NHS
Yorkshire
Ambulance Service
NHS Trust

Health IT Clinical Safety Policy

Document Author: Deputy Medical Director

Approved: July 2024

Document Reference	PO – Health IT Clinical Safety Policy – July 2027
Version	V: 3.0
Responsible Director (title)	Executive Medical Director
Document Author (title)	Deputy Medical Director
Approved by	Clinical Governance Group
Date Approved	July 2024
Review Date	July 2027
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal and Public Website

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
0.1		Deputy Medical Director	D	
0.2	11/2/2020	Deputy Medical Director	D	Update following feedback from the Digital Management Group and the AD of Performance Assurance and Risk
1.0	11/3/2020	Deputy Medical Director	A	Approved at TMG
1.1	3/5/2022	Acting Medical Director	D	2 yearly review
1.2	May 2022	Deputy Medical Director	D	Approved at CGG
2.0	July 2022	Risk Team	A	Approved at TMG
2.1	July 2024	Deputy Medical Director	D	Overall review. Updated process and responsibilities.
2.2	July 2024	Risk Team	D	Moved on to new Trust template.
3.0	August 2024	Risk Team	A	Policy approved within July 2024 Clinical Governance Group
A = Approved D = Draft				
Document Author = Stephen Dykes, Deputy Medical Director				
Associated Documentation: Risk Management Policy Risk Management and Assurance Strategic Framework Clinical Risk Management Plan Hazard Log Template Clinical Safety Case Template				

Staff Summary

This Health IT Clinical Safety Policy outlines the processes to be followed to ensure that all health IT used to support care within the Yorkshire Ambulance Service NHS Trust (YAS) is developed, implemented and used in as safe manner
DCB0129 sets clinical risk management requirements for manufacturers of Health IT systems and DCB0160 establishes the framework within which clinical risks associated with the deployment and implementation of a new or modified Health IT system is properly managed.
A Health IT system is one that can be used to support or influence the administration of healthcare to a patient. If clarification is required of whether any system falls within scope of this policy this should be raised with the nominated Clinical Safety Officer (CSO) for clarification.
In the deployment of a Health IT System, clinical risk management is an essential activity in ensuring the system does not compromise patient safety.
Introduction of any Health IT system, update or change will be managed through the existing change control process and will require a clinical safety case to be completed by the Clinical Safety Officer
In the procurement of a Health IT System YAS must ensure that the Manufacturer and the Health IT System complies with DCB0129

1.0 Introduction

1.1 This Health IT Clinical Safety Policy outlines the processes to be followed to ensure that all health IT used to support care within the Yorkshire Ambulance Service NHS Trust (YAS) is developed, implemented and used in as safe manner.

1.2 This policy provides a framework that promotes the effective risk management of health IT and addresses the requirements of DCB 0129 and DCB 0160 as approved by the Department of Health and Social Case under section 250 of the Health and Social Care Act 2012

1.3 In line with current DCB practice, each standard comprises:

- a specification, which defines the requirements and conformance criteria to be met by the user of the standard - how these requirements are met is the responsibility of the user
- implementation guidance, which provides an interpretation of the requirements and, where appropriate, defines possible approaches to achieving them

1.4 DCB0129 sets clinical risk management requirements for manufacturers of Health IT systems and DCB0160 establishes the framework within which clinical risks associated with the deployment and implementation of a new or modified Health IT system is properly managed.

2.0 Purpose/Scope

2.1 The aim of the policy is to ensure that all of the organisational staff involved with the development, implementation and use of health IT systems are aware of the activities that are required to be undertaken to ensure patient safety is improved rather than compromised from the introduction of health IT systems.

2.2 This policy applies primarily to critical health IT systems and significant updates or upgrades that have a substantial impact on patient safety. For existing systems, a tailored approach is adopted to ensure the efficient and effective use of resources while maintaining high standards of patient safety.

2.3 For existing health IT systems, the Trust will develop a baseline safety case that summarises the safety history and current safety status of each system. This baseline safety case will serve as a foundational document for ongoing safety management.

2.4 A preliminary risk assessment will be conducted for existing systems to identify and prioritise potential hazards based on their impact on patient safety. This assessment will guide the focus of the streamlined risk assessment process.

2.5 The Trust will implement a streamlined risk assessment process for existing systems, focusing on high-priority risks identified during the preliminary assessment. This approach ensures that significant risks are managed effectively without necessitating a full risk assessment for every system.

2.6 Continuous monitoring and periodic reviews will be conducted to ensure the ongoing safety of existing systems. This includes monitoring for any emerging risks and updating the baseline safety case as necessary to reflect changes in the system's safety status.

2.7 Minor updates, local customisations, and specific configurations of existing health IT systems will follow a simplified risk assessment process. These changes will remain subject to the Trust's change control policy.

2.8 The specific approach employed for each health IT system shall be delineated in an individual clinical risk management plan. Such plans may be maintained as separate documents or integrated within the overarching project plans, and shall, in all cases, be subject to oversight by the Clinical Safety Officer.

2.9 A Health IT system is one that can be used to support or influence the administration of healthcare to a patient. If clarification is required of whether any system falls within scope of this policy this should be raised with the nominated Clinical Safety Officer (CSO) for clarification. This nominated person provides clinical and organisational leadership on health IT Patient Safety on behalf of the Organisation.

2.10 The Clinical Safety Officer will oversee the risk management process for existing systems, ensuring that all high-priority risks are addressed, and that the overall safety of these systems is maintained through ongoing monitoring and periodic reviews.

3.0 Process

3.1 Health IT Clinical Risk Management (CRM) Governance Arrangements

3.1.1 In the deployment of a Health IT System, clinical risk management is an essential activity in ensuring the system does not compromise patient safety.

3.1.2 General requirements for effective clinical risk management are:

- a complete understanding of the Health IT System to be deployed and used
- an appropriate awareness of clinical risk management
- an awareness of how clinical risk management aligns with any wider governance processes
- a fully defined clinical risk assessment process which incorporates the application of recognised and rigorous methodologies
- a risk assessment to be carried out completely and competently
- the implementation of any required clinical risk control measures
- any residual clinical risks are appropriately documented
- appropriate lifecycle management is in place.

3.1.3 The responsibility for Health IT clinical safety resides with the Chief Clinical Information Officer (CCIO)

3.1.4 Introduction of any Health IT system, update or change will be managed through the existing change control process and will require a clinical safety case to be completed by the Clinical Safety Officer.

3.1.5 Organisational management of Health IT-related risks are as per the existing management arrangements through the Clinical Governance Group providing assurance at the Quality Committee. Any health IT related risks with a sufficiently high rating will be entered into the corporate risk register and moderated through the Risk and Assurance Group in line with the Trust's Risk Management and Assurance Strategic Framework

3.2 **Procurement**

3.2.1 In the procurement of a Health IT System YAS must ensure that the Manufacturer and the Health IT System complies with DCB0129. Risks to patient safety can be considerably reduced through intelligent procurement. A formal framework for procurement should therefore be an integral component of clinical risk management. Yorkshire Ambulance Service should:

- ensure that the Manufacturer has assessed the clinical risks associated with the Health IT System to be deployed in compliance with DCB0129
- request that the Manufacturer's safety documentation is provided as this will form a key input into the Health Organisation's own clinical risk management activities
- request that a Manufacturer agrees to implement new or updated standards that are applicable to the Health IT System that is to be deployed.

3.2.2 YAS may procure and deploy a Health IT System from a Manufacturer which is not DCB0129 compliant. In this situation the Health IT System may not be supported by accompanying clinical risk management or safety documentation which may result in:

- an increased risk to patient safety
- YAS having to produce the safety material that should have been provided by the Manufacturer.

3.2.3 YAS, as a result of conducting its own clinical risk assessment, may decide that the benefits of deploying a Health IT System which does not satisfy the requirements of DCB0129 outweigh any associated risk to patient safety. The deployment of a non DCB0129 compliant Health IT System, or any change to an existing health IT system that results in that system being non DCB0129 compliant, would have to be authorised by Top Management under requirement 2.2.2 of this standard.

3.3 Personnel

3.3.1 Roles and responsibilities for the following clinical safety related positions are defined in the appendix.

- Chief Clinical Information Officer
- Chief Digital Information Officer
- Clinical Safety Officer

3.4 **Health IT Clinical Risk Management Deliverables**

- **Clinical Risk Management File**
  YAS will establish a Clinical Risk Management File (CRMF) for each safety related health

IT system. The purpose of the CRMF is to provide a central repository where all safety related information pertaining to the healthcare IT system is stored and controlled.

- **Clinical Risk Management Plan**
  YAS will establish a Clinical Risk Management Plan (CRMP) for each safety related health IT system. The purpose of the CRMP is to identify the clinical risk management activities that are to be undertaken and the phasing of these activities in the project lifecycle. The CRMP will also identify the resources required to discharge these clinical risk management activities.

- **Hazard Log**
  YAS will establish and maintain a Hazard Log (HL) for each safety related healthcare IT system. The HL will be made available within the CRMF. The purpose of the HL is to manage the effective resolution and communication of hazard risk within The Organisation.

- **Clinical Safety Case**
  YAS will establish and develop a Clinical Safety Case (CSC) for each safety related Health IT system.

- **Clinical Safety Case Report**
  YAS will issue a Clinical Safety Case Report (CSCR) for each safety related healthcare IT system. The CSCR will be issued to support initial deployment and will be updated during the lifecycle of the healthcare IT system should the safety characteristics change. The HL will be made available within the CRMF.

3.5 **Health IT Clinical Risk Management Activities**

- **Hazard Identification**
  YAS will conduct hazard identification workshops to identify potential hazards associated with the deployment and use of a Health IT system. The CSO will be responsible for facilitating such workshops and ensuring attendance from appropriate representatives. Typically, representatives from the following domains will be required: IT, Clinical, Operations. The workshops will have minutes taken and a copy stored in the CRMF. If a Health IT solution is deemed not to be safety related then this decision will be formally recorded. Where any third-party components are used to support the healthcare IT system then they will be considered in the scope of the hazard identification activities and subsequent risk assessment. Where none are used a positive declaration to this effect will be recorded in the minutes. All identified hazards will be recorded in the Hazard Log.

- **Risk Assessment**
  YAS will conduct health IT system risk assessment in accordance with the Risk Management Policy. The Hazard Log will be updated to capture the risk assessment.

- **Risk Evaluation**
  YAS will conduct healthcare IT system risk evaluation in accordance with the Risk Management Policy. The Hazard Log will be updated to capture the risk assessment.

- **Risk Control**
  Where the initial risk evaluation is deemed unacceptable, further risk controls will be required. The Organisation will manage healthcare IT system risk in accordance with the Risk Management Policy
  Details of the risk control measure and evidence of effective implementation will be captured in the HL.

- **Deployment and Ongoing Maintenance**
  To support clinical safety activities undertaken during any deployment phases of a project or programme of work, the Change Control Process will be required to form a part of the overall approval process.

- **Incident Management**
  Clinical Risk Management activities within YAS and the healthcare IT programmes and services offered are completed within the corporate risk management strategy. Clinical safety related incidents are dealt with in a similar manner as other incident within the organisational such as financial, reputational, technical and other service impacting categories.

4.0 Training expectations for staff

4.1 Clinical Safety Competence and Training

4.1.1 All of the staff identified in the organisation chart, shall be sufficiently competent for the roles and task which they are asked to undertake. Where an individual does not have sufficient experience or knowledge then that person shall be monitored, and his/her work reviewed, by someone who has the necessary competence. Such supervision shall prevail until it is judged that the individual has amassed the necessary experience to undertake such tasks unsupervised.

4.1.2 In assessing competency, the different functional roles required to fully discharge the obligations of the Clinical Risk Management System, and the necessary skills and knowledge needed for each, shall be considered. Primary functional roles may include:

- Conducting discrete safety analyses (for example, a HAZOP or FFA) or defining the Hazard Risk Indicators for a particular project.

- Making a valid judgement on the safety tasks, activities and techniques required for a given Health Software Product in order to justify the comprehensiveness and completeness of the safety assessment and produce the safety argument with supporting evidence.

- Assurance of safety assessments and healthcare IT software products. Performance of safety techniques and development of the safety argument for a particular healthcare IT software product must be independent to any assurance activities for the same.

- Improving and refining the overall Clinical Risk Management System, for example, audit, process change, quality.

- Ownership and leadership, for example, ultimate safety accountability, culture change, influencing and strategic direction.

4.1.3 The first test in establishing competency shall be at the interview stage where potential staff shall be assessed against the above representative roles and agreed job descriptions. Thereafter, competence shall be monitored through the organisation's established appraisal scheme. Any perceived deficiencies identified during the course of the work or at the appraised stage, especially during probation, shall be addressed immediately, for example, through the assignment of a competent supervisor or the provision of suitable training.

4.1.4 All registered clinicians involved in safety roles shall, as a minimum, have completed an accredited training course.

4.2 **Training**

4.2.1 As part of the employment process and thereafter through the appraisal scheme, clinical safety personnel will undergo suitable training to develop, maintain or enhance their competency level. Such training can comprise:

- 'on the job' training conducted under supervision
- Internal training courses
- Approved external training courses.

4.2.2 All registered clinicians involved in clinical safety roles shall, as a minimum, have completed an accredited training course.

4.2.3 Completion of any safety training shall be recorded by the individual on the annual appraisal form.

5.0 Implementation Plan

5.1 The latest approved version of this Policy will be posted on the Trust Intranet site for all members of staff to view. Clinical Safety Officer sign off is a required part of the IT change request form.

6.0 Monitoring compliance with this Policy

6.1 Audits

6.1.2 Overview - Audits shall be undertaken to ensure that projects are adhering to the defined safety requirements. Such audits will focus on the **Clinical Safety Team** and **third-party** suppliers**.**

6.2 Internal Safety Audits

6.2.1 YAS shall undertake regular internal safety audits to ensure that projects undertaken within the organisation are compliant with this Clinical Risk Management System. These audits shall be conducted and recorded in accordance with the internal quality management procedure.

6.2.2 The scope of an internal safety audit will be the formal Clinical Risk Management System and the Organisation's documentation supporting this document.

6.3 Supplier Audits

6.3.1 YAS shall undertake regular third-party supplier audits, as a minimum annually, to ensure compliance with their Clinical Risk Management System. The audit shall focus on the Clinical Risk Management System, the evidence which demonstrates its effective operation and any issues arising from the deployment of the healthcare IT products and services. The basis for the audit shall be DCB 0129.

6.3.2 Supplier audits shall be conducted in accordance with the External Safety Audit Procedure.

7.0 References

7.1 DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems

7.2 DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems

8.0 Appendices

8.1 This documents includes the following appendices:

Appendix A – Definitions

Appendix B – Roles and Responsibilities

Appendix A - Definitions

Term	Definition
Clinical Safety Officer	Person in the organisation responsible for ensuring the safety of a Health IT System in that organisation through the application of clinical risk management.
Clinical risk	Combination of the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk analysis	Systematic use of available information to identify and estimate a risk.
Clinical risk control	Process in which decisions are made and measures implemented by which clinical risks are reduced to, or maintained within, specified levels.
Clinical risk estimation	Process used to assign values to the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk evaluation	Process of comparing a clinical risk against given risk criteria to determine the acceptability of the clinical risk.
Clinical risk management	Systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling clinical risk.
Clinical Risk Management File	Repository of all records and other documents that are produced by the clinical risk management process.
Clinical Risk Management Plan	A plan which documents how the Manufacturer will conduct clinical risk management of a Health IT System.
Clinical Risk Management Process	A set of interrelated or interacting activities, defined by the Manufacturer, to meet the requirements of this standard with the objective of ensuring clinical safety in respect to the development and modification of a Health IT System.
Clinical safety	Freedom from unacceptable clinical risk to patients.
Clinical Safety Case	Accumulation and organisation of product and business process documentation and supporting evidence, through the lifecycle of a Health IT System.
Clinical Safety Case Report	A report that presents the arguments and supporting evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment at a defined point in a Health IT System’s lifecycle.
Harm	Death, physical injury, psychological trauma and/or damage to the health or well-being of a patient.
Hazard	Potential source of harm to a patient.

Hazard Log	A mechanism for recording and communicating the on-going identification and resolution of hazards associated with a Health IT System.
Health Organisation	Organisation within which a Health IT System is deployed or used for a healthcare purpose.
Health IT System	Product used to provide electronic information for health or social care purposes. The product may be hardware, software or a combination.
Initial clinical risk	The clinical risk derived during clinical risk estimation taking into consideration any retained risk control measures.
Intended use	Use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer to customers.
Issue	The process associated with the authoring of a document. This process will include: reviewing, approval and configuration control.
Likelihood	Measure of the occurrence of harm.
Lifecycle	All phases in the life of a Health IT System, from the initial conception to final decommissioning and disposal.
Manufacturer	Person or organisation with responsibility for the design, manufacture, packaging or labelling of a Health IT System, assembling a system, or adapting a Health IT System before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party.
Patient	A person who is the recipient of healthcare.
Patient safety	Freedom from harm to the patient.
Post-deployment	That part of the lifecycle of a Health IT System after it has been manufactured, released, deployed and is ready for use by the Health Organisation.
Procedure	Specified way to carry out an activity or a process.
Process	Set of interrelated or interacting activities which transform inputs into outputs.
Release	A specific configuration of a Health IT System delivered to a Health Organisation by the Manufacturer as a result of the introduction of new or modified functionality.
Residual clinical risk	Clinical risk remaining after the application of risk control measures.

Safety incident	Any unintended or unexpected incident which could have, or did, lead to harm for one or more patients receiving healthcare.
Safety Incident Management Log	Tool to record the reporting, management and resolution of safety incidents associated with a Health IT System.
Severity	Measure of the possible consequences of a hazard.
Third party product	A product that is produced by another organisation and not by the Health IT System manufacturer. Examples include operating systems, library code, database and application servers and network components.
Top Management	Person or group of people who direct(s) and control(s) an organisation and has overall accountability for a Health IT System.

Appendix B - Roles & Responsibilities

Trust Board

The Chairman and Non-Executive Directors are responsible for ensuring that systems for governance, risk management and internal control are effective and maintained across all functions and at all levels of the Trust and will need to satisfy itself that all foreseeable hazards have been identified and that the clinical risk of such hazards has been reduced to acceptable levels. By authorising the deployment of the Health IT System, Top Management is accepting any residual clinical risk on behalf of the Health Organisation. Top Management remains responsible for authorising the deployment of a Health IT System. Within the Clinical Risk Management Plan, Top Management will need to specify those individuals who are able to approve the clinical risk management documentation. As a minimum this will be the Clinical Safety Officer.

Chief Clinical Information Officer

Accountable to the Executive Medical Director, the CCIO has designated responsibilities relating to clinical risk and is responsible for ensuring that Health IT systems meet the requirements of DCB0160 prior to deployment and use.

Chief Digital Information Officer (CIO)

The CDIO is responsible for ensuring that clinical risk management is integrated into the full lifecycle of any relevant Health IT system.

Clinical Safety Officer (CSO)

The person responsible for ensuring that the healthcare IT Clinical Risk Management System is applied to all clinical systems. The Clinical Safety Officer (CSO) for the Organisation is responsible for ensuring the safety of a healthcare IT system through the application of clinical risk management. The Clinical Safety Officer must hold a current registration with an appropriate professional body relevant to their training and experience. They also need to be suitably trained and qualified in risk management or have an understanding in principles of risk and safety as applied to healthcare IT systems. The Clinical Safety Officer ensures that the processes defined by the clinical risk management system are followed.

Risk and Assurance Group

The Risk and Assurance Group is a formally constituted sub-committee of Trust Management Group. It reviews, moderates and assures corporate-level risks and associated controls and mitigations. The Group receives reports on all directorate risk registers and specific risk issues from its members, including representatives from all other associated risk management groups.

Clinical Governance Group

The Clinical Governance Group provides a focus for clinical risk and quality issues. It receives reports by exception on clinical risk issues and is responsible for directing action to manage clinical risk.