a description of the support provided to patients/victims/families and staff following the incident

13.4 For **Serious Incidents** the report should be submitted to the Director assigned to deal with the **SI**, prior to presentation at the next Leadership Team meeting. The report will then be presented to the appropriate committee and the learning and actions arising from the investigation, disseminated to all staff in an appropriate format.

13.4.1 **Serious Incident** reports and action plans must be submitted to the relevant commissioner within 60 days of the incident being reported to the relevant commissioner, unless an independent investigation is required, in which case the deadline is 6 months from the date the investigation commenced. In certain circumstances, the organisation may find it difficult to complete a final report within these timescales. This might be due to:

- Enforced compliance with the timetable of an external agency, such as police, Coroner, Health and Safety Executive or Local Children Safeguarding Board or Safeguarding Adult Board
- Investigation of highly specialised and multi-organisation incidents, such as those involving a national screening programmes; or
- Incidents of significant complexity
- In such circumstances the commissioner and investigations team can agree an alternative timeframe. This should be clearly recorded and included in the serious incident report.

14 ROOT CAUSE ANALYSIS

14.1 The recognised system based method for conducting investigations, commonly known as Root Cause Analysis (RCA), should be applied for the investigations of Serious Incidents.

14.2 This endorses three levels of investigation (Appendix 7):

1) Concise investigation - suited to less complex incidents which can be managed by individuals or small groups of individuals at a local level. Commonly involves completion of a summary or one page structured template. Includes the essentials of a thorough and credible investigation, conducted in the briefest terms.

2) Comprehensive investigations – Commonly conducted for actual or potential 'severe harm or death' outcomes for incidents. Conducted to a high level of details, including all elements of a thorough and credible investigation. Includes use of appropriate analytical tools (e.g tabular timeline, contributory factors framework, change analysis, barrier analysis). Normally conducted by a multidisciplinary team, or involves experts/expert opinion/independent advice or specialist investigator(s). Conducted by staff not involved in the incident, locality or directorate in which it occurred. Overseen by a member of staff at Deputy Director level or above. Led by person(s)) experienced and/or trained in RCA, human error and effective solutions development. Duty of Candour requirements must be fulfilled. May require management of the media via the organisation's communications department. Includes robust recommendations for shared learning, locally and/or nationally as appropriate. Includes a full report with an executive summary and appendices.

3) Independent investigations – Incorporates all of the descriptors outlined in the above section. In addition, may be suited to incidents where the integrity of the internal investigation is likely to be challenged or where it will be difficult for an organisation to conduct an objective investigation internally due to the size of organisation, or the capacity/ capability of the available individuals and/or number of organisations involved. Commonly considered for incidents of high public interest or attracting media attention.

The level of investigation should be proportionate to the individual incident. **Concise** and **Comprehensive** investigations should be completed within 60 days and **Independent** investigations should be completed within 6 months of being commissioned.

15 RIDDOR REPORTING REQUIREMENTS

15.1 The reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) requires the service to notify the Health and Safety Executive of accidents at work.

15.2 Primary Care 24 is required to report the following:

- **Death or major injuries** where an employee or a self-employed person working on PC24 premises is killed or suffers a major injury. It is also where a member of the public is killed or suffers an injury as a result of an accident and is taken to hospital from the site of the accident. Reportable major injuries include, fractures, amputation and loss of sight and chemical burns.

- **'Over three day'** injuries are those injuries at work, including acts of physical violence, where an employee, or self-employed person working on PC24 premises, suffers an injury which is not major but results in the injured person being away from work, or unable to do a full range of their normal duties for more than three days. This includes any days they would not normally be expected to work, such as weekends or rest days but excludes the day of the injury itself.

- **Certain diseases and dangerous occurrences**. For the full list of reportable incidents and occurrences, please see the Health and Safety Executive list of Reportable Incidents.

16 STATURORY NOTIFICATIONS TO THE CARE QUALITY COMMISSION

16.1 As part of the registration requirements of the Care Quality Commission, PC24 has a duty to notify and report specific incidents and events. These are summarised in the table below.

16.2 Table of statutory notifications under the Health and Social Care Act 2008

Regulation	Essential standards outcome	Notification

12	15	Changes to the provider's statement of purpose
14	27	Absence (and return from absence) of registered persons
15	28	Changes affecting a registered person
16	18	Death of a person who uses the service
17	19	Deaths and unauthorised absences of people who are detained or liable to be detained under the Mental Health Act 1983
18	20	Serious injuries to people who use the service
18	20	Application to deprive a person of their liberty (under the Mental Capacity Act)
18	20	Abuse and allegations of abuse involving people who use the service
18	20	Events that prevent or threaten to prevent the provider from carrying on regulated activities safely and properly
18	20	Incidents reported to or investigated by the police*
20†	n/a	Death of a woman after a termination of pregnancy*
21†	n/a	Death of a service provider (including a personal representative's plans for a service following the death of a provider)
22†	n/a	Appointment of liquidators

† these notifications are not part of an essential standards outcome. Please see the relevant regulation in the Care Quality Commission (Registration) Regulations 2009.

16.3 The Registered Individual will be informed of any potential notifications. It is the responsibility of the Registered Individual to inform the Chief Executive of this notification and to subsequently contact the Care Quality Commission.

16.4 Should deadlines not be met, numbers and details of overdue incidents and Sis will be escalated on a weekly basis to the Professional Leads, Divisional Directors and Clinical Directors via the Incident and SIRI Flash Report.

17 RECORD KEEPING

17.1 It is an essential part of incident management and investigation that good records are kept by all those involved. Records should always be contemporaneous. Within a reasonable time of the incident occurring, records should be made in order to ensure that reporting is as accurate as possible. All incidents should be recorded on the Datix Risk

Management Database. All hard copies of information should be kept safe and secure in accordance with PC24's Information Governance policies.

17.2 Reference should be made to PC24's Information Governance policies, particularly Confidentiality, Data Protection & Caldicott policy (PC24POL1). All reports should be anonymised. Reports transmitted electronically should be password protected.

18 LEARNING FROM INCIDENTS

18.1 The purpose of reporting and investigating incidents is to ensure that PC24 learns and prevents similar incidents from occurring in the future. Sharing learning is therefore crucial and should happen at all levels within PC24.

18.2 Team/Heads of Service should ensure that following any investigation, a full and robust action plan is created and implemented to resolve any issues or requirements identified through the investigation.

18.3 Learning from incidents should be widely shared with staff as well as across PC24 where appropriate and changes in practice should be embedded as appropriate to encourage organisational learning.

18.4 Individuals should also use the incident investigation and learning process towards their own continual professional development.

18.5 Directors are responsible for ensuring robust governance processes are in place to ensure that action plans are implemented and learning from incidents is shared between teams across PC24.

18.6 Where the incident has been classified as a SI, the learning from the investigation will be reported to the relevant Clinical Commissioning Group via the Commissioning Monitoring Board meetings.

19 COMMUNICATION

19.1 When an investigation is being undertaken in relation to an incident, staff should follow the PC24's Duty of Candour Policy PC24POL103 which provides guidance for staff and ensures that patients, service users, relatives and carers are provided with information prior to, during and after the investigation according to their wishes. Communications should be documented in line with these policies.

19.2 Some incidents may result in media interest. In these circumstances, wherever possible, patients, service users and their relatives and carers must be fully informed of any circumstances which involve them before any information is released to the media.

19.3 Heads of Service are responsible for providing adequate and appropriate support for staff following an incident, all support must remain confidential. Staff must be informed if an investigation is being undertaken into an incident in which they were involved and kept up to date with the progress of any such investigations, the eventual outcome and learning to be implemented. We appreciate that being part of a investigation can be distressing for some people. Managers should discuss the impact of the investigation on their team members and ensure that they are aware that staff counselling is available. Additional information on resilience is available from HR.

20 TRAINING

20.1 All personnel on appointment will attend Datix & Risk Awareness Training and introduction to this policy. See Training Needs Analysis in Appendix 15.

20.2 Heads of Service, Service Managers, Practice Managers, Clinical and Medical Leads require more detailed training. This should be include assessing and scoring incidents, managing the overall process, and undertaking investigations. Bespoke management of investigations will be provided. Over and above introduction to Root

Cause Analysis Training will be provided with a period of mentorship and support to provide assurance of learning.

20.3 Heads of Service, Practice Managers and identified clinical and medical staff who are required to investigate SI's will be supported by a fully trained member of personnel who has completed formal 3 day Root Cause Analysis Training.

20.4 Additionally, Board members benefit from training as part of their generic corporate development programme. This is to ensure that they properly understand patient safety and risk in the healthcare context generally and out of hours care specifically. This training includes an understanding of the interpretation of data regarding incidents, identification of trends and issues arising from incidents and on their role in overseeing and holding the organisation to account in relation to incidents and SIs.

21 IMPLEMENTATION

21.1 This Policy will be implemented via the document owner with the support of the Heads of Service, Associate Directors and any relevant Committees.

21.2 The document owner will outline the plan for implementation in conjunction with the production of the policy (Appendix 16). Training needs should be assessed and identified.

21.3 **Dissemination.** Once this policy has been approved, it will be loaded onto the staff intranet, this will be supported by a message through PC24's newsletter, NEWS24. Quality & Patient Safety team will be responsible for this action.

22 MONITORING COMPLIANCE

The Quality and Patient Safety Department responsible for monitoring compliance with this policy every 12 months or sooner to ensure that staff are

meeting the policy requirements. The following performance measures will be used:

Policy Requirement	Performance Indicator	Measure
Incidents being reported and managed in a timely way in line with this policy. Root Cause Analysis training will be provided to staff who may be identified to carry out an investigation.	90% or more of incidents are being signed off by managers or marked as "under review" within 1O days of the incident being reported.	• Reporting from Datix on Reporting and Management Timescales by the Safety & Quality Workforce Committee.
SI's are reported onto StEIS within 2 working days of the Quality & Patient Safety Department being notified of the incident	100% of SI's (or likely SI's) are reported onto StEIS within 2 working days of notification of the incident	Reporting on External Reporting requirements presented to Safety & Quality Workforce Committee
Staff receive training on reporting and managing incidents as part of Risk Training	100% of staff are up to date with Datix Awareness and Risk Management Training	Reporting on training compliance through SDU's to Quality and Patient Safety Department.

23 CONFIDENTIALITY

It is important that all investigations are conducted with due regard to confidentiality. Only those individuals who are required to be involved in the investigation should be informed about the process and its outcomes, subject to the full dissemination of learning and actions.

24 EQUALITIES AND HEALTH INEQUALITIES STATEMENT

PC24 is committed to an environment that promotes equality and embraces diversity in its performance as an employer and service provider. It will adhere to legal and performance requirements and will mainstream equality and diversity principles through its policies, procedures and processes. This policy has been implemented with due regard to this commitment. To ensure that the implementation of this policy does not have

an adverse impact in response to the requirements of the Equality Act 2010 this policy has been screened for relevance during the policy development process and a full equality impact analysis conducted where necessary. PC24 will take remedial action when necessary to address any unexpected or unwarranted disparities and monitor practice to ensure that this policy is fairly implemented.

25 PERSONAL INFORMATION STATEMENT

PC24 is committed to an environment that protects personal information aspects in the development of any policy. When proposing change there is a new requirement for policy writers to investigate when the personal information aspect of the policy complies with the data protection principles in Schedule 1 of the Data Protection Act 1998. All individuals with responsibility for reviewing/writing policies should consider Privacy Impact Assessment compliance.

This policy complies with the Data Protection Act 1998, therefore no Privacy Impact Assessment is necessary.

26 FINANCIAL IMPACT & RESOURCE IMPLICATIONS

Awareness and basic training of incident reporting, management and risk will be provided at PC24's Induction for new staff, additional training will be provided for staff who have not undertaken and incident awareness training. Staff who undertaken investigations must have undertaken PC24's approved Root Cause Analysis (RCA) training.

Continuous update, maintenance and licensing of the Datix Risk Management System require both resource and finance provided by the Quality & Patient Safety Team.

27 POLICY REVIEW

This policy will be reviewed 3-yearly or sooner if national guidance or legislation requires, or if there are changes to PC24's internal processes.

28 REFERECES

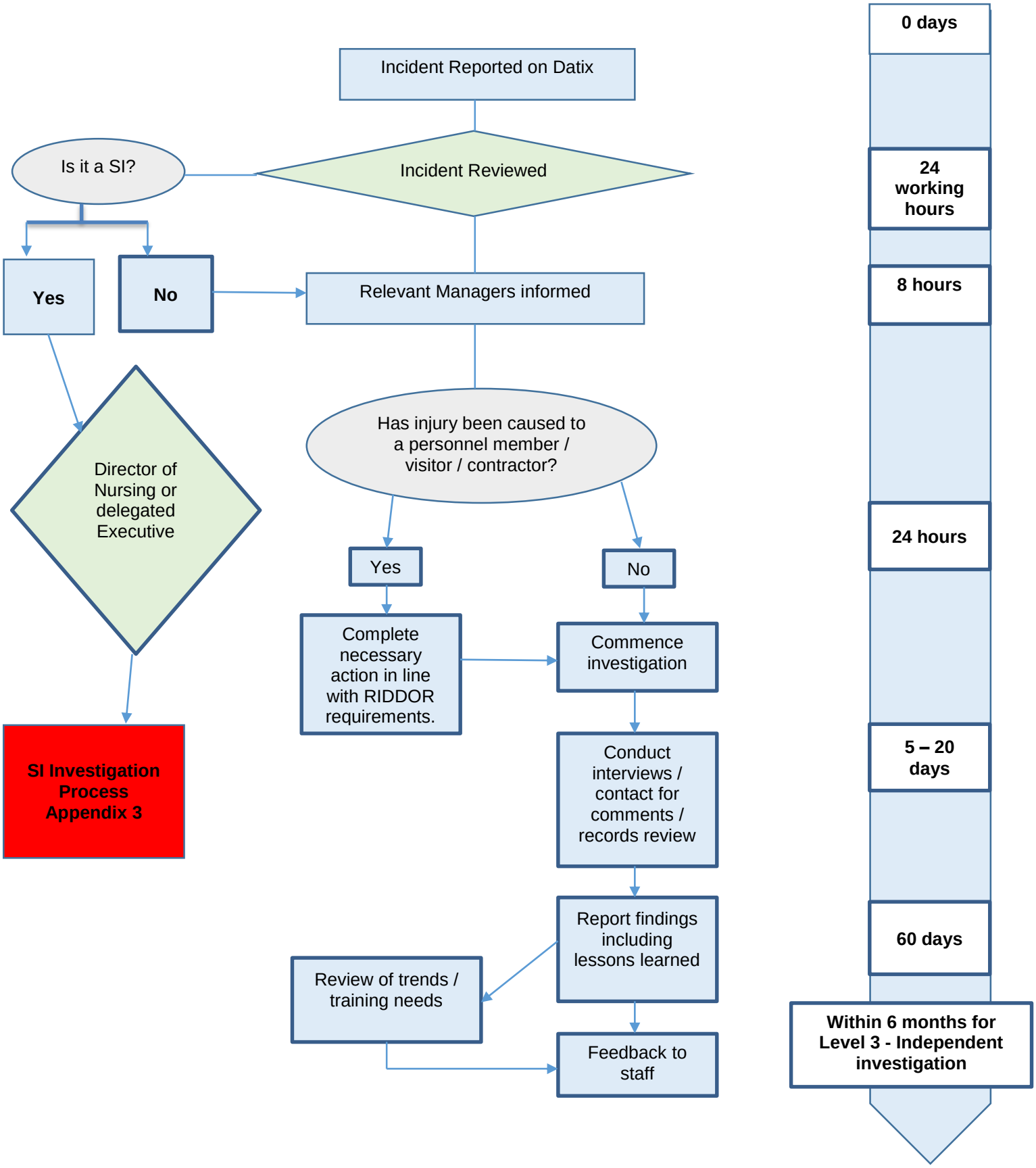
https://www.england.nhs.uk/patientsafety/wp-content/uploads/sites/32/2015/04/never-evnts-pol-framwrk-apr2.pdf

https://www.england.nhs.uk/patientsafety/wp-content/uploads/sites/32/2015/04/serious-incidnt-framwrk-upd2.pdf

http://www.hse.gov.uk/riddor/reportable-incidents.htm

END OF POLICY

APPENDIX 1 INCIDENT REPORTING PROCESS



APPENDIX 2 EXTERNAL REPORTING REQUIREMENTS FOR INCIDENTS

Incident Type	Agency To Notify	Person Responsible
Serious Incidents requiring investigation (SI), including serious physical assault on staff	Strategic Executive Information System (StEIS) Relevant Clinical Commissioning Group NHS England	Quality & Patient Safety Team
Information governance Incidents graded as SIs	Information Commissioner	Information Governance Manager
Serious injuries to staff at work or incidents which result in 7 or more calendar days off work	Health and Safety Executive Reporting of Incidents, Diseases or Dangerous Occurrences Regulation (RIDDOR}	Quality & Patient Safety Team
RIDDOR reportable Serious Injuries to patients	Health and Safety Executive Reporting of Incidents, Diseases or Dangerous Occurrences Regulation (RIDDOR)	Quality & Patient Safety Team
Medical Device failures	Medicines & Healthcare Regulatory Authority (MHRA)	Quality & Patient Safety Team
Incidents under Regulation 18 of the Health and Social Care Act (2008)	Care Quality Commission (CQC}	Quality & Patient Safety Team
Incidents leading to legal and/or insurance claims	Contacting Monitoring Board Company Insurance	Company Secretary
Notifiable diseases	Centre for Communicable Disease Control HSE Incident Contact Centre for RIDDOR	Registered Medical Practitioner (attending)
Infection control outbreaks	Health Protection Agency (HPA)	Director of Quality & Patient Safety

There will be situations where Managers may need to notify the Police, Professional Bodies or other organisations dependent on what further support is needed or where stakeholders or partner organisations need to be informed.

APPENDIX 3 INVESTIGATION TEMPLATE

Investigation Template – please complete all sections

Datix Reference No.		Risk Grading, Department, actual effect on patient/service and severity of incident	
Date Incident/ Complaint received			
Is this StEIS Reported Yes/No			
Incident Detail			
Duty of Candour / Involvement, support patient relatives, staff			
Investigation Type (Concise, Comprehensive, Independent)			
Investigation Lead / Team			
Terms of Reference			
Date Investigation Commenced			
Target Date for Completion			
Case / Adastra Number			
Contributory factors (internal / External)			
Care & Service Delivery Issues			
Investigation findings/conclusion			

Planned actions – please detail who these actions are assigned to (please use separate action plan if required).	
Feedback to individuals concerned	
Lessons Learnt	
Details of any disseminated learning/feedback	
Date investigation completed	

APPENDIX 4 ACTION PLAN TEMPLATE

Action Plan – Datix Reference No:

Action Plan Title	
Owner, designation	
Dept/Service	
Version (Title, date, initials)	
Risk Register link	

Issue Status	Completed	In progress, on track	In progress, off track	Not started

	Issue	Action	Who	By when	Progress	Status
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

APPENDIX 5 RISK SCORING MATRIX

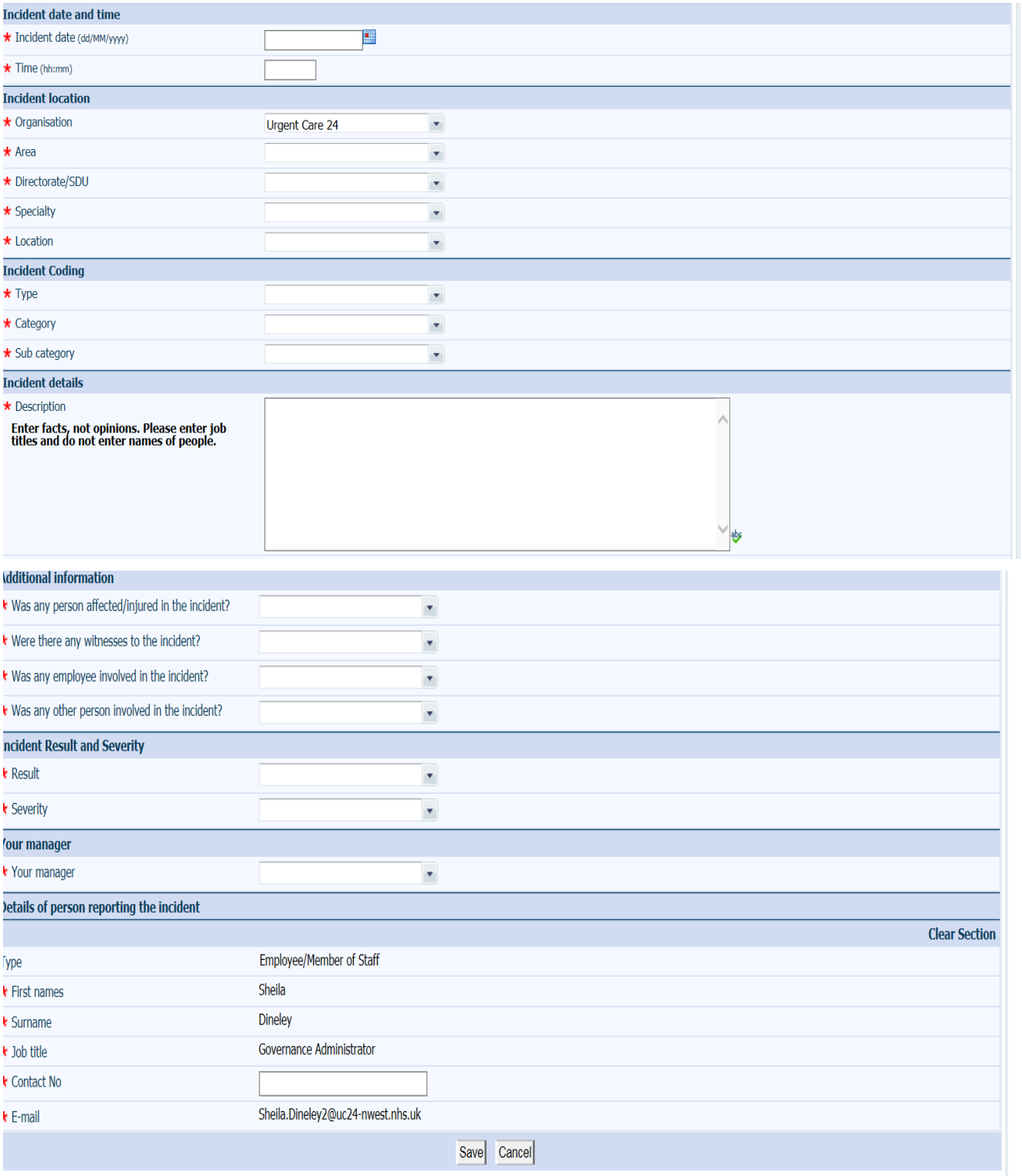
Likelihood (of hazard being realised)	Consequence				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Rare (1)	1	2	3	4	5
Unlikely (2)	2	4	6	8	10
Possible (3)	3	6	9	12	15
Likely (4)	4	8	12	16	20
Almost Certain (5)	5	10	15	20	25

Likelihood	Descriptor	Description
5	Almost Certain	Likely to occur on many occasions, a persistent issue
4	Likely	Will probably occur but is not a persistent issue
3	Possible	May occur/recur occasionally
2	Unlikely	Do not expect it to happen but it is possible
1	Rare	Cannot believe that this will ever happen

Consequence	Impact on individual	Actual or potential Impact on Organisation	Number of people involved	Complaint / Claim
Catastrophic (5)	Death/major/permanent incapacity/disability. Totally unsatisfactory patient outcome. Failure of critical system or project. Major financial loss.	Adverse national publicity, possible external investigation	Many, e.g. evacuation, patient safety	Certain
Major (4)	Extensive injuries/long term incapacity/disability. Patient outcome or experience significantly below reasonable expectation across the board. Failure of important system/project. Serious financial loss.	Service closure, RIDDOR reportable, long term sickness	Moderate Number, e.g. loss of records	Certain
Moderate (3)	Medical treatment required/some temporary incapacity. Partial resolvable failure of system.	RIDDOR reportable, short term sickness	Small numbers e.g. 3-10	Possible
Minor (2)	First aid/self-treatment/no incapacity. Identified financial loss.	Minimal risk to the organisation	Less than 3	Unlikely
Insignificant (1)	Potential to cause harm but impact was prevented/injury or illness not requiring intervention. Minimal/low financial loss	No risk at all to the organisation.	Less than 3	Possibility

APPENDIX 6 DIF 1 – DATIX INCIDENT REPORT

All incidents to be reported on Datix using the DIF 1 proforma.



APPENDIX 7 INVESTIGATION TYPES, LEVELS AND TIMESCALES

Concise – Level 1	Comprehensive – Level 2	Independent – Level 3
Timescale for Completion		
Internal investigations whether concise or comprehensive must be completed within 60 working days of the incident being reported		**6 months from the date the investigation is commissioned**
Most commonly used for Incidents, claims, complaints or concerns that resulted in no, low or moderate harm to the patient.	Commonly conducted for actual or potential 'severe harm or death' outcomes from incidents, claims, complaints or concerns.	As per Comprehensive, but in addition must be *commissioned and conducted* by those independent to the provider service and organisation involved.
Also useful as an executive summary to communicate findings from full, comprehensive or independent investigation reports, following actual or potential 'severe harm or death' outcomes.	Conducted to a high level of detail, including all elements of a thorough and credible investigation. Includes a full report with an executive summary and appendices.	Commonly considered for incidents, claims, complaints or concerns of high public interest or attracting media attention.
Commonly involves completion of a summary or one page structured template.	Includes use of appropriate analytical tools (e.g. tabular timeline, contributory factors framework, change analysis, barrier analysis).	Conducted for mental health homicides which meet Department of Health guidance.
Includes the essentials of a thorough and credible investigation, conducted in the briefest terms.	Normally conducted by a multi-disciplinary team, or involves experts/expert opinion/independent advice or specialist investigator.	Should be conducted where Article 2 of the European Convention on Human Rights is, or is likely to be, engaged
Involves a select number of RCA tools (e.g. timeline, 5 why's, contributory factors framework).	Conducted by staff not involved in the incident, locality or directorate in which it occurred.	
Conducted by one or more people (with a multidisciplinary approach if more than one investigator)	Overseen by a director level chair or facilitator.	
Often conducted by staff local to the incident	Led by person(s) experienced and/or trained in RCA, human error and effective solutions development.	
Should include person(s) with knowledge of RCA, human error and effective solutions development.	Includes patient/relative/carer involvement and should include an offer to patient/relative/carer of links to independent representation or advocacy services.	
If a patient is directly affected, they / relative/carer should be involved.	May require management of the media via the organisation's communications Department.	
Includes plans for shared learning locally and/or nationally as appropriate.	Includes robust recommendations for shared learning, locally and/or nationally as appropriate.	

APPENDIX 8 RISK ASSESSMENT TEMPLATE

Location/Activity:

Assessment date:

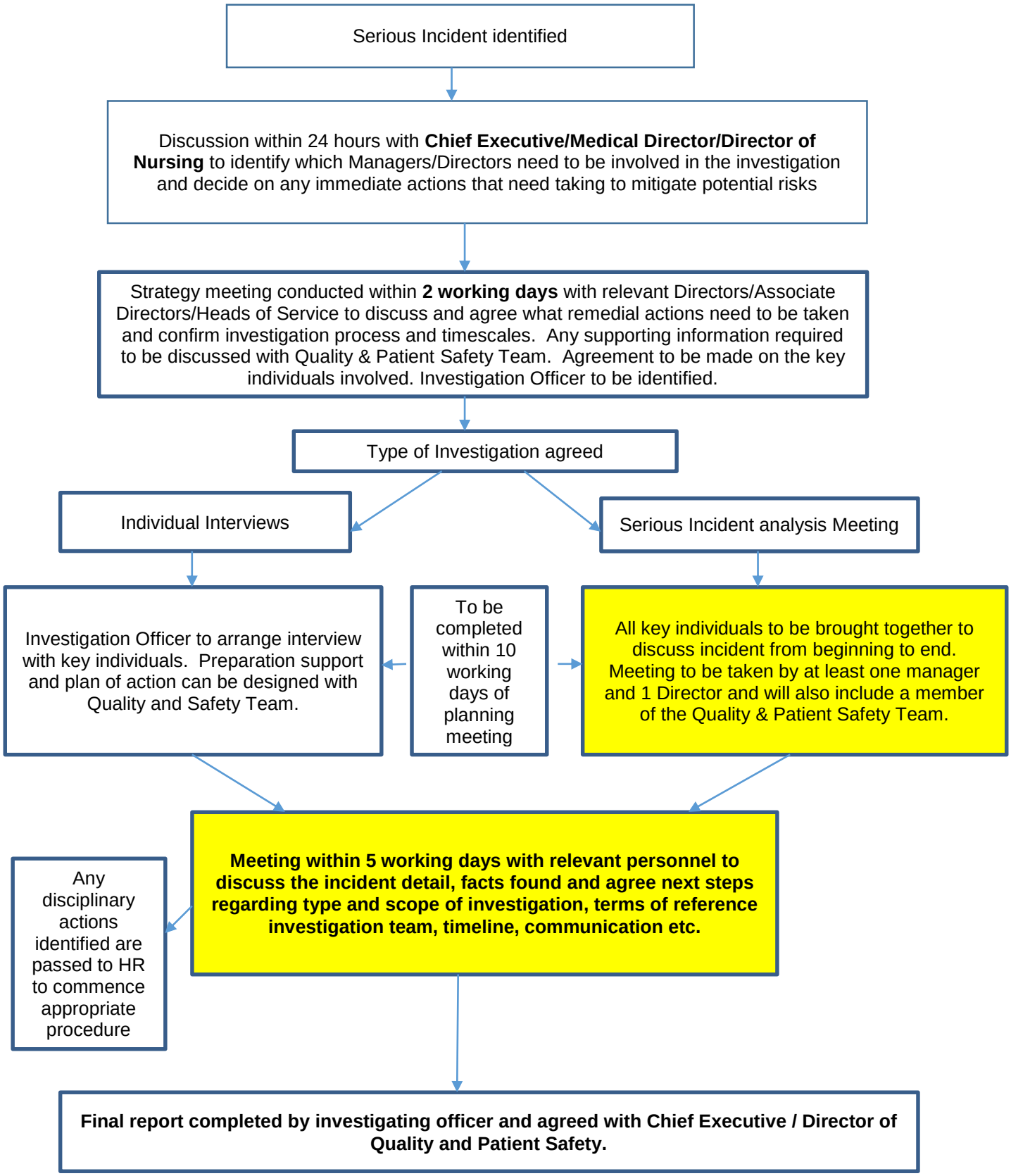
Assessor: Signature: Review date:

Ref	Hazards	Risks	People at risk	Current Control Measures	LxC = R			Is further action required (Y/N)
1.0								
2.0								

3.0								
4.0								

APPENDIX 9 CONCISE INTERNAL GUIDELINES – SERIOUS INCIDENT

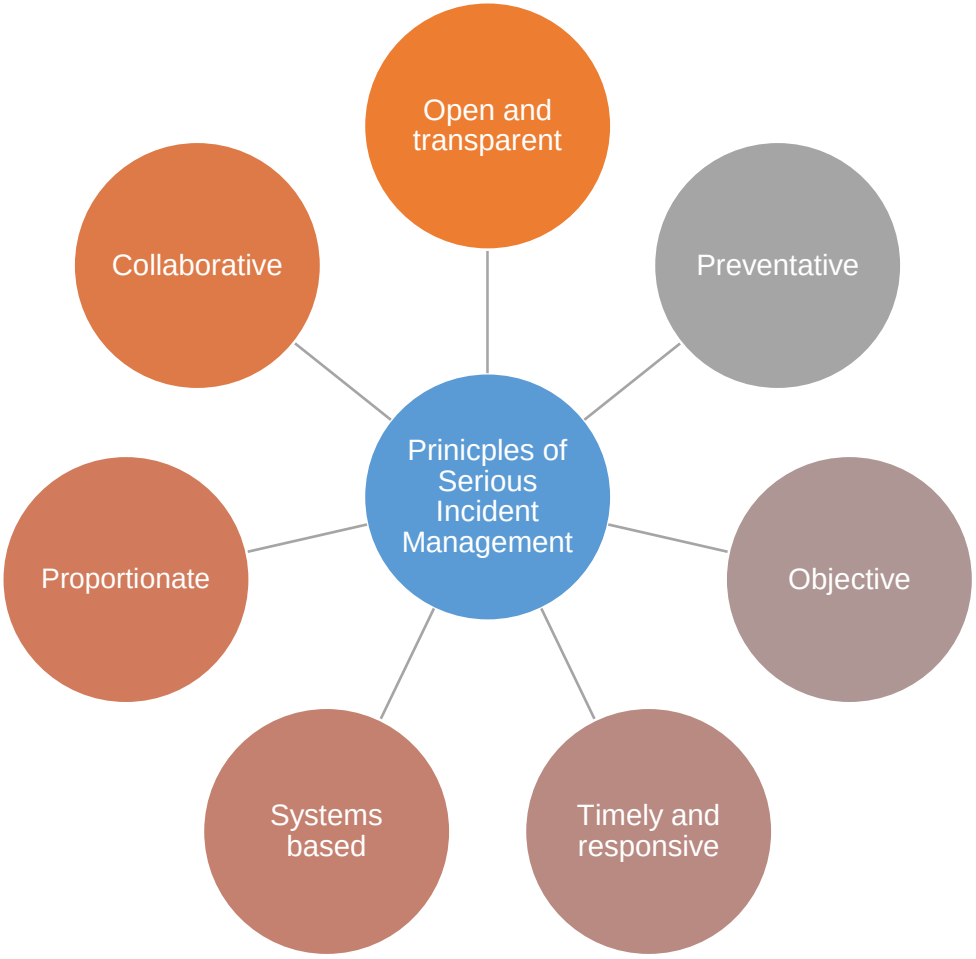
Concise internal guidelines for immediate actions once a Serious Incident has been identified



APPENDIX 10 SEVEN KEY PRINICIPLES OF SERIOUS INCIDENT MANAGEMENT

This Framework endorses the application of 7 key principles in the management of all serious incidents

Principles of Serious Incident Management



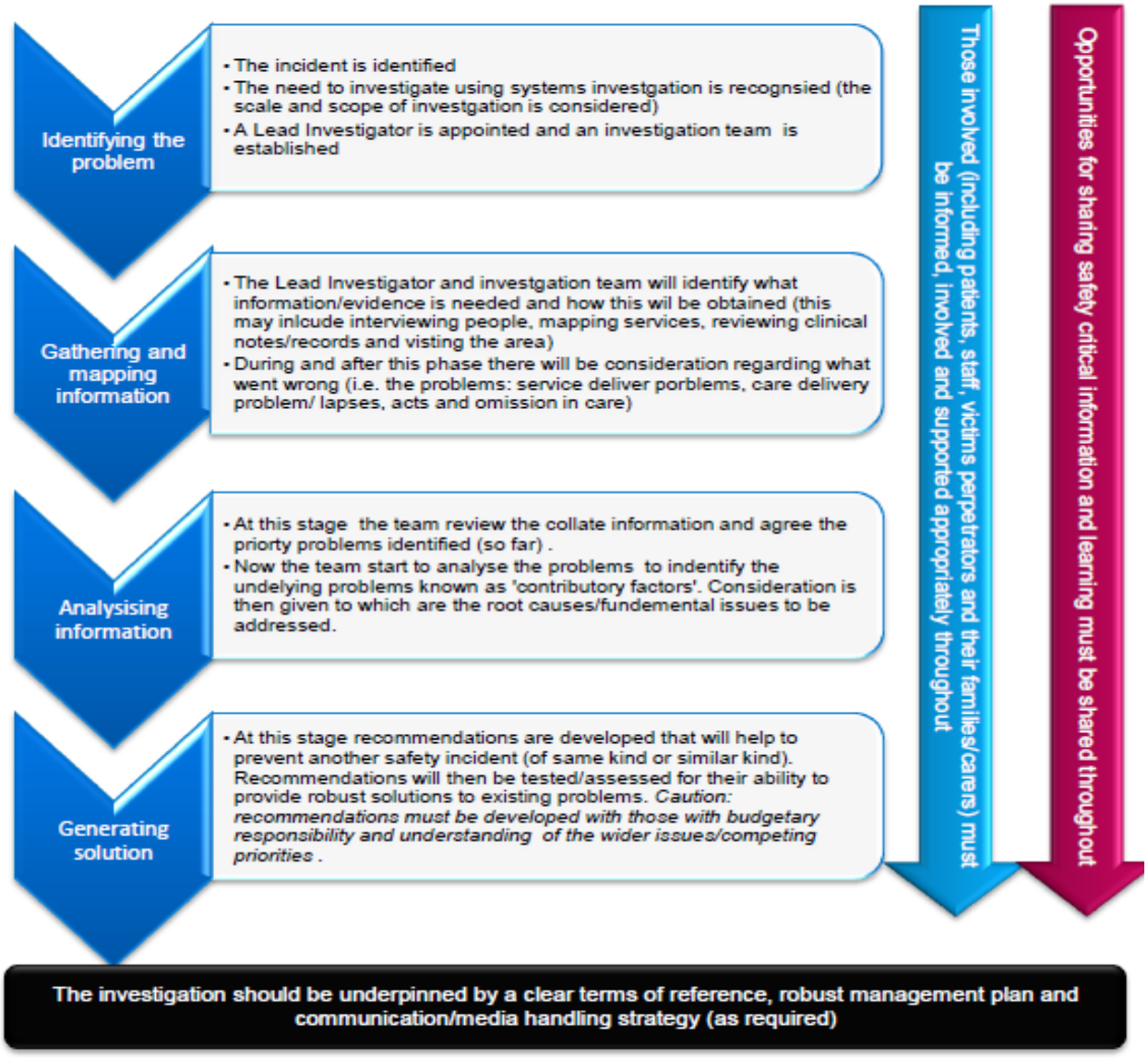
Key Principle	Supporting Information
Open and Transparent	The needs of those affected should be the primary concern of those involved in the response to and the investigation of serious incidents. The principles of openness and honesty as outlined in the NHS Being Open guidance and the NHS contractual Duty of Candour must be applied in discussions with those involved. This includes staff and patients, victims and perpetrators, and their families and carers. Openness and transparency (as described in 'Being Open') means: • Acknowledging, sincerely apologising and explaining when things have gone wrong; • Conducting a thorough investigation into the incident, ensuring patients, their families and carers are satisfied that lessons learned will help prevent the incident recurring; • Providing support for those involved to cope with the physical and psychological consequences of what happened. Saying sorry is not an admission of liability and is the right thing to do. Healthcare organisations should decide on the most appropriate members of staff to give both verbal and written apologies and information to those involved. This must be done as early as possible and then on an ongoing basis as appropriate. The NHS Litigation Authority provides advice on saying sorry available online from: http://www.nhsla.com/claims/Documents/Saying%20Sorry%20-%20Leaflet.pdf
Preventative	Investigations of serious incidents are undertaken to ensure that weaknesses in a system and/or process are identified and analysed to understand what went wrong, how it went wrong and what can be done to prevent similar incidents occurring again Investigations carried out under this Framework are conducted for the purposes of learning to prevent recurrence. They are not inquiries into how a person died (where applicable) as this is a matter for Coroners. Neither are they conducted to hold any individual or organisation to account. Other processes exist for that purpose including: criminal or civil proceedings, disciplinary procedures, employment law and systems of service and professional regulation, such as the Care Quality Commission and the Nursing and Midwifery Council, the Health and Care Professions Council, and the General Medical Council. In circumstances where the actions of other agencies are required then those agencies must be appropriately informed and relevant protocols, outside the scope of this Framework, must be followed. Organisations must advocate justifiable accountability and a zero tolerance for inappropriate blame. The Incident Decision Tree should be used to promote fair and consistent staff treatment within and between healthcare organisations.
Objective	Those involved in the investigation process must not be involved in the direct care of those patients affected nor should they work directly with those involved in the delivery of that care. Those working within the same team may have a shared perception of appropriate/safe care that is influenced by the culture and environment in which they work. As a result, they may fail to challenge the 'status quo' which is critical for identifying system weaknesses and opportunities for learning. Demonstrating that an investigation will be undertaken objectively will also help to provide those affected (including families/carers) with confidence that the findings of the investigation will be robust, meaningful and fairly presented.

	To fulfil the requirements for an independent investigation, the investigation must be both commissioned and undertaken independently of the care that the investigation is considering
Timely and responsive	Serious incidents must be reported without delay and no longer than 2 working days after the incident is identified (Part Three; section 3 outlines the process for reporting incidents). Every case is unique, including: the people/organisations that need to be involved, how they should be informed, the requirements/needs to support/facilitate their involvement and the actions that are required in the immediate, intermediate and long term management of the case. Those managing serious incidents must be able to recognise and respond appropriately to the needs of each individual case.
System Based	The investigation must be conducted using a recognised systems-based investigation methodology that identifies: o The problems (the what?); o The contributory factors that led to the problems (the how?) taking into account the environmental and human factors; and o The fundamental issues/root cause (the why?) that need to be addressed. Within the NHS, the recognised approach is commonly termed Root Cause Analysis (RCA) investigation. The investigation must be undertaken by those with appropriate skills training and capacity.
Proportionate	Typically, serious incidents require a comprehensive investigation, but the scale and scope (and required resources) should be considered on a case by-case-basis. Some incidents may be managed by an individual (with support from others as required) whereas others will require a team effort and this may include members from various organisations and/or experts in certain fields. In many cases an internally managed investigation can fulfil the requirements for an effective investigation. In some circumstances (e.g. very complex or catastrophic incidents spanning multiple organisations and/or where the integrity of the investigation would be challenged/ undermined if managed internally) an independent investigation may be required. In exceptional circumstances a regional or centrally-led response may be required.
Collaborative	Serious incidents often involve several organisations. Organisations must work in partnership to ensure incidents are effectively managed. There must be clear arrangements in place relating to the roles and responsibilities of those involved (see Part Two, section 2 and 3 below). Wherever possible partners should work collaboratively to avoid duplication and confusion. There should be a shared understanding of how the incident will be managed and investigated and this should be described in jointly agreed policies/procedures for multi-agency working.

APPENIDX 11 OVERVIEW OF THE INVESTIGATION PROCESS WITHIN THE NHS

This schematic provides a brief overview of a systems investigation for investigating serious incidents in the NHS. It requires a 'questioning attitude that never accepts the first response', and uses recognised tools and techniques to identify:

- The problems (the what?) including lapses in care/acts/omissions; and
- The contributory factors that led to the problems (the how?) taking into account the environmental and human factors; and
- The fundamental issues/root cause (the why?) that need to be addressed.



APPENDIX 12 THE SIX CALDICOTT PRINCIPLES

1 Justify the purpose(s) of using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2 Do not use patient-identifiable information unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3 Use the minimum necessary patient-identifiable information that is required

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4 Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5 Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6 Understand and Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation compliers with legal requirements.

Any breach of the above principles must be reported to the Caldicott Guardian (Director of quality and Patient Safety) and be followed up following the documented process.

APPENDIX 13 CHRONOLOGY

CHRONOLOGY

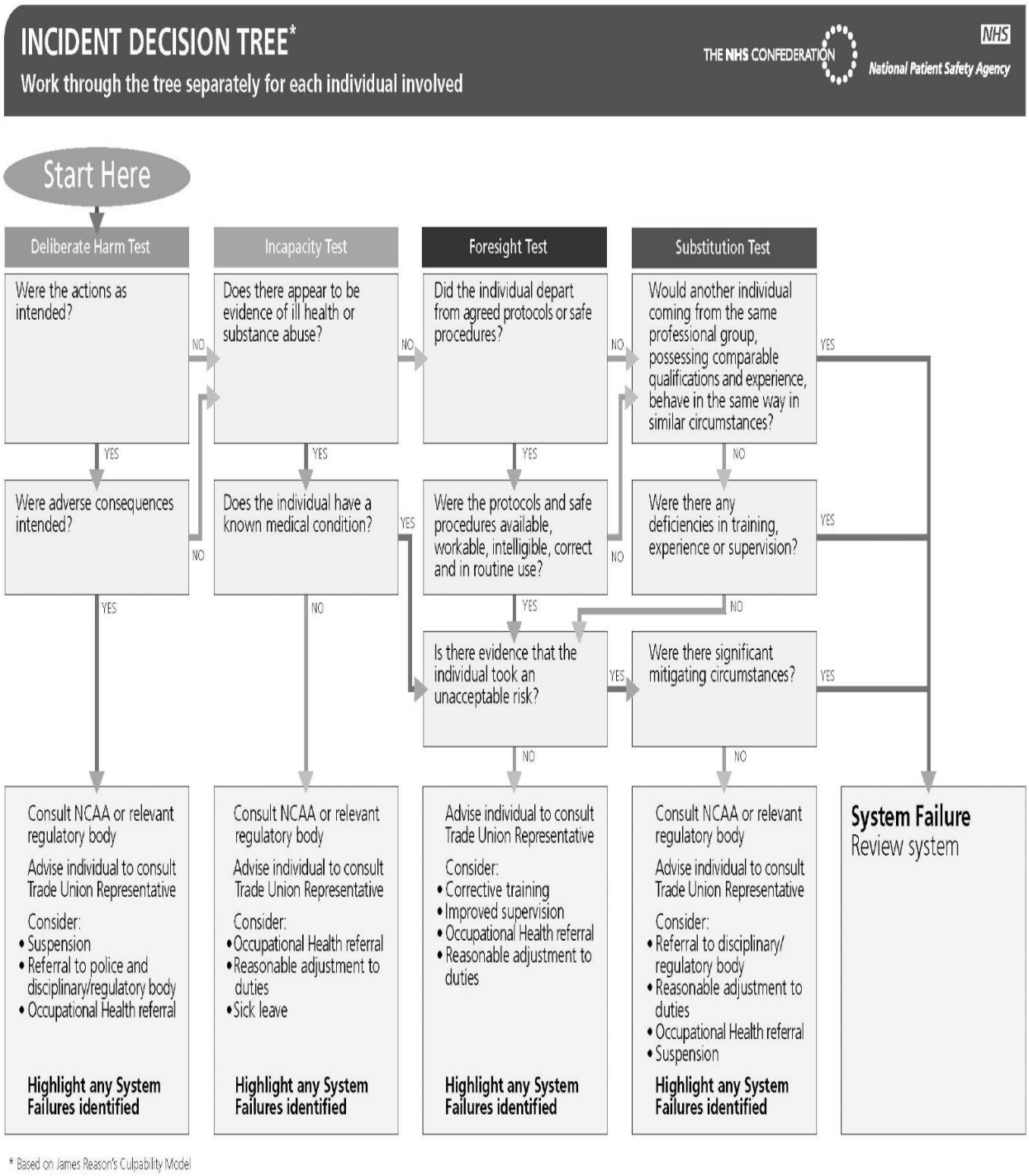
Complaint Datix Reference:

Please Note: All documentation relating to this incident/complaint, including emails must be uploaded onto Datix, filed in the appropriate folder on the shared drive and an entry made in this chronology for any action undertaken in respect of this complaint.

Item	Date	Time	Staff	Chronology (What happened)	Care Delivery Issues/Service Delivery Issues. Supplementary information	Notable Practice (areas of best practice)

APPENDIX 14 CLINICAL INCIDENT DECISION TREE

National Patient Safety Agency – Incident Decision Tree.



APPENDIX 15 TRAINING NEEDS ANALYSIS (TNA)

Training Programme	Course Length	Delivery Method	Staff Group	Recording Attendance	Strategic & Operational Responsibility
Root Cause Analysis Training	1 day	Face to face or classroom with period of ongoing mentorship and support	Senior Staff and /or those staff who have been identified to become investigating officers within their role	Quality & Patient Safety Team	Director of Nursing
Datix & Risk Awareness Training	2 hours	Face to face	All staff	Quality & Patient Safety Team	Director of Nursing
Datix Risk Management Training (DIF 2)	2 hours	Bespoke 1 -1	Directors, Associate Directors, Heads of Service, Practice Managers and Service Managers	Quality & Patient Safety Team	Director of Nursing

APPENDIX 16 POLICY IMPLEMENTATION PLAN

Question	Response	Additional resources If so identify	Timescale
Who does the policy affect	All PC24 Personnel	Nil	4 weeks
What additional Standard Operating Procedures or forms need to be included in the policy	As outlined in the appendices	Nil	As above
What is the proposed date of implementation	January 2017	Nil	As above
Is training required	Refer to TNA embedded in document.	Nil	
If so what training is required (attach separate training outline)	Refer to TNA embedded in document.	Nil	
Who will facilitate the training	Quality & Patient Safety Team and external providers as and when appropriate	Nil	
What audit processes have been identified	Refer to Monitoring and Compliance within the document.	Nil	