Tees, Esk and Wear Valleys
NHS Foundation Trust

Public – To be published on the Trust external website

Clinical Risk Management Procedure

Ref: CORP-0071-v1

Status: Approved
Document type: Procedure

Contents

1 Introduction

The application of health IT can help deliver better and safer care for patients and drive improvements in patient safety. However, the converse of that is also true. Health IT has the potential to introduce clinical risk which can lead to patient harm. The Trust recognises its responsibility to proactively manage those risks and aims to mitigate to 'As Low As Reasonably Practicable' (ALARP), any potential risks to patient safety, introduced by Health IT.

The Trust is required to adhere to local and international standards and regulations. In addition, they may require that their Health IT system suppliers also comply with specific safety requirements.

Manufacturers of Health IT systems in England and Wales, are required by NHS Digital and NHS England to comply with Safety Standard DCB 0129 as mandated by the Health and Social Care Act 2012. Healthcare organisations that deploy and use Health IT are required to comply with Safety Standard DCB 0160. This document sets out how the Trust will meet the requirements of DCB 0160 ("the Standard").

> Confirmation of these standards is mandated by NHS England without exception.

The Trust's Senior Management Team supports the necessary activities to achieve this goal. They will provide the appropriate resources to comply with the applicable standards according to industry good practice; and they will ensure that safety processes are embedded within business operations and that appropriate lines of escalation and reporting are in place.

The Clinical Safety Case procedure outlines the processes to be followed to ensure that all Health IT used to support care within Tees, Esk and Wear Valleys NHS Foundation Trust (TEWV) is developed, implemented, and used in a safe manner; including any changes or modifications made and decommissioning of an existing system.

This procedure is critical to the delivery of Our Journey to Change (OJTC) and our ambition to co-create safe and personalised care that improves the lives of people with mental health needs, a learning disability or autism. It helps us deliver our three strategic goals as follows.

Goal 1 (To co-create a great experience for patients, carers and families): Clinical safety supports the goal of delivering outstanding care by ensuring that Health IT systems and products have undergone a robust risk assessment that ensures safe effective digital care delivery.

Goal 2 (To co-create a great experience for our colleagues): Clinical safety of all Health IT products and systems ensures that the work environments, (face to face or virtual), and additional resources (products or systems), are clinically safe and fit for supporting clinicians to be proud of the service they deliver

Goal 3 (To be a great partner): Clinical safety is a key tool and is strategic in assisting the Trust when it works with key partners to ensure patients safety when jointly caring for patients, working across organisational boundaries to improve services.

Implementing this procedure provides assurance to all patients, carers, families, and staff that when introducing or changing Health IT products and systems any risk to patients' safety has been considered from the outset.

1.2 Purpose

This Process sets out how the Trust means to manage clinical risk during the initial deployment, and during ongoing use, of a product. Systematic processes and procedures that characterise and mitigate potential clinical risks will be implemented

Following this procedure will ensure that the Trust:

- Meets its legal obligations in carrying out a thorough clinical risk management process and mitigates against any hazards found as low as reasonably practicable, complying with the NHS digital Standards (Ref 3)
- Addresses any risks identified and applies mitigations to ensure those risks are acceptable or as low as reasonably practicable (ALARP)
- Complies with the requirement of 'clinical safety by design and default'
- Ensures the rights and freedoms of individuals are not compromised
- Supports the NHSE/ Digital Technology Assessment Criteria (DTAC) as part of the due diligence process.
- systems are reflective of the diverse patient population who access services to enable staff to capture accurate patients' demographic data

This document applies to all staff who are responsible for the safety of the Trust's Health IT systems and products through the application of risk management

1.3 Scope

The Trust is required to adhere to local and international standards and regulations. In addition, they may require that their Health IT system suppliers also comply with specific safety requirements.

Manufacturers of Health IT systems in England and Wales, are required by NHS Digital and NHS England to comply with Safety Standard DCB 0129 (Ref. 1) as mandated by the Health and Social Care Act 2012 (Ref. 2). Healthcare organisations that deploy and use Health IT are required to comply with Safety Standard DCB 0160 (Ref. 3). This document sets out how the Trust will meet the requirements of DCB 0160 ("the Standard").

Systems which do not directly impact the care of individual patients are excluded from the Standard's scope and will not be required to fulfil the process requirements set out in this document

> ! Issues relating to security, privacy, confidentiality or information governance will be managed through the Trust's Information Governance and Security frameworks and not through this Clinical Risk Management Process

1.4 Accountability

Top Management, the Clinical Safety Officer(s) and supporting personnel share the responsibility of clinical risk management activities.

However, accountability for clinical risk management and patient safety in Health IT systems sits with top Management (see section 2.1.1 Top Management and Clinical Safety).

1.5 Safety and External Stakeholders

The trust depends on suppliers of Health IT products, to address clinical safety when designing their products and to ensure their products meet the requirements of the manufacturer's safety standards DCB 0129 (Ref. 1).

1.6 Clinical Risk Acceptability

Each hazard identified during a safety assessment will be attributed a level of clinical risk according to the criteria set out in Appendix 3. Together the hazards and their associated clinical risk will comprise the safety profile. A project may only proceed if the clinical risk associated with the identified hazards are acceptable. A hazard will be deemed acceptable if:

- The Residual Clinical Risk is Low or Moderate
- The Residual Clinical Risk is Significant, but it can be evidenced that the hazard has been mitigated to, As Low As Reasonably Practicable, or (exceptionally);
- The Residual Clinical Risk is High or Very High but this can be justified based on a clinical risk-benefit analysis.

Should the Residual Clinical Risk be deemed Unacceptable, and this cannot be justified by the clinical benefits, the assessment will conclude that additional means of risk control must be implemented before the project can proceed.

2 Governance and Competencies

2.1 Key Stakeholders

The Clinical Risk Management Process will be executed by a Clinical Risk Management Team.

The Team will comprise:

- Chief Clinical Information Officer
- Clinical Safety Officer(s)

The core Clinical Risk Management Team will be supported by a number of contributory personnel who will provide subject matter and domain-specific expertise. The personnel involved in a particular project will be set out in the Clinical Risk Management Plan.

2.1.1 Top Management and Clinical Safety

The Standard sets out a series of expectations and requirements to be fulfilled by Top Management. The Trust has assigned the Chief Clinical Information Officer (CCIO) and Deputy Chief Information Officer (Deputy CIO) to act in the capacity of Top Management. The CCIO and The Deputy CIO will act as Top Management's representatives and Accountable Officers for the purposes of Clinical Risk Management.

It is Top Management's responsibility to ensure that:

- Patient safety receives the highest level of priority in the business and that clinical risk management is a key objective.
- A rigorous and systematic approach to clinical risk management is taken.
- Adequate resources are made available to those who are responsible for undertaking the activities set out in this policy.
- Competent personnel from each of the specialist areas that are involved in developing and assuring the Health IT System are assigned.
- A Clinical Safety Officer, meeting the requirements set out in the Standard is nominated.
- The hazard assessment process involves a multidisciplinary team.
- A policy for determining the criteria for risk acceptability is defined and documented.
- A review of the suitability of the risk management process is conducted at planned intervals to ensure continuing effectiveness and that any decisions and actions taken are documented.

2.1.2 Clinical Safety Officer(s)

The Clinical Safety Officer(s) (CSO) will be appointed by Top Management. The Clinical Safety Officer(s) will:

- Be a suitably qualified and experienced clinician with relevant clinical experience.
- Hold a current registration with an appropriate professional body relevant to their training and experience.
- Be knowledgeable in risk management and its application to clinical domains.

- Maintain a knowledge of the health IT system being implemented and the contribution of human factors to its safe operation.
- Preserve competency records to demonstrate their suitability for performing the role.

The Clinical Safety Officer(s) will be responsible for:

- Overseeing the clinical risk assessment and ensuring that clinical risk management activities are completed in accordance with the Plan.
- Reviewing and approving the deliverables.
- Contributing to the clinical risk analysis.
- Providing the necessary clinical expertise and domain knowledge.
- Ensuring that the Safety Case's conclusions are objective and based on available evidence.
- Raising with Top Management any hazards which are evaluated as being Unacceptable.
- Making recommendations to Top Management regarding the acceptability of the risk associated with the implementation of a system and therefore the decision to go-live or continue service.
- Monitoring and evaluating incidents and concerns raised during live service.
- Overseeing the update of the clinical risk management deliverables in light of changes to the product or service.
- Remaining knowledgeable about clinical risk management and the applicable standards.

The Clinical Safety Officer will not be charged with delivery objectives which could, or be perceived to be, in conflict with their role to objectively advise on the safety position of the product.

2.1.3 Contributory Personnel and Governance

Role	Responsibility
Digital Performance and Assurance Group (DPAG)	• Governance group for approval/rejection of CSC's where mitigated high risk has been identified.
Digital and Data Management Group (D&DM)	• Subgroup providing guidance/ direction and approving papers that report into DPAG.
Digital Programme Board (DPB)	• Governance group for approval/rejection of Digital Programmes.
Change Assurance Group (CAG)	• For the introduction or upgrade of IT systems. CAG is the governance group for ensuring a CSC has been considered / commenced or approved prior to pilot or deployment of a health IT system or product. That the CSC is reviewed through the lifecycle and at any significant changes in use or at point of decommissioning the product.
Technical security department	• Responsible for ensuring technical security and safety of health IT systems and products that impact on or support patient care delivery.

Information Governance department	• Responsible for ensuring information security and safety of health IT systems and products that impact on or support patient care delivery.
Project Manager	• The Project Manager is responsible for: • Day to day management of the project • Ensuring that requirements for individual products and deliverables are agreed and understood • Agreeing tasks and actions with project team members • Reporting on progress • Ensuring the project is managed appropriately and in accordance with the Trust's Programme & Project Approval Management Methodology • Risk management • Issue management • Project planning • Quality in the project • Ensuring adequate project administration support
Systems Owners	• Person or persons responsible for the management / control of a specific trust IT system or associated software • Attends Change Approval Group (CAG) meetings (with the Information Department contact) for changes requested. • Attends supplier contract and review meetings for the system(s) owned. • Ensures that DPIA documents are produced and reviewed on a yearly basis for system(s) owned. • Leads and advises on the Service requirements for the system(s) owned. • Leads and advises on the roadmap of the system(s) owned from a Service perspective including contract renewal and tender exercises. • Ensures that checks are undertaken to ensure that the correct members of staff have access to the system including the submission of OneForms for the processing of starters, amendments, and leavers.
Information Asset Administrator (IAA)	• Implement the Information Risk Policy and ensure procedures are followed; • Recognise actual/potential security incidents-consult with IAO; • Ensure information asset registers and information flow mapping is accurate, up to date and risk assessed; • Ensure information handling procedures are in place.
Information Asset Owner (IAO) also known as Clinical Owner	• Assigned ownership/responsibility of particular information assets and are responsible for providing assurances to the SIRO on security; • Maintain understanding of 'owned' assets and how they are used; • Who has access to assets and why; • What information is held, added and removed; • Understanding and addressing risks to the asset, and providing assurance to the SIRO; • Provides assurance to the SIRO on security and use of the assets.

2.1.4 Issues and Escalation

Should the Clinical Risk Management Team experience issues or constraints in discharging their responsibilities under DCB 0160, this will be escalated to the Chief Clinical Information Officer or Deputy Chief Information Officer.

3 Related documents

This procedure describes what you need to do to implement the risk management section of the Organisational Risk Management Policy.

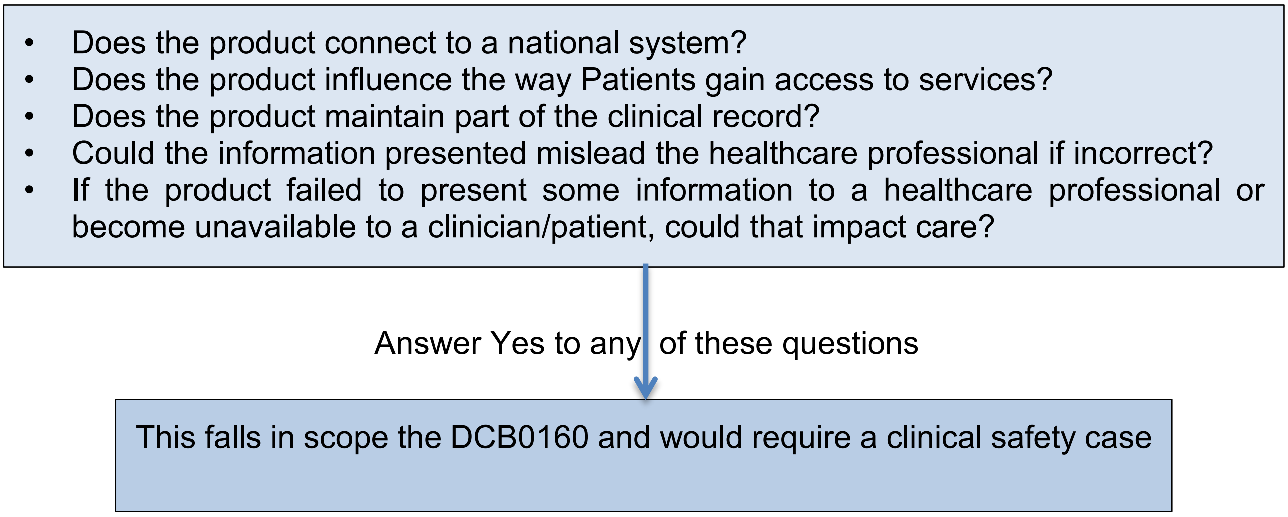
> ! The Organisational Risk Management Policy defines risk management which you must read, understand and be trained in before carrying out the procedures described in this document.

Clinical Safety Case documents may also refer to:

- Change Advisory Group (CAG) TOR
- Access to Information Systems Policy [IT-0031]
- Data Protection Impact Assessment (DPIA) Procedure [IT-0030-001]
- The introduction or upgrade of IT systems policy [IT-0032-001]
- Organisational Risk Management Policy [CORP-0066]
- Information Security & Risk policy [IT-0010]
- Maintenance of IT Systems policy [IT-0032]
- Incident reporting and serious incident review policy [CORP-0043]
- Digital and Data Services Change Advisory Group Procedure [IT-0032-004]

4 Clinical Risk Management Methodology

4.1 Identify need for and completion of Clinical Safety Case



- Does the product connect to a national system?
- Does the product influence the way Patients gain access to services?
- Does the product maintain part of the clinical record?
- Could the information presented mislead the healthcare professional if incorrect?
- If the product failed to present some information to a healthcare professional or become unavailable to a clinician/patient, could that impact care?

Answer Yes to any of these questions

This falls in scope the DCB0160 and would require a clinical safety case

⚠ It is important that this process is instigated prior to deployment of a system or product to ensure that it does not compromise patient safety

If you are not sure whether you need a CSC, email csoenquieries@nhs.net for advice.

4.2 Project Initiation

Clinical Risk Management activities will be applied to the deployment of all new safety-related health IT systems in the Trust. The Clinical Risk Management Team will be notified of the intention to deploy a new system through the IGG group as a project activity within the DTAC process. This is on the basis that the request has been approved via the project triage governance route.

The Clinical Risk Management Team will review the intended implementation and formulate a Clinical Risk Management Plan accordingly.

4.3 Project Deliverables

For each safety-related implementation the following deliverables will be produced:

1. Clinical Risk Management Plan (“the Plan”).
2. Hazard Log.
3. Clinical Safety Case Report (“CSCR”).

The deliverables will be kept up to date to reflect the scope of the live product. They will be subject to version control so that the status and most up to date version is clear and will be stored in the Clinical Risk Management File.

The deliverables will be aligned with the key project milestones and the intended delivery schedule set out in the Clinical Risk Management Plan.

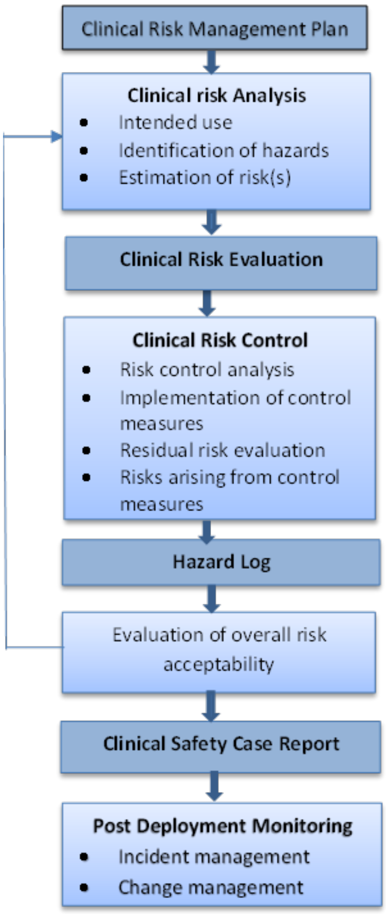
The deliverables will be consumed by the wider project team to input to and influence their own activities. When a deliverable is issued, the Clinical Safety Officer will notify the Project Manager of its existence.

4.4 Acceptance of clinical risk management deliverables

The deliverables will be approved by the CCIO and the Clinical Safety Officer.

4.5 Process overview

The following diagram sets out the overall Clinical Risk Management Process:


Clinical Risk Management Plan
Clinical risk Analysis
Intended use
Identification of hazards
Estimation of risk(s)
Clinical Risk Evaluation
Clinical Risk Control
Risk control analysis
Implementation of control measures
Residual risk evaluation
Risks arising from control measures
Hazard Log
Evaluation of overall risk acceptability
Clinical Safety Case Report
Post Deployment Monitoring
Incident management
Change management

The clinical risk management process is divided into a number of stages in Figure 1 of the DCB 0160 Standard. The steps within those stages are summarised in subsequent sections of this document as set out in the table below.

No	DCB 0160 Stage	Document section
1	Scope definition	7.2
2	Clinical Hazard/Risk identification	8.3
3	Clinical Risk estimation	8.4
4	Clinical risk evaluation	8.5
5	Control option analysis	8.6
6	Clinical risk-benefit analysis	8.7
7	Control measure implementation	8.8
8	Completeness evaluation and Delivery	9.4
9	Post-deployment monitoring	11
10	Modification	12

4.6 Examination of the Suppliers DCB0129 Materials

The supplier of the health IT system is required by NHS Digital to comply with DCB 0129 (Ref. 1). This will be enforced by including a suitable clause in the commercial contract with the supplier. The Trust will not contract with suppliers who do not comply with DCB 0129 or who cannot reasonably demonstrate that they have a strategy to comply within the timescales of the project.

The Clinical Safety Officer or Clinical Risk Manager will:

1. Request the Hazard Log and Clinical Safety Case Report from the supplier at the earliest opportunity after contract sign.
2. Review the supplier's DCB 0129 materials.
3. Document the findings in the DCB 0160 Clinical Safety Case Report.

5 Clinical Risk Management Planning

5.1 Clinical Risk Management Plan

Is a document which documents and schedules clinical risk management activities. It will be established at the beginning of a CSC and will include any variation of:

- The Intended Use of the product and the scope of the product under consideration.
- The scope of the planned risk management activities.
- The key stakeholders involved in the project.
- Verification activities.
- Activities related to change management and modification.
- Activities related to post deployment monitoring and incident management.
- Criteria for risk acceptability, based on the Trust's policy for determining acceptable risk (see Appendix 3).

The plan must be updated following any major change or incident, must be maintained throughout the life cycle of the system/product and must be reviewed yearly. The Plan will be approved by the Trust's Clinical Safety Sponsor and the Clinical Safety Officer.

5.2 The Scope of Clinical Risk Management

In the deployment, use, modification or decommissioning of a Health IT System, the scope of the Standard and this supporting guidance includes:

- All clinical functionality which could potentially cause harm to patients
- Operational use and potential misuse of the clinical functionality and it's potential to cause harm to patients
- Environmental considerations

- Organisational procedures

It may be determined that some areas of functionality do not impact clinical care or will only do so in a way that is indirect or incidental. In these cases, the implementation of the functionality will be deemed out of scope for further assessment and clinical risk

This standard applies to all HIT Systems including those that are also controlled by medical device regulations though the requirements are broadly consistent with the requirements of ISO 14971.

If the product includes third-party components (which may or may not originally be intended for health purposes) the Trust will include these components in the scope of the assessment if they have the potential to contribute to harm (see Section 10).

Functionality which does not impact clinical care or that does so in a way that is indirect, or incidental will be deemed out of scope for further assessment and clinical risk management. The reasoning and rationale behind this decision will be set out in the Plan.

In particular, the following categories of functionality will be considered as candidates for being excluded from the assessment:

- Functionality which is purely related to information governance, security or privacy of information.
- Functionality which would only lead to harm of staff members or users of the system rather than patients.
- Functionality which would only lead to patient harm very indirectly or under highly unusual circumstances.
- Functionality which would only be harmful if it was used maliciously.

Where functionality is deemed to be out of scope of the assessment the Trust will monitor this decision over time and undertake corrective actions should the functionality subsequently require clinical risk assessment.

6 Hazard Identification, Analysis and Evaluation

6.1 Purpose

The purpose of hazard identification and analysis is to identify and document known and foreseeable hazards to patients in both normal and fault conditions through the introduction of the Health IT system or product. The analysis will also establish the controls which are already present or need to be put in place to mitigate the risk to acceptable levels. This exercise culminates in the production of the Hazard Log.

The hazard log is a structured list of potential scenarios which could result in harm to an individual. For each hazard the impacts, causes and controls will be documented and the level of clinical risk for the hazard evaluated. The hazard log forms the data on which the rest of the assessment is based.

The Hazard Log will be authored by Clinical Safety Officer, reviewed by the Trust's Chief Clinical Information Officer and will be approved through the Trusts governance structure (see section 9.5).

6.2 Pre-Requisites

The following represent the input materials that will typically form the basis of hazard identification.

- Project Initiation Document.
- Product in a demonstration or test environment.
- Supplier's Hazard Log.
- As-is and To-be business processes.
- Product architecture.
- Any other design materials specific to the project.

The nature of these materials will vary from one project to the next and where there is significant variation, the approach will be set out in the corresponding Plan.

6.3 Hazard Identification

6.3.1 Hazard Identification Process (HAZID Workshop)

The Clinical Safety Officer and supporting personnel will review the input materials and conduct a Hazard Assessment during a HAZID workshop.

During the HAZID workshop users of the health IT system/product are invited where a demonstration of the system/product will initiate discussions about the use of the system/product so that potential hazards can be identified, and measures put in place to mitigate those hazards.

The workshop will identify Hazard causes, consequences and any existing controls. It will focus solely on 'clinical risk identification' which will later enable the assessment and evaluation of that risk, using the Clinical Safety Standards risk matrix (Appendix 3), to ensure appropriate controls are in place. This information will be incorporated into the hazard log and will be used to inform the Clinical Safety Case Report.

6.3.2 Attendees OF Hazard Workshop

Role	Responsibility
CSO	• Arrange and facilitate the workshop

The manufacturer	• Demonstrate the system and respond to queries
Project Manager/Team	• Identify potential risks and current controls
Information Governance	• Identify potential risks and current controls
Information Technology	• Identify potential risks and current controls
Clinician	• Identify potential risks and current controls
Service users/carer	• Identify potential risks and current controls

6.3.3 Analytical Method

A Structured What-If Technique (SWIFT) will be used to perform the hazards analysis. The Structured What-If Technique is a systematic method of hazard identification. The technique, carried out as a brainstorming activity, employs an analysis of potential deviations from the expected business process. Prior to the workshop, a series of guidewords (Appendix 5) will be sent to workshop participants. During the workshop, the clinical or system business process is broken down into individual tasks. The guidewords are tested against each task to generate ideas for hazards, causes and controls.

Additional guidewords may be generated in the course of a particular analysis. These ‘What If’ questions will be sent to the questions

Should the SWIFT technique be found to be inappropriate for the subject matter or additional rigour be required, the Clinical Safety Officer will consider employing other structured techniques such as Failure Modes and Effects Analysis (FMEA), Bow-Tie diagram or Fishbone diagram.

6.4 Risk Estimation

The potential severity of harm and the likelihood of that harm occurring must be estimated for each identified clinical hazard. A risk matrix, (Appendix 3) will be used to derive the clinical risk by combining the estimated severity of the risk and the likelihood of that risk occurring. Both initial and residual risk will be estimated, and the acceptability of each hazard will be tested against the criteria in Section 3.6. The Residual Clinical Risk associated with each hazard will collectively form the clinical risk profile and will be set out in the Safety Case.

On the basis that almost any hazard in health software could theoretically lead to death in extraordinary circumstances, in estimating clinical risk, a typical, real-world view of the severity and likelihood will be taken rather than considering exceptional or highly unusual cases. Hazards will be credible and realistic given the care setting into which the product will be deployed.

6.5 Risk Evaluation

Controls will be identified and documented for each cause of a hazard and the residual risk will be estimated and evaluated against the Risk Acceptability Criteria set out in Appendix A to determine whether or not it is acceptable.

The Initial Clinical Risk will be estimated taking into account only the typically employed environmental controls present in the target care setting. The Residual Clinical Risk will then take into account the additional controls employed to mitigate the clinical risk further.

Where the Residual Clinical Risk is found to be Acceptable or Tolerable, then no further action will be required other than to monitor the controls during live service. Should the level of clinical risk associated with a hazard change in the future, the clinical risk will be re-evaluated.

Where the Residual Clinical Risk is considered to be Undesirable or Unacceptable then options for further risk reduction will be explored through the process of control option analysis and a remediation plan may be put in place.

6.6 Control Option Analysis

Risk evaluation after the implementation of controls will reveal the degree of Residual Clinical Risk. If the Residual Clinical Risk remains Undesirable or Unacceptable, then further opportunities for risk mitigation will be sought. The Clinical Safety Officer will make recommendations as to whether the project can proceed based on the degree of Residual Clinical Risk.

Where a range of possible controls are available, those controls which are most likely to be effective in the context of the care setting will be prioritised. Any new controls introduced will be subject to an assessment to determine whether they could introduce hazards in their own right or could adversely impact the estimated clinical risk associated with existing hazards. In these circumstances, stakeholders may need to find a strategy which balances the risk, taking different controls and hazards into account.

6.7 Clinical Risk-Benefit Analysis

If the Residual Clinical Risk remains Unacceptable after all practicable measures to reduce the risk have been exhausted, this will be escalated to Top Management and the Trust will undertake a clinical risk-benefit analysis to establish whether the Health IT system is likely to provide more clinical benefit than harm. It is anticipated that this would only be undertaken in exceptional circumstances.

If the Residual Clinical Risk cannot be justified by the clinical benefits, the Clinical Safety Officer will recommend to Top Management that deployment of the product cannot proceed without further controls being implemented.

6.8 Control Measure Implementation

Prior to a system going live, controls will be validated to ensure that they have been correctly implemented. This will be achieved by tracing controls to evidence of their implementation.

The nature of that evidence will vary depending on the type of control but is likely to include configuration decisions, test scripts, training materials and standard operating policies. Where controls represent simple statements of fact about the product architecture or intended use, it may be possible to justify not tracing these to formal evidence.

The Trust will work with its users to evaluate the effectiveness of the controls put in place through testing and Post-Deployment Monitoring. The results of these activities will be recorded in the Clinical Safety Case Report.

6.9 Maintaining the Hazard Log

Hazard analysis will be undertaken continually throughout the life of the product until it is decommissioned, and the Hazard log must be maintained throughout the life cycle of the system/product, recording supporting information and evidence as it becomes available.

7 Safety Case Development

7.1 Purpose

The Clinical Safety Case is a structured argument which is supported by a body of relevant evidence that provides a compelling, comprehensible, and valid case that a system is safe for release. This brings together the data contained in the Hazard Log to form an argument which supports (or otherwise) the safety claims. This information is set out in a Clinical Safety Case Report.

7.2 Pre-Requisites

The following represent the input materials that will typically form the basis of the inputs to the Safety Case. Note that not all materials will necessarily be available for a particular project and any significant variation will be set out in the Clinical Risk Management Plan. It is noted that whilst the CSO will collate and review the materials below either the supplier or other members of the team and project will be the owners of each document.

- Supplier’s DCB 0129 materials.
- Project Plan.
- As-is and To-be Business Processes.
- Configuration Decision Log.
- Clinical Risk Management Plan.
- Hazard Log.
- Training Strategy, Training Needs Analysis and Training Logs.
- Test Strategy and Test Cases.
- Test Report.
- Product Training Materials.

- Standard Operating Procedures.
- Project Risk and Issue Log.
- Traceability between controls and evidence of implementation
- Trust DPIA
- Trust technical security assessment

7.3 Method

The Safety Case will be authored by Clinical Safety Officer according to the following steps:

1. Formulate the necessary pre-requisite materials.
2. Draft the report.
3. Present the report at the Digital and Data Management Meeting (D&DMM) and the Digital Performance and Assurance Group (DPAG)
4. Issue the approved report.

At a minimum, the Safety Case will include:

1. The scope and date of the risk assessment.
2. A description and identification of the product that was analysed (also taking into account the configuration of the release).
3. The identity of the Clinical Safety Officer.
4. The results of the clinical risk identification and estimation.
5. The methods employed for validating the presence of key controls.
6. Narrative summarising the common safety-related themes noted in the Hazard Log and notable hazards.
7. The residual risk profile and overall risk acceptability.
8. The results of the completeness review exercise.
9. Any notable recommendations for Top Management.

7.4 Completeness Evaluation and Delivery

Prior to deploying the system or release into the live environment, a review will be conducted to establish whether the safety assessment is complete. The review will consider:

- Whether all the activities set out in the Clinical Risk Management Plan have been completed.
- Whether all foreseeable hazards have been identified.
- Whether sufficient evidence has been gathered to verify the implementation of the controls set out in the Hazard Log.
- Whether an appropriate strategy is in place to monitor and manage clinical risk in live service.
- Whether all hazards have been mitigated to acceptable levels.
- Whether the requirements of the relevant Standards have been met.

The result of the review will be set out in the Safety Case.

7.5 Quality Assurance and Document Approval

This clinical safety case report and hazard log is to be discussed and approved at DDMM and for ratification at DPAG. This process is detailed within the Clinical Risk Management System. Where a suitable annex or addendum has been constructed, this will also be made available.

Residual risks may have follow-on actions following project closure and require monitoring. Those that remain will be logged on the Trust's risk management system Datix and a risk manager and owner assigned – see Operational Risk Policy for the Trust approach to managing risk.

Following Approval at DPAG, the Clinical Safety Case will be maintained throughout the life of the product until decommissioning. The clinical safety case report and the hazard log will be stored on the T:Drive; (T: clinical safety case reports) and become the responsibility of the clinical owner as agreed with the clinical owner and documented in the clinical safety case report These documents will be reviewed and updated as required. If no updates are made to the Safety Case during a period of 12 months, a routine update of the document will be performed.

8 Third Party Components

Many HIT Systems are reliant on the use of third-party products. A third-party component is a product that is produced by another organisation and not by the Health IT System manufacturer. Such products can introduce a variety of risks particularly where a HIT System is reliant upon it or interoperates with it. Risks may also arise when software updates or patches are applied to these products. Such products are, however, unlikely to have been risk assessed for health applications by the original supplier.

Where third party products and health software interact, the Trust will need to ensure that its own clinical risk management process takes this into account.

Suppliers who are compliant with DCB0129 are required as part of their clinical risk assessment activities to consider any third-party product incorporated into their Health IT System. The Trust should:

- confirm that any third-party product used has been considered in the Supplier's safety documentation
- review the extent of the Supplier's contractual responsibilities for risk control both for original supply and for updates and patches which may be passed to the Trust through them. In this situation there should be a requirement for the Supplier to maintain the associated Clinical Safety Case Report and provide updates highlighting changes in the level of risk

A summary of the third-party component assessment will be documented in the Safety Case if the Trust introduces such components.

9 Post Deployment Monitoring and Incident Management

The Trust acknowledges that the risk profile of the product can change as more is learnt about the characteristics of the system/technical infrastructure, and its implementation, the effectiveness of controls and the way in which it is operated. In live service, the system will be monitored by the clinical owner to ensure that the conclusions set out in the Safety Case remain valid and that the scope of the assessment remains in line with that of the live product. Safety incidents will be logged and subject to assessment. Where appropriate, the clinical owner will contact the CSO who will re-evaluate the risk, and update and re-issue the contents of the clinical risk management file as agreed in the clinical safety case report.

9.1 Approach

9.1.1 Service Desk

The Trust operates a service desk system which enables users to log calls for review and action. Calls are logged in an electronic tool called Alemba Service Management. The Service Desk team will have access to the clinical safety log (appendix 6) which lists all active clinical safety cases and identifies clinical owners and CSO lead.

9.1.2 Clinical Incident Reporting

In addition to the service desk, the Trust operates a clinical incident reporting system in the form of Datix. A Datix form must be completed and submitted within 24 hours of the incident identifying whether it is an actual or potential serious incident. During the subsequent investigation, if a system or infrastructure is identified as being a contributing factor, the clinical owner will be notified. Datix team will have access to the clinical safety log which lists all active clinical safety cases and identifies clinical owners and CSO lead.

9.2 Escalation

Following identification of a potential safety incident, the clinical owner or IAA will contact the Clinical Safety Officer.

9.3 Assessment

The CSO, in conjunction with subject matter experts (including systems and technical experts), will review the issue. The level of Clinical Risk will be determined using the methods and criteria set out in the Clinical Risk Management Plan and Clinical Safety Case Report for the associated system. Assessment of the issue may involve discussion with the reporting user and other potentially impacted users.

Where warranted, the Clinical Safety Officer will formulate a brief Clinical Safety Issue Assessment. The assessment will include a description of the issue, the potential impact on the patient, the assessed level of Clinical Risk and any potential controls/mitigations. The document will serve to inform internal personnel to guide timely resolution of the issue. The assessment may be communicated to the supplier where appropriate and will be retained in the Clinical Risk Management File.

The Trust will where necessary, escalate the issue to the supplier according to the contractual arrangements in place. This escalation will include the Trust's view on the level of Clinical Risk. Where appropriate, the Trust's Clinical Safety Officer will request engagement of the supplier's Clinical Safety Officer to assist in the issue's remediation.

9.4 Update Safety Documentation

A log of the safety incident including its nature, event history and resolution will be maintained in the Trust's Clinical Risk Management File stored in the Clinical Safety Case Report File in the T:Drive, by the Clinical Safety Officer and will constitute the Safety Incident Management Log. The log will be reviewed at least monthly by the CSO and CCIO to assess progress, completeness and data quality.

The CSO will review the Hazard Log and determine whether the issue:

- Represents a new Hazard or Cause previously not identified
- Changes the level of Clinical Risk associated with an existing Hazard
- Demonstrates that an existing control is less effective than had previously been assumed

If the issue materially changes the Clinical Risk associated with the implementation and use of the system or infrastructure challenges assumptions made in undertaking the risk assessment, it may be appropriate to update and re-issue the Hazard Log and Clinical Safety Case Report for the system.

10 Modification and Change Management

From time to time an aspect of the system or infrastructure, its implementation or configuration may change. These changes will be subject to a clinical safety assessment to determine whether there is a change in the level of clinical risk and/or a need to update the deliverables.

The Clinical Safety Officer will monitor change via liaison with the appropriate owners, and through attendance at CAG, and undertake an assessment on those changes which have the potential to impact clinical care. The approach to this assessment will use the same methodology to that of the initial assessment and the extent will be commensurate with the scale of the changes and potential clinical risk.

10.1 Detecting Change

10.1.1 Changes Made by the Supplier

The manufacturer will inform the IAO, IAA, Technical Owner or system owner of a planned change to the system.

The Technical Owner will test those changes, identify any potential hazards and liaise with the CSO prior to CAG, to provide evidence of the outcomes of the testing and to establish whether the changes warrant a review of the CSC. The CSC and Hazard Log will be available to the technical owner via the clinical safety case reports file on the T:Drive.

10.1.2 Changes made by the Trust

Periodically the Trust may decide to make a change to configuration or ask the supplier to modify design. In these circumstances, the Trust will raise a Request for Change and follow the CAG (see section 5).

10.2 Impacting the Change

The Clinical Safety Officer will work with the project team to assess the change and determine the impact on the current Hazard Log and Safety Case for the product. This will include a re-evaluation of the overall clinical risk and its acceptability.

Where appropriate, the safety materials will be updated, or a suitable annex constructed. The techniques employed will be as set out in previous sections of this document.

10.3 Decommissioning

The Trust acknowledges that the decommissioning of a health IT system can be a safety-related activity especially where this includes a data migration process. Where the Trust undertakes a decommissioning exercise, this will be subject to clinical risk management. The assessment methodology and evaluation criteria will be the same as that set out above and the decommissioning activity will be overseen by the Clinical Safety Officer.

11 Clinical Risk Management File

All materials created during the initial and ongoing assessments will be maintained in the CSO Teams Channel. This will constitute the clinical risk management file. The file will be created at the start of a project and be maintained for the lifetime of the implementation. The Trust's document management system is secure and backed up on a regular basis.

The Clinical Risk Management File shall include (but not be limited to):

- The Clinical Risk Management Plan.
- The Hazard Log.
- The Clinical Safety Case Report.

The deliverables will reference several other artefacts including those which comprise the evidence on which the safety conclusions are drawn. These materials will either be kept in the clinical risk management file or their location referenced from within the file.

11.1 Review Clinical Safety Case

The CSCR and Hazard Log will be reviewed following any manufacturers change, internal change, any serious incident or as a minimum, yearly. This will be assured by a CSC log (appendix 6) saved in the Clinical Safety file on the T:Drive that will be maintained by the CSO and that details information pertaining to the clinical safety case including the clinical owner, approval and review dates.

12 Terms and definitions

The following terms apply. Additional terms are set out in Standard DCB 0160 (Ref. 3).

Term	Definition
CSO	Clinical Safety Officer
Clinical Safety Sponsor	means the person who is accountable for clinical risk management and patient safety.
Trust	Tees, Esk and Wear Valleys NHS Foundation Trust
Deliverables	means the Clinical Risk Management Plan, Hazard Log and Clinical Safety Case Report defined in DCB 0160 (Ref. 3).
DPAG	Digital Performance and Assurance Group
DPB	Digital Programme Board
DDMM	Digital and Data Management Meeting
DTAC	Digital Technology Assessment Criteria
Product	means an application, system or service used to support the delivery of clinical care.
Reasonably foreseeable misuse	means use by the operator in a way not intended by the manufacturer but which can result from readily predictable human behaviour.
Stakeholders	means those individuals with a professional interest in the development or implementation of a product.
Supplier	means the manufacturer of a health IT system which the Trust is implementing, has implemented or is planning to implement
Top Management	means person or group of people who direct(s) and control(s) the Health Organisation and has overall accountability for a Health IT System. The Trust has assigned the Chief Clinical Information Officer (CCIO) and Deputy Chief Information Officer (Deputy CIO) to act in the capacity of Top Management.

13 How this procedure will be implemented

- This procedure will be published on the Trust’s intranet and external website.

- Line managers will disseminate this procedure to all Trust employees through a line management briefing.

13.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
Top Management	e-learning	https://www.e-lfh.org.uk/programmes/essentials-of-digital-clinical-safety/	Once only
IT developers	e-learning	https://www.e-lfh.org.uk/programmes/essentials-of-digital-clinical-safety/	Once only
Project managers	e-learning	https://www.e-lfh.org.uk/programmes/essentials-of-digital-clinical-safety/	Once only
CSO's	e-learning and face to face Specific training (NHSD)	Foundation course Refresher training	Once only Minimum of 2 yearly

The e-learning is suitable for clinical and non-clinical staff. All staff working within the Trust will benefit from completing this training.

14 How the implementation of this procedure will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Digital Technology Assessment Criteria (DTAC)	Monthly	DPB/DDMM/DPAG
2	Independent audit	At request of Top Management	DPB/DDMM/DPAG

15 References

Ref	Title	Description
1	DCB 0129 Standard Specification	DCB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems – Specification. 02/05/18. Version 4.2.

2	Health and Social Care Act 2012	Health and Social Care Act 2012. https://www.legislation.gov.uk/ukpga/2012/7/contents
3	DCB 0160 Standard Specification	DCB 0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems – Specification. 02/05/18. Version 3.2.
4	Health and Safety Executive	https://www.hse.gov.uk/
5	DCB 0160 Implementation Guidance	DCB 0160 Clinical Risk Management: its Application in the Manufacture of Health IT Systems – Implementation Guidance. 02/05/18. Version 4.2.
6	DCB0160 Compliance assessment	DCB 0160 Compliance assessment v4.0. NPFIT-FNT-TO-TOCLNSA-1430.04. 19.07.2018.
7	IT-0032-004	Digital and Data Services Change Advisory Group Procedure

16 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	28 February 2023
Next review date	28 February 2026
This document replaces	n/a - new document
This document was approved by	IGG
This document was approved	21 December 2022
This document was approved by	DDMM
This document was approved	28 February 2023
An equality analysis was completed on this policy on	21 December 2022
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1	28 Feb 2023	New Procedure	approved

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	**Scope**
Name of service area/directorate/department	Clinical Safety Team - Digital and Data Services
Title	Clinical Risk Management Procedure
Type	Procedure/guidance
Geographical area covered	Trust-wide
Aims and objectives	For all health IT products and Systems that have the potential to result in patient harm: this procedure will ensure the Trust: • Complies with the requirements of the Data Coordination Board Safety Standard DCB0160 • Meets its legal obligations in carrying out a risk assessment of the impact of the Health IT product or system on patient safety • Identifies any potential risks to patient safety and mitigates those risks as low as is reasonably practicable • Ensures the rights and freedoms of individuals are not compromised • systems are reflective of the diverse patient population who access services to enable staff to capture accurate patients' demographic data
Start date of Equality Analysis Screening	09/12/2022
End date of Equality Analysis Screening	21/12/2022

Section 2	**Impacts**
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Patients, staff, carers and families, external stakeholders

Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO**
Describe any negative impacts	None
Describe any positive impacts	Implementing this procedure will provide assurance that Health IT products and services, prior to deployment have undergone stringent risk management process and are effective and safe for clinical use

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	DCB0160 Clinical Risk Management. It’s application in deployment and use of Health IT safety standard

Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	No
If you answered Yes above, describe the engagement and involvement that has taken place	
If you answered No above, describe future plans that you may have to engage and involve people from different groups	We are liaising with the Equality, Diversity and Human Rights team, who will review our procedure prior to presenting at governance groups, to ensure that are processes are inclusive and accessible

Section 4	**Training needs**
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	**Yes / No / Not applicable**	**Comments**
1.	**Title**		
	Is the title clear and unambiguous?	Y	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Y	
2.	**Rationale**		
	Are reasons for development of the document stated?	Y	
3.	**Development Process**		
	Are people involved in the development identified?	Y	
	Has relevant expertise has been sought/used?	Y	
	Is there evidence of consultation with stakeholders and users?	Y	
	Have any related documents or documents that are impacted by this change been identified and updated?	Y	
4.	**Content**		
	Is the objective of the document clear?	Y	
	Is the target population clear and unambiguous?	Y	
	Are the intended outcomes described?	Y	
	Are the statements clear and unambiguous?	Y	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Y	
	Are key references cited?	Y	
	Are supporting documents referenced?	Y	
6.	**Training**		
	Have training needs been considered?	Y	
	Are training needs included in the document?	Y	

	Title of document being reviewed:	Yes / No / Not applicable	Comments
7.	**Implementation and monitoring**		
	Does the document identify how it will be implemented and monitored?	Y	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Y	
	Have Equality and Diversity reviewed and approved the equality analysis?	y	31 Jan 2023
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Y	
10.	**Publication**		
	Has the policy been reviewed for harm?	Y	
	Does the document identify whether it is private or public?	y	Public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	

Appendix 3 – Risk Classification Matrix

Clinical Risk Management Risk Matrix

Likelihood	Very High	3	4	4	5	5
	High	2	3	3	4	5
	Medium	2	2	3	3	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3
		Minor	Significant	Considerable	Major	Catastrophic
		Consequence				

Risk Matrix key - Severity

5	Unacceptable level of risk. Mandatory elimination or control to reduce risk to an acceptable level
4	
3	Undesirable level of risk Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical.
2	Acceptable where cost of further reduction outweighs benefits gained.
1	Acceptable, no further action required

Hazard likelihood definitions

Likelihood Category	Interpretation
Very high	Certain or almost certain; highly likely to occur
High	Not certain but very possible; reasonably expected to occur in the majority of cases
Medium	Possible
Low	Could occur but in the great majority of occasions will not

Very low	Negligible or nearly negligible possibility of occurring

Hazard Consequence definitions

Consequence Classification	Interpretation	Number of Patients Affected
Catastrophic	Death	Multiple
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Multiple
Major	Death	Single
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Single
	Severe injury or severe incapacity from which recovery is expected in the short term	Multiple
	Severe psychological trauma	Multiple
Considerable	Severe injury or severe incapacity from which recovery is expected in the short term	Single
	Severe psychological trauma	Single
	Minor injury or injuries from which recovery is not expected in the short term.	Multiple
	Significant psychological trauma.	Multiple
Significant	Minor injury or injuries from which recovery is not expected in the short term.	Single
	Significant psychological trauma	Single
	Minor injury from which recovery is expected in the short term	Multiple
	Minor psychological upset; inconvenience	Multiple
Minor	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible severity	Single

Appendix 4 – Clinical Safety Case Deliverables Templates

Clinical Safety Case Deliverables Templates used by CSO(s):-

clinical_safety_hazard_log_template.xlsx

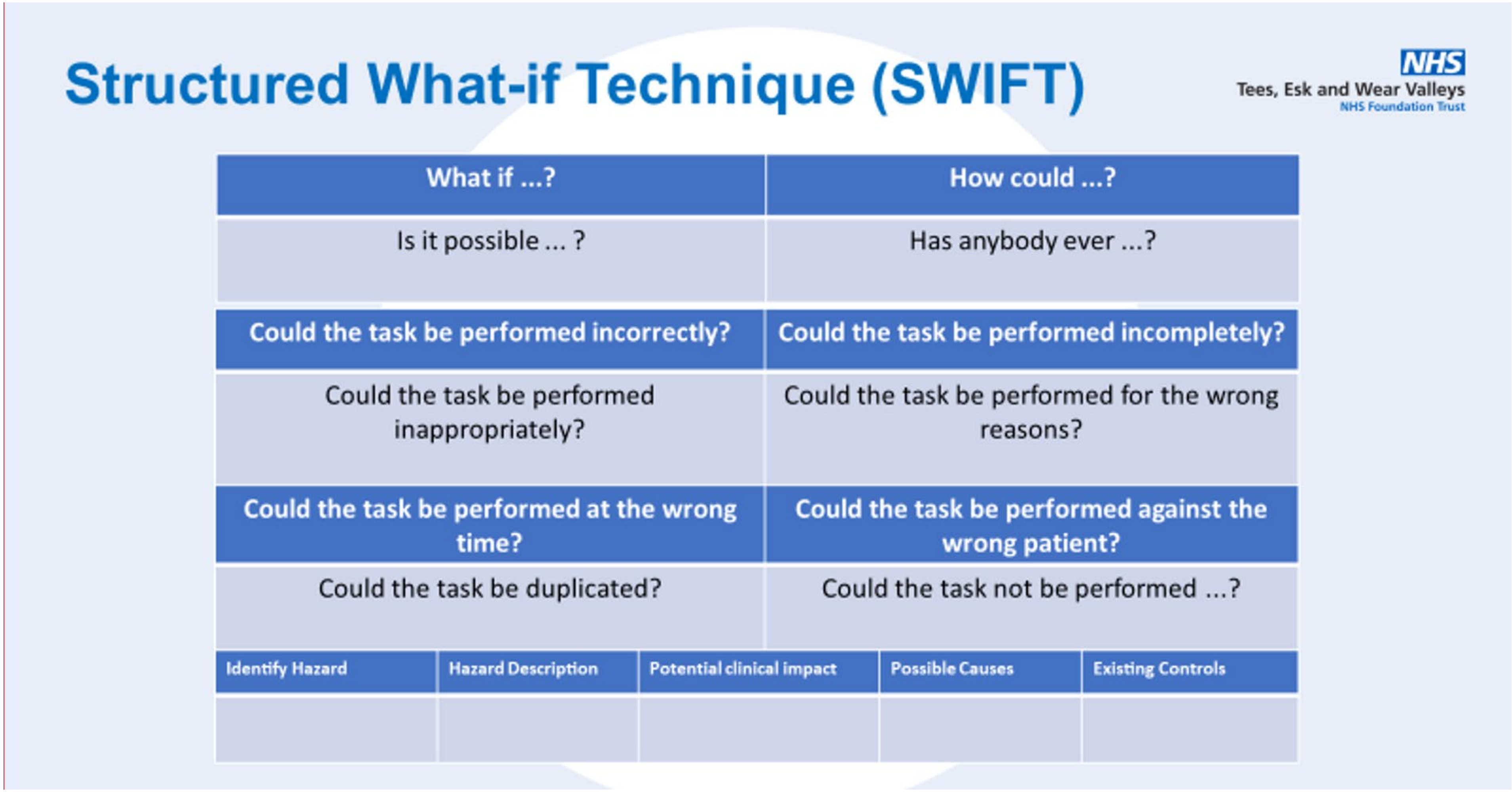
nhs_digital_clinical_risk_management_plan_template.docx

nhs_digital_clinical_safety_case_report_template.docx

These may be adapted from source documentation and guidance at NHS Digital: Clinical Safety documentation - NHS Digital

(Template listed above as accessed of 4th January 2023. Note as per NHS Digital these templates may be adapted as required by CSO(s) as required.)

Appendix 5 – Structured ‘What If’ Technique SWIFT



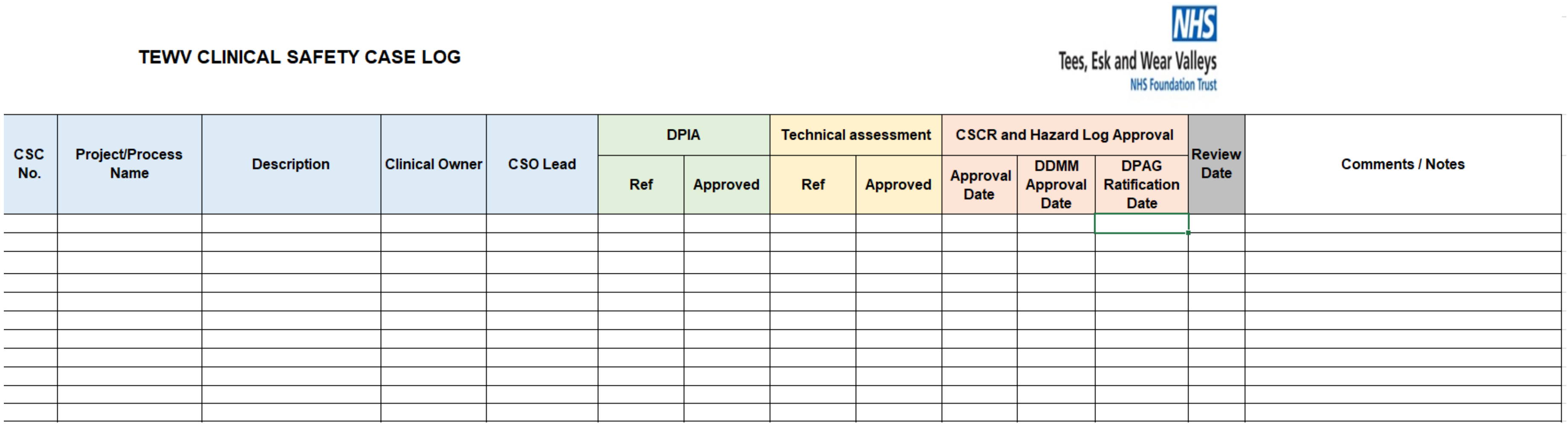
Structured What-if Technique (SWIFT)

NHS
Tees, Esk and Wear Valleys
NHS Foundation Trust

What if ...?	How could ...?
Is it possible ... ?	Has anybody ever ...?
Could the task be performed incorrectly?	**Could the task be performed incompletely?**
Could the task be performed inappropriately?	Could the task be performed for the wrong reasons?
Could the task be performed at the wrong time?	**Could the task be performed against the wrong patient?**
Could the task be duplicated?	Could the task not be performed ...?

Identify Hazard	Hazard Description	Potential clinical impact	Possible Causes	Existing Controls

Appendix 6 - Clinical safety Log



TEWV CLINICAL SAFETY CASE LOG

NHS
Tees, Esk and Wear Valleys
NHS Foundation Trust

CSC No.	Project/Process Name	Description	Clinical Owner	CSO Lead	DPIA		Technical assessment		CSCR and Hazard Log Approval			Review Date	Comments / Notes
					Ref	Approved	Ref	Approved	Approval Date	DDMM Approval Date	DPAG Ratification Date		

(Template for Clinical Safety Log as accessed of 4th January 2023. Note the log is a dynamic document and maybe amended by the CSO(s) as required.)

Clinical Safety Log is available via Trustwide Shares Drive T:\Clinical Safety