MSI Reproductive Choices UK

Incident Reporting Policy (Including the Patient Safety Incident Response Framework, Never Events and Information Governance incidents)

Version:	V4
Supersedes version:	V3
Applies to:	All colleagues
Approved by:	Policy and Document Approval Group (31st July 2025)
Executive Director Sign Off:	
Ratified by:	Integrated Governance Committee (5th August 2025)
Issue Date:	August 2025
Review Date:	August 2028
Written by:	Director of Nursing, Midwifery, and Quality
Accountable Team Member:	Director of Nursing, Midwifery, and Quality
Uploaded by:	Policy and Client Information Administrator
Linked MSI UK Policies:	• Patient Safety Incident Response Plan • Data Protection and Confidentiality Policy • Duty of Candour Policy • Infection Prevention and Control Policies • Information Governance Policy • Complaints Management Policy • Client Feedback Policy • Records Management and Disposal Policy • Risk Management Policy • Safeguarding Adults, Children and Young People Policy • Speaking Up Policy

Review and Amendment Log

Version No	Type of Change	Date	Description of change
V4	Major	July 2025	Just Culture Guide replaced with Being fair tool (Appendix 9). Guidance on when and how to use the tool Pg.14. New NHSE guidance added 'Patient safety healthcare inequalities reduction framework' Job titles updated Removed routinely taking witness statements following an incident
V3	Major	March 2024	Policy aligned with the NHS Patient Safety Incident Response Framework and Plan which replaces the NHS Serious Incident Framework (2015) and is a significant change to how client safety incidents are managed.
V2.1	Review	July 2022	Update of job titles and Governance meeting names, no change to process
V2	Review	June 2020	Updated processes for more robust incident management and added sections on learning from deaths
V1.1	Review	August 2018	Reviewed to consolidate incident reporting policy, with Serious Incident Reporting Policy and information governance requirements. Reformatted
V1	New policy	January 2017	New policy

Table of Contents

Policy Statement and Introduction

MSI UK recognises and is committed to creating a positive and safe environment for the people who use our services, their families/partners, visitors and colleagues. We have a responsibility to ensure that there are systematic measures in place for identifying, reporting, managing and investigating incidents to safeguard people, property, resources and reputation. This includes the responsibility to learn from these incidents in order to minimise the risk of them happening again and improve practice and organisational culture.

In complex healthcare systems, things can sometimes go wrong. Reporting and investigating how and why things go wrong is a fundamental principle of safety improvement, and system-wide incident investigation is an essential feature of safety management and learning systems in all safety critical industries.

Incidents continue to recur in different places and at different times, causing harm in similar ways. Ensuring that we can reliably report and respond to incidents with the purpose of identifying learning and improvements, therefore remains our priority. Our primary role for incident investigations is to thoroughly identify and investigate risks that span the system, examine the role of any part we (including external organisations) might contribute to those risks and develop effective safety recommendations that target the underlying systemic issues. A key function of these activities is to build collaborative, open and trusting relationships with our colleagues.

As an organisation providing NHS-funded care, we have a duty to demonstrate effective governance and learning for improvement following an incident and a responsibility to ensure that when an incident does happen, there are systematic measures in place for:

safeguarding people, property, the service's resources, and its reputation;
understanding why the event occurred;
ensuring that steps are taken to reduce the chance of a similar incident happening again;
reporting to other bodies where necessary;
sharing the learning within our organisation;
sharing the learning with other NHS organisations and providers of NHS-funded care.

In healthcare, major inquiries, and reviews continue to reveal considerable difficulties in how healthcare organisations investigate and learn from incidents both locally and nationally:

- Francis inquiries into the disaster at Mid Staffordshire
- Kirkup investigation into the tragedies at Morecambe Bay
- Berwick review of patient safety in the NHS and the Public Administration Select Committee inquiry into the investigation of clinical incidents
- Ockenden Review of the maternity services at the Shrewsbury and Telford Hospital Trusts

At MSI UK, our vision for incident reporting and investigation is to create a culture of '*learning not blaming*' and adopting an open and honest culture to incident reporting and learning. This creates an environment that encourages the reporting of all types of incidents to alert management and other colleagues to areas of risk at an early stage and to enable action to be taken. It is not possible to learn and improve after an event if we do not understand the causes. We recognise that even a '*simple'* error such as the administration of the wrong drug will often have many complex systemic causes, and it is increasingly recognised in healthcare that such systemic problems cannot simply be addressed by local initiatives. Therefore, it is key to have an organisational approach which drives learning and improvement at scale whilst remaining compassionate and supportive to those involved.

This policy is designed to assist the organisation to comply with requirements of external agencies such as the Care Quality Commission (CQC), Integrated Care Boards (ICB's), the Health and

Safety Executive (HSE), Department of Health the Security of Network and Information Systems Directive ("NIS Directive"), the Department of Health and Social Care (DHSC) as the competent authority from 10 May 2018 and the Information Commissioner's Office (ICO). Its primary aims are to reduce the risk of harm to clients and colleagues by improving the safety and quality of services and the environment in which they are delivered, and to ensure all incidents are reported appropriately and handled effectively in line with regulatory requirements.

Purpose

The purpose of this policy is to ensure the appropriate identification, reporting and investigation of incidents and near misses within MSI UK in support of a just culture which supports learning and improvements. This policy reflects an integrated system covering the reporting, investigation and learning from all adverse events involving clients, visitors and colleagues, as well as other types of events not directly involving people which could lead quality improvement and better use of resources.

We recognise that incidents may occur because of problems with systems and processes, that safety is provided by interactions between components and not from a single component. Responses do not take a person-centred approach where the actions or inactions of people, or ‘human error’ are stated as the cause of an incident. Human error is considered a symptom of the work system, not the cause. It is therefore our policy to promote a positive approach to incident reporting and investigation throughout the organisation.

This policy supports the requirements of the Patient Safety Incident Response Framework (PSIRF), which advocates a coordinated and data-driven response to patient safety incidents. It embeds patient safety incident response within a wider system of improvement and prompts a significant cultural shift towards systematic patient safety management. This policy supports the development and maintenance of an effective patient safety incident response system that integrates the four main aims of PSIRF:

1. Compassionate engagement and involvement of those affected by patient safety incidents
2. Application of a range of system-based approaches to learning from patient safety incidents
3. Considered and proportionate responses to patient safety incidents and safety issues
4. Supportive oversight focused on strengthening response system functioning and improvement.

This policy is consistent with the NHS England/ Improvement Guidance on Just Culture (2018) which aims to a conversation between managers about whether a colleagues involved in a patient safety incident requires specific individual support or intervention to work safely. The approach to a Just Culture is to support consistent, constructive and fair evaluation of the actions of colleagues involved in patient safety incidents (Appendix 9).

Scope

This policy applies to all permanent, locums, agency, bank and voluntary colleagues of MSI UK, acknowledging that for colleagues other than those directly employed by MSI UK the appropriate line management or escalation processes will apply.

It includes responses specifically to patient safety incidents for the purpose of learning and improvement across services provided by MSI UK. Learning responses can be applied to both clinical and non-clinical incidents. There is no remit to apportion blame or determine liability in a response conducted for the purpose of learning and improvement. Other processes, such as claims handling, human resources investigations into employment concerns, professional standards investigations and criminal investigations, exist for that purpose. The principle aims of each of these responses differ from those of a patient safety response and are outside the scope of this policy.

Definitions of Terms

We have set definitions in relation to incident management which can be found in Appendix 1.

Duties and Responsibilities

The following details the individual, centre, committee, group and roles and level or responsibility for incident and significant incident reporting and investigation.

Managing Director - The overall accountability for effective risk management in MSI UK, including incident reporting and management, lies with the Managing Director. They are the Accountable Officer with responsibility for ensuring that systems are in place to minimise risks, identify, and manage issues early and promptly. Accountability for management of financial (business) risk, including the correct application of Standing Financial Instructions and Standing Orders lies with the Head of Finance.

The **Director of Nursing, Midwifery, and Quality** is the appointed PSIRF Executive Lead with responsibility for risk and safety and, as such, is responsible for ensuring that MSI UK has appropriate arrangements for incident reporting, learning responses and applying identified improvements. They also have responsibility for:

- Notifying Executive Directors and Managing Director of significant incidents requiring Patient Safety Incident Investigation or Multi-Disciplinary Reviews, including severe or catastrophic harm incidents
- Final review and sign-off of Patient Safety Incident Investigations
- Ensuring that all areas of responsibility are triangulated with incident reporting and investigation a surveillance system;
- Ensuring there is a review of all incidents at local, regional and corporate levels and ensuring that remedial actions and organisational learning follows on from incident investigations;
- Ensuring the operational implementation, monitoring and reporting of key outcomes from this policy.
- Ensuring patient safety incident responses are coordinated and timescales met

Director of Nursing, Midwifery, and Quality and **Medical Director** are both responsible for medical and nursing issues, involvement, engagement and oversight in relating to incident management process. They are responsible for:

- Assessing incidents reported as major or catastrophic harm to determine what response is required. This is undertaken in conjunction with the other Directors above as appropriate.
- Supporting the Director of Operations with clinical operational delivery of all learning and improvements from incidents.
- Signing off completed PSII investigation reports.
- Seeking assurance on the implementation of this incident reporting policy and Patient Safety Incident Response Plan.
- Ensuring people affected by patient safety incidents are supported through compassionate engagement and involvement.

The **Director of Operations** is responsible for the operational delivery of all clinical services and, as such, supports the Executive level ownership for incidents relating to the delivery of operational services.

The **HR Manager** is responsible for ensuring that resources and organisational development incidents are identified, mitigated and managed. In rare instances, where there is suspected potential elements of colleagues' misconduct, the HR Manager refers to MSI UK's HR policies for further information.

Executive Directors are accountable for services in the areas within their remit, whether clinical, non-clinical or operational, ensuring incidents are appropriately identified, reported, and investigated as described in this policy are implemented

Deputy Medical Director: The Deputy Medical Director for EMA & Contraception, Named Safeguarding Doctor, Clinical & Medication Safety Officer is the Accountable Officer for Controlled Drugs. In this role, they will ensure that reports of any incidents involving Controlled Drugs is made to the relevant Local Intelligence Network (LIN) and the police where necessary.

Head of Quality & Governance is responsible for:

- Ensuring that effective incident reporting and investigation and learning systems and processes are in place
- Learning responses are delivered in line with PSIRF to support an open, learning culture
- Monitor the quality of learning responses other than PSII through a sampling approach
- Ensuring learning from incidents is shared across the organisation
- Oversees Patient Safety Incident Investigations
- Ensures the Patient Safety Incident Response Plan is reviewed and updated accordingly

Quality & Governance Business Partners are responsible for:

- The day-to-day implementation and management of the incident policy and plan.
- Supporting all colleagues at all levels, to ensure that this policy is implemented in the specific region where they are based.
- All incidents, near and misses are reported and managed in line with this policy; are discussed at local governance meetings and shared with colleagues.
- Ensuring the day-to-day management of all activities relating to Datix
- Ensuring timely reporting to external agencies for example the ICB and CQC

Patient Safety Specialists (PSSs), provide expert support, facilitate the escalation of safety issues or concerns and play a key role in the development of safety culture, systems and improvement activity. Support, oversee and improve the quality of incident reporting, including external reporting to partners and the Learning From Patient Safety Events (LFPSE). PSSs supports local implementation of the Patient Safety Incident Response Framework.

Data Compliance Manager and Data Protection Officer and **Senior Information Risk Officer (SIRO)** are responsible for:

- Reporting relevant information governance incidents to the Information Commissioner, in accordance with the Commissioners' guidance, the Data Protection Act 2018 (DPA18) and the UK General Data Protection Regulation (GDPR).
- Promoting a culture of information governance incident reporting, encouraging colleagues to report information governance incidents in a timely manner.
- Ensuring all reportable information governance incidents are communicated to the relevant external organisations as required by regulation or contractual obligation.
- Advising on the identification and reporting of significant information governance incidents relating to real or suspected breaches of confidentiality, integrity or availability of MSI UK information.

- Ensuring appropriate training on the reporting of data incidents is provided.
- Advising MSI UK management on all aspects of Information Governance including implementing controls to prevent breaches from occurring.
- Adhering to regulatory requirements for information incident reporting.
- Assisting with monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the supervisory authority.
- Acting as an independent expert in data protection and reporting to the highest management level.
  .

Caldicott Guardian: the MSI UK Caldicott Guardian is the Medical Director and is responsible for:

- Ensuring the protection and use of person identifiable information;
- Ensuring it is only shared with those who have a justifiable need and that it is shared through safeguarding routes.
- Providing advice as appropriate to assist panels investigating information governance and information security incidents involving person identifiable data and in determining the most appropriate way to action the recommendations
- Ensures a system for information and cyber incident reporting is in place in MSI UK.
- Ensures a system for notification to external agencies is in place in MSI UK.
- Point of contact for information sharing breaches

Head of Information Services Governance

Advising on the identification and reporting of significant incidents relating to real or suspected breaches of system integrity or availability of MSI UK information systems.

Advising MSI UK management on all aspects of Information Security including implementing controls to prevent breaches from occurring

Named Nurse/Midwife Safeguarding Adults and Children: The Named Nurse/Midwife Safeguarding Adult and Children is responsible for ensuring that reporting framework for safeguarding operates and supports MSI UK's incident reporting and management policy

Quality & Customer Services Manager is responsible for managing the complaints process and for recording and maintaining complaints information for analysis and reporting. They are responsible for adhering to whilst working jointly to undertake complaint/incident investigation for the purpose of learning and improvements. They are the point of contact for all legal services cases and are therefore responsible for ensuring there is effective close working links in relation to incident reporting and investigation and claims

The Senior Health and Safety Lead is responsible for:

- Identifying specific health and safety and security risks from incident investigation, ensuring risks are adequately assessed, recorded and mitigated.
- ensuring that RIDDOR incidents are investigated appropriately by local managers. T
- reporting RIDDOR incidents to the Health and Safety Executive within the timeframes specified in the (HSE) RIDDOR regulations.

Registered Managers: are responsible for the quality and safety of the centres provided within their centres. Each Registered Manager has responsibility therefore to ensure the principles and practice as described in this policy is embedded within their centres through clear communication with all colleagues in their centres and effective clinical governance and operational management arrangements. Registered Managers should demonstrate their commitment to compassionate engagement and involvement to people affected by patient safety incidents including colleagues, patients and their family/carers.

Subject Matter Experts (Specialists): are responsible for:
Leading or delegating as appropriate the investigations related to their areas of specialism.
Ensuring that learning and improvements identified from incidents related to their specialism is disseminated across the organisation.

Clinical Services Matrons, Clinical Team Leads have a responsibility to: ensure that all their colleagues are familiar with the procedure for incident reporting and that they carry out this procedure when such situations arise;
carry out an initial investigation of any incident, decide on appropriate actions to deal with the immediate situation and prevent the incident from recurring;
ensure that for all incidents have the appropriate learning response applied as outlined in MSI UK Patient Safety Incident Investigation Plan (PSIRP)
ensure effective communication with individual clients about specific incidents that may have affected them, including meeting Duty of Candour requirements where appropriate and with support from senior leadership;
notify the CQC, the relevant ICB (through local contracts managers), or other external bodies of incidents according to external reporting requirements;
isolate and, when necessary, remove faulty equipment from service to avoid risks to clients or colleagues;
ensure colleagues can attend and participate in learning responses and learning from all incidents is fed back to all colleagues at local team meetings/briefings, training needs identified, and subsequent changes in practice monitored.

Doctors caring for clients involved in an incident are responsible for ensuring that a review is undertaken of the person as relevant. They will be notified when a client under their care has been involved in an incident and will be expected to participate fully in the learning response and investigation, including where interviews are required to inform findings.

Pharmacist is responsible for ensuring MSI UK meets the requirements for supporting the reporting and investigating medications incidents.

Speak Up Guardians are responsible for supporting colleagues when they have a concern so that they feel able to raise matters freely and safely in relation to client safety, treatment, or standards of care. This is key role in helping to increase the profile or raising concerns in MSI UK and the Guardian can provide confidential advice and support to colleagues in relation to concerns they have. The Guardian provides support to ensure that employee concerns have been fully explored to the satisfaction of the employee and that colleagues have been responded to appropriately.

Patient Safety Partner(s) (PSP) are volunteers that can influence and improve safety within healthcare. They work alongside our colleagues, patients, families and communities to represent their voices. PSPs can support design of new initiatives that reduce patient safety healthcare inequalities. Following corporate induction in line with other MSI UK employees, PSPs participate in design and development of incident response processes including learning reviews, engagement and involvement, contributing to patient safety meetings, reviewing incident response papers and investigation reports. The PSP is a key stakeholder in quality management processes and reviewing the implementation of safety improvement actions. The PSP is invited to attend oversight committees including Complaints, Litigation, Incidents, Patient Feedback and Safeguarding Group, PSII final panel reviews, MDTs, the Integrated Governance Committee and groups which report into IGC, such as Safeguarding and Infection Prevention and Control.

PSPs work for MSI on a voluntary basis and report into the Head Quality and Governance. They are paid expenses for their expertise and a mutually agreed PSP agreement is signed which outlines how they will be supported, expectations and interaction. The role has been developed by NHS England to help improve patient safety across healthcare in the UK and will evolve over time. PSPs may join PSP networks with local NHS trusts and/or other independent healthcare organisations.

Head of External Affairs is responsible for liaising with the Quality Team on any incidents that may become subject to public interest to ensure that prompt and proactive media management action is taken.

All Colleagues are accountable for complying with the identified standards and safe systems of work specific to their roles, whether identified in national, professional or MSI UK policy, procedures and guidelines. They are responsible for:

- being accountable and taking all incidents seriously;
- being aware of, familiarising themselves with, and knowing how to implement the incident reporting procedure;
- reporting all incidents, near misses, however caused, through identified channels to ensure prompt action is taken using existing reporting systems within MSI UK in accordance with our policy.
- cooperating fully in incident investigations and learning responses.
- Managing incidents, including improving the delivery of services through the implementation of corrective/mitigating actions and preventative actions plans through identified learning

MSI UK Assurance meetings

The Integrated Governance Committee (IGC) is a committee of the Board and meets quarterly. Its duties include a review of reports concerning the aggregation of incidents, complaints and claims. The IGC is responsible for assuring itself that the processes in place for reporting, investigation and learning following incidents are effective and that these are used to improve practice nationally. The group can ask for further assurance where required.

The Medical Advisory Committee (MAC) is committee of the Board and meets quarterly. Its duties include a review of clinical data and concerns, including treatment outcomes, transfers to the NHS, adverse clinical events and overseeing the completion of actions arising from Patient Safety Incident Investigations.

Local Integrated Governance Meetings are held each quarter with regional local management teams. The purpose of the meeting is to provide assurance and exceptions in relation to patient safety including the review of incident themes, significant incident management, risks and safety improvement actions. This meeting reports into the IGC.

Patient Safety Incident Investigation Final Report Review Meeting
All individual PSII reports require a final review and sign off as complete by the board/senior leadership team. The PSIRF Executive Lead/Director of Nursing, Midwifery and Quality, is responsible for reviewing PSII reports in line with the patient safety incident response standards and signed off as finalised. They may be supported in this by relevant colleagues as appropriate.

Complaints Litigation Incidents Patient feedback, Safeguarding (CLIPS) meets weekly to provide a contemporaneous overview and provide support as required regarding all complaints, litigation, incidents, patient feedback and safeguarding issues, to ensure the appropriate response , and remedial action takes place. It also aims to identify on a continual basis all emerging themes ensuring any material risks are identified for inclusion on the appropriate risk register for onward management and mitigation. Centres present a 6 monthly analysis of themes and learning at CLIPS for the purpose of shared learning for improvement. CLIPS is a functional group rather than an assurance group.

Procedure

All incidents should be reported and managed in keeping with this policy and the Patient Safety Incident Response Plan (PSIRP), regardless of the setting where the incident occurred. It provides detailed guidance and tools to assist in the analysis and investigation of incidents.

Reporting an incident
Initial response and notification: An incident may be notified or identified by a client, visitor or any colleagues. It is important that all colleagues recognise when an incident has occurred and how to report it.

All Incidents should be reported using a Datix online incident reporting form on the MSI UK intranet (no login is required) within ***24 hours of occurrence***. **Guidance for colleagues on how to report incidents using Datix can be found on SharePoint.**

Once the incident is logged on Datix, an automatic email notification is provided to key individuals, such as the registered manager, local management team, lead clinician for the service, subject matter expert based on the incident type chosen and responsible lead e.g. Fire, Safeguarding, Clinical, to ensure that prompt and appropriate support is provided.

Patient Safety Incident Response Plan: MSI UK's Patient Safety Incident Response Plan (PSIP) is underpinned by this policy and outlines how we will respond to patient safety incidents, including local and national priorities for learning and improvement. The PSIRP is a live and evolving document which is reviewed at least annually with internal and external stakeholders. This review provides an opportunity to re-engage with stakeholders to discuss and agree any changes made in the previous 12-18 months. Updated plans will be published on our website.

A rigorous planning exercise will be undertaken every four years and more frequently if appropriate (as agreed with our integrated care board (ICB)) to ensure efforts continue to be balanced between learning and improvement. This more in-depth review will include reviewing our response capacity, mapping our services, a wide review of organisational data (for example, patient safety incident investigation (PSII) reports, improvement plans, complaints, claims, colleagues survey results, inequalities data, and reporting data) and wider stakeholder engagement

For Information Governance: The Data Protection Officer will determine whether an information governance incident is reportable to the ICO. If reportable, this will be done to the relevant supervisory authority within 72 hours of becoming aware of the breach. The notification will be made through the Data Security Protection Toolkit, which will notify the Department of Health and the Information Commissioners Office if the incident logged is of sufficient scale as determined by the predetermined scale and sensitivity factors. If the breach is likely to result in a high risk of adversely affecting individuals' rights or freedoms, the individuals must be informed without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

For Safeguarding: Appropriate actions undertaken as identified in the Safeguarding Policies

Immediate actions following an incident
When an incident is identified, prompt actions are necessary to reduce risk. Some incidents will require prompt and specific action to deal with the problem. This may include:

- Immediate contact with the person and/or their next of kin will be made by a specific person in the centre where the care took place, offering support and practical advice
- Providing immediate emergency care to the person involved in the incident
- Summoning assistance
- Ensuring all at risk; client, colleagues, visitors and others, are safe
- Making the surroundings safe to prevent immediate recurrence of the incident
- Treating/caring for others affected
- If equipment/device is involved, removing it from centre (marking it clearly “out of order”) and contacting the Senior Health & Safety Lead
- Retain any equipment that may have been at fault and if applicable check any medical devices with Senior Health & Safety Lead
- Notifying centres Registered Manager, Clinical Services Matron and the Executive Team
- If necessary, take picture evidence. This can be uploaded onto Datix
- Request that all those involved ensure documentation is factual, concise and complete
- Recording the action taken in the client’s records. Records might not be at hand, but they should be found and either tracked or made secure
- Colleagues to report the incident Datix as soon as possible
- Identify the initial level of harm and learning response required
- Reach out to the regional Quality & Governance Business Partner for advice and support when required

Grading of incident and level of investigation
The grade of the incident and level of investigation for all incidents must be proportionate to the type and severity of the incident. Appendix 3 provides guidance on grading and severity of all incident types. The PSIRP informs which learning response may be appropriate.

All incidents which do not require further investigation will be managed locally through the Datix Manager’s form known as the investigation (DIF2) form. See Initial Manager’s review below. The expectation is that the manager of the centre will complete the local investigation via Datix within 20 working days of the incident occurring.

Recording the appropriate level of harm associated with an incident is important so that;

- we have an accurate description of the event and its impact, based on the information we have at the time
- there is consistency and comparability within our data
- Duty of Candour and external notifications can be enacted appropriately

Where practical, it is good practice to discuss the level of harm with the patient affected and to consider the patients perspective on harm definitions within **appendix 1**.

Initial Quality and Governance team actions
The Quality & Governance Business Partners will ensure that all incidents reported via Datix are reviewed by the designated centre quality and governance team no later than 2 working

days following the report of an incident to:
Determine and confirm the type and level of harm
Identify the learning response required as defined in the PSIRP
Ensure relevant colleagues involved in incident support have been notified
Ensure subject matter experts are relevant to the incident have been notified

Initial Clinical Services Matron or Clinical Team Leader actions

When a patient safety incident is received by the Clinical Services Matron or CTL, it is their responsibility to ensure the following, using the Datix investigation (DIF 2)'s form:

- Acknowledge receipt of the incident within 3 days of receiving the notification, including updating the current status from "*In the holding area, awaiting review*" to "*Being reviewed*" via the Incident Handling section of the DIF2 form
- Review the Datix Incident Detail section of the DIF2 form to ensure agreement with the immediate actions taken, categorisation is appropriate; all relevant questions have been addressed.
- Aim to commence the necessary incident response for the purpose of learning and improvement. This is to enable the identification of any cause as well as any remedial actions that need to be taken to prevent similar incidents from occurring.
- If the incident meets the PSII threshold as defined in the PSIRP, the Matron or CTL should work with the designated quality and governance business partner to ensure the process is initiated. They will support the investigation process, including ensuring that the relevant support required by the team is being arranged
- Identify and provide the necessary support required by colleagues involved in or affected by the incident
- Make sure documentation within the client's record has been completed and only includes clinically relevant information
- Using the Datix Document section of the DIF2 form, upload any relevant documents, emails or attachment relating to the incident investigation
- Once the investigation has been completed, the investigator (if different) should notify the handler to ensure datix is updated with the learning and actions. The Matron or CTL should complete a final review of the incident form to ensure all relevant details are captured then update the status from "*Being reviewed*" to "*Final approval*". Learning and any other actions required must be recorded in the datix action log.

Supporting clients and families involved in an incident

MSI UK actively supports open relationships between healthcare organisations, healthcare teams, colleagues, clients, and their carers/family. When things go wrong, people affected by the incident must be treated with compassion and understanding. Effective communication with clients begins at the start of and throughout their care, and this should be no different when a client safety incident occurs. Openness about what happened and discussing client safety incidents promptly, fully and compassionately can help clients, families and carers cope better with the physical and psychological consequences of what happened.

An engagement lead should be established and the nine engagement principles outlined in Engaging and involving patients, families and staff framework should be flexibly applied to ensure that trust and respect for the team providing the care to the client is not lost:

1. Apologies must be meaningful and need to demonstrate understanding of the potential impact of the incident on those involved. An apology communicates a sense of accountability for the harm experienced, but not responsibility for it ahead of an investigation. Getting an apology right is important and is a crucial part of the Duty of Candour regulation.
2. Approach is individualised. Engagement and involvement should be flexible and adapt

to individual and changing needs which could be practical, physical or emotional.

3. Timing is sensitive and some people can feel they are being engagement and involved too slowly or too quickly or insensitively at times. Engagement leads should seek to understand timing and structure of engagement.
4. Those affected are treated with respect and compassion. We have a duty of care to everyone involved in a patient safety incident and the subsequent response.
5. Guidance and clarity are provided from the outset to ensure all affected are equipped for processes following a patient safety incident. Communications and materials should clearly describe the process and its process.
6. Those affected are heard, ensuring they are provided with an opportunity to be listened to and share their experience. This helps to build a comprehensive picture to support learning. Providing the opportunity to be listened to is also part of restoring trust and relations between organisations and colleagues, patients and families.
7. Approach is collaborative and open
8. Subjectivity is accepted as everyone will experience the same incident in different ways. No one truth should be prioritised over others. Engagement leads should ensure that patients, families, and healthcare colleagues are all viewed as credible sources of information in response to a patient safety incident
9. Strive for equity through appropriate responses, balance the opportunity for learning against the needs of those affected by the incident.

The investigation report must include and describe any client and/or family involvement and clearly identify a log of dates/times/discussions involved.

Supporting colleagues involved and/or affected by incident

When things do go wrong, it is not to be underestimated how difficult the situation can be for those involved. MSI UK recognises that in most cases, the cause of an incident may be a combination of events and, or factors that are not be linked solely to the actions of individuals.

Colleagues are seen to be involved in an incident by experiencing, witnessing, or being confronted with an incident or its aftermaths as well as being involved in the investigation or learning response for the incident. This can sometimes cause colleagues to experience strong emotional reactions that have the potential to produce distress at the time or later.

Support for individuals may include any or all the following, or additional measures where appropriate:

- All colleagues affected by an incident will receive initial support and advice from their line manager, engagement lead or a person of their choosing
- Support from the incident response lead to understand incident response, next steps, engagement and agree involvement processes. This can include sharing the Learn Together Patient Safety Incident Investigation Information Booklet.
- Assistance in recording key information, writing or reviewing statements if this is required, either from an MSI UK manager or the colleague’s union representative;
- Assistance undertaking Duty of Candour as per the Duty of Candour policy;
- Signposting to the Employee Assistance Helpline via the HR team;
- Referral to Occupational Health;
- Keeping individuals involved and updated on timelines of investigation progress, outcomes, and actions taken in response

When a clinical incident occurs, e.g. a drug error, the incident must first be investigated in accordance with the MSI UK Incident Reporting and Investigation Policy.

Being Fair Tool

Patient safety incidents are usually signs of underlying systemic issues that require wider system-level action. Singling out an individual is rarely appropirate. By treating our colleagues fairly, MSI UK can foster a culture of openess, equity and learning where colleagues feel confident to speak up when things go wrong. In rare circumstances, a learning response may raise concerns regarding an individuals conduct or fitness to practice. It is in these specific cicumstances that the being fair tool can help us decide what next steps to take. This tool replaces NHS Englands Just Culture Guide following a review of its effectiveness post tranisition to the Patient Safety Incident Response Framework.. The tool supports conversation and decision-making when the response identifies concerns that should be refered to the HR Manager and the Director of Nursing, Midwifery, and Quality. It ensures that colleagues are not treated unfairly after a parient safety incident. The tool is not for routine use and should only be used when concerns raised relate to a patient safety incident. Where criminal activity is suspected to have contributed to death or serious life-changing harm, you should refer the healthcare incident to the police and be guided by the memorandum of understanding between healthcare organisations and regulatory, investigatory and prosecutorial bodies.

Before using the tool. Consider the following questions (Sidney.Dekker, 2022):

- Who is hurt? (for example, colleagues, patients, family, visitors)
- What do they need? (for example, wellbeing support, information on what happened)
- Whose responsibility is it to meet that need? (for example, occupational health, patient safety lead)

Disciplinary and incident investigations are separate processes, and each process could contaminate the other. On occasions, if during the investigation, elements of misconduct or poor colleague performance are identified, this will be referred to the HR Manager. A decision will be taken collectively by the Director of Nursing, Midwifery, and Quality, the HR Manager and a Patient Safety Specialist as to whether disciplinary investigation or action is necessary.

If a disciplinary investigation and report is required, it will be a separate process and conducted independently of the patient safety incident investigation. The two investigation processes can run in parallel - if the investigations do not in any way interfere with each other.

Disciplinary process will not commence as a result of a patient safety related incident until at least the initial report of the investigation has been completed and reviewed. Disciplinary action should not form part of a response to an incident except in exceptional cases where one or more of the following apply:

> Where in the view of MSI UK, and/or any professional registration body, the actions causing the incident/arising from the incident were far removed from acceptable practice
> Where there was intent to harm and/or criminal offence has taken place
> Where there is a duty of care to the individual/individuals to prevent further risk to the business or its employees or thereselves
>
> The disciplinary investigation should include a culpability test as directed by the Being Fair Tool (Appendix 9) to determine final recommendations.
>
> Where there is failure to report an incident in which the colleague was either involved or about which they were aware.

In the event of the above mentioned exceptions, HR policies will be followed.

When an incident has resulted in moderate or severe harm to a client, this must also be reported to the Care Quality Commission (CQC). In the case of significant IG or cyber incidents, the incident should be raised on the NHS Digital Data Security and Protection Toolkit by the Director of Digital and Transformation, which will then automatically notify the ICO if the incident is of sufficient severity to cause risk or harm to the individuals impacted by the incident.

What happens once a moderate harm or greater incident is identified?

Learning responses and investigations are determined within our Patient Safety Incident Response Plan. Under the new NHS England's Patient Safety Incident Response Framework, we no longer respond to incidents defined by harm level alone. Although harm is still important, PSIRF supports organisations to respond to incidents and safety issues in a way that maximises learning and improvement, rather than basing responses on arbitrary and subjective definitions of harm. Beyond national set requirements, organisations can explore patient safety incidents relevant to their context and the populations served rather than those meeting a certain defined threshold. Therefore, we have identified and agreed investigation priorities within MSI UK as detailed within our Patient Safety Incident Response Plan. Depending on the type of incident, the incident may require a local review through After Action Review (AAR), a round table review through a Multi-disciplinary Team Meeting (MDT) if there is significant interest and/or involvement from an external body, such as the Police, NHS Trust, ICB or Media. Incidents requiring a Patient Safety Incident Investigation (PSII) are defined within our plan and can include any incident whereby the contributory factors are not well understood and/or learning is felt to be significant. The Registered Manager and the Quality and Governance Business Partner should complete an initial review of the incident and agree response required, using the PSIRP as a guide.

Incidents identified as requiring a Patient Safety Incident Investigation, should begin as soon as possible after the incident has occurred and completed within three months. This timeframe maybe extended with the agreement of those affected. The Patient Safety Investigator should be agreed by the Quality and Governance Business Partner and the PSII Investigator.

The Registered Manager of the service where the incident occurred is responsible for notifying the CQC and any other relevant bodies. The Registered Manager is responsible for ensuring that the Duty of Candour policy is applied.

The incident response should be discussed at the next Complaints, Litigation, Incidents, Patient Feedback and Safeguarding group which meets weekly and is attended by subject matter experts and members of the senior management team.

Investigation team

Colleagues leading patient safety incident investigations and learning responses must be familiar with the PSIRF aims and have received appropriate training which allows them to demonstrate competence in human factors and systems thinking investigative methodology, techniques and analysis and report writing. They should summarise and present complex information in a clear and logical manner, manage conflicting information from different internal and external sources, communicate highly complex matters in difficult situations. Colleagues would be expected to have received supervision in report writing.

In addition to having the necessary competence, the lead investigator must also be able to demonstrate objectivity, authority and credibility. Before a PSII is assigned to a trained investigator, it should be agreed with them that they have adequate time and capacity to complete a PSII to enable timely investigations. The lead investigator must consult with subject matter experts where appropriate, for example, a clinician or subject matter expert.

The investigation team must be sufficiently removed from the incident to be able to provide an objective view. The investigation team must have no conflict of interest in the incident, real or perceived. A PSII should not be completed by a line manager of those involved.

Engagement Leads

Engagement leads should communicate and engage with patients, families, colleagues and external agencies in a positive and compassionate way. They are required to listen and hear the distress in others in a measured and supportive way, maintain clear records of information gathered and contact with those affected, identify key risks and issues that may affect the involvement of those affected and recognise when those affected by patient safety incidents require onward signposting or referral for support services.

Addressing Health Inequalities

MSI UK is committed to ensuring our services and employment practices are fair, accessible, and appropriate for all. We believe that everyone should receive fair and equal services that take account of individual needs and backgrounds. Our Equality and Diversity Strategy sets out our commitment to ensuring that equality and human rights are considered in everything we do, using the NHS England » Patient safety healthcare inequalities reduction framework to support a culture of inclusive, safe care. This includes providing services, employing people, developing policies, and consulting with and involving people in our work, to enable us to communicate and manage equality commitments, Through PSIRF, we can apply a more flexible approach and intelligent use of data which can help identify any disproportionate risk to patients with specific characteristics.

Learning Responses

Patient Safety Incident Investigation (PSII)

A PSII is undertaken to identify new opportunities for learning and improvement. The aim of a PSII is to provide a clear explanation of how our systems and processes contributed to the incident, recognising that mistakes are human, PSII's examine system factors such as the tools, technologies, environments, tasks and work processes involved. Findings from a PSII are then used to identify action that will lead to improvements in the safety of the care clients receive.

A PSII begins as soon as possible after the incident has occurred by a person trained in Patient Safety Incident Investigation, SEIPS and Human Factors. If a PSII finds significant risks that require immediate action to improve safety, the investigator must escalate to a member of the executive team to ensure appropriate action is taken as soon as possible.

Incidents determined as requiring a PSII are defined within our Patient Safety Incident Response Plan. The plan is flexible and a PSII can be completed for an incident not listed if it is agreed there is significant learning to be had and /or the contributory factors are not well understood.

The investigator should use the Learning Response Review and Improvement Tool (see appendix 10) to inform the development of the written report. Following completion of the PSII, the investigator must share the findings at an internal PSII Panel. The panel should review the report considering the Learning Response Review and Improvement Tool. The PSII must share findings with the people involved before the report is finalised unless the people affected have declined to be involved.

Multi-disciplinary Team Review (MDT)

An MDT is a round table review of one or more client safety incidents to agree on key contributory factors and system gaps, explore a safety theme, pathway or process and gain insight into work as done in a health care system.

The MDT is attended by multiple stakeholders including colleagues affected by the incident, subject matter experts and members of the senior leadership team. External stakeholders should be invited to attend if involved. The meeting is usually one hour long and takes place by Microsoft Teams.

The MDT should review the incident through a SEIPS lens. The review evaluates what good looks like, what happened in this situation, what where the barriers and compares the good to the actual. The group agree next steps and actions required which inform the Duty of Candour letter, if applicable.

After Action Review (AAR)

AAR is a method of evaluation that is used when outcomes of an activity or event have been particularly successful of unsuccessful. It aims to capture learning from these tasks to avoid failure and promote successes for the future. An AAR is usually 30 minutes to one hour long and attended by internal stakeholders, including colleagues involved in the incident, a learning response lead and a member of the Quality & Governance team.

Please refer to MSI UKs Patient Safety Incident Response Plan which informs types of incidents an AAR is to be used.

SWARM

SWARM huddles are used immediately after an incident and integrates the SEIPS framework. Colleagues ‘swarm’ to the sight to swiftly analyse what happened and how to decide what needs to be done to reduce risk. The SWARM should be facilitated by a learning response lead who creates a safe space to ensure everyone’s voice is heard. Any actions or learning arising from a SWARM should be assigned on the relevant datix report and any wider learning shared. SWARM is particularly useful following an emergency transfer or scenario as it can prevent those involved forgetting key information due to time delays before their perspective on what happened is sought. Information can be obtained on what happened and ‘work as done’ before they leave the Centre. It can avoid fear, gossip and blame as it provides an opportunity to remind those involved that the aim following an incident is learning and improvement.

Action plan implementation and completion

An action plan will be developed as a result of the learning response or investigation, with learning and required improvements identified. Actions should be developed only when ‘work as done’ and system factors that influence work are understood. People involved in the patient safety incident, colleagues, patients, carers/families should be involved in providing perspectives and insights to develop actions. Please see NHS England Safety-action-development-v1.1 for further information on developing safety actions.

The action plan must demonstrate how each area for improvement was identified by the investigation and how it will be achieved. Actions should be SMART (specific, measurable, achievable, realistic and timely). They should also:

- Be documented in a Learning Response Report or in a Safety Improvement Plan as applicable
- Start with the action owner, e.g. ‘Deputy Medical Director’
- Be directed to the correct level of the system: that is, people who have the levers to activate change (ideally this should include the person closest to the work and who has been empowered to act).
- Be succinct: any preamble about the safety action should be separate.
- Standalone: that is, readers should know exactly what it means without reading the report.
- Make it obvious why it is required (i.e. given evidence in the learning response report

or safety improvement plan).

Safety actions must be added to the Datix action log and assigned to the agreed action owner. The overall action plan owner is the Registered General Manager of the incident location.

Safety action plans, progress and effectiveness should be shared with the relevant ICB at quarterly contract review meetings or more frequently as agreed with the ICB.
Implementation of actions should effectively prevent recurrence of the incident and/or minimise the harm that results. The appropriate centre local integrated governance meeting and/or corporate department responsible will be responsible for monitoring action implementation monthly to ensure actions are sustainable and impactful. The relevant designated quality & governance partner will provide a quarterly action plan update report at the local integrated governance meeting. The quality & governance partner will send a bi-weekly action plan monitoring reminder email to the relevant action.

Monthly progress and assurance updates on safety action plan implementation will be monitored via CLIPS. The effectiveness evaluation method used will be dependent on the actual outcome being measured. Utilising the MSI UK's Clinical effectiveness approach which uses a systematic approach to demonstrate that standards for care are being met/improved.

Completion of Patient Safety Incident Investigation action plans will be monitored internally by the Integrated Governance Committee. The progress of investigations and action completion is tracked on MSI UKs Investigation Tracker which is monitored and updated by the Quality and Governance Team.

Records management
Client records that are requested for an incident investigation will be scanned and uploaded to the relevant Datix entry, and the original client records returned, thus enabling them to be available for ongoing treatment.

PSIRF recommends that learning response leads move away from a reliance on documentation and written statements to listening to the views of those affected through interviews and discussions. All interview/meeting notes or written statements, if requested, must be uploaded to the incident file. All statements and interview records must be legible, dated and timed.

It is important for PSII incidents, that the information gathering log is used to keep a record of all information obtained to inform the investigation. This should be uploaded to the documents section on Datix. t

Patient Safety Incident Investigation and sign-off
The investigation report will be completed by the designated investigator with oversight from a Patient Safety Specialist (Head of Quality & Governance or Senior Quality & Governance Business Partner), using the MSI UK Patient Safety Incident Investigation (PSII) report template which is a national template from NHS England. The report template is designed to improve the recording and standardisation of PSII reports and facilitate national collection of findings for learning purposes, therefore the template must not be adapted. recommendations, and action plan templates. As the investigation report is written for learning it will be completely anonymised and a list of names retained for reference on Datix and/or electronic folder but kept separately to the report.

When writing the investigation report, only the initial of the person's first name will be used to demonstrate compliance with Information Governance rules; for example, if the person is Sally Wright, then they will be referred to as S within the report. The report version will be sent to the client and will refer to the person by the name. Colleagues involved in the incident or the investigation process will be referred to by their title within the report, not their first or full names. The core members of PSII Panel meetings include the Director of Nursing, Midwifery, and Quality, the Medical Director, a Patient Safety Specialist, Registered Manager, relevant subject matter experts such as the Director of Digital and Transformation, Ultrasound Scanning will attend as relevant to the incident being investigated. Information governance reports should be consulted on by the Director of Digital and Transformation and signed off by the SIRO. Cyber reports should be consulted on by the Head of IS Governance, the Director of Digital and Transformation and signed off by the SIRO.

The PSII Panel meeting must be assured that the investigation has been conducted to a high standard, that all reasonable outcomes have been drawn from the analysis contained in the investigation, and that the recommendations of the investigation are robust enough to act as mitigation against potential recurrence of an incident of a similar nature occurring again in the future.

After sign-off of the final report and recommendations by the PSII Panel group, the PSI investigation report will be submitted to the respective Integrated Care Board (ICB). The investigation and/or review report will not be forwarded to the ICB via the NHS Contracts team or shared with any other external stakeholder until formally approved by the PSII Panel Group. This will ensure that they are receiving the final copy of the report. A letter will be sent to the client (if they had stated they would like a copy of the investigation report) informing the investigation has been completed and offering the report and the opportunity to discuss the findings of the report should the client wish to do this.

Integrated Care Board (ICB) Management of Incidents
MSI UKs Patient Safety Incident Response Plan must be approved by a lead ICB who have an oversight role and responsibility to ensure that this policy and plan delivers effective responses to patient safety incidents. The lead ICB should be an integral collaborator in regular reviews of the plan.

Oversight of patient safety incident response has traditionally included activity to hold provider organisations to account for the quality of their patient safety incident investigation reports. Oversight under PSIRF focuses on engagement and empowerment, with the ICB’s role as a critical friend, providing external scrutiny and facilitating wider system learning.

MSI UK will notify the relevant ICB of clinical complications and safety incidents via the standard quarterly activity dashboards. Any incident agreed as requiring a PSII, the relevant NHS Contracts Manager or Registered Manager should notify the ICB without delay. In addition to this, the Registered Manager will notify the ICB within 24 hours if a client has required an emergency transfer to the NHS because of treatment at MSI UK. There is no requirement for a PSII to be signed off by the ICB, however, we will work in collaboration with them to support and facilitate cross-system learning for improvement. The ICB can also support engagement with other external agencies if required.

Learning from incidents, moderate or greater harm level incidents, PSII or death

The learning from incidents, moderate or greater harm level incidents or incidents which have had a PSII as defined within our PSIRP, is a dynamic process and is managed through multiple avenues. The following systems and processes are in place to support shared learning opportunities:

Organisational Learning

- Review of all incidents, arising themes, investigations, learning responses and improvement opportunities through the weekly CLIPS Group. Output from this Group is also disseminated to all centre/team managers, for further cascade to frontline colleagues.
- Review of incidents and themes through Local Integrated Governance Meetings.
- Presentation of incidents and PSII management performance to the Integrated Governance Committee and if required, the Integrated Governance Steering Group.
- Rapid Patient Safety Alerts for communicating immediate management advice from identified learning and improvement across the organisation.
- Production of reports for subgroups, e.g. Medicines Management, Safeguarding, Clinical Effectiveness, and Information Governance
- Business Update Bulletin (BUB) shared internally: Learning and improvement actions required are published on the necessary BUB channel.
- Monthly organisational induction days delivered
- Through quality & governance partners taking learning and improvement actions to their areas of work
- Task and finish groups for various improvement activities to address key issues and themes which emerge from incident reviews and investigation
- Monitoring the implementation of action plans monthly via designated local integrated governance meetings
- Monitoring and auditing key systems and processes via clinical effectiveness plan and policies, findings will be discussed via the relevant committees/groups within MSI UK
- Gap analysis against MSI UK's systems and processes undertaken of high-profile incidents that occurred in other organisations with the finding discussions at Integrated Governance Committee.
- Sharing the completed investigation report with the client, relative and colleagues involved
- Thematic reviews of common features to several incidents. Common features may include similar location, type of incident and the goal of the thematic review is to enable wider systemic learning from the incidents and to ensure that commonalities between individual incidents and investigations are identified and addressed

Learning From Patient Safety Events (LFPSE)

LFPSE is a new service launched in 2021, creating a single national system for recording and analysis of patient safety events that occur in healthcare. It replaces the National Reporting and Learning system (NRLS) and the Strategic Executive Information System (StEIS). LFPSE has two main services:

1. **Record a patient safety event** – organisations, colleagues and patient will be able to record the details of safety events, contributing to a national NHS wide data source to support learning and improvement
2. **Access data about recorded patient safety events** – providers can access data that has been submitted by their teams, to better understand their local recording practices and culture, and to support local safety improvement work.

LFPSE reportable patient safety incidents are reported via our incident management system datix. Data available on LFPSE will be reviewed and analysed by the Quality and Governance team to identify themes, risks and trends to inform safety priorities on an ongoing basis.

Learning from deaths

Learning from deaths of people in their care can help providers improve the quality of the care they provide to patients and their families, and identify where they could do more (NHSI, 2016).

A CQC review in December 2016, 'Learning, candour and accountability: a review of the way trusts review and investigate the deaths of patients in England found some providers were not giving learning from deaths sufficient priority and so were missing valuable opportunities to identify and make improvements in quality of care. In March 2017, the National Quality Board (NQB) introduced new guidance for NHS providers on how they should learn from the deaths of people in their care.

The NQB guidance outlines that all providers should have a policy in place setting out how to respond to the deaths of patients who die under your management and care. MSI UK has not developed a separate policy but has adopted the approach recommended by the NQB guidance should we have a death in the service. The approach adopted is to:

- report the death within the organisation and to other organisations who may have an interest (including the deceased person's GP).
- respond to the death of an individual with a learning disability or mental health needs, or maternal death.
- review the care provided to clients who are not considered to have been under our care at the time of death but where another organisation suggests we should review the care MSI UK provided to the client in the past.
- record the outcome of the decision whether to review or investigate the death, informed by the views of bereaved families and carers.
- engage meaningfully and compassionately with bereaved families and carers.
- offer guidance, where appropriate, on obtaining legal advice for families

External reporting

Care Quality Commission

All client safety incidents meeting moderate harm or above must be reported to the Care Quality Commission without delay by the Registered Manager.

Learn from Patient Safety Events

Reporting patient safety incidents to the national NHS 'Learning From Patient Safety Events '(LFPSE) service is encouraged for all reporters. LFPSE submissions are monitored by the Quality & Governance team to sense check submissions and offer guidance to reporters and reviewers

Integrated Care Boards

Emergency transfers as a direct result of treatment should be notified to the relevant ICB within 24 hours of transfer
Receipt by the Commissioners of targeted reports;
A quarterly meeting with the Commissioners at which various aspects of incidents are discussed, to provide assurance on organisational learning; this should include PSII's and learning identified, thematic reviews, actions from local learning responses.

Healthcare Safety Investigation Branch (HSIB)

HSIB undertakes patient safety investigations which can encompass any patient safety concern that occurred within NHS funded care in England after 1 April 2017. Incidents are selected based on the scale of risk and harm, the impact on individuals involved and on public confidence in the healthcare system, as well as the potential for learning to prevent future harm.

Maternity & Newborn Safety Investigations (MNSI)

MNSI investigate direct or indirect maternal deaths while pregnant or within 42 days of the end of the pregnancy. They may investigate maternal deaths that do not fit within these two categories.

Media interest incidents

Communications and media relations are an integral part of the significant incident process. It is, therefore, imperative that in the event of an incident attracting media attention, appropriate media handling strategies are put in place, liaising with the ICB. If the media, local or national, express an interest in any incident that has occurred then:

Redirect enquiries immediately to the communications team

Under no circumstances should any comments be made on the incident to the media

For incidents with media interest, a multi-disciplinary team review should be arranged as soon as possible. A member of the Communications Team will consult with the Director of Nursing, Midwifery, and Quality, the relevant managers, including the CSM to prepare the MSI UK's response. A member of the Comms team as appropriate will work closely with external agencies where required to agree media responses. At times this requires consideration of joint statements being co-produced with other agencies e.g. the police.

Where political interest is likely, MSI UK Head of External Affairs should be notified, who may liaise with ICB communications colleagues, local colleagues and the Department of Health on behalf of the region.

Raising Concerns

For colleagues who have any concerns around what is happening in their workplace – for example, regarding the delivery of care or services, conduct, poor practice, dangers to the public/colleagues/environment -- in the first instance they should report via this policy or in confidence to their line manager. However, if they are unsatisfied that their concerns have been addressed, or if they need to raise the concern anonymously, then the Raising Concerns route should be pursued. Please refer to the MSI UK Speaking Up Policy on the MSI UK intranet.

Informing the Police

It is the responsibility of the person in charge of the centre at the time of an adverse event to ensure that the police are informed of the death or injury of any client, employee, visitor, volunteer, contractor, where the person in charge considers there to be unusual, suspicious or unlawful circumstances. Any equipment involved should be retained until the police have visited. The Registered Manager is responsible for external reporting for incidents investigated by the police.

Managing Incidents Across Organisational Boundaries

Occasionally, when incidents occur at the interface between organisations, this is where the greatest risks exist and clarity about responsibilities and accountabilities for those risks is most difficult to ascertain. Where this occurs, only by working closely and collaboratively with another organisation to jointly investigate can opportunities to improve quality and learn across pathways be identified.

MSI UK will endeavour to involve partner organisations in all aspects of its incident management across organisational boundaries as appropriate, or as required by contract, through Multi-disciplinary Team (MDT) reviews. Such organisations include those that host MSI UK services,; those that deliver services jointly or share joint appointments, and those partner organisations with which MSI UK needs to work closely, including other NHS organisations, ambulance services, private hospitals, private medical insurers (PMIs), Social Services, the Police, statutory and voluntary bodies, and client representative groups.

Health and Safety and Security Incidents

Under RIDDOR some work-related accidents, diseases and dangerous occurrences must be reported. This requirement covers all work activities, but not all incidents. The common report is for injuries to colleagues which result in an absence from duty of more than 7 consecutive days. Dangerous occurrences such as failure of lifting equipment, explosion, and failure of supporting structures also require HSE reporting.

The Head of Health and Safety will be involved in the investigation of all health and safety and security incidents.

Information Governance (IG) Incidents

The Data Protection Officer will review all information governance incidents reported to determine the type and level of investigation required to ensure compliance against the IG toolkit

All significant IG Incidents Requiring Investigation (SIRI) will be led by the Data Protection Officer as outlined in the IG policy.
Any IG SSIRI must be reported to the Department of Health and Social Care and the Information Commissioner's Office (ICO) via the NHS Data Security and Protection Toolkit within 72 hours of becoming aware of the incident. This reporting will be undertaken by the Data Protection Officer after liaising with the Caldicott Guardian and the SIRO.

The Data Protection Officer will lead the investigation of all IG incidents deemed to be a high-level incident or significant incident according to this policy with review and sign-off responsibility being carried out by the SI Panel Group. The IG Committee will have oversight of all IG related incidents, including the monitoring of IG incident action plans.

Reporting to external agencies/organisations

Where required through local or national protocol, we are required to inform external agencies and organisations in the event of specific types of incidents. Appendix 6 sets out external reporting requirements.

The MSI UK Risk Register

Where there is a theme or trend identified from incidents reported and measures cannot be taken locally to immediately and completely prevent recurrence, then a risk assessment must be undertaken and recorded via Datix Risk Register. Individual incidences should be linked to the entry on the Risk Register.

Training Requirements

We are committed to equipping colleagues with the necessary skills required to undertake their roles competently and confidently. In turn, colleagues must take responsibility for developing these skills and participating in the lifelong learning process

All colleagues complete training in Incident Reporting, Human Factors and Essentials for Patient Safety as part of their mandatory training programme. Real time training compliance and reports are available for managers and leads via iLearn reports. Compliance is monitored by Registered Managers and the quality and governance team.
Colleagues will be given the following training in accordance with the training needs analysis:

- Systems based Patient Safety Investigator training for all general managers, leaders and patient safety specialists with responsibility for investigating incidents and leading learning responses. This is to enable investigators to investigate incidents using systems thinking and the principles and tools to respond with the purpose of learning and improving. Roles allocated PSII training have been confirmed as having allocated time to complete PSIIs.

- Patient Safety Investigation leads also complete Investigative Interviewing and Involving those affected by patient safety incidents.
- Oversight of learning from patient safety incidents for colleagues in PSIRF oversight roles.
- In addition to Patient Safety Essentials, Investigators and Learning response leads will complete Access to Practice Level 2 and Involving those affected by patient safety incidents.
- All colleagues will complete patient safety essentials training as part of our mandatory training programme on iLearn. This will enable an understanding of an open, honest and fair culture, compassionate engagement and involvement, the purpose and process of investigations.
- Patient Safety Syllabus training for all staff provides the opportunity to improve understanding of patient safety , including risks related to healthcare inequalities.
- Board and Senior Leaders have a separate Patient Safety Essentials module to complete.
- Incident report training for all colleagues. This will give:
    - Context to patient safety and incident reporting principles
    - Understanding why and how to report incidents and record actions effectively and accurately taken
    - Guidance for all colleagues on how incidents are reported using Datix
    - Guidance for managers on identifying, managing, and approving incidents on Datix to meet external reporting requirements, including how to use Datix to search, report and analyse data for their service area.

Allocation of PSII's will be agreed by the Quality & Governance team and tracked on the incident investigation tracker. PSII investigations should be assigned out of region where possible to support a Just and Learning Culture. Colleagues that have completed system-based investigator training and access to practice may join investigation panels to develop their understanding and experience of using the process.
It is recommended that managers who have received investigator training lead at least one investigation per year under the supervision of the Patient Safety Specialists to maintain/retain continuous expertise. Learning response leads should contribute to a minimum of two learning responses per year.

Equality Impact Assessment

An Equality Impact Assessment has been conducted using MSI UK's screening tool. For full details please refer to Appendix 8.

Monitoring and Compliance

Objective	Monitoring Method	Monitoring Frequency	Responsible Person	Receiving Committee
The numbers of Incidents and PSIIs and any arising themes	Quality Dashboard/ Quality Assurance Report Information Governance Report Review of incident data, identification of key themes and learning	Quarterly Quarterly Quarterly Weekly	Director of Nursing, Midwifery, and Quality Director of Digital and Transformation Director of Nursing, Midwifery, and Quality Director of Digital and Transformation	Integrated Governance Committee (IGC) Information Governance Steering Group Complaints, Litigation, Incidents and Patient Feedback Group / Senior Leadership Team Local Integrated Governance Meetings; Local Team Meetings
Status update on PSIIs reported, under investigation, and actions outstanding	Quality Assurance Report Local Integrated Governance Meetings	Quarterly Quarterly	Director of Nursing, midwifery and Quality Registered Managers	Local Integrated Governance Meetings IGC
Implementation of recommendations and actions emerging from incidents	Reports Audits	Quarterly	Quality & Governance Partners	Local Governance Meetings IGC

Review

This policy should be reviewed every three years, or earlier considering any legislative or national professional guidance changes.

References

NHS Patient Safety Strategy: NHS England » The NHS Patient Safety Strategy
Patient Safety Incident Response Framework: NHS England » Patient Safety Incident Response Framework
Patient Safety Incident Response Standards including training requirements: B1465-5.-Patient-Safety-Incident-Response-standards-v1-FINAL.pdf (england.nhs.uk)
NHS Patient Safety Specialists: NHS England » Patient Safety Specialists
Engaging and involving patients, families and colleagues following a patient safety incident - B1465-2.-Engaging-and-involving...-v1-FINAL.pdf (england.nhs.uk)
Learning from Patient Safety Events NHS England » Learn from patient safety events (LFPSE) service
NHS England » Patient safety healthcare inequalities reduction framework
Learning From Patient Safety Events, Levels of Harm NHS England » Policy guidance on recording patient safety events and levels of harm
NHS England » Being fair tool: Supporting staff following a patient safety incident
Development of Safety Actions: B1465-Safety-action-development-v1.1.pdf (england.nhs.uk)
National Patient Safety Agency, Seven Steps to Patient Safety. 2004. (www.npsa.nhs.uk/sevensteps)
HSSIB Learning Response and Improvement assessment tool: Learning response review and improvement tool (hssib.org.uk)
Patient Safety Partner resources: NHS England » Framework for involving patients in patient safety: Appendices
NHS England, Never Events List, 2018. (https://improvement.nhs.uk/documents/2266/Never_Events_list_2018_FINAL_v5.pdf)
Learn Together investigation resources: Investigation resources – learn-together.org.uk
NHS England, Revised Never Events Policy and Framework, 2018.
NHS England Oversight Roles and Responsibilities - B1465-4.-Oversight-roles-and-responsibilities-specification-v1-FINAL.pdf (england.nhs.uk)
https://improvement.nhs.uk/documents/2265/Revised_Never_Events_policy_and_framework_FINAL.pdf
NMC/GMC, Openness and honesty when things go wrong: the professional duty of candour. 2015
Openness and honesty when things go wrong: the professional duty of candour (gmc-uk.org)
Care Quality Commission, Regulation 20: Duty of Candour, 2015 (updated June 2022)
Regulation 20: Duty of candour - Care Quality Commission (cqc.org.uk)
Data Security and Protection Toolkit: Help (dsptoolkit.nhs.uk)
Information Commissioners Office (ICO): Personal data breaches: a guide | ICO
Notification of data security breaches to the Information Commissioner's Office (ICO)

Appendix 1 – Definitions

Client / patient safety incident:	An unintended or unexpected incident that could have or did lead to harm for one or more clients. We use client and patient interchangeably throughout this policy. This is the person receiving care from MSI UK.
Health & Safety incident:	An unintended or unexpected incident that could have or did lead to harm of visitors and/or colleagues.
Adverse Clinical Incident:	An unavoidable clinical outcome, which may be a known risk of a procedure, e.g. uterine perforation during surgical abortion
Information Governance Incident:	Any incident involving the actual or potential loss of personal information that could have other significant impact on individuals
Near Miss:	Any incident that had the potential to occur but was prevented, resulting in no harm to people receiving care.
No Harm:	No physical or psychological harm. No adverse outcome caused to a person or the organisation - Any incident that ran to completion, but no harm occurred to people receiving care e.g. breach of confidentiality or other health records/documentation incidents with no adverse outcome. Being involved in any patient safety incident is not pleasant, no harm is used if you are not aware of any specific harm that meets low harm or greater criteria.
Harm	Physical or psychological injury or damage. Harm is generally considered to be unexpected if it is not related to the natural course of a person's illness, treatment or underlying condition, or the natural course of events if harm occurs to a person other than a client.
Low Physical Harm	Low physical harm is when ALL of the following apply: • Minimal harm, occurred – patient(s) required extra observation or minor treatment • Did not or is unlikely to need further healthcare beyond a single GP, community healthcare professional, emergency department or clinic visit • Did not or is unlikely to need further treatment beyond dressing changes or short courses of oral medication • Did not or is unlikely to affect the patient's independence • Did not or is unlikely to affect the success of treatment for existing health conditions
Moderate Physical Harm:	Moderate harm is when at least one of the following apply: • has needed or is likely to need healthcare beyond a single GP, community healthcare professional, emergency department or clinic visit, and beyond dressing changes or short courses of medication, but less than 2 weeks additional inpatient care and/or less than 6 months of further treatment, and did not need immediate life-saving intervention • has limited or is likely to limit the patient's independence, but for less than 6 months • has affected or is likely to affect the success of treatment, but without meeting the criteria for reduced life expectancy or accelerated disability described under severe harm.

Severe Physical Harm:	Severe harm is when at least one of the following apply: • permanent harm/permanent alteration of the physiology • needed immediate life-saving clinical intervention • is likely to have reduced the patient’s life expectancy • needed or is likely to need additional inpatient care of more than 2 weeks and/or more than 6 months of further treatment • has, or is likely to have, exacerbated or hastened permanent or long term (greater than 6 months) disability, of their existing health conditions • has limited or is likely to limit the patient’s independence for 6 months or more.
Catastrophic Harm / Fatal	Any unexpected or unintended incident that directly resulted in the death of one or more persons. You should select this option if, at the time of reporting, the patient has died and the incident that you are recording may have contributed to the death.
Psychological Harm	Harm that causes mental or emotional trauma. When recording psychological harm, you are not required to make a formal diagnosis; your answer should be an assessment based on the information you have at the point of recording and can be changed if further information becomes available
Low Psychological Harm	Low psychological harm is when at least one of the following apply: • distress that did not or is unlikely to need extra treatment beyond a single GP, community healthcare professional, emergency department or clinic visit • distress that did not or is unlikely to affect the patient’s normal activities for more than a few days • distress that did not or is unlikely to result in a new mental health diagnosis or a significant deterioration in an existing mental health condition
Moderate Psychological Harm	Moderate psychological harm is when at least one of the following apply: • distress that did or is likely to need a course of treatment that extends for less than six months • distress that did or is likely to affect the patient’s normal activities for more than a few days but is unlikely to affect the patient’s ability to live independently for more than six months • distress that did or is likely to result in a new mental health diagnosis, or a significant deterioration in an existing mental health condition, but where recovery is expected within six months
Severe Psychological Harm	Severe psychological harm is when at least one of the following apply: • distress that did or is likely to need a course of treatment that continues for more than six months • distress that did or is likely to affect the patient’s normal activities or ability to live independently for more than six months • distress that did or is likely to result in a new mental health diagnosis, or a significant deterioration in an existing mental health condition, and recovery is not expected within six months
Never Event	Never Events are defined as incidents that are thought to be wholly preventable because guidance or safety recommendations that provide strong systemic protective barriers are available at a national level and should have been implemented by all healthcare providers. Never Events will always be a reported and investigated as a patient safety incident investigation.

Duty of Candour	Openness and honesty when things go wrong. Sets out professional standards on what organisational colleagues in the UK should do if something goes wrong during patient care.
Just culture	The fair treatment of colleagues supports a culture of fairness, openness and learning by making colleagues feel confident to speak up when things go wrong, rather than fearing blame.
Accident	An unplanned, uncontrolled event, which has led to or could lead to injury to people, damage to equipment, buildings or the environment and/or some other loss.
After Action Review (AAR)	A method of evaluation that is used when outcomes of an activity or event, have been particularly successful or unsuccessful. It aims to capture learning from these tasks to avoid failure and promote success for the future.
Claim	In this context, a claim is defined as a formal or legal claim against the organisation.
Integrated Care Board (ICB)	A statutory NHS organisation which is responsible for planning and funding most NHS services to meet the health needs of the population within their geographical area.
Culture	Learned attitudes, beliefs and values that define a group or groups of people.
Duty of Candour	A statutory duty to inform clients/patients and where appropriate family and carers of any incidents that are categorised as moderate harm or severe harm. Providing them with an apology, keeping them informed of investigation and supporting them to deal with the consequences.
Engaging and Involving patients, families and colleagues	A national framework from NHS England to guide investigators or colleagues working in patient of family liaison roles, in involving patients, families and colleagues during investigations. It replaces previous guidance ‘Being Open’.
Hazard	A hazard is something (e.g. an object, unsafe act, or unsafe process) that has the potential to cause harm, loss or damage. Individual responsibilities are not however discharged by the mere completion of an incident reporting form and all reasonable steps should be taken at the time to minimise the risk of injury arising from any identified hazard
Learning from Patient Safety Events (LFPSE)	A new national service for the recording and analysis of patient safety events that occur in healthcare. LFPSE replaces the National Reporting and Learning System (NRLS) and the Strategic Executive Information System (StEIS).
Learning Response Toolkit	National guides and tools available from NHS England, for healthcare organisations to use to promote a range of system-based approaches for learning from patient safety incidents. These include Patient Safety Incident Investigation (PSII), After Action Review, Multidisciplinary Team Review, SWARM Huddle and Thematic Analysis.
Multidisciplinary Team Review	A meeting between members of health and care colleagues who are members of different organisations and professions, that work together to make decisions regarding the treatment of individuals and services users for the purpose of learning and improvements.
Incident	An unplanned untoward event, which has happened to, or occurred with person’s, colleagues or volunteers the result of which is harm
Information Governance Incident	An incident involving the loss or breach of Personal Confidential Data (PCD) which may require reporting to the Information Commissioners Office in line with the incident scoring checklist.

Information Governance Significant Incident Requiring Investigation (IG SIRI)	**Information Governance Significant Incident** Requiring Investigation (IG SIRI) includes: Information sent to the wrong recipient. Information filed against the incorrect record. Unauthorised disclosure of information. Receipt of malicious/threatening phone call i.e. bomb threat. Missing or amended accounting records. Attempts to obtain information by deception (e.g. bogus phone calls, social engineering or e-mails). Deliberate damage to property. Activation of intruder/fire alarms. Fraud (by colleagues, a third party or a member of the public). Cardholder data breaches. Unauthorised, unescorted visitors. Actual or attempted theft of property. Suspected or actual illegal activity (e.g. breaches of the Computer Misuse Act, Data Protection Act, General Data Protection Regulation, Designs Copyright and Patents Act, or use for storing illegal images or text) An Information Governance Cyber SIRI includes: Discovery of malicious or unauthorised software, such as a computer virus or computer game. Hacking or attempted hacking by colleagues, third-parties or outsiders. Unauthorised modification/removal of system software, hardware or connections. Connecting an unauthorised mobile device to MSI UK equipment. Unauthorised modification or deletion of system data. Disclosure of system data to unauthorised personnel. Suspected breach of software copyright. Suspected breach of the firewalls or malicious attack. Unattended terminals repeatedly left logged in. Repeated lock out of users' accounts due to repeated failure to enter correct password. Disclosure of Restricted or confidential information (especially passwords or other access control data) to unauthorised personnel Loss of portable computing equipment, e.g. laptop; mobile phone etc. Actual or attempted unauthorised entry to a secure area.
Investigation	An investigation is a careful search or examination of the incident, in order to discover the facts. Some level of investigation must be applied to every incident.
Near Miss Incident	An unexpected or unplanned untoward event that could have resulted in loss, damage, harm, injury or illness. Preventative change to procedure, process or systems may prevent an incident from occurring in the future
NHS Funded Healthcare	Healthcare that is partially or fully funded by the NHS, regardless of the provider or location.
Non-clinical incident	Non-clinical incidents are incidents which do not relate to the delivery of healthcare or clinical interventions and will usually involve colleagues/contractors or the public being injured or led to loss or damage to equipment/property, or other financial loss.

Patient Safety Incident Investigation (PSII)	A patient safety incident investigation is undertaken when an incident or near-miss indicates significant patient safety risks and potential for new learning.
Patient Safety Incident Response Plan (PSIRP)	The PSIRP supports this policy and sets out how we will respond to patient safety incidents to proactively seek learning for improvement. It is reviewed at least annually with the ICB but can be more often as it is a live, evolving document.
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR)	RIDDOR are adverse incidents that result in an injury to a colleague whilst at work and must be reported to the Health & Safety Executive. Accidents to members of the public or others who are not at work must also be reported if they result in an injury and the person is taken directly from the scene of the accident to hospital for treatment to that injury. The following injuries are reportable under RIDDOR when they result from a work-related accident (out of or in connection with work): • The death of any person (Regulation 6) • Specified Injuries to workers (Regulation 4) • Injuries to workers which result in their incapacitation for more than 7 days (Regulation 4) • Injuries to non-workers which result in them being taken directly to hospital for treatment, or specified injuries to non-workers which occur on hospital premises (Regulation 5) The Health & Safety Manager injuries reportable under RIDDOR
Risk	A situation involving exposure to danger. Risk is the probability of an outcome having a negative effect on people, systems or assets.
SIRO	The Senior Information Risk Owner (SIRO) is the accountable executive director with responsibility for Information Governance. The MSI UK SIRO is the Chief Finance Officer
SWARM Huddle	Swarm-based huddles are used as a rapid response to identify learning from patient safety incidents. Immediately after an incident, colleagues ‘swarm’ to the site to quickly analyse what happened, how it happened and decide what needs to be done to reduce risk.

Appendix 2 – MSI UK Zero Tolerance Incidents

The following types of incidents should always be reported and investigated. These incidents will always be escalated to the Executive Team:

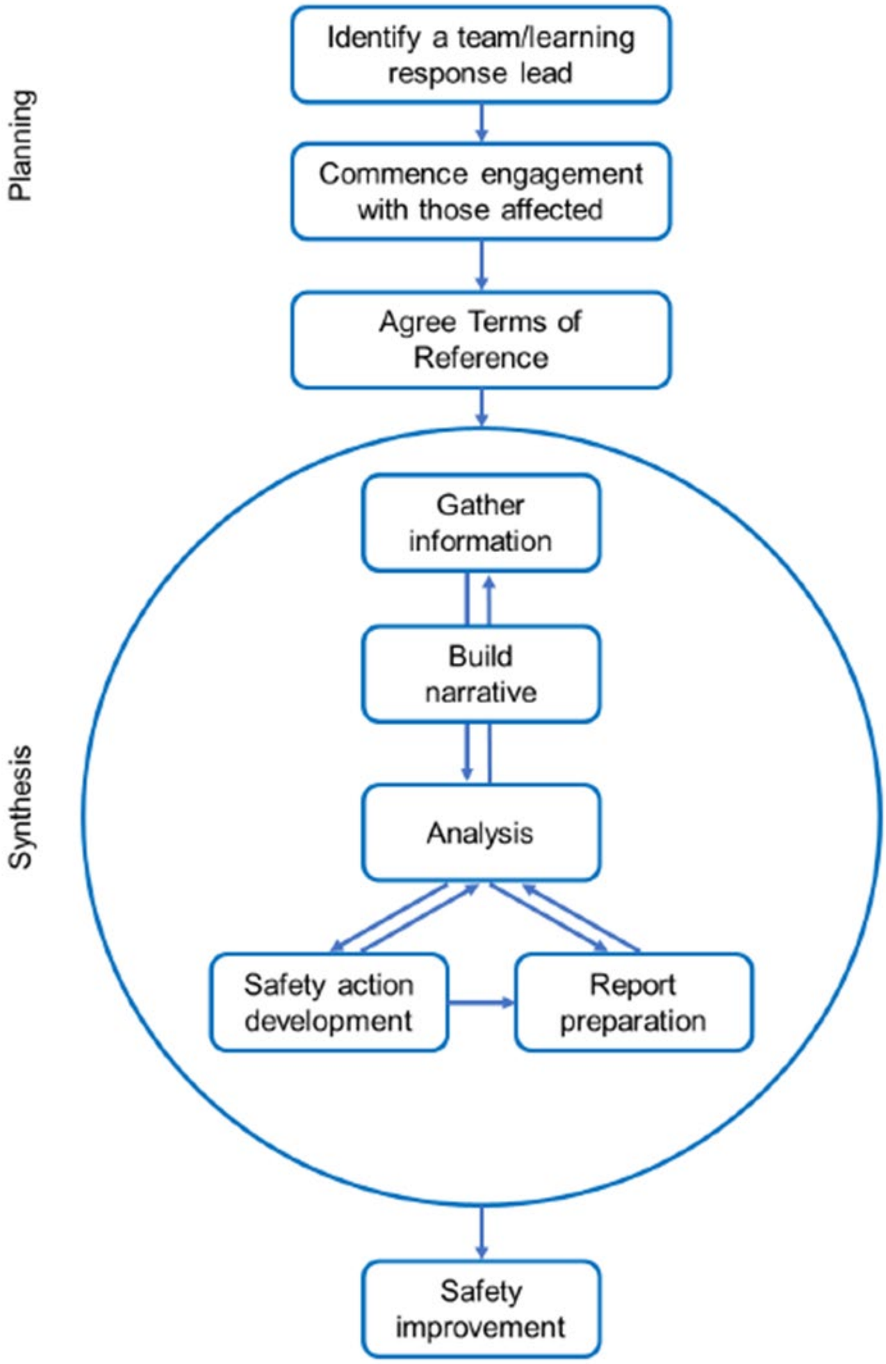
- Preventable clinical incidents that result in moderate or greater harm to our clients;
- Information Governance and cyber breaches that constitute a severe harm Incident or ICO Reportable breach will be reported via the Data Security and Protection Toolkit;
- Health & Safety incidents that result in moderate or greater harm to our clients, visitors and/or colleagues;
- Violence and aggression incidents resulting in moderate or greater harm to our colleagues;
- Incidents involving the bullying or harassment of our colleagues;
- Client or person involved not adequately Safeguarded.

Appendix 3 – Flow-Diagram of Incident Process and Reporting Timescales

Incident occurrs	Incident occurs Immediate actions taken to manage the situation safely Duty of candour and compassionate engagement begins – open and honest communication and explanation, verbal apology, establish support required and inform of next steps. Person who identifies or is notified of an incident, reports via Datix and to person in charge within 1 working day Auto email notifications are triggered to the relevant internal stakeholders Incidents have an initial review by the centre and the quality & governance team for the following: • Confirm incident grading and initial response required • Confirm notification of the incident to subject matter experts and other relevant individuals • Notification of incident to HR for colleagues identified as requiring support if indicated • Determine/confirm level of harm & learning response required • Notify the Executive Management Team of any incident requiring a PSII (as defined within the PSIRP), and/or an incident of severe/catastrophic harm • Incident notification to relevant external bodies; e.g. LFPSE, police, CQC, ICB etc (the relevant ICB should be notified of any incident requiring an emergency transfer as a result of treatment within 24 hrs)	
1-3 working days	Incident requiring PSII as defined within the PSIRP Schedule a local management review meeting, with relevant individuals and subject matter experts involved including a patient safety specialist Understand who requires support and ensure approach is individualised	Incident meets MDT, AAR or local level incident at this stage SWARM / de-brief huddle if appropriate (i.e. emergency scenarios/transfers) SWARM if appropriate (see PSIRP) is completed immediately after an incident and is led by a learning response lead CSM or Governance team assigns incident reviewer Confirm incident grade Documentation within client's notes confirmed as accurate and appropriate

3 – 15 working days	PSII Investigator and engagement lead are confirmed Contact made with client. Duty of Candour as per policy PSI investigator commences investigation using systems thinking and human factors methodology PSII Investigator plans investigation: team, subject matter experts, stakeholders Plans and commences engagement with those affected Agrees Investigation terms of reference Gathers information about what happened, use an evidence log and everyday work guides (i.e. observations, link analysis, interview tools) ,	Incident type & category confirmed Update incident status from “In the holding area, awaiting review” to “Being reviewed” Consider learning response required (see PSIRP) Engage and involve colleagues involved, learning response lead and other colleagues including relevant subject matter expert as appropriate Discuss incident and initial response at CLIPS Learning response lead commences required learning response Establish learning and agree next steps / actions Upload relevant learning response documentation to Datix
15 days – 60 days	PSII Investigator builds a detailed narrative from the information gathered Analysis of information – the PSII makes conclusions or findings to inform next steps Safety action development (see guide) Report preparation – PSII considers audience, timeframes for final report Once completed, the investigation report should be shared with the people involved and affected for feedback Investigation report submitted to the PSIRF Executive Lead and Panel for sign-off and approval Share completed investigation report with internal and external stakeholders as required (ICB and/or CQC once internally approved and signed off) Final Duty of Candour completed Actions are added to the action log and effectiveness of these are monitored through local governance and Medical Advisory Committee meetings Any new risks identified are added to the Risk Register Quality & Governance Team review the LFPSE report Learning is shared at CLIPS and other agreed platforms internally	Learning response, findings and agreed safety actions are shared with CLIPS group Incident handler approves & closes investigation by day 15 Updates incident status from “awaiting final approval” to “finally approved” Any new risks identified to be added to the Risk Register Actions added to the action log are monitored through local governance and Clinical Effectiveness Group (CEG) to assess impact and effectiveness

Appendix 4 – Overview of patient safety incident investigation stages*



**NHS England Patient Safety Incident Investigation*

Appendix 5 – Reporting to External Agencies

Agency	Circumstance	Reporter
Care Quality Commission	Notifications under CQC regulatory scheme	Registered Manager / Nominated Individual
Counter Fraud Agency	Actual or suspected fraud	Anyone
Health and Safety Executive	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR), place a legal duty on employers to report work-related deaths [1], major injuries [2] or over-three- day injuries [3], work related diseases [4], and dangerous occurrences (near miss accidents) [5].	Registered Manager, CSM or Operations Managers in discussion with the Head of Health and Safety
Department of Health / NHS Digital	All incidents raised on the NHS Digital Data Security and Protection Toolkit are notified to the Department of Health	Director of Digital and Transformation Head of IS Governance SIRO Caldicott Guardian
Disclosure and Barring Service	Dismisses or withdraws permission for an individual to engage in a regulated or controlled activity, or would have done so had that individual not resigned, retired, been made redundant or been transferred to a position which is not a regulated or controlled activity because they think that the individual has: engaged in relevant conduct satisfied the Harm Test; or received a caution or conviction for a relevant offence	HR Manager
Information Commissioner	All reportable information governance SIRIs and Cyber SIRIs	Director of Digital and Transformation in discussion with SIRO

Agency	Circumstance	Reporter
Learning From Patient Safety Events (LFPSE)	External reporting of patient safety incidents for the purpose of learning and improvement	Quality & Governance Partners
Medicines and Healthcare Products Regulatory Agency (MHRA)	Suspected safety problems with medicines, medical devices, blood and blood components	Colleagues who discovers the problem in discussion with Pharmacy Services (Medication), Head of Health and Safety (Medical Devices).
Police	Death or injury where it is considered there are unusual or suspicious circumstances Theft of / malicious damage to, MSI UK property. Arson	Medical Director/ Director of Nursing, Midwifery, and Quality (or their delegates). Estates and Facilities Lead (Head of Health and Safety) Fire Safety Leads (Centres, Regional and Corporate)
Professional Regulatory Bodies.	Where there are concerns about the practice of a healthcare professional.	Medical Director/ Director of Nursing, Midwifery, and Quality (or their delegates).
NHS Resolution (CNST)	Incidents where there are likely to be claims require, where practicable, to be notified to NHSRs as early as possible.	Quality & Customer Services Manager
ICB	Incidents requiring a PSII to the relevant ICB. In addition, learning from thematic reviews and other learning responses.	Accounts Manager or Registered Manager

Appendix 6 – Assessing the Severity of the Incident Guide (IG SIRI) – Data Security and Protection Toolkit

Establish the likelihood that adverse effect has occurred

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Both the adverse effect and likelihood values form part of the breach assessment grid.

There are a limited number of circumstances where, even when an organisation is aware of a breach of personal data, there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive.

Under the following circumstances notification may not be necessary;

- encryption – where the personal data is protected by means of encryption.
- ‘trusted’ partner - where the personal data is recovered from a trusted partner organisation.
- cancel the effect of a breach - where the controller can null the effect of any personal data breach.

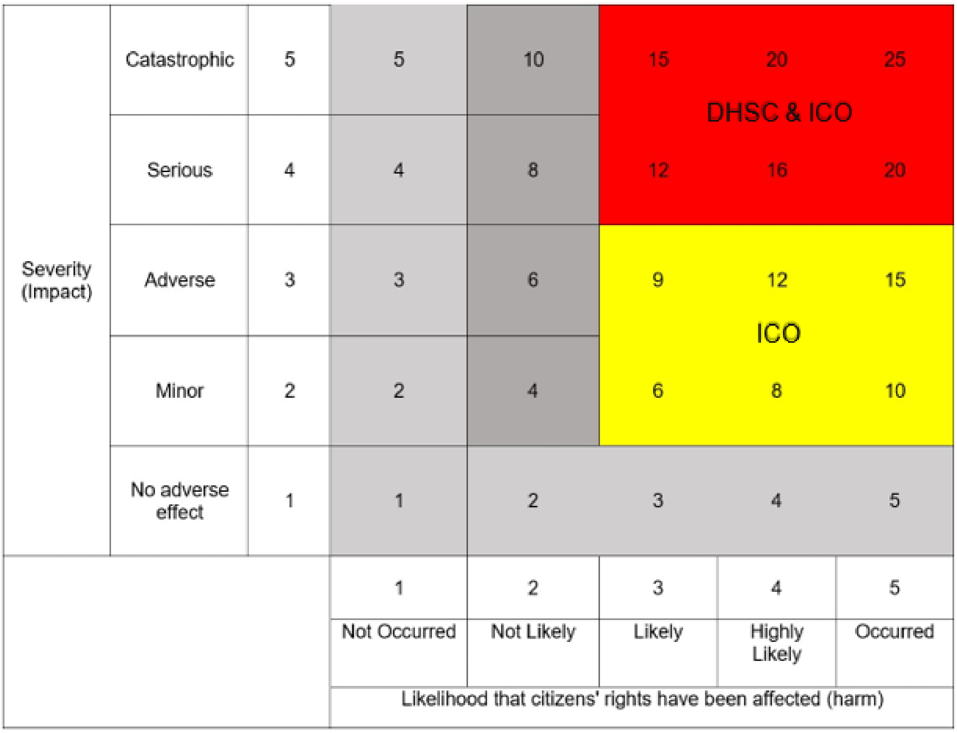
Example of how the ‘trusted’ partner can be used to contain a breach

There may be a confidentiality breach, whereby personal data is disclosed to a third party or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered “trusted”. In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery.

In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller must keep information concerning the breach as part of the general duty to maintain records of breaches.

Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “green breaches” being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.



Severity (Impact)	Catastrophic	5	5	10	15	20	25
						DHSC & ICO	
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
						ICO	
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

Or in narrative

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, the incident is reportable and full details will be automatically emailed to the ICO and the NHS Digital Data Security Centre.
The DHSC will also be notified where it is (at least) likely that harm has occurred, and the impact is at least serious.

Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores. If a breach involves certain categories of special categories/vulnerable groups, it must be assessed as at least:

A Likelihood of ‘Not likely or incident involved vulnerable groups (where no adverse effect occurred)’ Not Likely on the grid.
and
A Severity of ‘Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred’. Minor on the grid.

So even where an incident involves special categories/vulnerable groups, on the breach assessment grid above, it would be a minimum of 4 and so would not always be reported to the ICO. It would be reported to the ICO if the Likelihood of harm is assessed as at least ‘Likely’.

Special Categories of personal data

For clarity, special categories under GDPR are;
- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,

- and the processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person’s sex life or sexual orientation

For clarity, special categories under GDPR not listed above include;

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

Criminal convictions and offences under Article 10 of the GDPR is further explained in the Data Protection Act 2018 Part 2, Chapter 2, S10 (2) and includes -

the alleged commission of offences by the data subject;
or
(b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

Assessing risk to the rights and freedoms of a data subject (likelihood)

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Depending on the outcome of the scoring matrix contained in this guide the risk may be high risk and be significant enough to notify to the ICO. If there is any doubt that a breach is significant enough for notification it is always best to notify.

A tabular conversion table at Reporting schema for data breaches from 25 May 2018’ lists how previous data breach reporting maps to the GDPR categorisations. A full list of rights and freedoms is given at the following link and the above are a summary of the main results of a breach on those rights.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

What to include in the notification

Article 34 of the GDPR outlines what must be communicated to the relevant authority and this has been included in this reporting tool.

The GDPR requires that the following information be included in any notification;

> a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
>
> the name and contact details of the data protection officer or other contact point from whom more information can be obtained.
>
> a description of the likely consequences of the personal data breach.
>
> a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Incident Management and breach reporting

Breach reporting may form part of an ongoing incident management or it may be historical. The steps to breach reporting should be complimentary to incident management and not in replacement of it. The DSP Incident Reporting Tool should not be used in place of an incident management process. It is solely for the purposes of reporting to the relevant regulatory authority. There is a legal requirement to maintain a local file containing the particulars of the breach and subsequent investigation and action, if any.

Details of the incident management process in relation to an organisation's responsibility under the data security standards (Data Security Standard 6 Responding to Incidents) is available here:

https://www.dsptoolkit.nhs.uk/Help

When to report within 72 hours

The GDPR Article 33 requires reporting of a breach within 72 hours. For urgent security, related incidents that require immediate assistance and support an organisation is advised to contact the Data Security Centre (formerly known as CareCERT) helpdesk immediately on 0300 303 5222or contact enquiries@nhsdigital.nhs.uk . As previously stated, this tool is for notification and local incident management must still be carried out.

This 72 hour starts when an organisation **becomes aware** of the breach which may not necessarily be when it occurred. An organisation must have a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised. This means that once a colleague or the public has reported a breach this is the point that an organisation is aware. The actual incident may have occurred some hours, days or weeks previously, but it is only when an organisation is aware that the breach has occurred that the 72 hours to notification period starts. Where the 72 hours' deadline is not met, an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

In the event that the Data Security and Protection Incident Reporting Tool is unavailable, users may choose to either report the incident via the ICO helpline on 0303 123 1113
(ICO normal opening hours are Monday to Friday between 9am and 4.30pm).

Or

report when the Data Security and Protection Incident Reporting tool is available noting the reasons for delay in the relevant part of the form.

What to expect once the incident reported

Once an incident meets the threshold for reporting and is reported using the Data Security and Protection Incident Reporting Tool a notification message is presented on the Incident Reporting screen displaying:

- 'Incident Reported'
- confirmation that the ICO has been informed and
- an incident reference number from the incident reporting tool

Shortly after the incident has been reported the reporting organisation will receive:

- an email from the ICO to confirm receipt of the notification and
- an ICO case reference number

This ICO case reference number should be quoted in any correspondence with the ICO in relation to the incident as this is the key reference used by the ICO.

Up until the incident has been reported and notified the incident may be edited in the Data Security and Protection Incident Reporting Tool. However, once reported, the incident can no longer be edited. It will be displayed on the Incident Reporting screen and be available in **read-only** format.

Any updates to the incident should be notified to the ICO by email, quoting the ICO case reference number.

What to expect if an incident is not reportable to the ICO/DHSC

If after completing the assessment of likelihood of impact to citizens' rights and freedoms, the impact of the incident does not meet the threshold for reporting, then the incident will not be reported to the ICO and DHSC and no further information is required.

The incident reference will be displayed, and a record will be stored on the Reporting an Incident screen in a read-only format. Once the incident is in read-only format, if more information becomes available about the incident which would make the incident reportable, then a new incident should be reported.

Local records required for an incident notified to the ICO

A local file, which may be requested by the Information Commissioner, must be maintained which must contain the following sections;

- the facts relating to the breach.
- its effects.
- the remedial action taken.

The local file of the investigation may be an incident management system (Datix for MSI UK). It may be in any format but if requested by the regulator such as the Information Commissioner it must be passed to them.

Communication of a personal data breach to the data subject
Article 34 of GDPR requires any personal data breach, that is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected.

Any communication must contain the following four elements

- a description of the nature of the breach;

- the name and contact details of the data protection officer or other contact point from whom more information can be obtained

- a description of the likely consequences of the personal data breach

- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

A communication is not necessary in the following three circumstances

- the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach for example the data were encrypted.

- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.

- it would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.

The ICO has produced a guide which may be found on its website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

If an organisation decides not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel organisations to inform affected individuals if it considers there is a high risk. Organisations should document their decision-making process in line with the requirements of the accountability principle.

Reporting schema for data breaches from 25 May 2018

The questions asked of organisations reporting an incident are:

ID	Information Requested
1	Organisation Name
2	Organisation Code
3	Name of the person Submitting incident
4	Email Address of person Submitting incident
5	Sector
6	What has happened?
7	How did you find out?

8	Was the incident caused by a problem with a network or an information system?
9	What is the local ID for this incident?
10	When did the incident start?
11	Is the incident still on going?
12	Have data subjects or users been informed?
13	Is it likely that citizens outside England will be affected?
14	Have you notified any other (overseas) authorities about this incident?
15	Have you informed the Police?
16	Have you informed any other regulatory bodies about this incident?
17	Has there been any media coverage of the incident (that you are aware of)?
18	What other actions have been taken or are planned?
19	How many citizens are affected?
20	Who is affected?
21	What is the likelihood that people's rights have been affected?
22	What is the severity of the adverse effect?
23	Has there been any potential clinical harm as a result of the incident?
24	Has the incident disrupted the delivery of healthcare services?
25	Which of these services are operated by your organisation?

The table below incorporates the Article 29 working party categorisation of confidentiality, integrity and availability breaches against the historic SIRI and cyber SIRI classifications. Additionally, the last column has the current ICO categorisations for illustration in a like for like comparison of old to new.

Type of breach Art 29 WP	Sub type Art 29 WP	SIRI tool	Cyber SIRI tool	ICO categorisation including new cyber breach types
Confidentiality				
	Unauthorised or accidental disclosure	B Disclosed in Error	Phishing emails	Data sent by email to incorrect recipient
		H Uploaded to website in error	Social Media Platforms	Data posted or faxed to incorrect recipient
		J Unauthorised Access/Disclosure	Spoof website	Failure to redact data
			Cyber bullying	Information uploaded to webpage
				Verbal disclosure
				Failure to use bcc when sending email
				Data sent by email to incorrect recipient
				Cyber security misconfiguration (e.g. inadvertent

				publishing of data on website; default passwords)
				Cyber incident (phishing)
	Unauthorised or accidental access	I Technical security failing (including hacking)	Hacking	Insecure webpage (including hacking)
		J Unauthorised Access/Disclosure		Cyber incident (key logging software)
Availability				
	Unauthorised or accidental loss	A) Corruption or inability to recover electronic data	Denial of Service (DOS)	Loss or theft of paperwork
		C) Lost In Transit		Loss or theft of unencrypted device
		D) Lost or stolen hardware		Loss or theft of only copy of encrypted data
		E) Lost or stolen paperwork		Data left in insecure location
				Cyber incident (other – DDOS etc.)
				Cyber incident (exfiltration)
				Cryptographic flaws (e.g. failure to use HTTPS; weak encryption)
	Unauthorised or accidental destruction	F) Non-secure Disposal – hardware	Malicious internal damage	Insecure disposal of paperwork
		G Non-Secure Disposal – paperwork		Insecure disposal of hardware
Integrity				
	Unauthorised or accidental alteration	K Other	Web site defacement	Other principle 7 failure
				Cyber incident – unknown (e.g. data published on Pastebin but no information on how compromise occurred)

Appendix 7 – Information Governance Serious Incident Breach Types Defined Data Security and Protection Toolkit

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

The table below provides detailed definitions and examples of IG Incident Reporting. Many data incidents will involve elements of one or more of the categories in this table. For reporting, the description which best fits the key characteristic of the incident should be selected.

Breach Type	Examples/incidents covered within this definition
Lost in transit	The loss of data (usually in paper format, but may also include CD's, tapes, DVD's or portable media) whilst in transit from one business area to another location. May include data that is; Lost by a courier; Lost in the 'general' post (i.e. does not arrive at its intended destination); Lost whilst on site but in situ between two separate premises / buildings or departments; Lost whilst being hand delivered, whether that be by a member of the data controller's colleagues or a third party acting on their behalf 'lost in transit' would not include data taken home by a colleague for the purpose of home working or similar (please see 'lost or stolen hardware' and 'lost or stolen paperwork' for more information).
Lost or stolen hardware	The loss of data contained on fixed or portable hardware. May include; Lost or stolen laptops; Hard-drives; Pen-drives; Servers; - Cameras; Mobile phones containing personal data; Desk-tops / other fixed electronic equipment; Imaging equipment containing personal data; Tablets; Any other portable or fixed devices containing personal data; The loss or theft could take place on or off a data controller's premises. For example, the theft of a laptop from an employee's home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk.

Lost or stolen paperwork	The loss of data held in paper format. Would include any paperwork lost or stolen which could be classified as personal data (i.e. is part of a relevant filing system/accessible record). Examples would include;
	medical files;
	letters;
	rotas;
	employee records
	The loss or theft could take place on or off a data controller's premises, so for example the theft of paperwork from an employee's home or car or a loss

	whilst they were travelling on public transport would be included in this category. Work diaries may also be included (where the information is arranged in such a way that it could be considered to be an accessible record / relevant filing system).
Disclosed in error	This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This would include situations where the information itself hasn't actually been accessed. Examples include: Letters / correspondence / files sent to the incorrect individual; Verbal disclosures made in error (however wilful inappropriate disclosures / disclosures made for personal or financial gain will fall within the s55 aspect of reporting); Failure to redact personal data from documentation supplied to third parties; Inclusion of information relating to other data subjects in error; Emails or faxes sent to the incorrect individual or with the incorrect information attached; Failure to blind carbon copy ('bcc') emails; Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data; Disclosure of data to a third-party contractor / data processor who is not entitled to receive it
Uploaded to website in error	This category is distinct from 'disclosure in error' as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include; Failures to carry out appropriate redactions; Uploading the incorrect documentation; Lack of permission controls The failure to remove hidden cells or pivot tables when uploading a spreadsheet; Failure to consider / apply FOIA exemptions to personal data
Non-secure Disposal – hardware	The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include; Failure to meet the contracting requirements of principle seven when employing a third-party processor to carry out the removal / destruction of data; Failure to securely wipe data ahead of destruction; Failure to securely destroy hardware to appropriate industry standards; Re-sale of equipment with personal data still intact / retrievable; - The provision of hardware for recycling with the data still intact
Non-secure Disposal – paperwork	The failure to dispose of paperwork containing personal data to an appropriate technical and organisational standard. It may include; • Failure to meet the contracting requirements of principle seven when employing a third-party processor to remove / destroy / recycle paper; • Failure to use confidential waste destruction facilities (including on site shredding); • Data sent to landfill / recycling intact – (this would include refuse mix ups in which personal data is placed in the general waste);

Technical security failing (including hacking)	This category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include: • Failure to appropriately secure systems from inappropriate / malicious access; • Failure to build website / access portals to appropriate technical standards; • The storage of data (such as CV3 numbers) alongside other personal identifiers in defiance of industry best practice; • Failure to protect internal file sources from accidental / unwarranted access (for example failure to secure shared file spaces); • Failure to implement appropriate controls for remote system access for employees (for example when working from home) In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate this risk. A technical security incident may also be a Cyber incident **A technical security incident may also be a Cyber incident**
Corruption or inability to recover electronic data	Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption of care / adverse clinical outcomes. For example; • The corruption of a file which renders the data inaccessible; • The inability to recover a file as its method / format of storage is obsolete; • The loss of a password, encryption key or the poor management of access controls leading to the data becoming inaccessible
Unauthorised access/disclosure	The offence under section 55 of the DPA - wilful unauthorised access to, or disclosure of, personal data without the consent of the data controller. **Scenario 1** An employee with admin access to a centralised database of patient details, accesses the records of her daughter's new boyfriend to ascertain whether he suffers from any serious medical conditions. The employee has no legitimate business need to view the documentation and is not authorised to do so. On learning that the data subject suffers from a GUM related medical condition, the employee than challenges him about his sexual history.
Other	This category is designed to capture the small number of occasions on which a principle seven breach occurs which does not fall into the aforementioned categories. These may include: • Failure to decommission a former premise of the data controller by removing the personal data present; • The sale or recycling of office equipment (such as filing cabinets) later found to contain personal data; • Inadequate controls around physical employee access to data leading to the insecure storage of files (for example a failure to implement a clear desk policy or a lack of secure cabinets).

Appendix 8 – Equality Impact Assessment

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the document/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	▪ Gender (including gender reassignment)	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
	Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are there any valid exceptions, legal and/or justifiable?**	No	
4.	**Is the impact of the document/guidance likely to be negative?**	No	
5.	**If so, can the impact be avoided?**	N/A	
6.	**What alternative is there to achieving the document/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	
8.	**Date Reviewed:**	July 2025	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the author, together with any suggestions as to the action required to avoid/reduce this impact.

Appendix 9 – Being Fair Tool: Supporting staff following a patient safety incident

If no or unsure, continue by asking the further substitution test questions

1b. Was the individual included when their peer group received relevant training? **1c Have you considered the experience and background of the individual (including differences in training practices between organisations or internationally and cultural differences)?** **1d. Was supervision in line with expected practice?**	**If no to any,** or the answer is unknown, discuss with the individual's supervisor or education lead. Continue with the systems-based learning response. Only continue with the tool if there are ongoing concerns that an individual's action may have been reckless, wilfully neglectful or malicious.

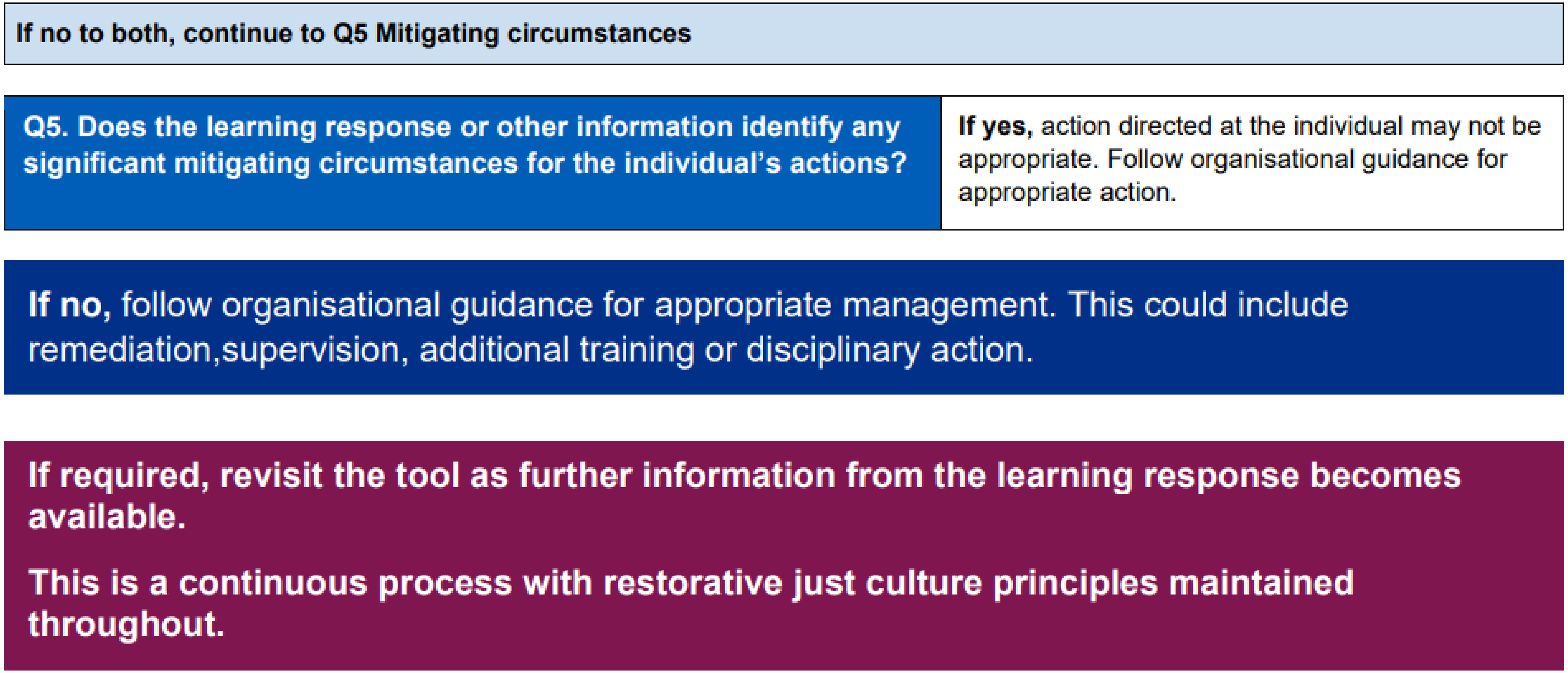
Questions	Action to take
Q1 Substitution test – to ensure wider system issues have been fully considered	
1a. Does the learning response indicate that staff in the same peer group as the individual involved and with comparable experience and qualifications would have acted in the same way in similar circumstances?	**If yes**, continue with the systems-based learning response. Only continue with the tool if there are ongoing concerns that an individual's action may have been reckless, wilfully neglectful or malicious.

If yes to all, continue to Q2 Foresight test – **to ensure wider system issues have been fully considered**

2a. Does the learning response identify any agreed protocols or accepted practices that apply to the individual's action or omission in question? **2b. Does the learning response find these protocols to be workable and reflective of accepted practice?**	If **no to any**, continue with the systems-based learning response. Only continue with the tool if there are ongoing concerns that an individual's action may have been reckless, wilfully neglectful or malicious.

If yes to all, continue to Q3 Deliberate harm test

Q3. Based on what is known, is there any suggestion of recklessness, wilful neglect or an intention to cause harm?	**If yes,** follow organisational guidance for appropriate action, including contacting any relevant external organisations: for example, professional regulatory bodies, the police or, if statutory safeguarding processes need to be adhered to, the relevant lead – that is, person in position of trust (PIPOT) for adult abuse and local authority designated officer (LADO) for child abuse.



If no to both, continue to Q5 Mitigating circumstances

Q5. Does the learning response or other information identify any significant mitigating circumstances for the individual's actions?

If yes, action directed at the individual may not be appropriate. Follow organisational guidance for appropriate action.

If no, follow organisational guidance for appropriate management. This could include remediation,supervision, additional training or disciplinary action.

If required, revisit the tool as further information from the learning response becomes available.

This is a continuous process with restorative just culture principles maintained throughout.

Appendix 10 Learning Response Review and Improvement Tool

Learning Response Review and Improvement Tool

Report details:	**ID**:	**Title**:

Development of this tool was informed by a research study which identified ‘traps to avoid’ in safety investigations and report writing. The tool was originally developed by NHS Scotland. It has been further refined in collaboration with the Health Services Safety Investigations Body (previously the Healthcare Safety Investigation Branch) and NHS England after being piloted in approximately 20 NHS trusts and healthcare organisations in England. The content validity of the tool is currently being assessed.

How to use this tool	The tool is intended to be used by: 1 Those writing learning response reports following a patient safety incident or complaint, to inform the development of the written report. 2 Peer reviewers of written reports to provide constructive feedback on the quality of reports and to learn from the approach of others.

Area of review (Descriptor)		**Rating scale** (Please insert 'X' in the applicable box)			**Comments/examples of text quotes** Add comments to clarify your ratings, this may be things that can be improved or content that you thought worked well and should be used in other reports
1	**People affected by incidents are meaningfully engaged and involved** The report demonstrates evidence that all those affected by the incident such as colleagues, patients, families and carers have been actively listened to and emotionally supported where required (i.e. interviews and perspectives of those affected are included in the report).	Good evidence □	Some evidence □	Little evidence □	
2	**The systems approach is applied** The report demonstrates consideration of system-based performance influencing factors (e.g. task complexity, technology, work procedures, workplace design, information transfer, clinical condition of patient, stress, fatigue, culture, leadership/management, policy/regulation) and how these interacted to contribute to the incident in question.	Good evidence □	Some evidence □	Little evidence □	

3	**‘Human Error’ is considered as a symptom of a system problem** ‘Human error’ or similar (e.g. nurse error, medical error, loss of situation awareness) is not concluded to be the ‘cause’ of the incident. Instead, multiple contributory factors which influenced the event are explored.	Good evidence □	Some evidence □	Little evidence □	
4	**Blame language is avoided** Language does NOT directly or indirectly infer blame of individuals, teams, departments, or organisations and/or focus on human failure (i.e. the nurse failed to follow policy; the doctor lost situation awareness).	Good evidence □	Some evidence □	Little evidence □	
5	**Local rationality is considered** The report clearly explains why the decisions and actions taken by individuals involved felt right at the time (i.e. the situation and context faced by those individuals is explored and described).	Good evidence □	Some evidence □	Little evidence □	

6	**Counterfactual reasoning is avoided** The report focuses on what happened and understanding why and NOT what people, departments or organisations 'could' or 'should' have done during or before the incident.	Good evidence □	Some evidence □	Little evidence □	
7	**Safety actions/recommendations are effective** Safety actions/recommendations proposed: • have been developed collaboratively with relevant staff/stakeholders and with consideration of wider organisation priorities and improvement work • focus on system elements (IT, equipment, care processes/pathways) not individuals • are specific, robust and actionable i.e. they don't add to 'safety clutter' • are accompanied by a plan to monitor progress over time • are demonstrably linked to the evidence and findings in the report.	Good evidence □	Some evidence □	Little evidence □	

8	**The written report is clear, easy to read and anonymised** The report is concise, written in plain English, uses inclusive language and anonymised i.e. it is written to 'inform rather than impress'.	Good evidence □	Some evidence □	Little evidence □	
9	**General comments** Is there anything else that can be improved or content that you thought worked well and should be used in other reports?				