Digital Clinical Safety Management Policy (N-065)

Version Number:	1.0
Author (name & job title)	Stephen Robson, Clinical Safety/Information Governance Officer
Executive Lead (name & job title):	Hilary Gledhill, Director of Nursing
Name of approving body:	QPaS
Date full policy approved:	1 June 2022
Date Ratified at Trust Board:	27 July 2022
Next Full Review date:	June 2025

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	
Date EMT as approving body notified for information:	

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. INTRODUCTION

This document outlines the Clinical Risk Management System (CRMS) and addresses the requirements of the mandated Clinical Safety Standards DCB 0129 and DCB 0160 and follows best practice as promoted by NHS Digital.

All healthcare IT systems/software used in relation to patient care within the Humber Teaching Foundation Trust must be developed, implemented and used in a safe and controlled manner.

It defines the clinical safety activities that must be completed in accordance with the Clinical Safety Standards. It also outlines when the Clinical Safety Officer (**CSO**) must be involved.

This CRMS will be reviewed and maintained in accordance with the Trust's Document Control Policy.

1.1. Purpose

The aim of the CRMS is to ensure that all of the Trusts staff involved with the development, implementation and use of healthcare IT systems/software are aware of the activities that are required to be undertaken, to ensure patient safety is not compromised by the introduction of such healthcare IT system(s)/software.

The Trust is required to adhere to national Information standards created and monitored via the Data Coordination Board **(DCB)** within NHS Information Standards frameworks.

This Clinical Risk Management System will be reviewed periodically to ensure that:

- changes in working practices are incorporated
- issues identified though an established internal audit programme are addressed
- the safety approach continues to adhere to the requirements of applicable international standards
- the system continues to protect the safety of patients in a complex and changing environment.

1.2. Audience

This document is for the all staff that are involved in ensuring the safety of healthcare IT systems/software, products or services.

2. SCOPE

This policy applies to the Trust and to all subsequent updates or upgrades to systems/software. The policy also applies to any local customisations or specific configurations made to a healthcare IT system by the Trust. It also addresses the Medical Device Regulations. If clarification is required of whether any system(s) falls within scope of this CRMS this should be raised with the nominated Clinical Safety Officer (CSO) for clarification. This nominated person provides clinical and organisational leadership on healthcare IT Patient Safety on behalf of the Trust.

3. ABBREVIATIONS

CRMS	Clinical Risk Management System
CSO	Clinical Safety Officer
DCB	Data Coordination Board
SCCI	Standardisation Committee for Care Information
DDG	Digital Delivery Group
HL	Hazard Log

CRMP	Clinical Risk Management Plan
CRMF	Clinical Risk Management File
DPIA	Data Protection Impact Assessment
MHRA	Medicines and Healthcare products Regulatory Agency

4. DUTIES AND RESPONSIBILITIES

The following defined roles are involved in clinical risk and safety process/system:

Chief Executive The Chief Executive is ultimately responsible for the content of all policies and their implementation.

Director of Nursing, Allied Health and Social Care Professionals – is responsible for ensuring clinical risk management is discharged appropriately and has the overall responsibility for the implementation of the risk management strategy

Chief Clinical information officer – is responsible for physician leadership to support the ongoing development and implementation of electronic health information systems related to the delivery of patient care across the organisation

Chief Information officer – is responsible to report to the executive team and trust management board regarding IT clinical risks as required, and to review and formally co-sign off the assessments (alongside the CSO)

Senior Information Risk Owner (SIRO) is the senior manager with Board level responsibility for information governance.

Clinical Safety Officer – is accountable for clinical safety ensuring that effective clinical risk management is carried out by organisations that are responsible either for manufacturing or deploying health IT systems, working alongside the Clinical Systems Team, to ensure full compliance when deploying new projects

All Staff - have a duty to comply with this policy. All staff involved in the provision, development, maintenance, deployment, implementation and reporting of a healthcare IT system/software are responsible for clinical safety activities. This includes:

- Following internal process to ensure the CSO is involved where necessary, this includes clinical systems, audit for forms, patient incidents, new software/services
- Escalating and reporting incidents on Datix using the existing risk management policy – recognising where a clinical safety incident may be applicable
- Ensuring the CSO is involved at the beginning of a project and included in workshops and mapping processes so to ensure appropriate hazard identification can be performed. Contact CSO at stephen.robson9@nhs.net

5. HEALTHCARE IT SYSTEM

The responsibility for healthcare IT Clinical Risk Management within the Trust resides with the Nursing and Quality directorate. Organisational management of healthcare IT related risks is as per the existing management arrangements as specified in the Trusts Risk Management Policy. Any new or amended processes, software or hardware involving personal confidential information will require the completion of a Data Protection Impact Assessment (**DPIA**). The assessment includes a section on Clinical Safety. All DPIA's are signed off by the Information Governance Group and published on the Trust's website. Please see Data Protection Impact Assessments (SOP16-005) for further details.

As well as the policies and procedures already in place within the Trust there are Clinical Safety Activities which should be noted. The nominated Clinical Safety Officer is responsible for the list below however it is non-exhaustive:

- Involvement in the procurement process for any new systems/software
- Engagement with various teams to develop Clinical Safety Plan(s) in relation to the Healthcare IT system/software
- Perform Hazard Workshop(s)with relevant teams in relation to system/software
- Creation of a Hazard Log for each system/software
- Creation and maintenance of Clinical Safety Closure Reports for each systems/software
- CSO should be Included in new developments
- CSO should review any release(s) before go-live
- Involved in the Incident management process and reviews
- Review Information government document's which may have a clinical safety implication

Clinical Safety documentation is to be created and templates of these are available here.

6. HEALTHCARE IT CLINICAL RISK MANAGEMENT (CRM) GOVERNANCE ARRANGEMENTS

The trust has various groups where the CSO or suitable representative should be present and any Healthcare IT system/software discussed and reviewed. Some of these groups include:

- Clinical Risk Management Group (CRMG)
- Quality and Patient Safety Group (QPaS)
- The consideration of clinical safety as part of the Data Protection Impact Assessment (DPIA) process is provided through the Information Governance Group (IGG)
- Digital Delivery Group (DDG)

7. CLINICAL RISK MANAGEMENT DELIVERABLES

7.1. Clinical Risk Management File

The Trust will establish a Clinical Risk Management File (**CRMF**) for each safety related healthcare IT system/software/product/service. 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.

7.2. Clinical Risk Management Plan

The Trust will establish a Clinical Risk Management Plan (**CRMP**) for each safety related healthcare IT system/software/product/service. 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. This must be done at the start of any healthcare IT projects and approved by the CSO.

7.3. Hazard Log

The Trust will establish and maintain a Hazard Log (**HL**) for each safety related healthcare IT system/software/product/service.

The Hazard Log will be made available within the CRMF. The purpose of the Hazard Log is to manage the effective resolution and communication of hazard risk within the Trust.

This must be created at the start of a healthcare IT project, reviewed weekly (if appropriate) by the team(s) and approved by the CSO.

7.4. Clinical Safety Closure Report

The Trust will issue a Clinical Safety Closure Report (**CSCR**) for each safety related healthcare IT system/software/product/service. The CSCR will be issued to support initial deployment and will be updated during the lifecycle of the healthcare IT system etc. should the safety characteristics change. The CSCR will be made available within the CRMF.

8. HEALTHCARE IT CLINICAL RISK MANAGEMENT ACTIVITIES

8.1. Hazard Identification

The Trust will conduct hazard identification workshops to identify potential hazards associated with the deployment and use of a healthcare IT system/software/product/service. The CSO will be responsible for facilitating such workshops and ensuring attendance from appropriate representatives. Typically, representatives from the following domains will be required:

- Clinical Systems Team
- Pharmacy Team including Pharmacists and Pharmacy Technicians
- Clinical Safety Officer
- IT if required
- Patient Safety Team
- Clinical Leads and/or operational teams

The workshops will have minutes taken and a copy stored in the CRMF. If a healthcare IT solution is deemed not to be safety related then this decision will be formally recorded.

The CSO will then raise this decision with the Information Governance Group and any other group deemed necessary.

Where any third-party components are used to support the healthcare IT system/software/product/ service then they will be considered in the scope of the hazard identification activities and subsequent risk assessment and reported directly to the third party for resolution. All identified hazards will be recorded in the Hazard Log (HL) and scored according to the nationally approved system. The nationally approved clinical safety matrix is different to that of the Risk matrix held by the trust. The matrix can be found in the appendices.

The mechanism's used to determine the hazards will be the Structured What If Technique (SWIFT) and the ALARP system. SWIFT is a hazards analysis method that uses structured brainstorming with guide words and prompts to identify risks. ALARP, which stands for "as low as reasonably practicable" is a principle is that the residual risk shall be reduced as far as reasonably practicable by introducing controls and mitigations

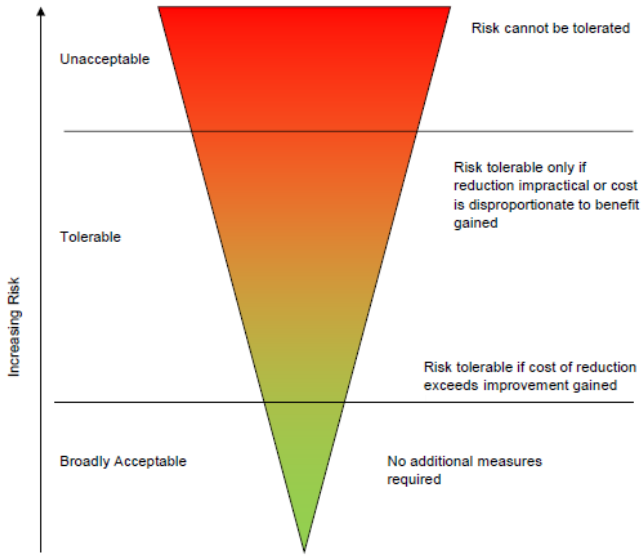

Figure 3 ALARP Triangle

Diagram above shows the ALARP Principle

8.2. Risk Assessment

The Trust will conduct healthcare IT system risk assessment in accordance with the Risk Management Policy.

The Hazard Log will be updated to capture the risk assessment.

8.3. Risk Evaluation

The Trust will conduct healthcare IT system risk evaluation in accordance with the Risk Management Policy.

The Hazard Log will be updated to capture the risk evaluation.

8.4. Risk Control

Where the initial risk evaluation is deemed unacceptable, further risk controls will be required. The Trust 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 Hazard Log.

The diagram below shows the various levels at which the CSO will be involved in Clinical Risk Management, this is derived from the DCB0160 Clinical Safety Standards.

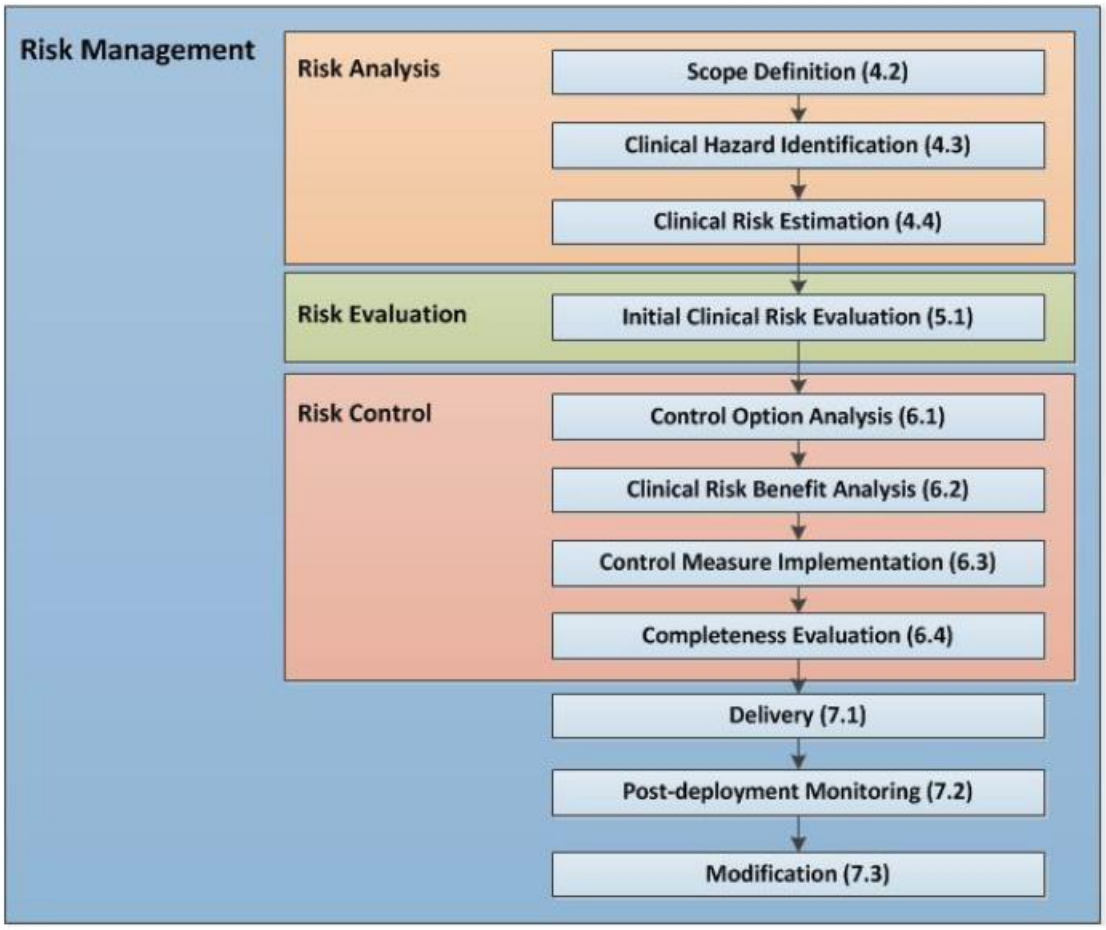

Figure 1 Clinical Risk Management Process

8.5. Deployment and Ongoing Maintenance

To support clinical safety activities undertaken during any deployment phases of a project or programme of work the following documentation will be required to form a part of the overall approval process:

- Project Initiation Document – third party supplier
- Project Plan
- Project Business Mapping
- Risk Register
- Weekly highlight reports
- Digital Delivery Group minutes or evidence from additional meetings relating to the specific project.
- Fallback Solution
- Change Management controls
- Witness Testing including test in test, user acceptance testing and any reports must be disclosed.

8.6. Incident Management

Clinical Risk Management activities within the Trust and the healthcare IT programmes and services offered are completed within the Risk Management Policy. As such clinical safety related incidents are dealt with in a similar manner as other incident within the Trust. The Incident Reporting Policy and Quality Impact Assessment Guidance is available for all staff and trust wide. These procedures are in place and require all staff within the organisation to adhere to. If related to patient safety or clinical harm then the CSO is required to assess the impact on patient safety if severity dictates.

8.7. Medical Device Directorate

Due to changes in regulations since 1 January 2021, all medical devices, including in vitro diagnostic medical devices (IVDs), placed on the Great Britain market need to be registered with the MHRA. The new Medical Device Regulation changed the law and process of certification for medical software, this includes:

- Software intended to provide information used to take decisions with diagnosis or therapeutic purposes are now Class IIa.
- Software, where these decisions have an impact that may cause a serious deterioration of a person's state of health or a surgical intervention, are Class IIb.
- Software, where these decisions have an impact that may cause death or an irreversible deterioration in a person's health, are Class III.
- All other medical device software is Class I.

Examples of software likely to be classified as a class II medical device:

- Dose calculators (e.g. insulin/general)
- Image diagnosis (e.g. melanoma)
- Algorithms calculating observations to signal a warning (e.g. in electronic patient records)

The Trust develop in-house tools and use various software to aid in daily clinical practice such as excel spreadsheets and calculators. After engagement with the MHRA they confirmed that any developments created in house for use within the Trust would be exempt from the need to register tools/software as a medical device class1.

9. PROCEDURAL DOCUMENTS TO THE POLICY

All documents listed below can be found on the Humber intranet Policies and Procedure pages

Clinical Policies and procedures

- Incident Reporting Policy and Procedure (N-038)
- Quality Impact Guidance (G389)

Corporate Policies and procedures

- Data Protection Impact Assessments (SOP16-005)
- Risk Management Policy (N-064)
- Document Control Policy (C-003)

10. TRAINING AND SUPPORT

All staff responsible for clinical safety 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.

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 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.

10.1. Training

Clinical safety personnel should 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 if available
- Approved external training courses

All registered clinicians involved in clinical safety roles shall, as a minimum, have completed an accredited training course. Completion of any safety training shall be recorded by the line managers on the annual appraisal form.

11. REFERENCE TO ANY SUPPORTING DOCUMENTS

- DCB 0160
- DCB 0129
- Hazard Log Template
- Clinical Safety Plan
- Clinical Safety Closure Report

12. AUDITS

12.1. 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 work streams and Third-Party suppliers**.**

12.2. Internal Safety Audits

The Trust shall undertake regular internal safety audits to ensure that projects undertaken within the Trust are compliant with this Clinical Risk Management System. These audits shall be conducted and recorded in accordance with the internal quality management procedure.
The scope of an internal safety audit will be the formal Clinical Risk Management System and the Trusts documentation supporting this document.

12.3. Supplier Audits

The Trust 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.

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

Appendix 1: Risk Classification Matrix:
Clinical Safety Framework as defined by NHS Digital

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 2: Likelihood as defined by NHS Digital

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

Appendix 3: Likelihood vs Severity as defined by NHS Digital

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
		Severity				

Appendix 4: Score Definitions as defined by NHS Digital

5	Unacceptable level of risk
4	Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level
3	Undesirable level of risk. Attempts should be made to eliminate the hazard or implement control measures 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 or where further risk reduction is impractical
1	Acceptable, no further action required

Appendix 5 Equality Impact Assessment

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: **Clinical Risk & Safety Management System Policy**

2. EIA Reviewer (name, job title, base and contact details): **Stephen Robson Clinical Safety/Information Governance Officer, Humber Teaching NHS Foundation Trust, stephen.robson9@nhs.net**

3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? **Policy**

Main Aims of the Document, Process or Service
The Clinical Risk & Safety Management Policy outlines the Trusts processes for managing clinical safety activities and for the provision of assurance in areas of clinical risk. It underpins the current Risk Management Strategy. It is supported by current mandated NHS safety standards under the Health and Social Care Act 2012.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed?	How have you arrived at the equality impact score?
1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender re-assignment	Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	LOW	
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical Learning Mental health (including cancer, HIV, multiple sclerosis)	LOW	
Sex	Men/Male Women/Female	LOW	
Marriage/Civil Partnership		LOW	
Pregnancy/ Maternity		LOW	
Race	Colour Nationality Ethnic/national origins	LOW	
Religion or Belief	All religions Including lack of religion or belief and where belief includes any religious or philosophical belief	LOW	

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Sexual Orientation	Lesbian Gay men Bisexual	LOW	
Gender Reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	LOW	

Summary

Please describe the main points/actions arising from your assessment that supports your decision. The policy is a trust approach which affects the processes rather than the individuals, when individuals are involved in clinical safety activities they should apply a situation/service specific equality impact assessment.	
EIA Reviewer: ***Stephen Robson***	
Date completed: -***28 January 2022***	Signature: ***Stephen Robson***

Appendix 6: Document Control Sheet

This document control sheet must be completed in full to provide assurance to the approving committee.

Document Type	Policy		
Document Purpose	Clinical Risk & Safety Management System		
Consultation/Peer Review:	Date:	Group/Individual	
List in right hand columns consultation groups and dates	09/03/2022	Information Governance	
	14/4/2022	Digital Delivery Group	
	01/06/2022	QPAS	
Approving Committee:	EMT	Date of Approval:	17 July 2022
Ratified at:	Trust Board	Date of Ratification:	27 July 2022
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*	Any Clinical Safety Officer employed or contracted by the trust must hold a current valid professional registration and Clinical Risk Management Training	Financial Resource Impact	Further training of Clinical Safety Officers will incur costs to the trust
Equality Impact Assessment undertaken?	Yes [ ]	No [ ]	N/A [X] Rationale:
Publication and Dissemination	Intranet [✓]	Internet [ ]	Staff Email [✓]
Master version held by:	Author [ ]	HealthAssure [✓]	
Implementation:	*Describe implementation plans below - to be delivered by the Author:*		
	• Communication sent to all staff via usual comms channel • Training suggestion presented to the trust • Visibility in teams across the trust to establish a good clinical safety process		
Monitoring and Compliance:	Annual Audits to be performed		

Document Change History: (please copy from the current version of the document and update with the changes from your latest version)			
Version number/name of procedural document this supersedes	*Type of change, e.g. review/legislation*	*Date*	*Details of change and approving group or executive lead (if done outside of the formal revision process)*
0.1	*New document*	*13/11/19*	*New document* *Discussed at QPaS – agreed more work needed and be changed to change into Policy template*
0.2	*Review and amended to reflect current legislation*	*12/01/21*	*Editorial text changes*
0.3	*Review*	*28/01/2022*	*Review and update CSO details and links to relevant documents*
0.4	*Review*	*17/05/2022*	*Changed name of policy, editorial text changes*
1.0	*Review*	*1/06/2022*	*Reviewed at QPaS and approved* *Approved at EMT July-22 and ratified at Trust Board 27-July-22*