East London NHS Foundation Trust

ELFT Digital

Clinical Safety Policy

Version:	2.0
Ratified by:	Digital Strategy Board
Date ratified:	
Name of originator/author:	Professor Ben Wright, Associate Medical Director for Clinical Information, ELFT (IT) Clinical Safety Officer
Name of responsible committee/individual:	Digital Strategy Board
Circulated to:	Service Delivery Board, IM&T Advisory Committee, (IT) Change Control Board
Date issued:	
Review date:	
Target audience:	Digital Department Informatics Department Procurement Team Finance Department Digital Champions Clinical Systems Digital Department Clinical Safety Officers Service Directors Clinical Directors Heads of Service

Version Control Summary

Version	Date	Author	Status	Comment
0.1	30/12/2015	Dr Ben Wright	Draft	Initial draft for consultation prior to approval
0.2	17/3/2016	Dr Ben Wright	Draft	Post consultation, pre-approval
0.3	24/03/16	Dr Ben Wright	Draft	Post consultation with IT Change Control Board
1.0	12/05/16	Dr Ben Wright	Approved	Approved for circulation
1.1	18/06/2020	Professor Ben Wright	Draft	Revision
1.2	29/09/20	Dr Paul Gilluley	Draft	Revision
1.3	30/09/20	Professor Ben Wright	Draft	For final consultation
1.4	01/11/20	Dr Sebastian Alexander	Draft	Unofficial consultation with National Clinical Safety Officer
2.0	06/11/20	Professor Ben Wright	Final Draft	For Approval

Contents

Table of Contents

Glossary and Abbreviations

ALARP	As Low As Reasonably Practical – This approach of balancing risk mitigation against resource availability is no longer an approved methodology because even if further mitigation is impractical, a significant residual risks may still be unacceptable. Where a significant risk remains unmitigated for practical reasons, the nature and severity of the residual risk together with the rational for failure to mitigate these risks should be clearly documented and highlighted.
System CCB	The system Change Control Board for each clinical system. This is convened and chaired by the Digital System Owner. The System Clinical Safety Officer must be a member of this board. The System Change Control Board reviews system configuration, development, deployment, Safety Case Report, Hazard Log and safety events.
Clinical Information System	The term Clinical Information System is synonymous with Health Information System (see below).
Clinical Safety Case Report	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 digital System's lifecycle.
Clinical Safety Officer	Person in a Health Organisation responsible for ensuring the safety of Health digital Systems in that organisation through the application of clinical risk management. They must be a suitably qualified and experienced clinician, with a current registration, be knowledgeable in risk management and its application to clinical domains.
DSB	Digital Strategy Board
Health information system	In this policy document, a health information system is defined as an electronic system that stores and manipulates organised, structured health related data (information) about identifiable people and makes this available to a range of stakeholders, this may include the health (or medical) record, decision support and communication between stakeholders and systems that alter, guide or direct clinical decision making. A health information system can therefore be made up of different components including: - An electronic health or medial record - A patient portal or communication system - Clinical decision support system (a system that uses information to guide or direct clinical care).

	- Clinical quality improvement systems where this makes available information about specific individuals or directly alters the care of identified specific individuals. o e.g. systems that use predictive modelling to identify specific high-risk patients. o Not systems that support quality improvement at a collective/group/service level. - Clinical quality assurance systems where this makes available information about specific individuals that impacts on their clinical care. o e.g. prompts completion of an outstanding risk plan for a specific individual. o Again not systems that support quality assurance at a collective/group/service level.
MAY	MAY or the adjective “OPTIONAL” mean that an item is truly optional.
MUST	This word or the terms “REQUIRED” or “SHALL”, mean that the definition is an absolute requirement of the specification.
MUST NOT	This word or the terms “SHALL NOT”, mean that the definition is an absolute prohibition of the specification.
Residual Risk	This is the risk that remains after the mitigations (the planned actions intended to reduce the risk) have been implemented.
SHOULD	This word, or the adjective “RECOMMEND” mean that there may exist valid reasons in particular circumstance to ignore a particular item, but the full implications must be understood and carefully weighted before choosing a different course.
SHOULD NOT	This phrase or the phrase “NOT RECOMMEND” mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described within this label.
System Clinical Safety Officer	An ELFT clinician, who is trained in DCB0160 (or under supervised training) who has lead ownership of the named clinical system and responsible for preparing and maintaining the hazard log and safety case report. They are responsible for ensuring the safety of that Health digital Systems through the application of clinical risk management. They must be a suitably qualified and experienced clinician, with a current registration, be knowledgeable in risk management and its application to clinical domains. They also review adverse events related to their system reported on DATIX in conjunction with the System Digital Owner. Prepare a summary of their findings in Datix for review by the Trust Clinical

	Safety Officer and update their hazard log and safety case report as appropriate and then notify relevant parties. There shall be at least one System Clinical Safety Officer for each clinical system (e.g. EMIS Clinical Safety Officer). They report to the Trust Clinical Safety Officer.
System Digital Owner	The System Digital owner is an ELFT employee who is experienced in the configuration, use and deployment of the named system. They will usually be a member of the Digital Department however for smaller specialist systems may be an administrator or manager within the directorate where the system is deployed. They will also ensure that the trust's commercial relationship with the supplier adheres to standing policies and processes. All clinical systems will have a named digital owner e.g. EMIS Digital Owner. The System Digital Owner will report to the Trust Systems Manager who will supervise and develop the member of staff in this area of practice.
Trust Clinical Safety Officer	Person in ELFT responsible for ensuring the safety of Health digital Systems in that organisation through the application of clinical risk management.
Clinical system manager	Person in ELFT responsible for managing Clinical information systems

Related Documents

These documents provide additional information and are specifically referenced within this document.

Ref	Title	Hyperlink
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
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
3.	Medical Device Regulations	https://www.gov.uk/guidance/medical-devices-conformity-assessment-and-the-ce-mark

Executive Summary

This document sets out how ELFT will comply DCB0160 as required in Information Standard Notice AMD 25/2018[1] – which ensures that Trusts have in place processes for detecting and managing clinical risks associated with the deployment and use of health information systems. This standard applies to clinical software within and without medical devices.

ELFT has a network of trained Digital Clinical Safety Officers. Each system will have a named clinical safety officer who will support multidisciplinary teams complete safety assessments of both new health information systems and modifications to existing systems. They will record their findings and proposed risk mitigation in a Hazard Log and prepare a Clinical Safety Case for their system. These clinical safety officers will be supervised and supported by the Trust Clinical Safety officer who will also review and approve their reports and recommendations before they are presented to the Digital Strategy Board.

Before deployment of any new digital system that manages patient information which influences patient care, authority to deploy will be sought from the Digital Strategy Board (DSB). For changes in the system (e.g. an upgrade) or scope of deployment where assessment shows that there is an *increase* in the residual (post mitigation) risk to “Undesirable” (NHS Digital Category C) authority to deploy will be sought from the Digital Systems Management Board and Safety Group, chairs action of this group or ELFT Chief Digital Officer. Where the residual risk *increases* to Category D (mandatory elimination) and cannot be mitigated, authority to deploy will be sought from the Digital Strategy Board (DSB). Systems with Category E risk (unacceptable) will not be deployed.

Where the modification to an existing system reduces or does not alter the risk, the Trust Clinical Safety Officer can authorise deployment of the system.

A central repository of documents will be held for each system. The Clinical Safety Case will be circulated to relevant Service Directors who will be responsible for implementing and monitoring the implementation of identified mitigations into their services.

Safety events will be monitored and managed through the ELFT DATIX system and a composite analysis of safety events with recommendations presented to the Digital Strategy Board every 12-18 months.

[1] 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#current-release

Introduction

Providing reliable access to appropriate clinical information is best achieved using dedicated electronic health information systems. An electronic health information system will include an electronic medical record[2] together with electronic clinical decision tools, (it may also include patient portal and communication systems, quality improvement systems and quality assurance systems, see glossary for definition). The benefits from implementing these systems can be optimised if risks associated with their deployment, modification, use and failure are mitigated to an acceptable level.

There is no longer a clearly defined boundary between medical devices and clinical software systems. Therefore, (excluding devices that have no software), and in accordance with DCB0160, physical medical devices will follow the standards and practices set out in this policy. In this instance the Lead Nurse for Physical Health will take the role of Device Safety Officer and be responsible for preparing the hazard log and safety case report for those devices for presentation to the Digital Strategy Board in alignment with relevant medical device regulations[3]. Medical devices that are software will be managed in accordance with electronic health systems clinical safety workflow.

DCB0160[4] is one of two[5] eHealth safety standards published by the Information Standards Board for Health and Social Care. This standard requires organisations to undertake a clinical risk management assessment of health digital systems. NHS England has mandated ISB0160 in their Operating Models. This document specifies the DCB0160 requirements *in italics* and then specifies how ELFT will comply with these.

Purpose

This document sets out what is acceptable to ELFT as acceptable thresholds for clinical information safety.

This document defines the process for detecting and mitigating risk when deploying or altering health information systems, the governance of system deployment and changes, and for providing assurance of adherence to this process.

This document sets out ELFT's Safety Incident Management Process which is the process for detecting post deployment adverse events resulting from health information systems use or failure.

[2] An electronic medical record (EMR) is best understood as the digitisation of the individual paper record. An electronic health record (EHR) is EMR that is both mobile with the Service User and integrates clinical information from all health providers involved in that person's care.

[3] https://www.gov.uk/guidance/medical-devices-conformity-assessment-and-the-ce-mark

[4] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/0160252018spec.pdf

[5] The second eHealth safety standard is DCB0129 and applies to system suppliers (manufacturers) who are also required to evidence that they have minimised the risk that health Digital will adversely impact patient safety.

Scope

In Scope

This document applies to all electronic systems used to store or manipulate clinical information by ELFT or ELFT sub-contractors; this includes non-health products or commercial off the self-products used in health digital systems.

The regulation includes evaluation of the impact of the following on clinical safety:

- Digital environment
- Interoperability
- Cybersecurity
- Mobile platforms
- IT network and IT security

The scope is limited to the management of risks related to patient safety.

Out of Scope

The following are out of scope for this policy and the ELFT Clinical Information Process:

- Word processing systems (e.g. Notepad, MS Word, MS Excel) and dictation software (e.g. Dragon Medical One); where these are used to create and manipulate text for subsequent use without a significant duration of information storage.

  Rational: this due to instrumental use by the operator in delivering an intended product or outcome. In these cases, "instrumental use" anticipates that there will always be significant errors in the initial content of the text or material produced as an expected and anticipated outcome of system use and the system user, as a routine action, is expected to correct this product to ensure that the final product is fit for purpose akin to using a key board or writing implement. Systems that have a patient information workflow e.g. eScription which manages digital dictation, would be ***in scope***.

- Telecommunication devices (phones, video conferencing).

  Rational: this is due to the instrumental use by the operator in delivering an intended communication as a transient, non-persistent information flow. Where information is likely to persist (e.g. messaging) and thereby contribute to patient care, this would be ***in scope*****.**

Duties

DSB0160 (section 2.2) sets out the responsibilities in Health Organisations these are specified in this document *in italics* below.

Top Management Responsibilities

> *In implementing the clinical risk management process for a given deployment, Top Management MUST:*
>
> > *Make available sufficient resources*
> >
> > *Assign competent personnel from each of the specialist areas that are involved in deploying and subsequently using the health IT system*
> >
> > *Nominate a Clinical Safety officer*
>
> *Top Management MUST authorise the deployment of the Health IT system accepting any residual risk on behalf of the Health Organisation.*

In ELFT, these “Top Management Responsibilities” are held by the Chief Medical Officer and the Chief Digital Officer on behalf of the Trust Board, supported by the Digital Strategy Board. In the absence of both the Chief Medical Officer and the Chief Digital Officer these responsibilities are delegated to a nominated deputy.

Clinical Safety Officer and Staff Competencies

DSB0160 (section 2.3) specifies that *Clinical Safety Officers:*

> *MUST be a suitably qualified and experienced clinician.*
>
> *MUST hold a current registration with an appropriate professional body relevant to their training and experience*
>
> *MUST be knowledgeable in risk management and its application to clinical domains*
>
> *MUST make sure that the processes defined by the clinical risk management process are followed.*

Competencies of Personnel:

> *Personnel MUST have the knowledge, experience and competencies appropriate to undertaking the clinical risk management tasks assigned to them.*
>
> *Competency and experience records for the personnel involved in performing the clinical risk tasks MUST be maintained.*

In ELFT, there will be a single nominated Trust Clinical digital Safety Officer, with a group of trained digital safety officers who will be clinical staff. Each clinical system will have a named clinician who is trained in clinical safety and has deep knowledge of the relevant clinical system (e.g. EMIS Clinical Safety Officer).

The System Clinical Safety Officer is responsible for:

1) Co-ordinating the evaluation of the system (or modules) and preparation of the hazard log
2) Updating the hazard log following changes to the system.
3) Reviewing Datix reports related to the system, preparing initial reports if indicated and updating the hazard log if indicated.
4) Preparing the clinical safety case and presenting this to the Digital Strategy Board following approval by the Trust Clinical Safety Officer.
5) Updating the clinical safety case as needed
6) Escalating safety events and issues to the Trust Clinical safety officer.

The role of the Trust digital safety officer is to:

1) To develop the professional cohort of system clinical safety officers through recruitment, appointment, supervision and line management.
2) Review safety case reports and make recommendations on alterations and approve final reports before submission to the Digital Strategy Board.
3) Review hazard logs and safety case reports to determine if they require Digital Strategy Board approval before progressing.
4) Review the assessments of Datix Reports and the associated recommendations prepared by clinical system owners.
5) Prepare an annual clinical safety review containing a thematic summary of digital safety events with recommendations to the Digital Strategy Board.
6) Prepare other recommendations as required.

In the absence of the Trust digital Safety Officer, this responsibility will be delegated by the Trust Clinical digital Safety Officer to an appropriate senior clinician, trained in digital Clinical Safety with experience in digital Clinical Safety Management.

Management responsibility is to ensure that services using clinical systems make clinician’s time available within their job plan to attend relevant training and management of their nominated clinical system.

System specific clinical safety officers are required because of the complex interaction between clinical systems, clinical practice and context. This complexity requires a dedicated individual to have sufficient familiarity with the use of the specific system in the specific context of use.

The provision of staff time needed for the System Clinical Safety Officer will be formalised within their job plan. Staff time will be allocated by the directorate using the clinical systems. This will be no less than one day per week per individual and may require as much as 2 days a week for complex systems. In addition, they will require time to attend the digital clinical risk basic training and biannual refresher training. The cost of this training will be funded from the digital department budget. The costs of the ELFT Clinical Safety Officer will be met centrally.

Where directorates fail to provide the necessary staff resource the matter will be raised in the first instance with the Service Director for resolution.

This will enable ELFT to develop a cohort of staff who are expert in the safe use of health information systems in clinical services.

Because safe use of clinical systems are co-terminus with optimal benefits realisation we envisage that system clinical safety officers will also have a key role to play in Digital transformation and optimisation of clinical system use.

Finance and Procurement

> *In the procurement of a Health IT System*[6] *the Health Organisation MUST ensure that the Manufacturer and the Health IT system complies with DSB0129.*

This responsibility will be held jointly by the Chief Financial Officer and Chief Digital Officer who will, as part of the procurement process, require the supplier of the health information system(s) to comply DSB0129.

Trust employees are prohibited from the procurement and deployment of any digital system that impacts on patient care without approval from the Chief Digital Officer.

The Tendering process for health information systems

The tendering process will stipulate:

- During the bidding process; "if awarded, where the bidder is supplying a health information system, the bidder agrees to comply fully with DSB0129 including full disclosure of the current un-abridged Clinical Safety Case Report for all health information systems that they supply or use in the delivery of their service."
- The penalty for not providing a current un-abridged Clinical Safety Case Report and Hazard log, shall, at the sole discretion of the Chief Financial Officer, lead to disqualification of the bidder.

Contract Negotiation and Health Information Systems

During the contract negotiation with the supplier, the contract will include clauses to the effect:

- "The supplier undertakes to comply fully with DSB0129 including full disclosure of the current un-abridged Clinical Safety Case Report and Hazard Log for all health information systems supplied or used in the delivery of their service

[6] In this document the terms Health Digital System and Health information system are interchangeable and are defined in the glossary (Page 5)

before initiation of their service or within 5 working days of contract agreement which ever is more favourable to the supplier.

- The supplier undertakes to provide a copy of any subsequent modifications to the Safety Case Report or Hazard Log within 5 working days of the modification and provide further electronic copies of the full, current, unabridged clinical safety case report and Hazard Log on request from the Trust Clinical Safety Officer or authorised deputy.
- Where the supplier fails to provide a clinical safety case report and hazard log within 5 working days, the penalty will be 1% of the total annual contract value for every 5 subsequent working days to a maximum annual penalty of 10% of the annual contract value. ”

Regular Clinical Risk Management Process Review

> *The Health Organisation MUST formally review its clinical risk management process at planned, regular intervals.*

In ELFT the Digital Strategy Board will review and approve this policy document. Subsequent review will occur after three years and no less frequently than every five years. Significant changes in good practice or policy will prompt an earlier review at the discretion of the Chief Medical Officer, Chief Digital Officer or Trust Clinical Safety Officer.

Threshold for acceptable clinical information risk and standard risk analysis.

The analysis and threshold for acceptable risk will adhere to the NHS Digital protocol for clinical risk management, this is set out in detail in appendix A. Individual harm will be rated Minor, Significant, Considerable, Major, and simultaneous harm to multiple people will be rated significant, considerable, major and catastrophic. Likelihood will be rated very low, low, medium, high and very high.

Likelihood will be estimated across the full range of services planned in the full deployment, not limited to the scope of the pilot of initial deployment. When the scope of the final deployment changes, the safety case will be updated accordingly.

Severity and likelihood will be combined and evaluated as either;

A- acceptable, no further action required,
B- acceptable, further risk reduction impractical (outweighs benefit to be gained),
C- undesirable, further reduction required unless impractical,
D- mandatory elimination of hazard or additional controls required,
E- unacceptable.

Category risks B to E will be reported in the safety case report.

Digital Clinical Risk Management Process

> DSB0160 – 2.1.1 requires that *The Health Organisation MUST define and document a clinical risk management process which recognises the risk management activities shown in Figure 1*, this is repeated in below.

Figure One: Risk Management (elements as defined by DSB0160)

Risk Analysis	(a) Scope definition
	(b) Clinical Hazard Identification
	(c) Clinical Risk Estimation
Risk Evaluation	(d) Initial Clinical Risk Evaluation
Risk Control	(e) Control Option Analysis
	(f) Clinical Risk benefit Analysis
	(g) Control Measure Implementation
	(h) Completeness Evaluation
	(i) Deployment
	(j) Post Deployment Monitoring
	(k) Maintenance
	(l) Decommission

ELFT will fulfil these requirements as follows:

The scope definition (a) will be incorporated with the Clinical Risk Management Plan which will set out the scope of use, domains of the system to be reviewed, and identify the system clinical safety officer who will lead the review by the multidisciplinary team according to the standard ELFT digital clinical safety evaluation process set out in this document. Planned deviations from this process will be specified. Sections (b) to (h) will be carried out by the multidisciplinary team conducting the digital clinical safety evaluation using the hazard log to structure the review and record the findings.

Based on the findings recorded in the hazard log the digital safety officer conducting the review will prepare a Safety Case report focussing on residual hazards above the threshold for acceptable clinical information risk. To meet deployment requirements (i) the safety case report will be reviewed by the ELFT Digital Clinical Safety Officer for approval and form the basis for seeking the authority to deploy. The allocated clinical safety officer will update the hazard log to a new version and document the outcome of the decision to authorise deployment.

Post deployment monitoring (j) will use the trust DATIX system for all safety events. All DATIX clinical information reports will be reviewed and graded. Those with a significant clinical information element arising from a health information system will be reviewed and the relevant actions recorded including updating the hazard log for that system.

Events reported on DATIX will be identified against the relevant clinical system and the digital clinical owner for that system will carry out a review and prepare recommendations. These will be reviewed by the Trust Clinical safety Officer and if appropriate the clinical system owner will prepare an update for the system hazard log and safety case.

Before deployment of any new digital system that manages patient information which influences patient care, authority to deploy will be sought from the Digital Strategy Board (DSB). Where health information systems are modified or updated as part of ongoing maintenance (k), or unanticipated increase in scope of deployment where assessment shows that there is an *increase* in the residual (post mitigation) risk to "Undesirable" (NHS Digital Category C) authority to deploy will be sought from the Digital Systems Management Board and Safety Group, chair's action of this group or ELFT Chief Digital Officer. Where the residual risk *increases* to Category D (mandatory elimination) and cannot be mitigated, authority to deploy will be sought from the Digital Strategy Board (DSB). Systems with Category E risk (unacceptable) will not be deployed.

The functionality of decommissioned systems is usually transferred to a successor system. Prior to deployment of the new system, the new system and the migration plan will be subject to safety evaluation. The decommissioning of the existing system, transfer of data and functionality and commissioning of the new system will be considered and planned together to ensure continuity and safety. The safety case report for this process will be used as the decommissioning plan (l). Where there is no successor system then a standalone safety case will be used.

Clinical Risk Analysis

Clinical Risk Analysis Process

> *The Health Organisation MUST implement the clinical risk analysis activities defined in the clinical risk management plan.*
>
> *Clinical risk analysis SHOULD be carried out by a multi-disciplinary group including a Clinical Safety Officer.*
>
> *The extent of the clinical risk analysis MUST be commensurate with the scale, complexity and level of clinical risk associated with the deployment.*

Clinical risk analysis will be carried out by a multi-disciplinary group and will include a clinical practitioner trained in (clinical) digital safety evaluation. Where an area of functionality has safety implications which are administrative, or related to the background functioning of the system (e.g. printing a letter correctly or registering a system user on a system) these analyses may be carried out by a multi-disciplinary team without clinical membership provided one member of the team has received digital safety training.

Health digital System Scope Definition

> *The Health Organisation MUST define the clinical scope of the Health IT System which is to be deployed.*
>
> *The Health Organisation MUST define the intended use of the Health IT System which is to be deployed.*
>
> *The Health Organisation MUST define the operational environment and users of the Health IT System which is to be deployed*

The Health digital System Scope will be defined in the ELFT Clinical Information Safety Hazard Log for each system.

Identification of hazards to patients and estimation of clinical risk

> *The Health Organisation MUST ensure that the clinical risks from all identified hazards have been considered and accepted.*
>
> *The Health Organisation MUST identify and document known and foreseeable hazards to patients both normal and fault conditions through the introduction and use of the Health IT System.*
>
> *For each identified hazard the Health Organisation MUST estimate, using the criteria specified in the clinical risk management plan, the severity and likelihood of the hazard and the resulting clinical risk.*
>
> *For each identified hazard, the Health Organisation MUST evaluate whether the initial clinical risk is acceptable. This evaluation MUST use the risk acceptability criteria defined in the Clinical Risk Management Plan.*
>
> *If the initial clinical risk is acceptable, then the risk control requirements defined* [below] *do not apply to this hazard.*
>
> *The Health Organisation MUST ensure that the clinical risks from all identified hazards have been considered and accepted.*
>
> *The Health Organisation MUST assess any local customisations prior to deployment.*

The evaluating multi-disciplinary team will record their findings in the system specific Hazard Log using the trust template. The ELFT Clinical Information Safety Case Report for each system will contain a copy of the system specific Clinical Safety Hazard Log as set out in the appendix.

The Hazard log will identify the hazard (the name of the hazard), describe the hazard and its impact. The team will evaluate the pre-mitigation risk and list identified causes. Mitigations will be identified and grouped under configuration, training and business and the residual risks quantified. Residual risks in category D or E are defined as unacceptable. Some category C risks may also require further action.

Clinical Risk Control and Clinical Risk Benefit Analysis

The Health Organisation MUST identify appropriate clinical risk control measures to remove an unacceptable clinical risk.

Proposed clinical risk control measures MUST be assessed by the Health Organisation to determine whether:

- *New hazards will be introduced as a result of the measures*
- *The clinical risks for previously identified hazards will be affected.*

The Health Organisation MUST manage any new hazards or increased clinical risks in accordance with sections 4.4 to 6.4 (these sections are set out in this document).

The Health Organisation MUST evaluate the residual clinical risk. This evaluation MUST use the risk acceptability criteria defined in the Clinical Risk Management Plan.

Where a residual clinical risk is judged unacceptable, the Health Organisation MUST identify additional clinical risk control measures in order to reduce the clinical risk.

If the Health Organisation determines that no suitable risk control measures are possible then the Health Organisation MUST conduct a clinical risk benefit analysis of the clinical risk.

Where a residual clinical risk is deemed unacceptable and further clinical risk control is not practicable, the Health Organisation MUST determine if the clinical benefits of the intended use outweigh the residual clinical risk.

If the clinical benefits do not outweigh the residual clinical risk, then the clinical risk remains unacceptable and the deployment SHOULD be re-appraised.

The Health Organisation MUST undertake a formal review of the Health IT System prior to its deployment to ensure that all of the requirements of this standard have been addressed.

The Health Organisations MUST assess any local customisations prior to deployment.

The results of this review MUST be recorded in the Clinical Safety Case Report.

The risk control requirements set out above will be fulfilled within the standard clinical risk assessment set out above in the section “identification of hazards to patients and estimation of clinical risk”. This assessment includes identifying mitigations for identified risks. Any residual category C, D or E risks will be specified in the safety case report the assessing team will set out the following in the clinical safety report:

(1) Specify the residual risk (category C, D or E)
(2) Specify the benefits related to the implementation
(3) Assess the impact on patient care and safety on the balance between the residual risk and anticipated benefits of system deployment.
(4) On this basis recommend whether or not to deploy the system. Category E risks would mandate recommendation for non-deployment.

This assessment will be set out in the current trust clinical safety template (in the appendix) and updated with subsequent system upgrades or extensions of system deployment.

Implementation of clinical risk control measures and post-deployment monitoring

> *The Health Organisation MUST implement the clinical risk control measures identified [in the hazard assessment]*
>
> *The Health Organisation MUST verify each clinical risk control measure implemented*
>
> *The Health Organisation MUST verify the effectiveness of each clinical risk control measure implemented*
>
> *The Health Organisation MUST establish, document and maintain a process to collect and review reported safety concerns and safety incidents for the Health IT System following its deployment.*
>
> *The Health Organisation MUST assess the impact of any such information on the on-going validity of the Clinical Safety Case.*
>
> *Where any such evidence is assessed to undermine the Clinical Safety Case, the Health Organisation MUST take appropriate corrective action in accordance with the Clinical Risk Management Plan and document it in the Clinical Safety Case Report.*
>
> *The Health Organisation MUST ensure safety related incidents are reported and resolved in a timely manner.*
>
> *A record of safety incidents, including their resolution, MUST be maintained by the Health Organisation in a Safety Incident Management Log.*

The clinical safety report for each system will document mitigations for each risk. These are the clinical risk control measures required to mitigate the risk to an acceptable level. These clinical safety reports shall be provided to the service director and clinical director who will require heads of service to incorporate the relevant actions into their operating policies. Verification of implementation will form part of the team or directorate’s normal operational governance processes. The Directorate Management Teams will document adherence to the mitigation plans in their minutes and copy relevant minutes to the Trust clinical safety officer.

Management of adverse events

All adverse events associated with health information systems will be reported using the ELFT DATIX System.

The report in Datix will categorise these events against the identified system in question. Each report will be reviewed by the System Clinical Safety Officer and if necessary by the System Digital Owner. These will be managed using the current assurance mechanisms and where appropriate the Trust Clinical Safety Officer will be notified. Depending on the findings the hazard log will be updated and if necessary the clinical safety case report revised.

ELFT DATIX shall function as the Safety Incident Management Log and contain the necessary sections to document the review and recommendations following adverse events.

Digital System Maintenance (and upgrades)

> *The Health Organisation MUST apply their clinical risk management process to any modifications or updates of the deployed Health IT System.*
>
> *The application of this process MUST be commensurate with the scale and extent of the change and the introduction of any new clinical risks.*
>
> *The Health Organisation MUST issue a Clinical Safety Case Report to support any modifications to the Health IT System that changes its clinical risk.*

Before each system modification the impact of these modifications will be reviewed by a multidisciplinary team. The results of this review will be recorded in an updated version of the pre-existing hazard log. The Clinical Safety Report will then be updated accordingly; this will include a new date and version number.

Improvement or no change in the risk profile, once approved by the Trust Clinical Safety Officer, will result in automatic authority to deploy.

Risk increases to category A or B will be approved at the discretion of the Trust Clinical Safety Officer or escalated to the Digital Systems Management Board and Safety Group.

If assessment shows that there is an *increase* in the residual (post mitigation) risk to “Undesirable” (NHS Digital Category C) authority to deploy will be sought from the Digital Systems Management Board and Safety Group (which must always include an appropriately qualified Clinical Safety Officer), chairs action of this group (under the advice of an appropriately qualified clinical safety officer) or ELFT Chief Digital Officer (again under the advice of an appropriately qualified clinical safety officer).

Where the residual risk *increases* to Category D (mandatory elimination) and cannot be mitigated, authority to deploy will be sought from the Digital Strategy Board (DSB).

Systems with Category E risk (unacceptable) will not be deployed.

System Decommissioning

> *The Health Organisation MUST apply their clinical risk management process to a Health IT System that is being decommissioned.*
>
> *The application of this process MUST take into account the deployment of any succeeding Health IT System.*
>
> *The application of this process MUST take into account the migration of data between the decommissioned Health IT System and the succeeding Health IT System.*
>
> *The Health Organisation MUST issue a Clinical Safety Case Report to support decommissioning of the Health IT System.*

Where a system is being decommissioned, this nearly always results in migration of function or data to a successor system. The clinical safety assessment of the existing system will be updated to include the data migration. The clinical safety case report of the successor system will be revised as appropriate.

Project Safety Documentation and Repositories

Clinical Risk Management File

> *The Health Organisation MUST establish at the start of a project a Clinical Risk Management File for the Health IT System.*
>
> > *The Clinical Risk Management File MUST be maintained for the life of the Health IT System.*
> >
> > *All formal documents and evidence of compliance with the requirements of this standard MUST be recorded in the Clinical Risk Management File.*
> >
> > *Any decisions made that influence the clinical risk management activities undertaken MUST be recorded in the Clinical Risk Management File.*

An electronic folder will be opened for each system which will contain the current Hazard Log and Clinical safety case for the system as they are updated.

Clinical Risk Management Plan

> *The Health Organisation MUST produce at the start of a project a Clinical Risk Management Plan, which will include risk acceptability criteria, covering the deployment of a new Health IT System.*
>
> *A Clinical Safety Officer MUST approve the Clinical Risk Management Plan.*
>
> *If the nature of the project changes, or key people change, during the deployment, use, maintenance or decommissioning of a Health IT System, then the Clinical Risk Management Plan MUST be updated.*
>
> *The Clinical Risk Management Plan MUST be maintained throughout the life of the Health IT System.*

The Clinical Risk Management Plan will be set out at the start of the Hazard log. The Risk management plan is for a multidisciplinary team to review the system functionality that will be implemented or changed, to identify and assess hazards associated with this, to record these hazards in a Hazard Log, to advise on mitigations for these hazards in the log and re-evaluate residual risk. The findings must then be summarised in a safety case report. Following approval the safety case report will be disseminated to relevant stakeholders, specifically the relevant Service Director and Clinical Director.

Hazard Log

> *The Health Organisation MUST establish and maintain a Hazard Log.*
>
> *A Clinical Safety Officer MUST approve each version of the Hazard Log.*
>
> *An issued Hazard Log MUST accompany each Clinical Safety Case Report.*

The assessing team will use the ELFT Hazard Log template to record their findings and recommendations and embed the current Hazard Log in the Safety Case Report. The resulting safety case report and hazard log will be reviewed by the trust Clinical Safety Officer for approval.

Clinical Safety Case

> *The Health Organisation MUST develop and maintain a Clinical Safety Case for the Health IT System.*

The assessing clinical safety team will prepare a clinical safety case using the ELFT template. This will be stored electronically in the system clinical risk management file.

In addition to specifying the risk, the report will specify mitigations that require on going application. For example, a completed change to the configuration that has been implemented will not be specified but training (which requires repetition) or Business

Change (which requires integration into business processes and ongoing monitoring) will be specified as these are required by Service and Clinical Directors.

Clinical Safety Case Reports

> *The Health Organisation MUST produce a Clinical Safety Case Report to support each lifecycle phase (i.e. deployment, use, maintenance and decommissioning) of the Health IT System.*
>
> *A Clinical Safety Officer MUST approve each Clinical Safety Case Report.*

The assessing team will either prepare or update the clinical safety case report as relevant to the system implementation or change. Previous approved versions of the reports will be stored. These documents will be archived electronically in the clinical risk management file.

Safety Incident Management Log

> *The Health Organisation MUST maintain a Safety Incident Management Log.*

Safety incidents will be recorded using the ELFT DATIX system. Following completion of the report, these will be reviewed by the relevant system clinical safety officer who will summarise the key findings and recommendations. Where appropriate the system Hazard Log and Safety Case Report will be updated and disseminated accordingly.

Change Control process and Clinical Safety Management

Change initiation

Request to change the clinical system are made through the digital change control process. The clinical system owner completes a review of the change and updates the system hazard log. If necessary, the safety case is also updated and submitted to the Digital Systems Management Board and safety group. Possible outcomes are shown in the table below:

Clinical Safety Case Report status.	Clinical Safety Assessment	Possible outcomes
Not completed	n/a	Request declined Or Proceed to digital safety evaluation.

Completed	New system	Request declined Or Proceed to Digital Strategy Board for authority to deploy
Completed	Existing system with authority to deploy, risk decreases or does not change following proposed deployment, or risk increase limited to a category A or B risk.	Clinical safety approval from Trust Clinical Safety Officer.
Completed	Existing system with authority to deploy, risk increases following proposed deployment with additional residual category C only	Request declined Or Category C risk: Digital Systems Management Board and Safety Group authorises deployment Or Some category C risks refer to Digital Strategy Board for authority to deploy
Completed	Existing system with authority to deploy, risk increases following proposed deployment with additional residual risks category D and E risks	Request declined Or category D and E risks refer to Digital Strategy Board for consideration

Authority to deploy new systems will be recorded in the hazard log of the system and minutes of relevant meetings.

Urgent and out of hours authorisation to deploy

It can be necessary to deploy a system upgrade or modification either out of hours or when there is insufficient time to consult with the Digital Systems Management Board and Safety Group or Digital Strategy Board. Typical scenarios include:

(a) A system upgrade which occurs out of hours to minimise disruption, safety tests can only occur on the live system (usually with the option of “rolling back” the system to the earlier state).

(b) Where a serious error or fault develops or is discovered in a system and a “hot fix” is developed and offered by the supplier.

In these circumstances:

(a) The proposed deployment must be assessed by a clinician trained in clinical safety; the assessment (and corresponding team size) should be appropriate to the proposed change.

(b) Where the overall residual risk of the proposed change (including allowance for benefit resulting from the improvement in system functionality) is less than or the same as the original risk, (or overall increase in mitigated risk is category A or B) deployment can be authorised by either

   (i) The Trust Digital Clinical Safety Officer or in their absence

   (ii) A delegated authorised Digital Clinical Safety Officer

(c) Where the overall residual risk increases resulting in new category C risk the authority of either: The Chief Medical Officer or The Chief Digital Officer acting on the advice of an experienced Digital Clinical Safety Officer (the Trust Clinical safety officer or in their absence an authorised deputy or the System Clinical Safety Officer) must be sought to proceed with the deployment.

Appendices

Appendix A – Detailed discussion of evaluation if clinical system risk grading, contrasting the National approach with the ELFT Risk Grading Policy

The analysis and threshold for acceptable risk will adhere to the NHS Digital protocol as set out on the clinical risk management plan template[7] this differs from the ELFT Risk Management Strategy[8] in the following ways:

Assessment of severity: in contrast with usual clinical risks and adverse events, clinical information systems are more likely to harm many patients at once, this is captured and reflected in the severity of harms which reduces the top grade of harm for an individual patient from 5 to 4 and increases all grades of harm by one point if more than one patient is likely to be harmed. Usually the numbers of patients being harmed following an individual incident is less than 10, if there is a likelihood that many multiples will be harmed i.e. tens to hundreds, consider increasing the harm by a further point. Note, the likelihood should relate to the specific severity. If multiple people are harmed because the event is recurrent alter the likelihood rating accordingly. This is shown in the table below:

Severity 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

[7] https://digital.nhs.uk/binaries/content/assets/website-assets/services/clinical-safety/nhs_digital_clinical_risk_management_plan_template-1.docx
[8] http://elftintranet/download/115765d0-b6d7-4286-bd56-f3e751919009/f/TBD-2014-09-25_Revised_DRAFT_Risk_Management_Strategy_March_2014.pdf

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 consequence	Single

The likelihood of the risk causing harm is similar to the ELFT risk management approach, and is graded very low, low, medium, high and very high however specific indices for these grades of frequency are not provided.

Gradations in risk assessment

Similar to the ELFT risk management approach, the two parameters are combined, however the NHS Digital framework recognises the non-linear nature of this combination and therefore categorises the resulting risk into five grades shown in the table below:

NHS Digital		ELFT Risk Management		
E	Unacceptable level of risk	25	20	Escalate to Directorate Risk Registers will be considered for escalation to the Corporate Risk Register or BAF. Notification takes place through submission of the Directorate Risk Registers to the SDB. Control measures should be put in place, which will have the effect of reducing the impact of an event or the likelihood of an event occurring. A number of control measures may be required. 15-25 Significant resources may have to be allocated to reduce the risk. Where the risk involves work in progress urgent action should be undertaken.
D	Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level	16	15	
C	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	12	8	Immediate action must be taken to manage the risk and entered on the Service Risk Register and considered for escalation to the Directorate Risk Register via local team meetings and supervision. Control measures should be put in place, which will have the effect of reducing the impact of an event or the likelihood of an event occurring. A number of control measures may be required. Resources may have to be allocated to reduce the risk. 4-14
B	Acceptable where cost of further reduction outweighs benefits gained or where	4	3	

	further risk reduction is impractical			
A	Acceptable, no further action required	2	1	On or below this level a risk is acceptable however existing controls should be monitored locally within Directorates and local Governance groups and adjusted regularly. No further action or additional controls are required. 1-3

The combination of likelihood and severity creates the following risk matrix:

Likelihood					
Very High	C	D	D	E	E
High	B	C	C	D	E
Medium	B	B	C	C	D
Low	A	B	B	C	D
Very Low	A	A	B	B	C
	Minor	Significant	Considerable	Major	Catastrophic
	Severity				

The exact translation between NHS Digital and ELFT's risk management matrices are shown below:

Translation matrix between NHS Digital and ELFT, differences highlighted in blue boarder

Severity ELFT Likelihood		Negligible		Minor		Moderate		Major		Catastrophic		
Almost Certain	5	C	5	D	10	D	15	E	20	E	25	Very High
Likely	4	B	4	C	8	C	12	D	16	E	20	High
Possible	3	B	3	B	6	C	9	C	12	D	15	Medium
Unlikely	2	A	2	B	4	B	6	C	8	D	10	Low
Rare	1	A	1	A	2	B	3	B	4	C	5	Very Low
Severity		Minor		Significant		Considerable		Major		Catastrophic		NHS Digital

The NHS Digital framework both ignores rare and negligible risks and has greater gradations for low frequency and minor risks, reflecting the need to manage these with greater sensitivity in clinical systems as the majority of harms arise from frequent minor and significant risks.

All risks will be captured in the hazard log for that system and category C to E risks will be reported in the safety case report.

Having estimated the likely harm that is representative for that event, safety officers will estimate the likelihood for that specific harm across the whole estate where that element is (or will be) in use. Thus if only a small number of staff use a function in a system (or a small number of staff use the system) infrequently then the estimated risk will be considerably less than if all system users (or a large number of system users) access that functionality on a regular basis. Scope of use should be for the maximum anticipated use following full and compete deployment. For example, for planned deployment across the whole trust, frequency estimates should be for all users not the initial limited pilot.

Acrobat Document

ELFT RISK GRADING MATRIX

Appendix B – ELFT Clinical Safety Evaluation Hazards Log Template

ELFT Hazard Log template

ELFT Hazard Log
Final 2020.xlsx

Appendix C – ELFT Clinical Information Safety Case Report Template

System Safety Case
Report template.doc.d