Medicus.

Clinical Safety Case Report

Table of Contents

⚠ Commercial confidential

⚠ This is a controlled document.

Introduction

This Safety Case Report outlines the clinical risk management activities, including the hazard and risk analysis that underpin the safety case for the Medicus Electronic Patient Record (EPR).

This document also needs to be considered in conjunction with the Hazard Log, which provides **a** detailed breakdown of the risk analysis and controls that have been implemented by Medicus Health, or should be implemented by the deploying organisation.

To support deploying organisations in considering all risks, we also provide a summary of the high level risks and suggested controls but this is outside of the scope of DCB0129 and not a subsitute for the Hazard Log.

Purpose of this Document

This document describes how Medicus Health has conducted clinical risk management to ensure patient safety with respect to the Medicus EPR, and the activities that occur to ensure we meet the requirements of DCB0129.

The DCB0129 standard focuses on clinical risk management undertaken by Medicus Health. It involves identifying potential hazards, assessing risks, and documenting risk control measures in a Safety Case and Hazard Log. These documents provide a detailed analysis of the system's safety profile, including identified hazards, risk mitigation strategies, and residual risks.

When transitioning from manufacturing to deployment and use, as governed by DCB0160, these DCB0129 documents become important inputs. The DCB0129 Safety Case and Hazard Log offer an understanding of the risks associated with the Health IT System and the controls implemented and required to mitigate these risks.

The documented risk control measures in the DCB0129 safety case form the foundation for the deploying organisation to ensure the correct training is undertaken, and in developing Standard Operating Procedures (SOPs) and Business Continuity Plans (BCPs) required by DCB0160. This integration ensures that the safety measures designed during the manufacturing phase are effectively implemented during deployment and use.

This document does not detail how a deploying health organisation should conduct the DCB0160 but does recommend it conducts it in accordance with the DCB0160 standard.

Scope

The scope of this Clinical Safety Case is the Medicus EPR Version 1.6 (including all minor and patch versions e.g. 1.6.1.0).

Medicus is a single product with multiple modules. The modules vary based on the intended use and type of healthcare organisation.

The version number referenced in this Safety Case Report will always reflect the overall product version.

Interoperability is an integral part of a functioning healthcare system and Medicus is integrated with a number of third party systems to provide the service our customers need. Where these integrations present a clinical risk, the risk is documented in our Hazard Log.

For the purpose of clinical risk management, the scope of interoperability is limited to the data or clinical workflows processed within the Medicus infrastructure. Once data leaves the Medicus infrastructure, the risk is transferred to the third party system.

Relevant Standards

The following standards are relevant to the Medicus Clinical Risk Management System:

- DCB0129
- DCB0160
- ISO 20000:2018
- ISO 27001:2022
- UK Medical Device Regulations 2002 (Device registration record: https://pard.mhra.gov.uk/manufacturer-details/114289)

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.

Term	Description
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.
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

Term	Description
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.
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.

Executive Summary Safety Statement

[Dr Imran Khan, Clinical Safety Officer]

This Safety Case Report is designed to be iteratively updated as new capabilities of the Medicus EPR are introduced. This version represents a progressive enhancement of the clinical risk management activities aligned with the latest software release of the Medicus EPR.

Clinical risk management has been conducted in accordance with the DCB0129 standard, and all hazards associated with the Medicus EPR have been systematically identified, assessed, and documented within the accompanying Hazard Log (Appendix A).

The section titled “Hazard Log Change History” provides details specific to the updates captured in this version of the Safety Case, including any new or modified workflows, along with clarification of existing hazards impacted by these changes and any newly identified hazards.

The table below summarises the outcomes of the clinical risk management activities. It shows the total hazards identified and evaluated. The residual risk associated with each cause or hazardous situation has been assessed, and the resulting risk profile for the software version above is presented below:

Risk Rating	Definition	Initial	Residual
5	Unacceptable level of risk	**0**	**0**
4	Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level	**0**	**0**
3	Undesirable level of risk. Attempts should be made to eliminate the hazard or implement control measures to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical	**74**	**0**
2	Acceptable where cost of further reduction outweighs benefits gained or where further risk reduction is impractical	**23**	**92**
1	Acceptable, no further action required	**3**	**8**
Total		**100**	**100**

⚠ **Please note:** There are hazards above which initially represent undesirable risks that require practice training, and/or business processes to reduce the risk to an acceptable level.

> These risks are therefore transferred to the deploying organisation. There is an assumption that the deploying healthcare organisation carries out a careful assessment of these transferred risks as described in the DCB0160 to assure themselves they have reduced the risk to an acceptable level. It is the responsibility of the deploying healthcare organisation to consider all hazards and suggested controls to ensure that they have appropriate local processes in place. To help with this, please refer to the full Hazard Log.

System Definition / Overview

Overview

In England, Medicus is procured under the Tech Innovation Framework and assures against the Digital Care Services Capabilities & Standards as a foundation solution for use in GP Practices.

Appendix C - NHS DSIC (Digital Services for Integrated Care) Catalogue Capability & Standards Mapping contains a detailed breakdown of the assured standards for deployment within this release, including a mapping to the Medicus modules.

Intended Use

The broader system itself has been architected in a way that ensures transferability between different healthcare settings and functionality is turned on/off based on the type of deploying organisation.

For the purpose of this Clinical Safety Case, Medicus is intended to be used by all staff (clinical or otherwise) in primary healthcare settings.

The system is designed to be a complete solution for the organisation's record keeping, workflow/process management, reporting & data returns and, interoperability with interfaces outside of the organisation.

System Modules

This table outlines the broad modules of the Medicus clinical system.

Core Modules

Platform & Infrastructure	Organisation Configuration	Data Migration
Staff & User Management	Information Governance	Patient Registration (incl. GP2GP)
Patient Information Maintenance	Communications	Front Door
Scheduling & Appointments	Consultations & Care Record	Prescribing & Medicines Management

Referrals	Investigation Requesting & Results	Workflow
Population Health Management	Vaccinations	Reporting & Data Returns
Inbound Referrals & Case Management	Panic Button	

Interoperability Modules

NHS App / Other PFS Apps	Diagnostic Device Integrations	Local Shared Care Record Data Provider
Summary Care Record Data Provider	GP Connect Access Record Data Provider	

Core Modules

Each of the core modules is explained below.

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 we take appropriate steps to ensure a reliable and resilient service.

Organisation Configuration

The organisation configuration module contains functionality to setup and maintain basic information about the organisation (e.g. name, correspondence address) that are used in other parts of the system. It also includes specific credentials or configuration for integration workflows such as the NHS Message Exchange for Social Care and Health (MESH) interoperability mechanism.

Data Migration

The data migration module deals with practice migrations from other clinical systems.

Currently, Medicus can migrate GP Practices from:

- Cegedim Vision
- EMIS Web

- TPP SystmOne
- Advanced Docman 10

During the implementation phase we discuss the Data Migration Process with each GP Practice to ensure all parties understand what is involved. It would not be appropriate to detail the whole process within this Safety Case Report however, Appendix J, K, L & M give a general overview of the activities undertaken (including validation exercises).

Please note the statement on transfer of data recorded inside a consultation template within TPP SystmOne (Appendix M).

Staff & User Management

The user management module contains the features that govern staff access to Medicus (e.g. are the credentials provided to login correct? What permissions do they have?)

Medicus supports multiple authentication methods, including Multi-Factor Authentication (MFA) using authenticator apps or 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 has a large number of IG features to ensure good data governance and auditability.

This includes:

- 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
- Permission to view recording when accessing external care records such as the Summary Care Record & GP Connect record
- Record snapshots to view patient's record on a previous date
- Functionality to mark record elements as confidential from third parties, redacted from patient online access or redacted due to RCGP exclusion set rules

Patient Registration (incl. GP2GP)

One of the key administrative functions of Medicus is managing the inbound flow of patient registrations (and outbound flow of de-registrations). The patient registration module handles all of the features that a practice needs to register patients, permanent or otherwise.

This module also includes GP2GP functionality to request the patient's EHR from the previous GP practice and integrate it into Medicus for onward use.

Patient Information Maintenance

The patient information maintenance module contains functionality such as identify patients (e.g. patient finder) and management of patient administrative, demographic or contact information.

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

This module also covers the management of proxy access to online services, including the recording of patient contacts, their verified relationship to the patient, the legal basis for access, the scope of permissions granted, and the end date of access.

Communications

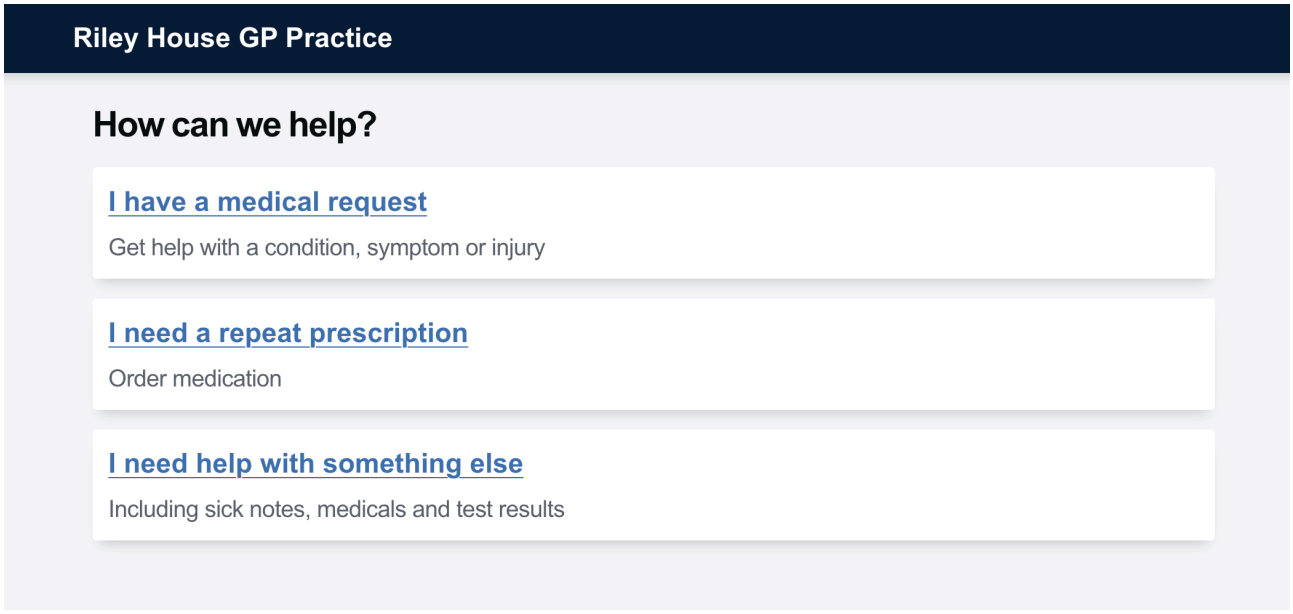
The communications module deals with everything related to communicating with patients, including but not limited to asynchronous communication channels like SMS or email, and synchronous channels such as telephony.

The module is a foundation for several other modules such as appointments, care consultations, or front door.

Front Door

The front door module is designed to support practices manage the flow of inbound patient requests on the day. This includes online consultation requests or administrative queries.

One of main features of the front door module is the Medicus patient portal which is unique to each organisation and can be hosted from their website. The patient portal allows patients to access the service via the web.



Note: The patient portal is the same product as the Medicus clinical system but architected using a lightweight user interface (e.g. minimal Javascript) for low quality devices or internet connections.

There is a large overlap between the patient communications, scheduling & appointment management, prescribing and consultations & care record modules.

Scheduling & Appointments

The scheduling & appointments module contains features to schedule staff, rooms or configure appointment availability, including the type of service being offered and the mode of delivery (e.g. face to face vs telephone),

The module also covers appointment booking and ongoing management (including cross organisation booking), including on the day appointment workflows such as arriving patients ready for their consultation.

Consultations & Care Record

Maintaining a repository of patient care records is one of the primary functions of a system like Medicus.

The phrase “Consultations & Care Record” is used to describe the recording of all clinical information except for medication, referrals and investigation results (which have their own modules due to complexity and safety considerations). Examples include consultation notes, allergy information and problems.

The patient’s “Journal” view provides a temporal history of the patient’s care and SNOMED CT is the native clinical coding taxonomy used throughout the care record.

Prescribing & Medicines Management

The prescribing module contains the functionality for clinicians to manage the medication regimens of patients, such as creating new prescriptions, sending them to a pharmacy via the NHS Electronic Prescription Service for collection, or conducting medication reviews and adjusting the patient's plan accordingly.

Decision support is provided at the point of prescribing to improve safety and the following checks are supported:

- Allergy and sensitivity checking
- Age, sex & condition contraindications, precautions or warnings
- Pharmacological equivalents - duplicate therapy, ingredients or drug equivalents
- Interactions with other medication
- High risk messages such as those issues by the MHRA

The majority of this data is provided by FDB Multilex and then integrated into Medicus so that no external calls are made to third party services.

Referrals

The referrals module contains the functionality for healthcare organisations to manage the referral pathways of patients who are being sent for further care elsewhere (e.g. to the hospital for a specialist assessment).

Investigation Requesting & Results

The investigation requesting & results module allows practitioners to manage the process of requesting investigations (pathology and imaging), including integrations with lab order systems such as Clinisys ICE.

Results are typically received via MESH using standardised NHS Edifact formats and then integrated into the workflow module for review and filing.

Workflow

The workflow module spans across the entire system to bring all work into a single place so that it can be easily tracked and managed.

Largely focussed around the creation of "tasks", the workflow management module is a key clinical safety control to ensure that important work isn't hidden or missed.

A centralised module displays all tasks for the healthcare organisation and there are more specific features across the system to view specific task information (e.g. All tasks assigned to my team or only specific types of task).

Each user's homepage is optimised to display all of the things that are assigned to them and pending completion.

The workflow modules also describes the features available for healthcare organisations to manage outbound and inbound document workflows (e.g. scanning post).

The module includes other features such as instant messaging (Medicus chat).

Population Health Management

The population health management module provides the functionality for practices to monitor patients requiring active management of their conditions (e.g. Asthma, Diabetes). This includes registers of patients, dashboards to monitor what needs to be done and, for whom.

The module handles all statutory reporting of QOF, Local Enhanced Services and other contractual requirements.

Vaccinations

The vaccinations module is a specialist module to deal with adherance to the national vaccination programme and other vaccination related features.

The module utilises a lot of the building blocks of consultations & care record or long term condtion management.

Reporting & Data Returns

In addition to providing relevant record keeping and workflow management tools for healthcare organisation, Medicus is also used to query the vast amounts of healthcare data stored within the database of each organisation (tenant).

The reporting and data returns area covers bespoke reports created by the practice and some NHS England data exports such as General Practice Appointments Data (GPAD) and other bulk data extracts.

Inbound Referrals & Case Management

The inbound referrals & case management module allows practices who operate additional healthcare services to effectively manage and treat these patients. For example, community diagnostic services.

Panic Button

The panic button module provides specialist functionality to trigger urgent requests for assistance via both physical (fixed to the desk) and virtual (available in-app) buttons.

Interoperability Modules

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.

This includes but is not limited to:

NHS App / Other PFS Apps

As well as being a user-facing application that is used at the point of care by clinicians, Medicus is also a platform for patients to interact with their health record and to perform actions such as managing their appointments or prescriptions. This includes the NHS app.

Where proxy access has been configured, authorised proxies may also interact with the patient's record via PFS. Medicus records a log of GP Connect PFS access activity per patient.

Medicus also integrates with the NHS Login (Users endpoint and Provisioning endpoint) by allowing users to see a patient's current NHS login account details or provision a P9 verified NHS login account or upgrade an existing account to P9.

Diagnostic Device Integrations

The diagnostic device integration module allows practices to connect some of the hardware based diagnostic devices in use such as blood pressure & ECG machines.

Local Shared Care Record Data Provider

Different regions have their own local Shared Care Record programme to join up the different patient records from across healthcare providers. Each region typically uses a different shared care record provider and there is a need for Medicus as a master clinical system to provide data feeds to support local shared care.

Summary Care Record Data Provider

The NHS Summary Care Record is a national programme to create an electronic record of important patient information, created from GP medical records. Summary Care Records can be seen and used by authorised staff in other areas of the health and care system involved in a patient's direct care.

https://digital.nhs.uk/services/summary-care-records-scr

The requirements for the Medicus Summary Care Record integration are provided and assured by NHS England.

NHS England performed their own hazard assessment on the Summary Care Record interoperability standard and considered these hazards when specifying the requirements for system suppliers.

During the assurance process, the NHS Summary Care Record Team verified that we have:

1. Mitigated all risks specified in the Summary Care Record Risk Log
2. Satisfied all clinical scenarios in the CMV Clinical Assurance Test Scripts
3. Met all of the GP Summary Requirements Refactored for SCR FHIR API v6.0

4. Controlled all known clinical Hazards to acceptable risk tolerance level by implementing the design controls specified by the Summary Care Record programme or other forms of control

There is an assumption that consuming healthcare organisations are able to operate without the Summary Care Record or confirm information with patients themselves (or relatives/carers) if needed.

GP Connect Access Record Data Provider

GP Connect allows authorised health and social care workers in a variety of care settings to access their patients' GP records.

https://digital.nhs.uk/services/gp-connect

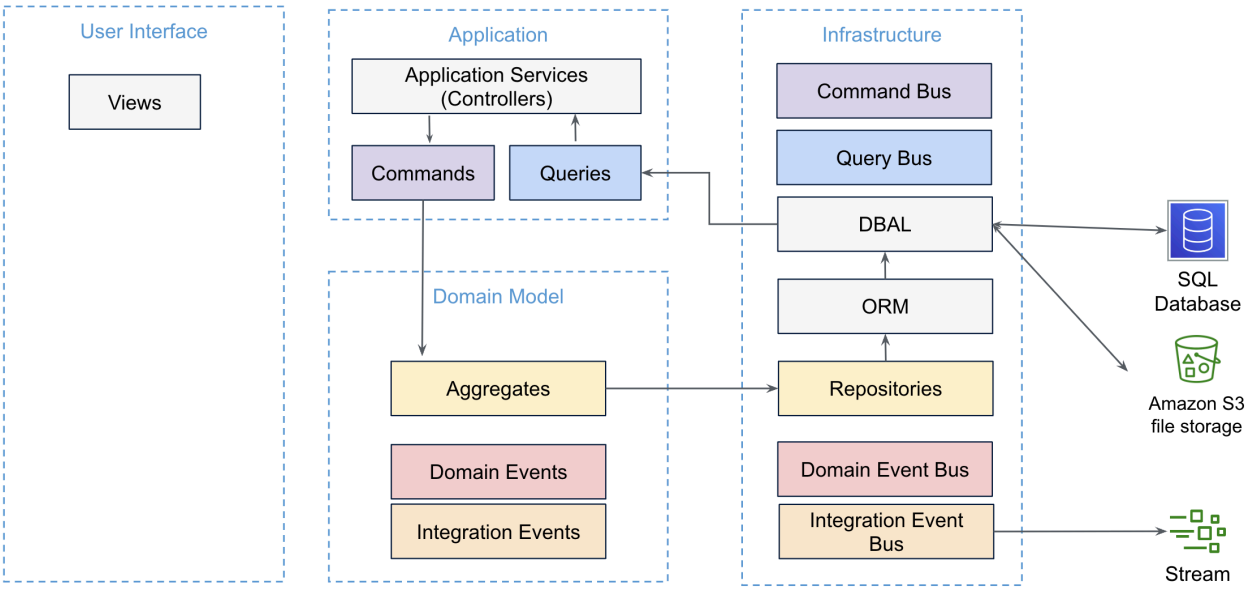
The requirements for the Medicus GP Connect Access Record integration (Structured & HTML) are provided and assured by NHS England.

During the assurance process, the NHS GP Connect Team verified that we have:

1. Implemented a Data Provider API that passes all tests in the Automated Test Suites
2. Satisfied all scenarios in the Manual Test Packs
3. Met all of the GP Connect 1.6.0 non-functional and IG requirements
4. Controlled all known clinical Hazards to acceptable risk tolerance level by implementing the design controls specified by the GP Connect programme or other forms of control

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:

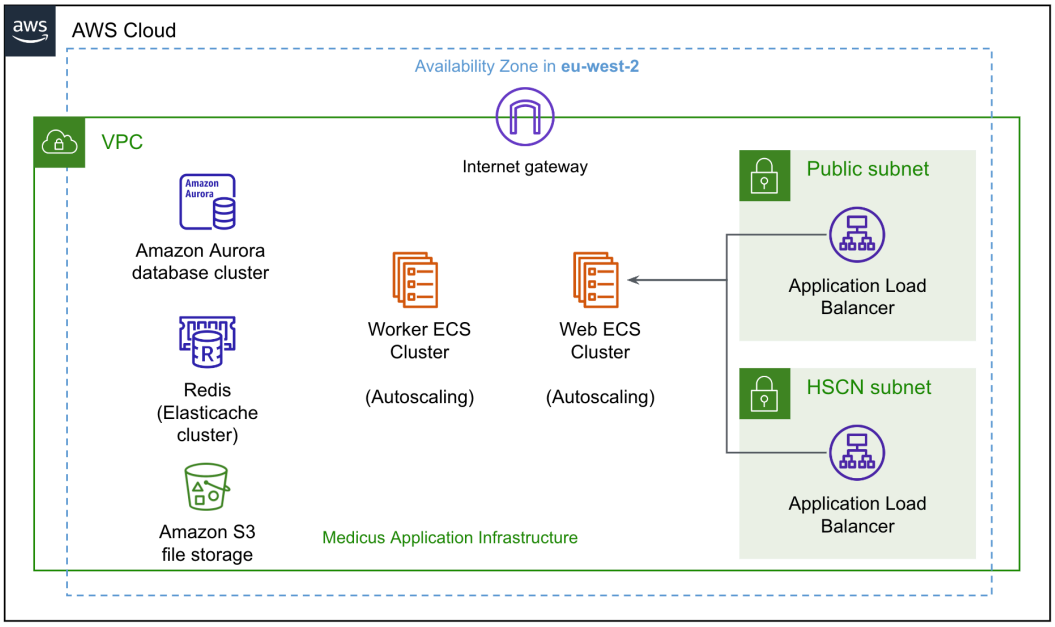


Separately, we maintain approximately 50 different standalone client libraries that are then incorporated into the main product.

The main technology stack is PHP (Symfony + Doctrine), PostgreSQL (Relational Database Service (RDS) Aurora Serverless), deployed on Amazon Web Services (AWS) infrastructure using Terraform.

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

We operate two auto-scaling clusters of Elastic Container Service (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.

Physical or Virtual Panic Button

Medicus has implemented both a virtual and physical panic button and integrated it within the system and the risks associated with each are highlighted in the hazard log.

However, it should be noted that the virtual panic button can be used without either the physical button or the desktop being installed. There are inherent risks to this as the chance of an alert received decreases considerably as a user would have to have the web app open and in focus to receive the alert.

The physical button and desktop application are architected to ensure the highest possible chance of a panic or emergency button triggering an alert and getting a response.

Medicus therefore recommends health organisations install the desktop application to minimise the risk of alerts being missed. If not, the deploying health organisation would need to carry out further risk assessments (under their own DCB0160) to assess the acceptability of this risk to their organisation.

Third Party Integrations

Medicus is integrated with a number of third party products to deliver the service. The integrations mentioned below are more tightly integrated than others and have been called out as such. Hazards relating to any integrations are covered in the Medicus Hazard Log as appropriate.

FDB Multilex ASCII Data Files

Medicus uses the ASCII data files product, offered by First Data Bank (FDB) to offer prescribing decision support and dose suggestions.

The clinician considerations behind using the Multilex product are:

1. Maintaining a comprehensive drug and decision support database is not within the current experience of Medicus as a new system supplier and therefore we chose to use a product recommended to us by others in the industry. FDB is a large and reputable supplier of clinical content relating to medicines and prescribing decision support
2. Upon inspection of the clinical risk management procedures in place at First Data Bank, we are happy that has a clinical risk management system compliant with DCB0129 and have provided us with their Clinical Safety Case Report as evidence

3. Since February 2023, FDB has been compliant with ISO 13485:2016 - https://www.fdbhealth.co.uk/about-us/press-releases/2023-02-20-fdb-achieves-iso-13485-2016-certification

NHS England Interoperability APIs

Medicus is integrated with a range of APIs provided by NHS England to fulfil mandatory requirements of a foundation clinical system. These include services such as Electronic Prescribing, Electronic Referrals and Summary Care Record.

NHS England assumes the responsibility for operation and maintenance of these APIs and acts as an accreditation body for the use of these APIs in Medicus.

Clinical Content

Clinical content such as consultation templates, patient queries (e.g. patients with Asthma) and other content based on national guidelines can improve the standardisation and safety of patient care.

Medicus holds partnership agreement with relevant providers to enable GP Practices to use their content within the product. The provider themselves hold the relevant certifications in both clinical safety and information security to meet our high standards.

From a clinical risk management perspective, any functionality that powers third party content is controlled by Medicus and the content itself is the responsibility of the third party provider in their own safety case.

Information Security

We take information security very seriously and are proud to exceed the industry standard when it comes to information security. We are fully accredited against ISO 27001:2022 and have completed the NHS Digital Data Security and Protection Toolkit assessment (YGMYW).

We conduct regular penetration tests to identify and manage vulnerabilities.

Our ICO registration number is ZA625889.

We have also been fully assured by NHS England against the Information Governance GP IT Futures overarching standard.

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 processes in place in the event of the system being down for any reason.

We maintain an ISO 27001 compliant Information Security Management System and an ISO 20000 compliant Service Management System, both of which have been fully audited by Lloyds Register on behalf of UKAS.

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

Medicus as a Medical Device

Medicus Health is managed as a Class 1 Digital Medical Device as set out in its Declaration of Conformity (UK MDR 2002). The products covered in this document are in conformance with the requirements of Medical Devices Regulations 2002 (SI 2002 No 618, as amended) (UK MDR 2002).

Medicus as an entire product is considered and controlled as a medical device rather than individual aspects or modules of the product.

Clinical Risk Management System

Our Clinical Risk Management System (CRMS) is used to manage the overall approach to risk management during the ongoing the design and development of Medicus.

Documentation is maintained, tracked and auditable, including risk management analysis and activities in an appropriately secured enterprise cloud environment.

Roles and Responsibilities

Role	Responsibilities
CEO	• Accountable officer for regulatory compliance and assurance • Agree on the clinical safety management process at an executive level
Clinical Safety Officer	• Ensure that clinical risk management activities are completed in accordance with the Clinical Risk Management Plan • Review and approve of all safety documentation including Clinical Safety Case Reports and Hazard Logs • Review of evidence in the Clinical Risk Management File to ensure it is complete and supports the Clinical Safety Case Report

Quality Assurance Lead	• Lead the clinical quality assurance team in checking and testing new functionality or updates/fixes to existing functionality • Ensure risk control processes are applied correctly • Ensure hazard log and incident logs are updated in accordance with processes. • Assist in analysing the root cause of significant events and work with the clinical and development teams to implement timely fixes/ updates
Product Lead	• Responsible for defining requirements and managing the development of changes/updates • Ensure clinical risk control procedures are followed throughout the development of the product. This includes product fixes and new features • Assist in analysing the root cause of significant events and work with the clinical and development teams to implement timely fixes/ updates
Engineering Lead	• Agree on top-level clinical risk management processes in agreement with the CSO • Ensure clinical risk control procedures are followed and reviewed/ implemented to reflect best practice • Responsible for submission to regulatory authorities for quality and service management • Facilitate required actions from analysing the root cause of significant events
Subject Matter Experts (inc. Clinical)	• Provide context and insight into clinical risk management activities

Top Management

The following people are accountable for the operation of the Medicus Health CRMS:

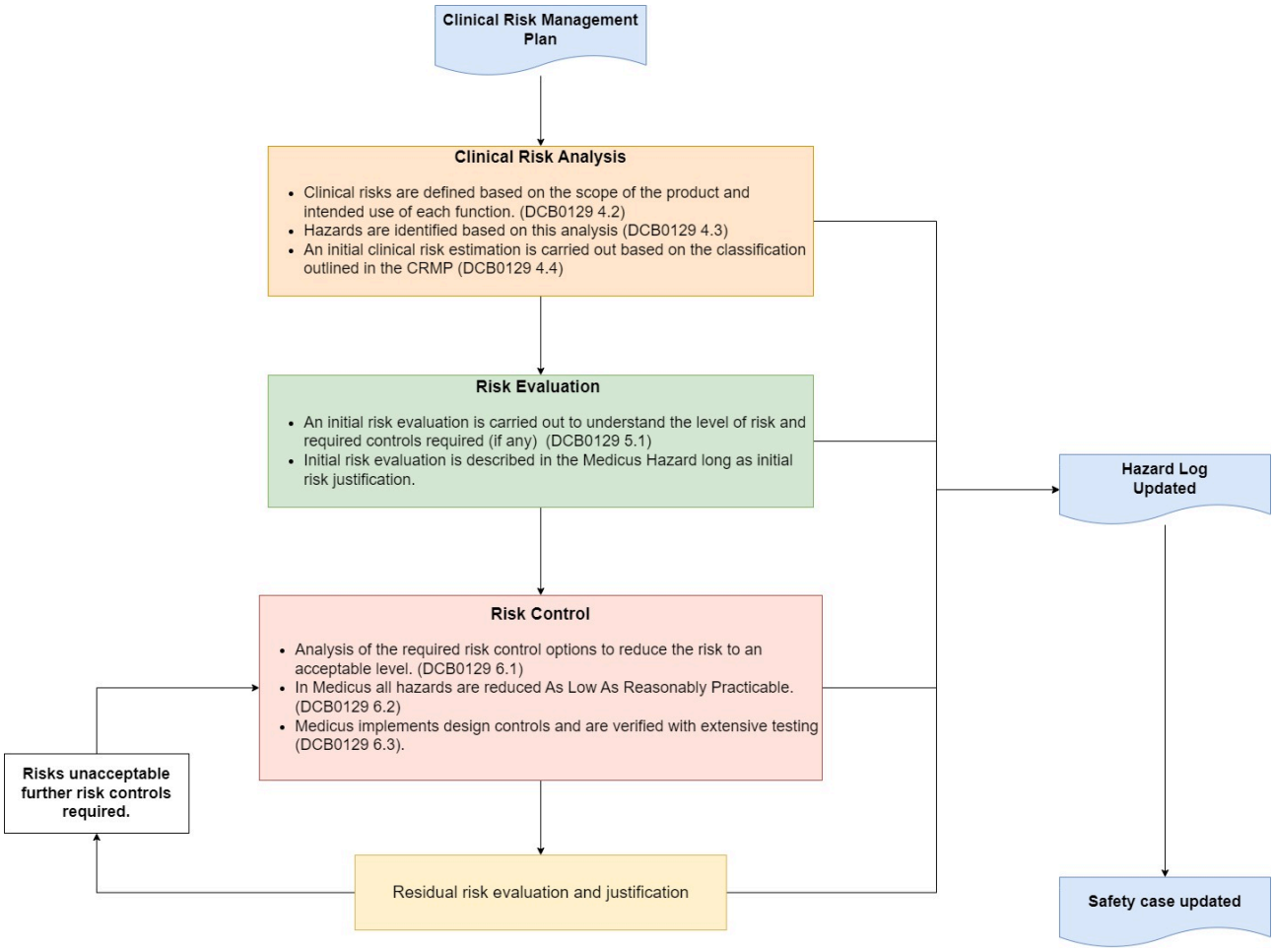
- Emile Axelrad (CEO)
- Dr Imran Khan (Clinical Safety Officer)
- Tim Gray (Chief Product Officer)
- April Armitage (Head of Client Services & Delivery)
- Andrew Smith (Head of Engineering)
- Ronan O’Connor (Head of Product)

All members of top management have completed the NHS Clinical Safety Officer or Clinical Safety Practitioner training.

Clinical Risk Management Process

Key elements of the Clinical Risk Management Process are depicted in the below diagram and expanded upon in the subsequent sections.

Appendix F also details the full Clinical Risk Management Process followed by Medicus Health on an ongoing basis.



Clinical Risk Analysis

Initial Clinical Risk Analysis

During the initial development of Medicus, we worked closely with experienced clinical staff to forensically assess the clinical risk of each functional area of the product. Often, this process also involved the

assistance of NHS England programme teams as the EPR scope was being developed and assured for use in the NHS.

Both preliminary and functional hazard identification was performed and captured in our Hazard Log.

NHS England Primary Care Test Lab (PCTL) Clinical Engagement Sessions

In the run up to our GP Practice MVP Pilot and First of Type as an EPR, Medicus and NHS England clinical colleagues conducted a series of clinical risk analysis sessions that involved live demonstrations of both the system functionality and clinical risk management activities performed by Medicus internally.

These sessions were named the Primary Care Test Lab (PCTL).

The sessions involved a systematic walk through of the areas of the product that would be used during the pilot and offered the chance for the NHS England clinicians to identify areas of clinical risk that could be improved, with the aim of reducing potential harm to patients.

The output of these sessions were incorporated into the Hazard Log that accompany this report.

The PCTL output reports are also included as appendices to this clinical safety case.

GP Practice “MVP Pilot”

On 15th November 2023, we piloted Medicus in a controlled environment, testing lots of the functionality that would be used when a GP Practice used it as their main EPR but with additional clinical safety mitigations and “hyper care” service management.

The pilot was conducted at Omnia Practice in Birmingham and involved 60 nursing home patients.

The patient records were transferred to Medicus and all consultations and prescribing was done from the system.

Key information:

- The pilot ran for 4 weeks and Medicus was fully utilised during this period for patient consultations, prescribing and referrals.
- 19 NHS national services were put live in 1 week
- 6 Omnia team members used Medicus in live, recording 87 consultations for 51 patients
- 0 HSSI incidents were raised
- The pilot ran successfully for the intended duration (15 Nov -19 Dec)
- 100% service uptime was achieved

The aim of the MVP was to validate as much of the product from a functional and clinical safety perspective & identify potential improvements for the future.

There was only one clinical safety issue raised as a result of the pilot which was related to users accidentally keying in the wrong quantity for a prescription (5656 tablets and 2828 tablets respectively). We have since implemented additional controls to reduce the likelihood of this issue occurring again.

First of Type GP Practices

From 30th September 2024, Medicus was used within the NHS live estate as the EPR for Park Road Surgery in Teddington.

From 2nd December 2024, Essex House Surgery in Barnes also migrated to use Medicus and finally Ingleton Avenue Surgery in Welling deployed Medicus on 20th January 2025.

The aim of the First of Type was to operate Medicus as a full EPR in the live estate but supported by NHS England Live Services & Programme teams to resolve any issues.

The First of Type period ran for 6 months and provided valuable learning and insights from both a customer satisfaction and clinical safety perspective.

Key information from all 3 surgeries (up until 27th Feburary):

- Number of EPS prescriptions: 100,390
- Number of e-RS directly bookable referrals made: 1976
- Number of e-RS triage referrals made: 2620
- Number of e-RS A&G referrals made: 700
- Number of consultations recorded: 227,360
- Number of PDS traces: 727,132
- Number of Summary Care Record updates: 485,848
- Number of investigations requested (tQuest): 23,179
- Number of NHS003 investigation results received: 27,474
- Number of NHS004 investigation results received: 412
- Number of immunisation updates received: 28,622
- Number of successfully outbound GP2GP transfers: 1004
- Number of successful inbound GP2GP transfers: 1273
- Number of eMED3 fit notes issued: 471
- Number of GP Connect ARS HTML requests: 7664
- Number of GP Connect PFS Access Record requests: 6178
- Number of GP Connect PFS prescription requests: 21
- Number of GP Connect Appointment Booking Requests: 219
- Number of GP Connect Send Documents Sent: 184
- Number of GP Connect Send Documents Received: 204

There were 4 clinical safety incidents raised in our Clinical Safety Incident log, all of which were fully addressed and provided valuable input into the safe design of Medicus:

CSI-1: 2024-10-01 Duplicate prescriptions sent to EPS

- An invalid prescription (based on the FHIR specification) that had been imported caused a failure half way through bulk sending prescriptions to EPS which rolled back the transaction in the Medicus database (a common enterprise software design pattern to prevent data corruption) and allowed the user to click “Issue” again. A fix was put in place to strengthen the business logic.

- As a result of this incident, we also increased our monitoring of tooling such as Sentry to be better alerted of service incidents (status updates e.g. for degraded service come into a Slack channel monitored by our DevOps / SRE team)

CSI-2: 2024-10-16 Document matched to the incorrect patient

- Patient matching rules where no NHS number is present were strengthened to check the patient's name, date of birth, and address (previously we checked name and date of birth which is how the error occured). HAZ-383 was uplifted to include new design controls

CSI-3: 2024-11-07 Medication prescribed to patients who are allergic

- Even though sensitivity alerts and the patient's allergies were clearly presented on screen, a patient was prescribed medication they were allergic to. A further design control was implemented to force users to confirm the existence of the sensitivity alert. HAZ-67 was uplifted to include new design controls

CSI-4: 2024-12-09 EPS: Duplicate prescriptions reported

- A problem updating the prescription task counters after bulk issuing prescriptions to EPS prescription request task failed which rolled back the transaction in the Medicus database. Corrective action was taken to split up the transactions for sending prescriptions to EPS that register the different stages in the database so that it is possible to check "Have I already tried to send this prescription to EPS?". Upon detecting any issues, our live services team are notified and so is the user on screen. To date this additional design control has proven very effective and has only been triggered in scenarios that identified problems with the EPS FHIR API that were subsequently passed on to the NHS EPS team for resolution. HAZ-99 was uplifted to include new design controls

NHS England Clinical Safety Group (CSG) "Full Roll Out Approval"

The NHS England Clinical Safety Group (CSG) is a committee of clinical safety experts that review the Medicus Clinical Safety Case to ensure that the system is safe for deployment in NHS England GP Practices.

Because of the size and complexity of Medicus, "full roll out approval" for Medicus as a primary care EPR was granted by CSG in 3 parts:

1. Approval for a Nursing Home MVP
2. Approval for a First of Type
3. Approval for Medicus to exit First of Type and be rolled out across the NHS (FRA)

For some NHS assurance programmes, we are also required to revisit CSG to seek approval for the deployment of new functionality.

Ongoing Agile Development Cycle

During the ongoing development of Medicus, we maintain a detailed scope definition in Confluence to help the clinical risk management team assess the impact of any changes. This is referred to as our “Product Documentation”.

As part of our agile development cycle, clinical risk is then assessed on any new scope (e.g. new functionality) or changes to the existing scope (e.g. changes to existing functionality). These assessments are carried out on all proposed development in a document called a Change Proposal.

Preliminary and functional hazard identification is performed against the Change Proposal and any identified Hazards or Causes are captured in the Hazard Log that accompanies this report once the functionality is eventually released. It is not permitted for Change Proposals to be developed & released without having multiple risk owner sign offs, one of those being clinical safety.

When conducting clinical risk assessment, we also consider previously documented hazards from interoperability programmes within NHS England (e.g. GP Connect, EPS, SCR) and a record of the mapping from NHS England Hazard Logs to the Medicus Hazard Log is available in the supporting documents of this report.

Clinical Risk Evaluation

For each Hazard or Cause that we find, we first estimate how likely and how severe the harm to the patient or user could be. This is our initial clinical risk evaluation. We compare this evaluation with our risk tolerance, which is the level of risk that we are willing to accept and think is reasonable for Medicus. Our risk tolerance is based on the Clinical Risk Management Plan that we have created following the DCB0129 standard.

If the initial clinical risk evaluation is higher than our risk tolerance, then we need to take actions or put controls in place to reduce the risk. If it is lower or equal, then we can accept the risk as it is or choose to reduce it further if practicable.

The process is further defined in our Clinical Risk Management Plan and in accordance with DCB0129.

> ⚠ **Please note:** For all risk evaluations, there is an assumption that deploying healthcare organisations already take actions to ensure safe practice and reduce patient safety incidents.
> Examples include only allowing trained prescribers to issue new medication to patients inline with professional guidelines.
> Any additional controls applied or suggested by Medicus Health are aimed at further reducing the clinical risk. That is to say, Medicus is not and should not be the only control when ensuring safe practice.

Clinical Risk Control

If a Hazard or Cause has a Clinical Risk higher than our risk tolerance, we assess the options to reduce the risk by implementing additional controls.

The Hazard Log details a number of controls as described below.

The Hazard Log does not describe how each control contributes to the overall risk reduction. Therefore, it is assumed that all the controls described are necessary to achieve an acceptable Clinical Risk. For example, if a risk requires Design, Training and Business controls to mitigate it, the residual risk is evaluated based on the presence of all these controls.

HIT Design Controls

For each functional area, we validate prototyped designs of both the user interface, technical implementation and business logic before any code is written. This allows us to assess the impact that a specific control will have on reducing the clinical risk.

The Hazard Log reflects the design controls that are inherently part of the risk mitigation process. During development, design controls that are included in the Hazard Log are tracked by the development team accordingly to ensure they have been implemented and we have processes in place to ensure the reliability and integrity of the code developed.

Features used as design controls are required to have evidence of testing before they can be released as described below.

Testing

As a company, we employ a variety of testing techniques to ensure quality and prevent regressions, which is crucial for maintaining clinical safety. Our primary method is automated testing, which provides scalable risk reduction for Medicus as a product.

The specific testing requirements for any product change or feature are outlined in the Product Change Proposal document controlled under our ISO 20000 compliant Service Management System (fully assured by Lloyds Register (Appendix D)). Each requirement (including but not limited to design controls) has corresponding tests in the codebase to prove the functionality works as expected and protect against regression. This may include multiple tests to fully cover a specific requirement.

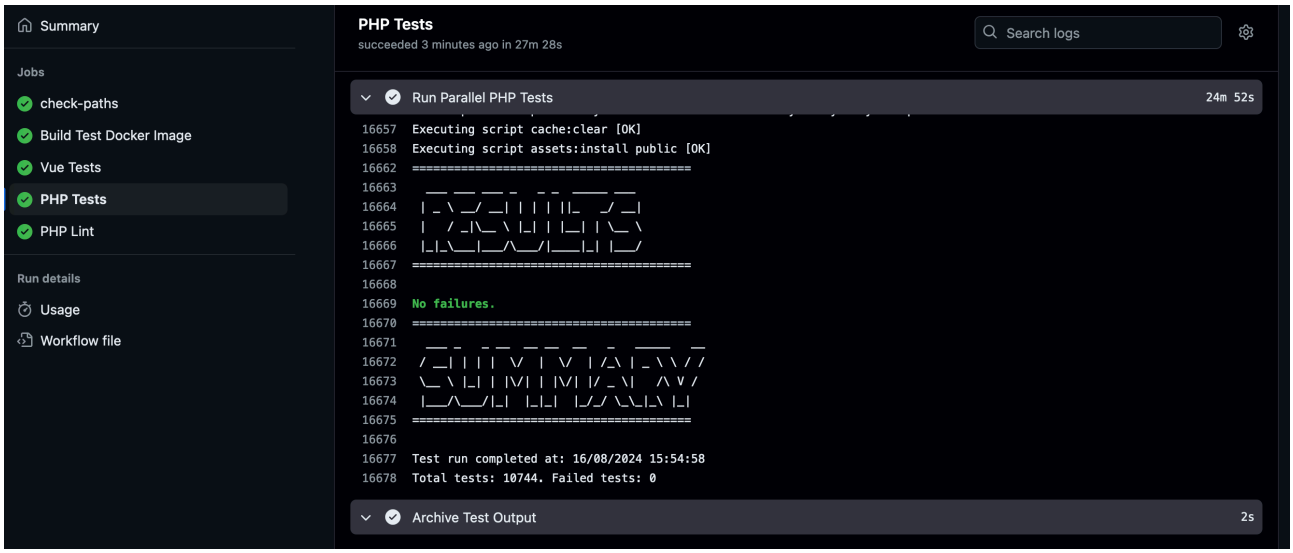
Further automated quality controls include, visual regression tests, end-to-end user interface tests and static code analysis.

Additionally, changes are assessed before release by senior members of the change management team to ensure they fulfil the requirements of the design control. Examples include but are not limited to, acceptance testing and Code Review. These actions are fully auditable within our software development tooling.

For specific functionality, NHS assurance is also required to ensure the functionality behaves as intended. Assurance covers a mixture of automated test packs, live witness tests and clinical reviews (including clinical safety). Evidence of conformance can be provided upon request.

Although automated testing is one of our primary controls, for operational reasons, we do not include a reference to every automated test within this Safety Case (there are over 10,000 and this number increases with every release). That said, our automated test suite is executed whenever a Pull Request is merged and

deployed into the main codebase (see example screenshot below) and it is not possible for Software Engineers to merge newly written or modified code if the automated test suite fails. The automated test suite covers the entire system and this serves as a key control in our operational design to prevent defects being released into the main codebase and therefore the production environment.



Because of the nature of our development process (which is by design), we do not carry forward outstanding test issues and therefore this element of DCB0129 is addressed upstream. We believe this approach has a material impact on the overall safety of the Medicus EPR.

Training Controls

There are a number of issues that are identified in the Hazard Log where the mitigation of the clinical risk relies on other factors including training of users. Where a training control is suggested, we will provide materials to support the training against each Hazard in the Hazard Log.

There will understandably be an overlap with other business controls in certain instances. For example, whilst training on effective user access and authentication allows users to be set up correctly, there needs to be a business processes that answers questions around who needs access and why. These issues will be raised as part of the training when required.

Users will be able to access training & support materials that enable these controls to be realised via our Help Centre and we will ensure each of the training controls can be adequately traced back to the Hazard Log so that training can be implemented prior to deployment.

Healthcare organisations are required to undertake a formal programme of risk management whenever they implement a health IT system as set out in DCB0160 and we will provide support in order that the organisation understands the activities required to implement the product safely. This is achieved through describing the business control requirements in the hazard log and responding to any concerns or queries a deploying health organisation may have.

Business Controls

The Hazard Log attempts to identify and describe any business processes and changes required in order to mitigate against the Hazard. For example, where there may be a risk of patients receiving medication that could cause them serious harm, we may recommend that the healthcare organisation ensures all prescribers are suitably qualified and experienced.

Prior to deployment, we will highlight these controls to the deploying healthcare organisation to ensure that they are aware of the transferred risks.

Healthcare organisations are required to undertake a formal programme of risk management whenever they implement a health IT system as set out in DCB0160 and we will provide support in order that the organisation understands the activities required to implement the product safely. This is achieved through describing the business control requirements in the hazard log and responding to any concerns or queries a deploying health organisation may have.

Hazard Log Change History

[This section was added in January 2026 in response to feedback from the NHSE Clinical Safety Group (CSG) and therefore only contains a partial change history]

Safety Case Version	Summary of Changes
1.17	Corrected incorrect Hazard numbers.
1.16	**GP Connect Access Record Structured Specification Uplift (v1.5.0 to v1.6.2)** This version incorporates the clinical risk assessment for the NHS DSIC Roadmap item RM223: GP Connect Access Record Structured specification updated from version 1.5.0 to 1.6.2. The hazard log was reviewed and existing GP Connect Provider risks were previously captured. Additional specific causes were previously identified and documented within the following such as: HAZ-1282: Dosage instructions not mapped accurately in Structured Dose Syntax elements.

Safety Case Version	Summary of Changes
1.15	**Additional DPS Vaccination Extracts (Adults & Neonatal, Infants & Toddlers)** This version incorporates the clinical risk assessment for the NHS DSIC Roadmap items: Adult Vaccination Expansion Uplift and Neonatal, Infants and Toddlers Immunisation Uplift. Changes include the addition of COVID-19 as a point of care immunisation and new DPS extracts for. No new hazards were identified as there had been included for RM282. The following existing hazards were reviewed and confirmed as covering this change: • HAZ-1042: Patient does not receive a vaccination for which they are eligible • HAZ-1046: A patient is inappropriately vaccinated • HAZ-1050: Delay in patient receiving a vaccination
1.14	**TPP SystmOne Data Migration - Template Context Loss.** Clinical Safety Position adopted following clinical risk benefit analysis under DCB0129 sections 6.1.5, 6.1.6 and 6.2.1 in the context of the first-of-type TPP migration → Medicus at Old Forge Surgery. HAZ-1249 remains Transferred and cause ***Migrated consultation content is presented without clinical context and the loss is not visible to the clinician*** remains. Proceeding on the basis of clinical risk benefit analysis acceptance recorded in the CRMF.
1.12	**Adult Vaccination Expansion Uplift - COVID-19** This version incorporates the clinical risk assessment for https://nhse-dsic.atlassian.net/wiki/spaces/DCSDR/pages/14330888257/Adult+Vaccination+Expansion+Uplift and specifically COVID-19. One new cause was added to HAZ-1046: A patient is inappropriately vaccinated: • Clinician records the incorrect vaccine product

Safety Case Version	Summary of Changes
1.10	**National Proxy Service Implementation** This version incorporates the clinical risk assessment for changes implementing NHS England's National Proxy Service requirements within Medicus: • **RM256**: Mandating proxy access and enabling proxy access for baby patient registrations • **RM263**: Verified candidate relationships via the NHS Validation and Relationship Service (VRS) • **RM267**: Proxy visibility, activity logging and access lifecycle management A mapping from the NHS England GP IT Supplier Proxy Hazard Log (v1.0) to the Medicus Hazard Log has been completed and is available on request. HAZ-72 -Unauthorised third party accesses confidential patient information or services inappropriately. Causes added: • Patient coerced into agreeing to proxy access at the practice • Proxy access is granted to an unauthorised or unsuitable individual • Proxy access provides either more information than necessary • Proxy misuses legitimate access beyond intended care purpose HAZ-1166 - Patient/Proxy is unable to access information they require for self-management or when presenting to another healthcare professional HAZ-1303. Cause added: • Delay in proxy setup leaves dependent patient without online access support

Safety Case Version	Summary of Changes

1.8	**DigiMeds Emergency Supply**
	
	The DigiMeds Emergency Supply messaging standard is new functionality that allows pharmacies to send structured messages to the patient's registered GP Practice when emergency supply of medicines is provided by the pharmacy.
	
	Full information about the DigiMeds Emergency Supply messaging standard can be found here: DigiMeds Emergency Supply
	
	During the Hazard Assessment, new causes were added to the following Hazards:
	
	• HAZ-297: Patient receives inappropriate dosage of prescribed medication
	  • Clinician isn't aware the patient has received emergency supply of medication at another healthcare setting
	  • Clinician unable to determine if patient received correct quantity of medication during emergency supply from pharmacy
	• HAZ-464: Patient takes too much medication compared with prescribed regimen
	  • Clinician isn't aware the patient has received emergency supply of medication at another healthcare setting
	• HAZ-99: Patient receives medication that should have been ceased
	  • Patient receives an over supply of medication because clinician isn't aware the patient has received emergency supply of medication at another healthcare setting
	
	The following existing Hazards are also relevant to the DigiMeds Emergency Supply functionality:
	
	• HAZ-838: Inbound document is not processed appropriately or in a timely manner
	  • Cause: Wrong patient is automatically matched by Medicus
	  • Cause: Wrong NHS number sent by the sending system
	  • Cause: MESH mailbox missing or incorrectly configured
	  • Cause: Message is received for a patient no longer registered at the practice
	• HAZ-73: Clinician makes incorrect decisions based on an incomplete medical history
	  • Cause: Third party reported medications are not correctly or sufficiently entered into the clinical system

Safety Case Version	Summary of Changes
	First of Type Plan: Given the small number of practices currently using Medicus, we will operate the first of type across all of them. The practices are: • Park Road Surgery (H84002) • Essex House Surgery (H84023) • Ingleton Avenue Surgery (G83024) • Wilmslow Health Centre (N81086) • Witley & Milford Medical Partnership (H81031) • Burnett Edgar Medical Centre (A82071) In order to exit first of type, the following deployment verification criteria must be met: • Up to 6 sites • 17 consultations successfully received by each site and filed into the patient record (100 in total) • No HSSIs • No clinically impacting incidents • One-week stability period Additionally, we considered at least one consultation from each provider (PSL, Cegedim, Sonar, PharmOutcomes) but this is not within the control of Medicus and therefore it was excluded as a deployment verification criteria.

Appendices

(Available on request)

- **Appendix A** - Medicus Hazard Log
- **Appendix B** - Medicus Clinical Risk Management Plan
- **Appendix C -** NHS DSIC (Digital Services for Integrated Care) Catalogue Capability & Standards Mapping - The assured NHS standards/capabilities, including a mapping to the Medicus modules to aide understanding for those more familiar with DSIC language
- **Appendix D** - ISO 20000:2018 certification
- **Appendix E** - NHS England Clinical Risk Analysis Traceability - Evidence of the clinical risk analysis provided by NHS England for specific national capabilities such as the Electronic Prescribing Service that was used when conducting our own clinical risk analysis
- **Appendix F** - Medicus Health Clinical Risk Management Process
- **Appendix G** - Clinical Risk Management Process Example
- **Appendix H** - NHS England PCTL Report (MVP Pilot)
- **Appendix I** - NHS England PCTL Report (First of Type)
- **Appendix J** - Cegedim Vision Data Migration Process
- **Appendix K** - Advanced Docman 10 Data Migration Process

- **Appendix L** - EMIS Web Data Migration Process
- **Appendix M** - TPP SystmOne Data Migration Process

Document Control

Document Control Reference

Related Documents	Control Requirements
DCB 0129 Control Statements	3.5 - Clinical Safety Case Report

Document Approval

Name	Role	Date
Dr Imran Khan	Clinical Safety Officer	04 Sep 2026
Tim Gray	Chief Product Officer	04 Sep 2026

Document Version History

Version	Date	Revision	Author
0.1	21 Aug 2023	Initial draft	Dr Imran Khan
0.2	15 Sep 2023	Draft revisions based on NHSE feedback	Tim Gray
0.3	19 Sep 2023	Draft revisions based on NHSE feedback	Tim Gray
0.4	10 Oct 2023	Draft revisions based on NHSE feedback during CSG approval sessions	Tim Gray

0.5	19 Oct 2023	Draft revisions based on NHSE feedback during CSG approval sessions	Tim Gray
0.6	26 Oct 2023	Included open hazards & justification	Tim Gray
0.7	31 Oct 2023	Revision following comments from NHS E	Dr Imran Khan
0.8	07 Nov 2023	Additional clarifications on HAZ-67 having outstanding issues.	Tim Gray
0.9	13 May 2024	Revisions to prepare safety case report for GP Practice First of Type launch	Dr Imran Khan
0.10	28 Jul 2024	Revisions based on comments from NHS England	Dr Imran Khan
0.11	08 Aug 2024	Revisions based on comments from NHS England + inclusion of Cegedim Vision data migration	Dr Imran Khan
0.12	15 Aug 2024	Minor uplift following GP Connect PFS Hazard Mapping + addition of Docman data migration	Tim Gray
0.13	16 Aug 2024	Expanding on testing to validate design controls work as expected.	Tim Gray

0.14	20 Aug 2024	Statement confirming UAT sessions	Tim Gray
0.15	05 Sep 2024	Include additional testing information at the request of NHSE	Tim Gray
0.16	10 Sep 2024	Minor uplift to include a small summarisation of key findings in our own Hazard Assessment	Tim Gray
0.17	17 Sep 2024	Updated Hazard numbers	Tim Gray
0.18	17 Dec 2024	Updated cause numbers	Tim Gray
0.19	07 Jan 2025	Remove incorrect reference to organisational controls document	Tim Gray
1.0	22 Apr 2025	Finalisation of the safety case report for full roll out	Dr Imran Khan
1.1	07 May 2025	Inclusion of TPP SystmOne data migration.	Tim Gray
1.2	13 Jun 2025	Uplift to cause numbers after resolving CSG caveats to include additional data migration risks.	Tim Gray

1.3	24 Jun 2025	Uplift to cause numbers in response to NHSE feedback on CSG caveats.	Tim Gray
1.4	10 Oct 2025	Update cause numbers - DigiMeds Emergency Supply assurance.	Tim Gray
1.5	14 Nov 2025	Update cause numbers.	Tim Gray
1.6	29 Nov 2025	Update cause numbers.	Tim Gray
1.7	12 Jan 2026	Minor amendments	Tim Gray
1.8	26 Jan 2026	Restructuring of executive summary and introduction of Hazard Log Change History as part of DigiMeds Emergency Supply CATR.	Tim Gray
1.9	10 Feb 2026	Further amendments following DigiMeds Emergency Supply CSG review	Tim Gray
1.10	23 Feb 2026	Amendments to the safety case and hazard log following partial implementation of Proxy access.	Imran Khan
1.11	02 Mar 2026	Amendment to add NHS Login user and provisioning endpoints.	Imran Khan

1.12	10 Mar 2026	Version history update to include https://nhse-dsic.atlassian.net/wiki/spaces/DCSDR/pages/14330888257/Adult+Vaccination+Expansion+Uplift [specifically COVID-19].	Tim Gray
1.13	12 May 2026	Clarification of EPR product version reference in Scope section to resolve NHSE CSG version ambiguity.	Imran Khan
1.14	18 May 2026	Evidence of consideration of TPP SystmOne to Medicus Data Migration and template context loss	Imran Khan
1.15	09 Jun 2026	Confirmation of Hazards for POC and DPS extracts for Children and Adults.	Imran Khan
1.16	16 Jun 2026	Confirmation of Hazards in assurance of encompassing Access Record Structured Specification	Imran Khan
1.17	04 Sep 2026	Updated Hazard Numbers	Tim Gray