Albert Health Clinical Safety Management File

None

Albert Health

Table of contents

1. Clinical Safety of the Albert Health Voice-based Digital Health Platform Project

1.1 Intended Use and Important Limitations

The Albert Health Voice-based Digital Health Platform is intended as an adjunct to existing clinical care provision, supporting patients in managing enteral nutrition at home. It is not intended as a replacement for standard channels of communication between Health Care Professionals (HCPs) and patients.

The UK-localised version is the only version considered by this Clinical Safety Documentation.

The Telehealth features of the Albert Health application are not being used in the UK version and have not been reviewed.

1.2 Digital Technology Assessment Criteria (DTAC)

- DTAC is a UK(England)-only grouping of assessment criteria. It is relatively new, and aims to simply bring together and harmonise *existing* assessment criteria for digital technologies. More information is available on the NHSX website
- DTAC incorporates the DCB0129 and DCB0160 standards for clinical safety, which the Albert Health Voice-based Digital Health Platform is compliant with.

1.3 DCB0129 and DCB0160 Compliance

This Clinical Safety Management File includes all documentation relevant to the Manufacture of clinical software (DCB0129). It is intended that Clinical Safety Officers in implementation sites will be able to easily obtain this Clinical Safety Management File and use it to develop their DCB0160 (Implementation) Clinical Safety Case.

1.4 DCB0129 Hazard Log

Our Hazard Log is managed on GitHub in the open. Details of how this works are here.

1.5 Downloading this documentation as a PDF

We have prepared this documentation using the tools of the modern Web (MarkDown, static HTML site generation) in order to present a linkable, searchable, interactive documentation site which is version controlled using Git and is openly available.

We are aware that some organisations may wish to download a 'simulated paper' document such as a PDF, and for this reason we have set up the site to automatically generate a PDF version of the entire documentation, which can be downloaded here

Last update: May 4, 2023

Created: May 4, 2023

2. Business Continuity

2.1 Business Continuity

2.2 Disaster Recovery

Last update: May 4, 2023
Created: May 4, 2023

3. Clinical Safety Case Report

Last update: May 4, 2023

Created: May 4, 2023

4. Clinical Risk Management Plan

4.1 Purpose

The aim of the Clinical Risk Management Plan is to ensure that all of the Albert Health Clinical Safety Team involved with the development, implementation and use of Healthcare 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 Healthcare IT systems.

The Albert Health Clinical Safety Team is required to adhere to National Information standards created and monitored via the Data Coordination Board (DCB) within NHS Information Standards frameworks.

The mechanisms used are approved process Clinical Risk Management System compliance documents.

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

- changes in working practices are incorporated.
- issues identified through 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.

4.2 Audience

This document is for the Albert Health Clinical Safety Team staff that are involved in ensuring the safety of the Albert Health Healthcare IT systems, products or services, but is made publicly available as part of our commitment to transparency and open governance.

4.3 Scope

This policy applies to the the Albert Health Clinical Safety Team's organisation and to all of the Albert Health Clinical Safety Team's IT systems. The policy also applies to any local customisations, upgrades or specific configurations made to a Healthcare IT system by the Albert Health Clinical Safety Team.

If clarification is required of whether any system 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 Organisation.

4.4 Definitions

Note - Also see the Albert Health Risk Management Strategy

CSO: Clinical Safety Officer - 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.

DCB: Data Coordination Board

4.5 Healthcare IT Clinical Risk Management (CRM) Governance Arrangements

The responsibility for Healthcare IT CRM within the Organisation resides with the Clinical Safety Officer

Organisational management of Healthcare IT related risks is as per the existing management arrangements as specified in the Organisation’s Risk Management Strategy.

4.5.1 Clinical Risk Management Team Organisation Chart

4.5.2 Personnel

Clinical Safety Officer

Clinical Safety Officer Name: REMOVED Clinical Safety Officer Contact: clinicalsafety@albert.health

Chief Executive Officer

4.6 Governance

Governance for patient safety within the Organisation is provided through the following forums:

4.6.1 Clinical Risk Meetings

- Clinical Safety is discussed as a fixed item on the two-weekly Sprint Planning Meeting at which the project is planned and priorities set for the next sprint of development.
- In the event of an **urgent** clinical safety issue or incident, a supplementary Clinical Risk meeting is held at the earliest possible time.

4.6.2 Issue tracking

4.7 Deliverables

4.7.1 Clinical Risk Management File (this repository)

The Albert Health Clinical Safety Team will establish a Clinical Risk Management File (CRMF) for each safety related Healthcare IT system. The purpose of the CRMF is toprovide a central repository where all safety related information pertaining to the Healthcare IT system is stored and controlled. This GitHub repository contains out Clinical Risk Management File.

4.7.2 Clinical Risk Management Plan (this document)

The Albert Health Clinical Safety Team will establish a Clinical Risk Management Plan (CRMP) for each safety related Healthcare 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.

4.7.3 Hazard Log (Issues in this repository)

The Albert Health Clinical Safety Team will establish and maintain a Hazard Log (HL) for each safety related Healthcare IT system. The HL will be controlled and configured in accordance with the Organisation document control /quality management policy [provide a reference].

4.7.4 Clinical Safety Cases

The Albert Health Clinical Safety Team will establish and develop a Clinical Safety Case (CSC) for each safety-related Healthcare IT system:

- Albert Health Voice-based Digital Health Platform

4.7.5 Clinical Safety Case Reports

The Albert Health Clinical Safety Team 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 CSCR will be controlled and configured in accordance with the Organisation’s document control policy [provide a reference]. The HL will be made available within the CRMF.

4.8 Healthcare IT Clinical Risk Management Activities

4.8.1 Hazard Identification

The Albert Health Clinical Safety Team will conduct hazard identification workshops to identify potential hazards associated with the deployment and use of our Healthcare IT system. The Clinical Safety Officer will be responsible for facilitating such workshops and ensuring attendance from the Albert Health Clinical Safety Team. Typically, representatives from the following domains will be required:

- Technical testing team
- User research and User Experience team
- Clinical testing team
- Statistical support
- Project Board

The workshops will have minutes taken and a copy stored in the Clinical Risk Management File.

If a Healthcare IT solution is deemed not to be safety related then this decision will be formally recorded.

The technical team will advise on the best mechanism for addition of new issues to the the Albert Health Clinical Safety Team's project management workflow.

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 areused a positive declaration to this effect will be recorded in the minutes.

All identified hazards will be recorded in the Hazard Log.

4.8.2 Risk Assessment

the Albert Health Clinical Safety Team's Health will conduct Healthcare IT system risk assessment in accordance with the Risk Management Strategy. The Hazard Log will be updated to capture the risk assessment.

4.8.3 Risk Evaluation

The Albert Health Clinical Safety Team will conduct Healthcare IT system risk evaluation inaccordance with the Risk Management Strategy. The Hazard Log will be updated to capture the risk evaluation.

4.8.4 Risk Control

Where the initial risk evaluation is deemed unacceptable, further risk controls will be required. the Albert Health Clinical Safety Team will manage Healthcare IT system risk in accordance with the Risk Management Strategy.

Details of the risk control measure and evidence of effective implementation will be captured in the Hazard Log.

4.8.5 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.

4.8.6 Incident Management

Clinical Risk Management activities within the Organisation and theHealthcare IT programmes and services offered are completed within the corporate risk management strategy. As such, clinical safety related incidents are dealt with in a similar manner as other incidents within the organisational such as financial,reputational, technical and other service impacting categories.

4.8.7 Safety Incident Management Process

4.8.8 Security Incident Management Process

Security issues may be responsibly disclosed to security@albert.health for immediate action. We recognise and respect the work of security researchers and will treat your contribution with gratitude and appropriate action. We do not engage in vexatious CMA litigation.

Internally we treat security issues with the highest priority. Once the 'acute phase' of any security threat is handled, we will then follow the Safety Incident Management Process, usually converting to a public GitHub Issue.

4.9 Clinical Safety Competence and Training

4.9.1 Overview

The clinical safety activities described in this Clinical Risk Management System shall be undertaken by competent staff. Suitable training shall be undertaken by staff to maintain and expand their level of competence.

4.9.2 Competency

All of the staff identified in the organisation chart, shall be sufficiently competent for the roles and tasks which they are asked to undertake. Where an individual does not yet 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 (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.
- 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.
- All registered clinicians involved in safety roles shall, as a minimum,have completed an accredited training course.

4.9.3 Training

- 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.
- 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 individual on the annual appraisal form.

4.10 Audits

4.10.1 Overview

Audits shall be undertaken to ensure that projects are adhering to thedefined safety requirements. Such audits will focus on the **ClinicalSafety Team** and **third-party** suppliers.

4.10.2 Internal Safety Audits

- the Albert Health Clinical Safety Team 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.
- The scope of an internal safety audit will be the formal Clinical Risk Management System and the Organisation’s documentation supporting this document.

4.10.3 Supplier Audits

The Albert Health Clinical Safety Team 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 DCB0129.

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

Last update: May 4, 2023
Created: May 4, 2023

5. Clinical Risk Management System

5.1 Albert Health Clinical Safety Team

5.1.1 DATE

5.2 Document Management

5.2.1 Revision History

- This document is versioned in Git and published in GitHub.
- Refer to the document's Releases section in GitHub to see a history of releases.
- This document was created from the Clinical Safety Management Plan templates provided on the NHS Digital Website.

5.2.2 Reviewers and Process

This document must be reviewed by:

The review mechanism for update is via Pull Request review on GitHub, with opportunity for reviewers to comment and amend the text.

5.2.3 Approvers and Process

This document must be **approved** by:

- REMOVED, Clinical Safety Officer, Albert Health Clinical Safety Team
- Following satisfactory review by the Reviewers, the nominated Approvers merge the pull request into the main branch of the code.

5.3 - The current version of this document will always be selected as the 'default branch' in GitHub

5.3.1 Related Documents

5.4 Introduction

This Clinical Risk Management System (CRMS) outlines the processes to be followed to ensure that all healthcare IT used to support care withinthe Organisation is developed, implemented and used in a safe manner.

This CRMS provides a framework that promotes the effective risk management, by the Organisation, of potential health IT hazards andoperational incidents.

This CRMS complements existing risk management processes that should be defined in the Royal College Digital Growth Charts Team's Risk Management Strategy and wherever practical, uses existing procedures, processes and governance arrangements.

This CRMS addresses the requirements of DCB0129 and DCB0160 and follows best practice in clinical safety, development practice, security, and transparency.

This CRMS will be reviewed and maintained in accordance with the the Royal College Digital Growth Charts Team's policies.

Last update: May 4, 2023
Created: May 4, 2023

6. Contact the Albert Health team

6.1 General Enquiries

Last update: May 4, 2023

Created: May 4, 2023

7. Downloads

7.1 PDF export

Use the button below to download this entire site, compiled to a structured PDF document

Download full Clinical Safety Management File in PDF format

Last update: May 4, 2023

Created: May 4, 2023

8. Albert Health Voice-based Digital Health Platform Hazard Log

In keeping with our commitment to transparency and openness, our Hazard Log is publicly visible and managed in GitHub using the Issues feature.

Each Issue represents a Hazard potentially affecting the project.

Hazards can be viewed (and indeed commented on, discussed, and improved) at the URL below:

https://github.com/Albert-Health/albert-health-clinical-safety/issues

Instead of the more usual and somewhat outdated and chaotic 'spreadsheet' model, often used for Hazard Logs, we are using the Issues facility in GitHub to record Hazards.

- *Labels* are used to annotate Hazard Issues with `severity-` and `likelihood-` scores, from which we can derive a `risk-level-`. See all Labels here
- *Milestones* are used to designate the Initial Risk Assessment and Residual Risk Assessment. See all Milestones here

Most importantly, the **discussion and evidence** relating to any given risk is included in the recording of the risk. A complete history of the labelling is kept in the issue. Spreadsheet-based risk and hazard handling is inferior to this model, because spreadsheets are unsuited to discussion, text handling, and long-form discourse.

A Hazard which is *never* recorded in any Spreadsheet-based Hazard Log is 'Accidental deletion of a Hazard before it has been mitigated/risk-eliminated', yet anyone who has used a spreadsheet knows how easy it is to accidentally delete or modify a cell or row inadvertently. Put simply, a spreadsheet is a poor choice of technology for managing text and a totally unacceptable choice of technology for handling Hazards, yet it has become the industry standard across the NHS simply because the Hazard Log template issued by NHS Digital is a spreadsheet. Building and releasing an open source, free **Hazard Log management platform** would have been much a better approach, which NHS DIgital had ans still has the resources to do, but lack of understanding about the case of need limits their capability to execute on this.

8.1 Monitoring of Risk

8.1.1 Risk Matrix and Acceptability Criteria

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				

8.1.2 GitHub Labels

Using the Label search feature, one can search for Hazards at any Risk Level, in order to triage the most risky Hazards for further action.

risk-level-5-unacceptable
risk-level-4-mandatory-risk-elimination
risk-level-3-undesirable
risk-level-2-acceptable
risk-level-1-acceptable

- We can filter for multiple labels.

8.2 Hazard Deletion

Hazards are **never** deleted but may be *closed* if there is no residual hazard and they are no longer relevant.

8.3 Alternative views

Using the GitHub Projects you can create a tabular (Excel-style) view, or a Kanban (Trello) view of your Hazards. Using built-in GitHub Issues and Pull Requests features you can link Hazards to their mitigations in code, to show a chain of evidence of clinical safety improvements.

8.4 Creating a Hazard

1. Navigate to Issues
2. Click on New Issue
3. Use the **Hazard Issue Template** to guide you through adding the necessary information.
4. Label according to Severity and Likelihood, then calculate Risk Level.
5. Assign to CSO REMOVED (@REMOVED)
6. Save by 'committing' to the repository.
7. Review and ensure complete.
8. Invite others to review and comment using @mention or by sharing the URL

Last update: May 4, 2023
Created: May 4, 2023

9. Determination of Medical Device eligibility

Determination of the class of medical device applicable was performed using the MHRA Medical Device Class tool on 20th October 2022 by REMOVED, with reference to relevant supporting documents and legislation.

It was determined that the Albert Health platform **does not** constitute a medical device.

9.1 References

- EU Exit and post-transition guidance, Regulation of Medical Devices Webinar - October 2020, webinar by MHRAgovuk on YouTube
- EU Medical Device Regulation (MDR)
- EU Declaration of Conformity
- CE Marking

Last update: May 4, 2023
Created: May 4, 2023

10. Security

Security is taken extremely seriously by this project and we are complying with the Data Security and Protection Toolkit (DSPT) which is part of latest NHS Digital Data Security Standards.

10.1 Deployment Security 'Code Chain'

10.1.1 Development machines

10.1.2 Code Repositories

10.1.3 Deployments of the server

10.1.4 Code 'Promotion' Safety Strategy

10.1.5 Cyber Essentials

Last update: May 4, 2023
Created: May 4, 2023

11. Third Party Tools Safety

11.1 List of Third Party Tools

11.2 Cloud Services Providers

Last update: May 4, 2023
Created: May 4, 2023