Medicus.

Clinical Safety Case Report (Safeguarding)

Table of Contents

Introduction

This document describes the clinical safety case for the implementation of the Medicus, a primary care system solution for the purposes of Safeguarding Case Management. It describes the clinical risk management activities including hazard assessment, Clinical Risk Evaluation and Clinical Risk Controls for the Medicus system to be deployed for the purposes of Safeguarding Case Management only.

It has been prepared in compliance with the NHS Digital standards as defined in the documents Clinical Safety Requirements DCB0129.

In England, the full Medicus product operates under the Tech Innovation Framework and is working towards being a complete primary care system, assuring against GP IT Futures Capabilities & Standards capability framework as a foundation solution.

The modules of this release of Medicus are categorised below:

- Platform & Infrastructure
- Authentication & Access Control
- Information Governance
- Patient Information Maintenance
- Safeguarding Case Management
- Interoperability

This document represents the clinical safety case for the solution. The various components of the solution are described in this document. This document needs to be considered in conjunction with the Hazard log which forms part of the compliance documentation for DCB0129:2018 - Clinical Risk Management; its Application in the manufacture of health IT system

Glossary of Terms

Term	Description
Acceptable	means an acceptable level of residual risk that may be accepted in a given context as categorised in the residual risk acceptance categories. A low rated risk based on severity and likelihood
Clinical Hazard	means a potential source of harm to a patient, or state of a system or an event, that presents the potential for such harm to arise.
Clinical Risk	Defined as the combination of the probability of the of a clinical hazard occurring and the impact of that occurrence
Clinical Risk Management	Management and assessment of any clinical hazards and clinical risks in relation to delivering and operating the solution. This involves placing emphasis on identifying circumstances where use of the Solution may put patients at risk of harm and proposing actions to prevent or control those risks.
Clinical Risk Management Activities	Means the clinical risk management activities carried out by the Supplier as part of CRMS.
Clinical Risk Management Products	Means the products related to clinical risk management which the supplier is required to deliver to the Healthcare Organisation such as the Safety Case and hazard Log as defined in the DCB0129 Standard
Clinical Risk Management System (CRMS)	Means the Supplier's document (process and documentation) which provides guidance supporting the requirements in terms of the due diligence and in the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling clinical risk.
Clinical Risk Management File	Repository of all records and other documents that are produced by the clinical risk management process. For Medicus this is through products from Atlassian including Jira and Confluence.
Clinical Safety	Freedom from unacceptable clinical risk to patients.
Clinical Safety Case	Accumulation and organisation of product and business process documentation and supporting evidence, through the lifecycle of a Health IT System.

Term	Description
Clinical Safety Case Report	A Report that presents the arguments and supporting evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment at a defined point in a Health IT System's lifecycle.
CSO	Clinical Safety Officer.
Deploying Organisation	Organisation that is deploying the Health IT System used for a healthcare purpose.
Frequency	A measure of the rate at which an event such as a clinical hazard might occur
Harm	Death, physical injury, psychological trauma and/or damage to the health or well-being of a patient.
Hazard	Potential source of harm to a patient.
Hazard Log	A mechanism for recording and communicating the on-going identification and resolution of hazards associated with a Health IT System.
Health Organisation	Organisation within which a Health IT System is deployed or used for a healthcare purpose.
Health IT System	Product used to provide electronic information for health or social care purposes. The product may be hardware, software or a combination.
Initial clinical risk	The clinical risk derived during clinical risk estimation taking into consideration any retained risk control measures.
Intended use	Use of a product, process or service in accordance with the specifications, instructions and information provided by the manufacturer to customers.
Likelihood	Measure of the occurrence of harm.
Lifecycle	All phases in the life of a Health IT System, from the initial conception to final decommissioning and disposal.
Patient safety	Freedom from harm to the patient.

Term	Description
Safety incident	Any unintended or unexpected incident which could have, or did, lead to harm for one or more patients receiving healthcare.
Safety Incident Management Log	Tool to record the reporting, management and resolution of safety incidents associated with a Health IT System.
Severity	Measure of the possible consequences of a hazard.

System Definition and Scope

Safeguarding services are fully integrated multi-agency teams that bring together key safeguarding agencies including professionals from social care, police, health and education. This enables the multi-agency team to appropriately review information systems, share all appropriate information in a secure environment, and ensure that the most appropriate response is provided to effectively safeguard and protect the at-risk person.

The team focuses on receiving referrals for persons believed to be at risk of significant harm, including domestic abuse. Each agency within the service has access to their own systems and share information as appropriate with key partners.

From this, we carried out our own analysis of the requirement and the current scope is:

- Tracing a patient on the PDS and then creating new safeguarding case
- Viewing all open cases
- Viewing the details of a single case
- Viewing the Shared Care Record for a patient
- Adding notes & documents to a safeguarding case
- Closing a safeguarding case

Intended use

Medicus is a patient record and workflow management system for use in primary care and will be considered a GP IT futures foundation solution in the future. For the purposes of this safety case, the intended use is for the management of safeguarding cases in a safeguarding service. Intended users of the Medicus system are all clinical and administrative involved with the Safeguarding management service.

It is not intended for use in private healthcare services or other jurisdictions.

Platform & Infrastructure

Platform & infrastructure is the term used to describe the underpinning technology stack that powers the features and functionality of Medicus.

Whilst platform & infrastructure is not a “module” of the product per se, it is relevant to the safety case because Medicus takes appropriate steps to ensure a reliable and resilient service.

Authentication & Access Control

Authentication & access control covers the features that authenticate a particular person to access the application (e.g. are the credentials provided to login correct?) and govern their access to specific parts of the system once authenticated.

Medicus operates a local authentication method which is a username and password. In addition to this, users can also login with NHS Smartcards (CIS2) as a trusted Single Sign On (SSO) provider.

For workflows that require access to NHS Spine Services (e.g. Personal Demographic Service), Medicus uses NHS Smartcards (CIS2) to obtain the necessary NHS API tokens that allow the user to perform the action or workflow.

Information Governance

As a clinical system that handles special category data, Medicus implements a large number of IG features to ensure good data governance and auditability.

Examples of this include:

- Legal audit logs that record every action taken
- Patient audit events to help users understand how a patient record has changed over time
- Privacy officer alerts for inactive patients

Patient Information Maintenance

Patient information maintenance includes features to identify patients (e.g. patient finder) and all active management of patient administrative, demographic and contact information.

Medicus is fully integrated with the NHS Personal Demographic Service (PDS) to help keep patient details up to date and accurate.

Safeguarding Case Management

The safeguarding case management module is a purpose-built feature to support safeguarding services manage their caseloads, including reviewing health records in a single, secure system.

It should be noted that the safeguarding case management module is not intended to replace the clinical or social care record of a particular patient.

Interoperability

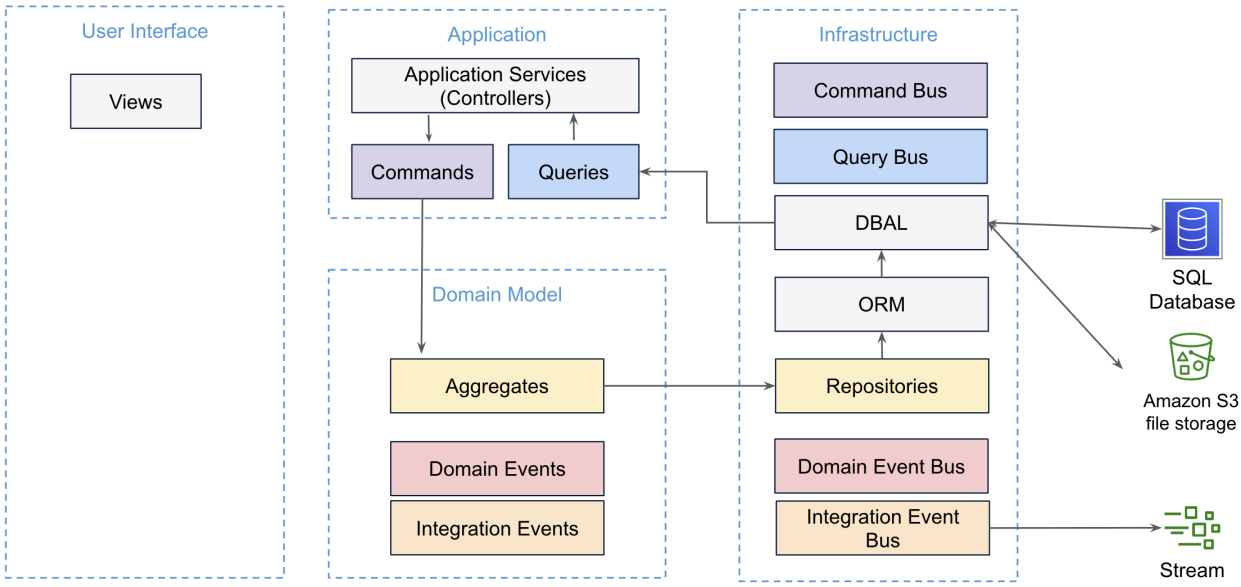
A key aim of Medicus is to support better interoperability between clinical systems and there are a number of integrations that we maintain that help healthcare professionals access the data they need regardless of system boundaries.

Currently these are:

- Intersystems Shared Care Record viewer

Technical Specifications

Medicus is a cloud-based monolithic application that uses a typical enterprise architecture pattern to separate concerns. It uses an orthogonal architecture that incorporates CQRS and DDD design patterns:

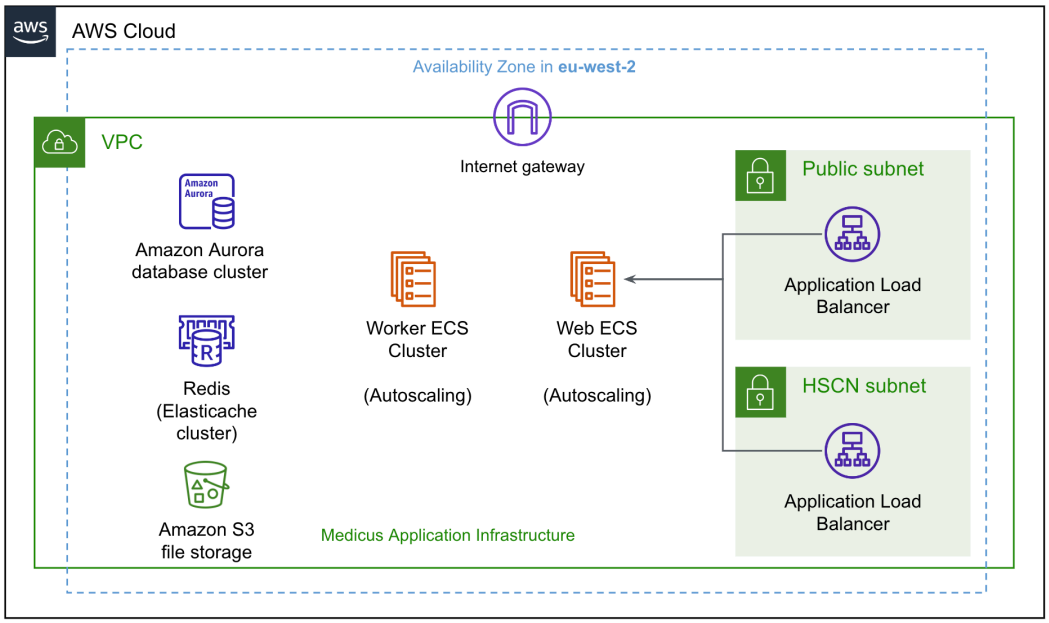


Separately, we maintain approximately 50 different standalone client libraries that are then incorporated into the main product.

The main technology stack is PHP (Symfony + Doctrine), PostgreSQL (RDS Aurora Serverless), deployed on AWS infrastructure using Terraform.

All infrastructure is stored as Terraform code in a git repository.

We operate two auto-scaling clusters of ECS instances, one to handle web (HTTP) requests, and a second to handle background jobs. The web cluster handle HTTP requests that route via an internet-facing load balancer, or via the HSCN-network load balancer.



Each healthcare organisation (tenant) has their own database on the AWS Aurora database cluster. This means that the persistence layer is single-tenanted, but the infrastructure is shared & multi-tenanted. All data is in the AWS London data centre (eu-west-2) in a managed RDS database and files are held in Amazon S3.

Dependencies

Medicus has some intrinsic dependencies based around how the solution is architected using cloud-based infrastructure such as Amazon Web Services. These are considered as system wide risks and are mitigated by the high availability nature of their operation:

- ECS uses multiple containers running across multiple availability zones behind a load balancer which automatically detects and removes any containers that fail the “health check”
- RDS (PostgreSQL Database) uses at least 1 read replica in a Multi-AZ cluster, with automatic failover if the main node fails
- ElastiCache (Redis) uses 2 nodes in a cluster with automatic failover
- Amazon S3 (File Storage) is already architected for extreme high availability as part of this AWS managed service

The extrinsic dependencies for Medicus primarily revolve around NHS Spine services which certain functionality relies upon. The NHS Spine services are high availability services, so the potential risk of system wide un-availability is reduced.

These risks are highlighted in the hazard log but are largely beyond the scope of the safety case.

Information Security

We take information security very seriously at Medicus and are proud to exceed the industry standard when it comes to information security. We are fully accredited against ISO 27001:2013 and have completed the NHS Digital Data Security and Protection Toolkit assessment.

We conduct regular penetration tests to identify and manage vulnerabilities.

Our ICO registration number is ZA625889.

Business Continuity

Business continuity is the joint responsibility of Medicus Health and each deploying GP practice, i.e. both organisations are expected to have the appropriate Business Continuity Plans in place in the event of the system being down for any reason.

We have been fully assured by NHS Digital against the Business Continuity and Disaster Recovery GP IT Futures standard.

Clinical Risk Management System

The Medicus Clinical Risk Management system outlines the overall approach to risk management taken by Medicus Health throughout the design and manufacturing of the Medicus system. Documentation is maintained, tracked and auditable. All risk management analysis and activities are also recorded and maintained in an appropriately secured enterprise cloud environment.

In summary the Clinical Risk Management System facilitates the Medicus Clinical Risk Management Plan which include includes:

- Planned risk management and identification activities.
- Assignment of responsibilities and authorities;
- Requirements for review and approval of risk management activities;
- Criteria for risk acceptability (Risk Matrix, risk-benefit analysis, etc.);
- Verification and validation activities;
- Collecting and review of production and post-production information;
- Documentation, reports and records.

Clinical Risk Management Team

- Dr Imran Khan (Clinical Safety Officer)
- Tim Gray (Chief Product Officer)
- Emile Axelrad (Acting Chief Technology Officer)
- Stephen Higgins (Head of Integrations)

Clinical Risk Management System Roles and Responsibilities

Quality and Compliance	● Establishes and maintains all risk management procedures and forms as part of the MH QMS
Product Development Team	● Ensures Design, Process and Software Risk Management procedures are followed, and activities are planned into projects and SDLC ● Leads and participates in all risk management activities ● Develops and maintains Hazard and Risk Logs ● Maintains Risk Management File
Clinical Safety Officer (within Product Development)	● Establishes Risk Management Plan ● Participates and guides in all risk management activities ● Assures all risks are identified, documented and mitigated to an acceptable level ● Provides clinical safety authorisation to proceed ● Develops Risk Management Reports and Safety Release Notifications ● Obtains Executive Management approvals

Business Management and senior leadership team	● Approval of Risk Management Plan and Risk Management Reports ● Approval of Safety Release Notifications

Clinical Risk Management Plan

Medicus has established and a clinical risk management plan that assessed each individual component of the system. The purpose is to carry out and identify clinical risk management activities that are required to be undertaken during the implementation and deployment of the system into the receiving health organisation.

A range of techniques applied at stages will be used to identify, assess and manage hazards including:

- **Preliminary Hazard Identification** – early, requirements-based hazard identification using known hazard checklists, subject matter expert reviews, medical device databases, past incidents/post market surveillance, literature reviews, clinical studies and brainstorming techniques such as Structured What If Technique (SWIFT).
- **Functional Hazard Identification** - systematic, end to end, step by step walkthrough of entire system, identifying potential failure modes and failure points using Functional Failure Analysis and Hierarchical Task Analysis (HTA).
- **Risk Analysis** - detailed analysis of all identified hazards including identification of cause-hazard-consequence sequences, identification of existing safeguards and an assessment of pre-control/ mitigation risk class.
- **Risk Control** – identification of design controls required to bring risks down to within tolerance.
- **Risk Evaluation** – final evaluation of residual risk demonstrating risk acceptance.
- **Risk Closure** – identification of overall safety case based on evidence and argument and summarised in the Risk Management Report.

Clinical risk criteria used to estimate clinical risk is as described in the DCB0129:2018 - Clinical Risk Management; its Application in the manufacture of health IT systems to evaluate the acceptability of the clinical risk.

All clinical risk activities documentation need to be approved by a member of the Senior Management Team and the Clinical Safety Officer.

Clinical Risk Analysis

The Clinical Safety Officer will ensure that the clinical risk management activities are implemented as documented in the Clinical Risk Management Plan. Due to the size and complexity of the Medicus product, risk analysis has been carried out by a number of different subject matter experts, Clinical Safety Officers, Technical Architects, Product Engineers and integration specialists from organisations such as NHS Digital.

Clinicians that will use Health IT System after deployment have been included in the process. Part of the PCTL Day one Lab was the involvement of a diverse set of expertise to more likely to result in hazards being identified which may have otherwise been missed.

Safeguarding Case Management Clinical Risk Scope

The clinical scope of Medicus product for Safeguarding Case Management and the Hazard analysis for this safety case is confined to:

- Its use for Safeguarding Case Management only.
- Each component of the Medicus product that has been considered to provide the Safeguarding Case Management solution.
- Third party application integration is limited to Intersystems Shared Care Record viewer and extrinsic systems described in the dependencies section of this document. There will be no “write back” to and external clinical system. Access to external records is limited to read only access to the Intersystems Shared Care Record and no clinical or personal information is cached or stored within the Medicus system.

There is no formal data migration and therefore existing data will be transferred manually by the healthcare organisation. This transfer is out of scope of this safety case.

The healthcare organisation is required to ensure that it has considered the use of Medicus system and its effect on current business processes through the application of the DCB0160. This consideration is also out of scope of this safety case.

Hazard Log

Medicus maintains a live hazard log which reflects the entire Medicus system. Hazards are tracked internally as issues in the clinical risk management system. The hazards can be grouped into functional areas if required. The hazard log currently consists of a total of 32 issues (hazards & causes) which were identified by the clinical safety management system process. Contextual details and supporting document references are referred to in the hazard log for completeness.

The hazard log itself is maintained in line with the expectations of DCB0129:2018 - Clinical Risk Management; its Application in the manufacture of health IT systems.

This hazard log is limited in scope to the hazards related to safeguarding services.

This includes the following hazards

Key	Summary	Status
HAZ-286	User views out of date information on Intersystems Shared Care Record	LIVE
HAZ-280	User can incorrectly interact with NHS Spine services	LIVE
HAZ-276	User can access restricted areas for their role	LIVE

Key	Summary	Status
HAZ-275	User has access to Medicus but cannot access the areas they need	LIVE
HAZ-239	User is unable to interact with NHS Spine services	LIVE
HAZ-237	Local Medicus record not updated correctly from PDS	LIVE
HAZ-221	User unable to view the Intersystems Shared Care Record	LIVE
HAZ-195	Patient misidentification or incorrect patient identification when using PDS	LIVE
HAZ-178	Delay in processing safeguarding case	LIVE
HAZ-66	Patient misidentification or inability to identify patient	LIVE
HAZ-65	User is incorrectly given access to Medicus	LIVE
HAZ-60	Medicus is unavailable	LIVE

12 issues

Clinical Risk Control

Risk control options have been considered for each hazard and cause that has been evaluated. Whilst risk reduction might not be required in all cases as the initial risk is acceptable, all risks have been considered.

Clinical risk control measures have been utilised to reduce the likelihood of a hazard occurring. With most of the hazards in the safeguarding management cases, risk control measures can reduce the likelihood but in most cases the severity remains unchanged.

Risk reduction has been considered throughout the development of Medicus. This has been considered in line with the DCB0129 namely:

1. The design of the system has been tailored to minimise the likelihood of a hazard.
2. Extensive testing and validation as described in the testing section of this document
3. Description of the business processes that must be followed to minimise risk and operate the product as it was intended.
4. Training to ensure staff are aware of how the product can operate and the conditions under which undesirable risk may arise.

Medicus will provide the required training and documentation to ensure that the organisation can mitigate the risks to an acceptable level as described in the hazard log.

With the risk controls in place, Medicus considers the level of risk to be acceptable.

Testing

When developing Medicus, we implement a range of testing techniques to ensure high product quality and protect against code defects.

Testing requirements are outlined in a Product Requirement Document (PRD) on Confluence along with the specification for how the feature should work.

The main technique we rely on is automated testing because it is the most scalable way to reduce risk on a product so complicated. When writing tests, our main priority is maximum coverage for all workflows and all points of entry into these workflows.

In addition to automated testing, we also:

- Perform manual acceptance testing
- Perform Peer Code Review on every Github Pull Request
- Perform automated visual regression testing on front end components (e.g. buttons)
- Run static code analysis on Github Pull Requests
- Enforce that all automated tests pass on a Github feature branch before allowing the code to be merged back into the main branch
- Undergo assurance with NHS Digital

Medicus embraces a culture of continuous improvement of our test processes. As part of our agile development cycles and management system reviews, we look to identify opportunities for improvement and incorporate them into our processes. This leads to improvements in the speed of running our tests, the tooling in our CI environment, the documentation of our tests and the technical tooling for writing and debugging tests.

Wherever possible, when fixing a defect or bug, we look to implement not just a fix, but also to add or modify an automated regression test to ensure that the defect can never re-occur.

Full details are available in the Medicus Test Traceability Report.

Quality Management

Medicus takes a systematic approach to quality for the software we offer to our customers. All members of the Medicus team adhere to our documented procedures for software development, testing & quality assurance (part of our Software Quality Management System) and release/deployment (part of our Service Management System).

This includes approval processes for new development, minimum testing expectations and standard operating procedures for how we release new versions of the product to customers.

Safety Incident Management

In line with our Patient Safety Incident Response Plan, we strongly encourage customers to report clinical safety incidents or near misses to us so that we can document, review, learn and take action as required. Patient safety is of paramount important to us and we seek to draw lessons learnt from every incident rather than attribute blame.

All incidents can be reported via our Service Desk (support@medicus.health) and will be escalated appropriately to the Chief Product Officer & Clinical Safety Officer.

Where appropriate, we will report incidents to NHS Digital via the Learn from patient safety events service (LFPSE) to improve safety understanding for other clinical systems as well.

Summary Safety Statement

Medicus has been evaluated against the intended use and a hazard and risk assessment has been performed by a multi-disciplinary team.

Further to the Medicus hazard assessment, a total of 12 hazards have been identified and analysed for safety risk.

- Residual risk for all 12 hazards has been reduced as far as possible (AFAP), pending further assurance and testing.
- 12 out of 12 hazards are within Medicus Health's risk tolerance range.
- 0 out of 12 hazards are outside of Medicus Health's risk acceptance criteria.

It is an important that all healthcare Organisations deploying Medicus Safeguarding Case Management perform a DCB0160 hazard assessment for the Medicus system, focused on usability, configuration, and understanding how they may mitigate the risks within their own organisation. The use of the Medicus Safeguarding Case Management for purposes other than that described in this safety case are considered out of scope and potentially could introduce unacceptable levels of risk.

Medicus will operate a clinical risk management system and incident management system throughout the lifecycle of the product. Medicus considers the product safe to use for Safeguarding Case Management.

Document Control

Approval

Name	Role	Date
Dr Imran Khan	Clinical Safety Officer	9th December 2022

Version History

Version	Date	Revision	Author
1.0	9th December 2022	Review and Approve Document	Tim Gray