South East Coast Ambulance Service NHS
NHS Foundation Trust

Incident Reporting Policy (DATIX) & Procedure

Contents

1 Introduction

1.1. South East Coast Ambulance NHS Foundation Trust (here after known as the Trust) is committed to an open and just culture on the reporting of incidents. This is to empower staff to report all incidents that affect the safety of patients, staff, contractors and the Trust no matter if harm has occurred or a near miss event. Evidence shows that health services with a higher reporting of incidents learn more from them than organisations with a lower figure. The aim for the organisation is to develop a culture where staff are praised for raising incidents where they have made a mistake. The organisation believes that operating units with a greater numbers of incidents reported are viewed positively, as they are considered to have a greater level of patient safety awareness. Staff that raise concerns are viewed positively rather than as trouble makers.

1.2. The Trust uses a system called DATIX to report all adverse incidents that occur within the Trust. DATIX is the Trust's database for incidents as well as complaints, claims, risks and safety alerts. Its purpose is the management of incidents and to facilitate learning from incidents to minimise and prevent future incidents to patients, staff and Trust. All users who have access to a Trust PC or an iPAD can log incidents on Datix via the DIF1 form.

2 Aims and Objectives

2.1. The objectives of this policy are as follows;

- Outline the process and the stages of incident reporting.
- Identify the responsibilities of individual posts and groups in response to the management of incidents.
- Understand what constitutes an incident.
- Ensure the Trust prioritises the management and governance of incidents.
- Maintain consistency in approach across the Trust.
- Ensure the Trust acts in a transparent manner.
- Involve and fully inform service users, stakeholders and staff and act in a manner consistent with Duty of Candour.
- Ensure there is an emphasis on learning and action is taken to minimise reoccurrence.
- Share learning across the Trust and when appropriate the Ambulance Service and wider NHS.

3 Definitions

3.1. **Incident:** Any adverse event or circumstance arising that could have or did lead to unintended or unexpected harm, loss or damage to patients, staff, visitors, carers, members of the public or Trust premises, property, other assets, information, or any other aspect of the organisation. They can involve any number of different factors, e.g. injury, damage, loss, fire, theft, violence, abuse, accidents, ill health, disruption to services etc. (Appendix A) provides an overview of incident types with a working definition.

3.2. **DIF1:** Datix Incident Form 1, the form that all staff have access to, to report Datix incidents.

3.3. **DIF2:** Datix Incident Form 2, the form that staff with Datix profiles have access to, to investigate/overview incidents.

3.4. **Near Miss or Preventable Incident:** An incident that did not lead to harm, loss or damage but had serious potential to do so, where lessons can be learnt to implement changes in procedures, processes and systems, for example a prevented clinical/patient safety incident.

3.5. **Serious Incident (SI):** an act or omission that results in; unexpected or avoidable death, unexpected or avoidable injury resulting in serious harm - including those where the injury required treatment to prevent death or serious harm, abuse, Never Events, incidents that prevent (or threaten to prevent) an organisation's ability to continue to deliver an acceptable quality of healthcare services and incidents that cause widespread public concern resulting in a loss of confidence in healthcare services (Serious Incident Framework, 2015). Please refer to the *Serious Incident Policy* for guidance on the management of Serious Incidents.

3.6. **Patient Safety Incident (PSI)**: Any incident that has involved or could have affected the safety of one or more service users. Patient safety incidents are reported anonymously to the National Reporting and Learning System (NRLS) database.

3.7. **National Reporting and Learning System (NRLS)**: A database that holds all NHS patient safety incidents and disseminates learning on a Trusts trends to facilitate learning.

3.8. **Duty of Candour (DoC)**: This is a statutory requirement which describes being open and honest in communication with patients for incidents that have resulted in moderate harm, severe harm and death.

3.9. **Hazard:** something with the potential to cause injury, ill health, harm, damage or loss and may include substances, equipment, or a work practice.

3.10. **RIDDOR:** Reporting of Injuries, Diseases, Dangerous Occurrences Regulations.

3.11. **Accident:** An unplanned and uncontrolled event that has led to harm to people, property or process. Examples include incidents that have caused Injury, ill health, loss or damage to equipment.

4 Responsibilities

4.1. **The Trust Board**: will receive information on incidents in order to seek assurance in relation to the incident management process. It will also consider the overall safety of the organisation based upon the trends and themes within reports.

4.2. **The Quality & Patient Safety Committee**: is directly accountable to the Board and seeks to provide assurance relating to systems and procedures relating to patient safety. The committee will receive reports relating to the incident management process and issues highlighted through investigations in order to provide assurance to the board, or to raise concerns.

4.3. **The Chief Executive Officer**: as Accountable Officer, has overall responsibility on behalf of the Trust Board for risk management and patient safety, including the management of incidents. The Chief Executive delegates specific roles and responsibilities to the appointed executive director/senior managers to ensure incident management is co-ordinated and implemented equitably to meet the Trust's objectives.

4.4. **The Director of Quailty and Nursing** : is responsible for the incident management process, including serious incidents. They have board level responsibility for quality, regulatory compliance, risk management, health & safety, safeguarding adults and children, patient experience and is the director with responsibility for decontamination, infection prevention and control. The Director of Nursing and Quality is executive lead for Duty of Candour and will ensure there is an open and transparent culture throughout the incident process.

4.5. **The Medical Director**: has delegated board level responsibility for Medicines Management, clinical outcomes and clinical effectiveness. The Medical Director is both the designated Controlled Drugs Accountable Officer and Caldicott Guardian.

4.6. **Executive Directors**: have unitary responsibility for the safety of services. Each Executive Director is also responsible for the safety of the services within their remit and as such will take the lead in the decision to escalate an incident into a Serious Incident as per the Serious Incident Policy.

4.7. **The Head of Risk Management**: is responsible for ensuring this policy is in line with government legislation, Department of Health and regulatory policy and frameworks. They are also responsible for ensuring the incident management process is not isolated and has integration with incident reporting processes and evaluation of patient experience and clinical outcomes.

4.8. **Datix Manager:** Has a responsibility to ensure that the Datix system is kept in line with current patient safety guidelines. Also to keep the system operable and to raise any issues with the system that cannot be solved in house to Information Technology or DATIX support.

4.9. **All staff:** have a responsibility for identifying, reporting and managing incidents. This includes improving the delivery/quality of services through the implementation of corrective/mitigating actions and preventative action plans through lessons identified.

Principles and Process Approach

4.10. An open approach to reported incidents will enhance the Trust's ability to learn. The Trust aims to move away from apportioning blame when an incident occurs and focus on Trust wide learning. The Trust promotes a culture that fosters learning and improvement whilst encouraging accountability by committing to an open and fair culture and promoting a non-punitive approach to the investigation of incidents.

4.11. This policy does not cover performance and disciplinary processes. The Trust recognises that a systems approach using a Root Cause Analysis (RCA) methodology to investigate incidents will offer the most effective opportunity to learn lessons and prevent reoccurrence.

4.12. Staff will not be subject to disciplinary action or suffer any material loss or disadvantage when an incident is the result of human error.

The following are guiding principles when assessing human error:

- The absence of criminal behaviour.
- The absence of patient abuse.
- The absence of gross negligence.
- The absence of an intention to cause harm to the patient.
- The absence of a drug or alcohol problem within the member of staff.
- The intention of the staff member was to do their best for the patient.
- The member of staff can offer an explanation/personal logic to their behaviour.
- Another body of individuals possessing the same level of skill and experience in the same set of circumstances would be likely to behave in the same way.

Types of Incidents to be Reported

4.13. The Trust operates an electronic incident reporting system for all incidents on DATIX. On submission of the report form an automatic notification is provided to key individuals, such as the line manager, occupational health or responsible lead to ensure that prompt and appropriate support is provided. All Trust staff must be able to access this system.

4.14. Where an incident relates to concerns raised by non-Trust members (members of the public or clinical staff from external organisations) this

must be raised on the electronic incident reporting system on their behalf by the member of staff receiving notification of the incident.

4.15. It is the responsibility of all staff to report any adverse incidents, potential incidents (i.e. near miss) and all identified hazards and risks. In all cases, reports must be made without delay on the electronic reporting system. All incidents must be recorded electronically within 24 hours of the incident.

4.16. Sub-contractors and consultant staff working on behalf of the Trust are equally required to report all adverse incidents. If staff are unable to access the electronic system, they will need to seek assistance from a Trust employee. Inability to access the electronic system is not an explanation for failing to report incidents.

4.17. It is essential that potential incidents (near misses) are also reported using the electronic system in order to maintain the Trust's proactive approach to both clinical and non-clinical incidents.

4.18. If, at the time of identifying the incident, the member of staff thinks the incident reaches the threshold of a serious incident then it must be reported to the responsible director (or their nominated deputy) within one working day as per the process set out in the Serious Incident Policy.

4.19. On receipt of the electronic incident form the Datix team will review the harm rating and actions to ensure they are proportionate to the level of harm incurred as a result of the incident. The Datix team will also responsible for additional reporting on specific types of incidents to specialist organisations .e.g. the weekly reporting of patient safety incidents to the NRLS.

5 Incident Grading

5.1. As part of the electronic recording of incidents must be initially graded to establish the level of harm caused (based on the National Patient Safety Agency guidance). The grades of harm include:

- No known harm
- Near Miss
- Low (minimal harm, injured party required extra observation or minor treatment)
- Moderate (short term harm, injured party required further treatment of procedure)
- Severe (injured party sustained permanent or long term harm)
- Death (caused as a direct result of the incident)

- Death (not caused as a direct result of the incident)

5.2. The level of investigation will be dependent upon the grade of harm and the types of incident. Incidents graded no harm, near miss or low harm will require a local investigation which should be completed within 20 working days using the RCA methodology.

5.3. Incidents graded moderate harm will need to undertake a concise RCA investigation within 20 working days. The concise RCA report template can be downloaded from Datix and should be uploaded to Datix once complete.

5.4. Consideration should also be given to risks arising out of incidents, viewed as serious enough to be placed on the Trust Risk Register at directorate, corporate or strategic level. Please email datix@secamb.nhs.uk to report a risk.

5.5. Incidents graded as moderate, severe harm and death will be reviewed by the weekly Serious Incident Group which is chaired by both the Medical Director and Director of Nursing.

5.6. At the DIF2, incident investigation stage, the investigator uses the 5x5 risk assessment matrix to establish the overall risk grading as shown below.

Table 1: Incident Grade = Consequence x Likelihood of recurrence

	Likelihood				
Impact	**1 Rare**	**2 Unlikely**	**3 Possible**	**4 Likely**	**5 Almost certain**
Catastrophic 5	5	10	15	20	25
Major 4	4	8	12	16	20
Moderate 3	3	6	9	12	15
Minor 2	2	4	6	8	10
Negligible 1	1	2	3	4	5

6 Incident Reporting Cycle

6.1. A process map supports this policy by identifying the expectations for the reporting and investigating of incidents and is supplied in Appendix B.

6.2. Before reporting an incident make sure the person/area is made safe.

6.3. Comply with ‘Being Open’ and the Duty of Candour requirements.

6.4. If any equipment/medication is involved, please note its serial number so that it can be tracked and mark it as out of service to stop repeat incident occurring. Arrange to have the item removed by reporting it to logistics.

6.5. Staff should ensure that a DIF1 is accurately completed as soon as practically possible after the event (usually within 24 hours). Including as much detail as possible so that investigators and Datix staff can investigate the incident without delay.

6.6. When the user selects their manager on the DIF1 form, they, along with their manager, will receive a notification that the incident has been put onto the DATIX system.

6.7. The manager/handler of the incident, if appropriate will then allocate an investigator within 5 working days. On occasions, the manager/handler will undertake the investigation themselves.

6.8. The manager/handler if applicable can assign one or more investigators to aid in the assistance of the investigation. The investigators have 20 working days to complete the investigation and when they have completed the work must report to the manager/handler that their section has been complete.

6.9. When the manager/handler has had feedback from the investigators and has completed the investigation then the incident should be moved by the manager/handler to awaiting final approval.

6.10. The Risk team then has 20 working days to review the DIF2 and approve it for closure if the investigation is satisfactory. If the DIF2 does not meet closure criteria, then it will be returned to the manager/handler through the DATIX feedback system with guidance on what needs completing to satisfy that criteria.

7 Reporting to External Agencies

7.1. When a member of Trust staff witnesses or subsequently discovers an incident caused by or occurring in another NHS Trust or healthcare organisation, an incident report should be completed in the usual way

giving as much information as possible so that the organisation can be contacted and the incident identified.

7.2. The Trust is required to regularly report all patient safety incidents (PSIs) to the National Reporting and Learning System and voluntarily reports security incidents to NHS Protect. This is undertaken by automatic scheduled uploading from the DATIX system to the National Reporting and Learning System database.

7.3. Some accidents at work constitute an Injury or Dangerous Occurrence reportable under RIDDOR. If so, the Datix team will ensure that RIDDOR is escalated to the Health & Safety Manager for external reporting to the Health & Safety Executive (HSE) via: http://www.riddor.gov.uk/

8 Duty of Candour & Confidentiality

8.1. Duty of Candour must be initiated where actual harm has occurred to a patient that has been assessed as incurring moderate and severe harm or death. It is the responsibility of the investigating manager to ensure Duty of Candour is actioned, recorded on Datix, and that the family/relatives are kept informed at relevant stages of the process.

8.2. Staff involved in the incident must also be open and honest with their colleagues, managers and relevant organisations and take part in reviews and investigations (when requested).

8.3. Any enquiries from the media will be answered as openly as possible but without compromising the confidentiality of those involved. All media enquiries must go through the Trust Communication's team by email comms@secamb.nhs.uk

8.4. Rarely, there may be an incident that is sufficiently serious but, due to the confidentiality of the individuals involved, it can-not be managed through the normal Serious Incident process. This could include incidents involving allegations against Trust Board members, or other sensitive issues. These should be exceptional and rare. The decision to manage the incident outside of the process must take place with the involvement of the Chief Executive Officer. The rationale for the decision should be recorded and discussed with the Chair. The adapted process must be documented on StEIS and sent to appropriate staff.

9 Competence

9.1. All members of staff should receive training on the appropriate DATIX modules if appointed as an Investigating Officer. However, the overriding priority is to ensure that investigations and learning is identified. Therefore, there could be occasions where the knowledge of the subject matter takes

precedent and the investigator will be asked to commence the investigation with support from a qualified investigator rather than training.

9.2. Where the investigating officer does not feel adequately trained or experienced then support or assistance should be sought from the DATIX or Serious Incident team. This is particularly important for Duty of Candour responsibilities as well as serious incidents.

10 Monitoring

10.1. The Executive Management Board have devolved responsibility from the Trust Board for ensuring adherence to this policy. They will also oversee a set of metrics to monitor the operational management of all incidents.

10.2. The Executive Management Board will receive a monthly report on incident trends for the organisation. On a quarterly basis, the Executive Management Board will receive a quarterly report on top of the monthly information. The Quality and Patient Safety Committee will also receive the quarterly report but not the monthly data. Both of these groups report into the Trust Board.

10.3. All new incidents received by the DATIX team are reviewed for Serious Incident status, RIDDOR, NRLS reporting and checked for the quality of data that has been reported. In addition, the Datix team will forward relevant reports to appropriate teams.

11 Audit and Review

11.1. The incident process will be audited at least every three years by internal audit to ensure systems and processes are as effective as possible.

11.2. This policy will be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced.

11.3. The DATIX system will be reviewed on a monthly basis through the full audit and the login audit to ascertain any breaches within the system.

12 References

NHSE Serious Incident Framework 2015

National Patient Safety Agency Website
http://www.npsa.nhs.uk/nrls/reporting/what-is-a-patient-safety-incident/

NHSE Never Events Update Jan 2018
https://www.england.nhs.uk/patientsafety/never-events/

Reporting injuries, diseases and dangerous occurrences in health and social care: Guidance for employers

http://www.hse.gov.uk/pubns/hsis1.pdf

2016/17 NHS Standard Contract

CQC Regulation 20 Duty of Candour

Health and Social Care Act 2008 (Regulated Activities) Regulations 2014

London Ambulance Service NHS Foundation Trust – Reporting Maternal Deaths on Datix, December 2016

Serious Incident Framework- frequently asked question (March 2016)

Appendix A: Types of Incidents (with working definition)

Patient Safety Incident: Any unintended or unexpected incident that could have or did lead to harm (e.g. injury, suffering, disability or death – physical, psychological or social) for one or more persons (adult and child) receiving NHS-funded healthcare, e.g. an occurrence, procedure or intervention which has or could have given rise to actual injury, or to an unexpected or unwanted effect.

Medication Incidents: Any incident involving a medicine. The Trust Medicines Management & Quality Team provides advice and support for managing and reporting medication incidents. In the event of the Trust being notified of a controlled drugs (CD) incident, this will be escalated to the Controlled Drugs (CDs) Accountable Officer.

Sudden Unexpected Death: Unexpected deaths are where a death has not been considered as the outcome. There are a number of circumstances where a death is reportable to the coroner and cases that meet the coroner threshold must be part of the incident process. These are;

- cause of death is unknown
- death was violent or unnatural
- death was sudden and unexplained
- person who died was not visited by a medical practitioner during their final illness
- medical certificate isn't available
- person who died wasn't seen by the doctor who signed the medical certificate within 14 days before death or after they died
- death occurred during an operation or before the person came out of anesthetic
- medical certificate suggests the death may have been caused by an industrial disease or industrial poisoning

Maternal Deaths: A maternal death is defined internationally as a death of a woman, during or up a year after the end of pregnancy (whether the pregnancy ended by termination, miscarriage or a birth, or was an ectopic pregnancy) through causes associated with, or exacerbated by, pregnancy (World Health Organisation 2010).

Health & Safety Incident: An unplanned and uncontrolled event that has led to or could have caused injury, ill health, harm to persons, damage to equipment or loss. Some accidents at work constitute an injury or a dangerous occurrence reportable under RIDDOR.

Buildings Incident: Where an incident occurs due to defects and failures in Trust Estates and Facilities:

COSHH (Control of Substances Hazardous to Health): COSH is the legal framework applied to most substances that are hazardous to health.

Medical Devices: An incident involving the use of medical equipment. The Head of Risk Management will advise the Medicines and Healthcare Products Regulatory Agency (MHRA) and ensure that any devices involved are isolated for inspection. The manufacturer/supplier, and will notify other Ambulance Trusts as necessary. Following the failure of a medical device the item of equipment must be immediately withdrawn from service and held securely for inspection.

Violence/Abuse/Discrimination: On receipt of a report of physical/ verbal assault or bullying, the manager will immediately complete the NHS Security Management Service *Report of a Physical Assault on NHS* Staff form for review and reporting onwards to the NHS Security Management Service. In such instances it may be necessary for the person involved to inform the police of the incident immediately. If so, the crime number should be recorded on the Datix incident form. All incidents of discrimination are reportable, including social, racial, religious, sexual, ethnic or age-related discrimination.

Fire Incident: Any incident involving a fire or any incident where the fire alarm sounds requiring evacuation (unplanned).

Security Incident (including Information Governance breaches): Any incident where a breach or a lapse of security is the dominating factor, e.g. theft or vandalism, premises window left open overnight, or data security incidents, e.g. missing health records, theft of a PC or unauthorised disclosure of patient identifiable information.

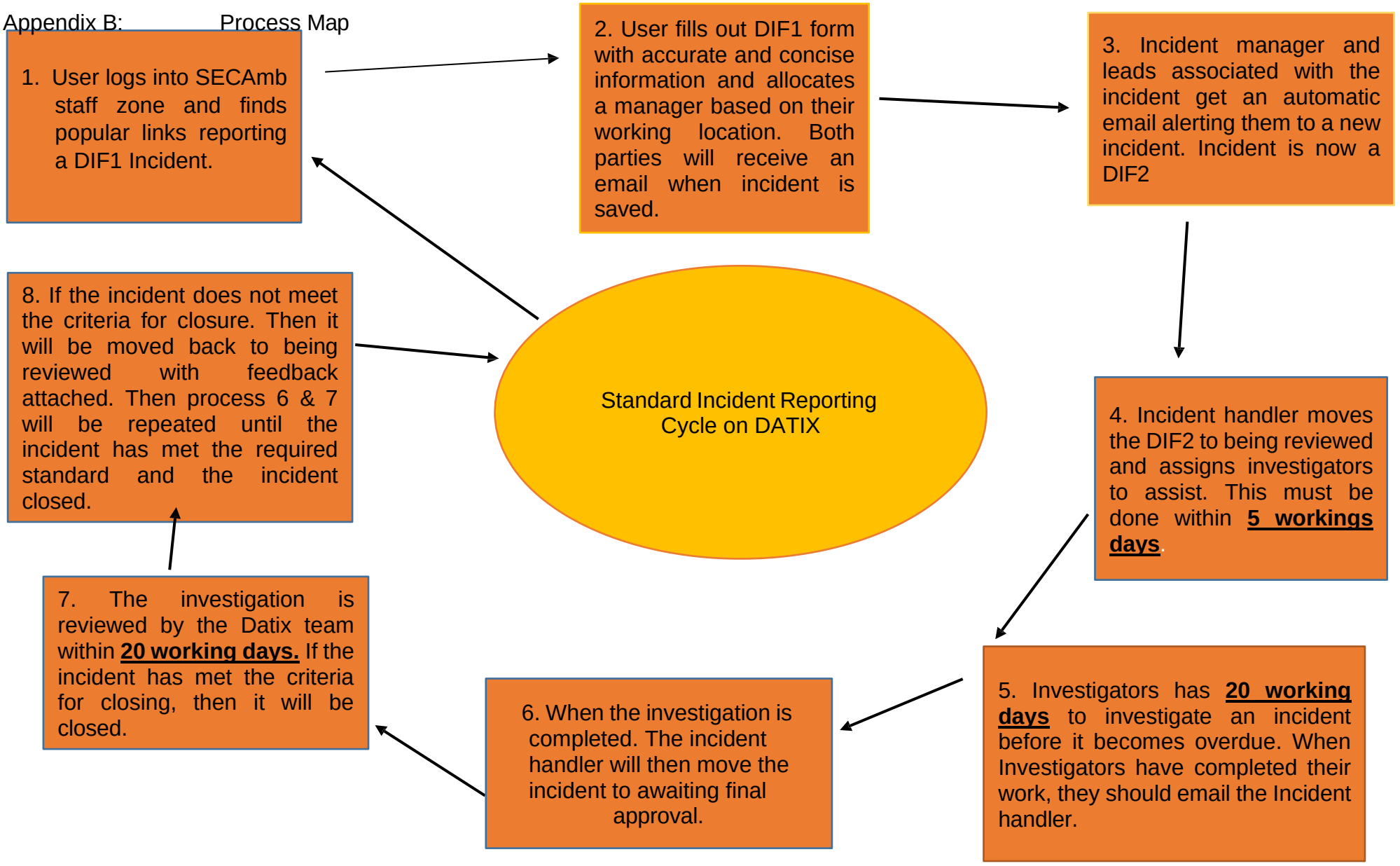
Information Technology (IT) incidents: In line with Health and Social Care Information Centre (HSCIC) Information Standards Board (ISB) guidelines and standards, IT systems implemented in healthcare settings must be delivered, deployed and operated in an acceptably safe manner for patients. Information technology incidents/failures, which has or has the potential to put patients at risk will be reported as a Serious Incident, this may include:

- Failure or loss of clinical systems
- Loss of clinical data with no access to back up
- Data corruption, such as incorrect merging of clinical records
- Inappropriate access to clinical records;
- Misuse of access rights, such as using smartcard to inappropriately view clinical records

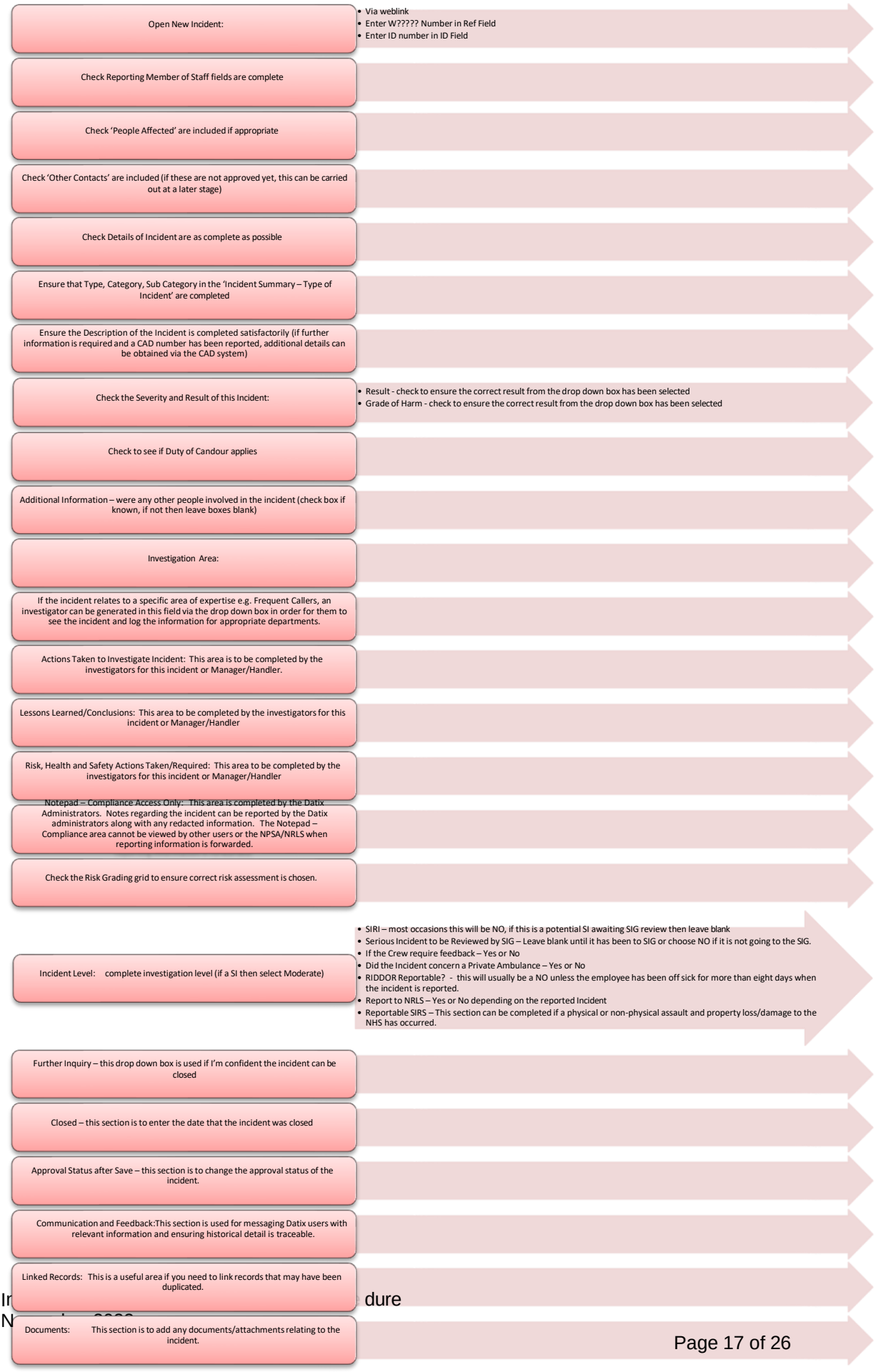
Infection Control Incident: MRSA Bacteraemia/Clostridium Difficile and outbreaks.

All patient safety incidents will be assessed to see if it meets the criteria for a Serious Incident. The assessment and reporting process is detailed in the supporting procedure.

Appendix B: Process Map



Appendix C: Initial First Checks of Incidents



Appendix D: Final Approving Incidents

Finally Approving DIF2

Name, Reference and Actions Section

- **Name** – This should be the patients name, if affecting a patient. A staff member name if affecting staff or if no person affected then a name of the incident that best describes the incident.
- **Actions**- Look at the actions section and do not close if any actions are outstanding. Return the incident to being reviewed and feedback to the handler to get these actions closed.

DIF1 Overview

- **Description** – Check this section for any person identifiable information and replace it with initials or job titles- any names move to the feedback and notepad section.

- **Action Taken** – This is the same as description.

- **Location –** Check this section to make sure that it is correct.

- **Coding –** Check this section, just in case there are better options available.

- **Additional Information –** Look to see if equipment/medication is filled out.

People Involved

- **Approving Contacts** – Make sure that all contacts have been approved and any contacts merged. This is to avoid any duplicates.

Investigation

- **Narrative of Investigation –** Remove any names and replace with job titles and or initials. Any names to be moved into the feedback and notepad section.

- **Lessons Learnt –** Narrative Of lesson learned and commucation given to the person(s) that have raised the incident.

Risk Gradings

- **Pre/Post Investigation Risk Grading-** Make sure that both of these are complete. Check against the 5x5 matrix guidance.

NRLS, RIDDOR, Serious Incidents and Duty of Candour

- **NRLS**- Look to see if stage of care, detail and adverse event is filled out on.

- **RIDDOR-** If RIDDOR has been selected as “Yes” then look at the audit trail to see if the Health & Safety Manager has filled this out
- **Serious Incident-** Review of this section to look at whether these fields have been completed- SI lead should advise if the incident can be closed.
- **Duty of Candour-** Review of this section to look at whether these fields have been completed- Head of Risk should advise if the incident can be closed.

Feedback & Notepad

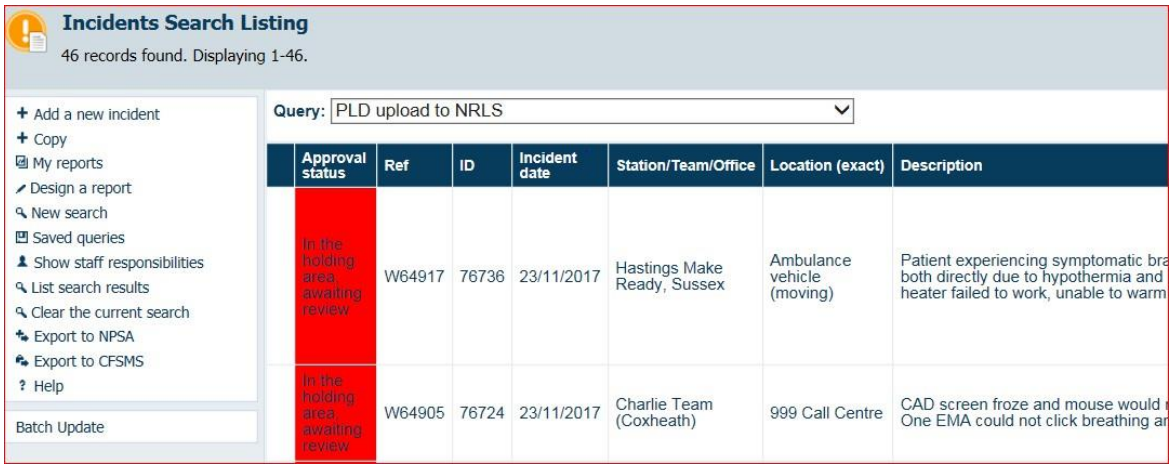
- **Incidents being returned to investigator-** If any incident does not meet the criteria for closure. Then the investigator is to be feedback to as to why the incident cannot be closed. To do this, select a user from staff and contacts attached to this record or all users that is linked with this record and write the reason as to why it is being returned. Return to the **name, reference and action** section and move the incident back to being reviewed. Otherwise the user won’t be able to view the incident.

Appendix E: Reporting to NRLS

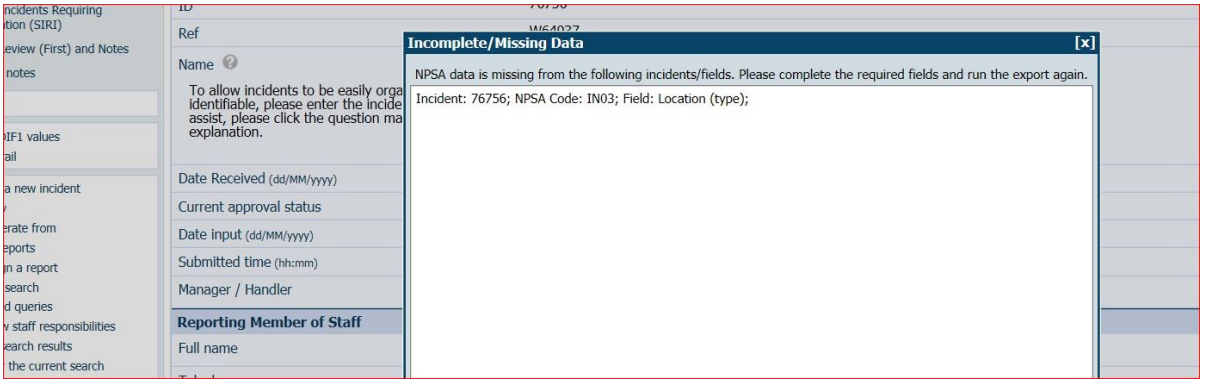
Uploading to NRLS

Run query from Jan 1 to yesterday for PSIs where export date is blank.

Click 'Export to NPSA' form left hand side of page

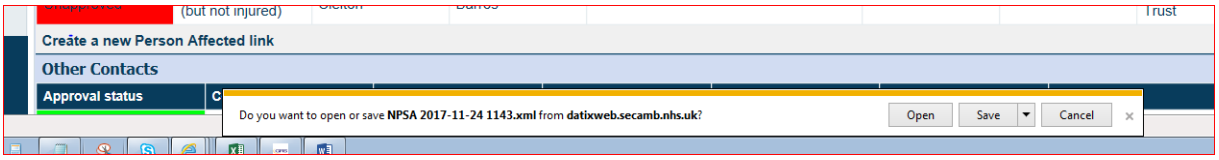


Amend any errors displayed by locating the incident and correcting or adding information as necessary.

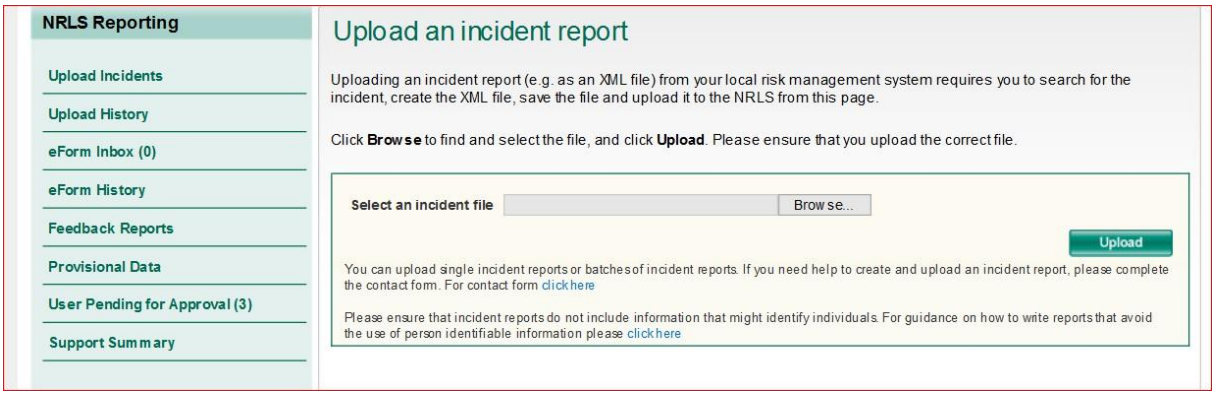


Refresh search and click on 'Export to NPSA' if any other errors are displayed repeat as above until no further errors are displayed.

When prompted to open or save the file appears at the bottom of the screen, select save and choose a suitable location to save to (usually desktop, for ease of access).



Login to NRLS Reporting then select 'Upload Incidents' from the left hand side of page



The next page to appear will be 'the Upload an incident report' Select browse and add the file previously saved above.

Appendix F: Reporting to STEIS

Reporting a Serious Incident

Reporting a serious incident must be done by recording the incident on the NHS serious incident management system, STEIS (Strategic Executive Information System), or its successor system. The serious incident report must not contain any patient or staff names and the description should be clear and concise. Ensure commissioners and other relevant parties are informed at the earliest opportunity and within 2 working days of a serious incident being identified.

Other regulatory, statutory, advisory and professional bodies should be informed about serious incidents depending on the nature and circumstances of the incident. Serious incident reports must clearly state that relevant bodies have been informed

In some circumstances, where a serious incident or multiple serious incidents raise profound concerns about the quality of care being provided, organisations should consider calling a Risk Summit, which provides a mechanism for key stakeholders in the health economy to come together to collectively share and review information. Most serious incidents will not warrant this level of response however.

All serious incidents which meet the definition for a patient safety incident should also be reported separately to the NRLS for national learning. Organisations with local risk management systems that link to the NRLS can report via their own systems. Organisations without this facility should report using the relevant NRLS e-form

Follow up information

An initial review (characteristically termed a ‘72 hour review’) should be undertaken and uploaded onto the STEIS system by the provider (offline submission may be required where online submission is not possible, see Appendix 6). This should be completed within 3 working days of the incident being identified. The aim of the initial review is to:

• Identify and provide assurance that any necessary immediate action to ensure the safety of staff, patients and the public is in place;
• Assess the incident in more detail (and to confirm if the incident does still meet the criteria for a serious incident and does therefore require a full investigation);

• Propose the appropriate level of investigation.

The information submitted as part of the initial review should be reviewed by the appropriate stakeholders and the investigation team (once in operation) in order to inform the subsequent investigation.

Appendix G: Never Event Reporting

1.1. Never Events are incidents that require full investigation under the Serious Incident framework. The requirements for reporting, principles for investigation, and the roles and responsibilities associated with the management and oversight of other Serious Incidents apply, including the need to fully and meaningfully engage patients, families and carers at the beginning of and throughout any investigation. Further information can be found in the Serious Incident framework.

1.2. As with other incidents that are classified as Serious Incidents, Never Events must be reported to both the strategic executive information system (StEIS) and the NRLS until the new patient safety incident management system is in place. Crucially, reports to both the NRLS and StEIS must clearly label the incident as a Never Event, even if this status is uncertain at the time of reporting (both systems contain a Never Events field). If necessary, and with provider and commissioner agreement, incident reports on StEIS can be retrospectively amended if it is found that the incident did not meet the definition of a Never Event. A clear audit trail explaining the rationale for the change and who authorised this should be recorded.

1.3. Organisational leaders (board or equivalent) are responsible for ensuring that any occurrence of a Never Event is analysed fully using a systems-based investigation method (such as RCA) to understand how and why it occurred (from a systems perspective). Leaders must then ensure that actions which measurably reduce the risk of recurrence are taken. Monitoring processes must support implementation and delivery of effective actions – this is the crucial aspect of this policy and framework.

1.4. Incidence of Never Events must be identified in the commissioner's annual report and the provider's quality accounts (ensuring patient confidentiality). This should include:
• Data on the type and number of Never Events, including historical context and related incidents
• The learning stemming from the incidents, with a particular focus on the system changes made to reduce the probability of recurrence
• How learning has been shared at all levels in the organisation and externally.

1.5. In some instances Never Events may be identified some time after they occurred. While delayed identification is not a factor in determining whether or not an incident is a Never Event, it may have a bearing on the improvements deemed

necessary following investigation (eg where subsequent procedural changes mean that additional action may be unnecessary).

1.6. Where a Never Event is discovered by one organisation but appears to be the responsibility of another, the ‘discovering’ organisation should inform the originating organisation and is not required to report the incident as its own.

1.7. Some definitions of Never Events have changed in this revision of the framework. Where incidents that used to meet the definition of a Never Event but no longer do so (for example, wrong level spinal surgery) are identified after publication of the new framework, they should not be reported as Never Events even if they occurred before publication. Previously reported Never Events, even if they no longer meet the definition of a Never Event, should not be retrospectively downgraded.

1.8. As a general rule, local healthcare organisations should consider the status of the incident at the time it occurred, particularly whether it met the Never Event criteria. If the incident pre-dated clear, easy to apply guidance on prevention or the introduction of the Never Event framework in 2009, it is not a Never Event. But if such guidance was available at the time but not acted on, the incident could be considered a Never Event in all but name, and treated appropriately.

Appendix H: New User Request Process

1. An email is received from a member of staff requesting Datix access
2. If there is no line manager approval, then an email will be sent back requesting that the line manager authorise the request.
3. The line manager must authorise the request then the Datix team will give the member of staff a username and password to gain access to the system.
4. Line manager authorisation email and email chain is stored on both the T:\Risk & Safety\DATIX\Datix User Request and the datix@secamb.nhs.uk mail box called user requests.