MINDBAY

Assuric
Assured Document

Clinical Risk Management Plan

The Clinical Risk Management Plan (CRMP) outlines the processes in place to assess and mitigate clinical risks and assure clinical safety of products, during the development, design and deployment phases of the product life cycle.

Document Management

Document filename: Clinical Risk Management Plan
Document version number: 1.0
Organisation: MindBay Technologies
Issue Date: Jul 25, 2025
Document Owner: Taha Ouertani

Document Version Control:

Title	Version	Date approved	Changes	Approver
Clinical Risk Management Plan	1.2	Jul 25, 2025, 09:40	Updated	Paul Jewell
Clinical Risk Management Plan	1.1	Jul 20, 2025, 12:24	Renamed product from WellnessOne to MindBay; no scope change.	Taha Ouertani
Clinical Risk Management Plan	1.0	May 27, 2025, 09:08	First version	Paul Jewell

Contents

Clinical Risk Management Plan

The Clinical Risk Management Plan (CRMP) outlines the processes in place to assess and mitigate clinical risks and assure clinical safety of products, during the development, design and deployment phases of the product life cycle.

Introduction

The Clinical Risk Management Plan (CRMP) outlines the processes in place to assess and mitigate clinical risks and assure clinical safety of MindBay Technologies (hereafter referred to as "we", "our", "us") products, during the development, design and deployment phases of the product life cycle.
This CRMP provides a framework that promotes effective risk management of potential health IT hazards and operational incidents. It describes how clinical risk management will be conducted to ensure patient safety. This CRMP identifies the means by which the product life cycle shall be controlled to ensure that the safety work is of high quality. This CRMP addresses the requirements of DCB0129 and DCB0160 and follows best practice as promoted by NHS England (previously NHS Digital).

Purpose

The aim of the CRMP is to define the implementation of our Clinical Safety Management System. It describes how we will conduct clinical risk management to ensure patient safety in line with DCB0129 and DCB0160 standards. It ensures that all staff involved with the development, implementation and use of our healthcare IT products and systems are aware of the activities that are required to be undertaken to ensure patient safety is improved, rather than compromised, from the introduction and deployment of our healthcare IT systems and products.
The CRMP identifies the means by which our products and services shall be controlled to ensure that the safety work is of high quality and conforming to any specific programme requirements.
We adhere to National Information standards created and monitored via the Data Coordination Board (DCB) within NHS Information Standards frameworks.
This CRMP will be reviewed and updated periodically, as decided by the product and safety teams, and the Clinical Safety Officer, 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.

The CRMP will be maintained throughout the life of our health IT products.

Background to clinical safety standards and requirements

Information standards provide the mechanism for introducing requirements to the NHS, those with whom it commissions services and its IT system suppliers. There are two Information Standards related to patient safety described below.

DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems

This standard sets clinical risk management standards for **manufacturers** of Health IT systems. It requires the manufacturer to establish a structure within which clinical risks associated with the design and development of a new Health IT system or the modification of an existing system are properly managed. It also ensures that outputs are clearly documented to provide evidence of compliance. Compliance with the standard ensures that the manufacturer has instigated a best practice clinical safety programme during the manufacture of the health IT system.

DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems

This standard requires health organisations **deploying** and **using** new or modified health IT systems to have a structure to manage clinical risks associated with that deployment. Many of the requirements in DCB0129 are repeated in DCB0160 for the health organisations.

Audience

The intended audience for this document are: MindBay Technologies employees, health institutions, care organisations and regional and national procurement and safety leads as required.

Scope

This document currently refers to the development, design and deployment of our products intended for feasibility and pilot stage.
The policy also applies to any subsequent updates or upgrades, or any local customisations or specific configurations made to a healthcare IT system. Any changes in phase scope, content and future phase development will be addressed in this document by a revised CRMP document. The revised documentation will be agreed with the Clinical Safety Officer and any partner organisations, to ensure correct governance and control is in place.
If clarification is required of whether any system falls within scope of this CRMP this should be raised with a member of the Clinical Safety team.

Abbreviations and Definitions

CSO: Clinical Safety Officer - the person responsible for ensuring that the healthcare IT Clinical Risk Management System is applied to all clinical systems.
DCB: Data Coordination Board

Service Overview

Company background

MindBay Technologies Ltd builds and operates digital mental health solutions developed through collaboration between mental health professionals and AI experts.
Our product, MindBay (the app), is an interactive, chat-based conversational agent that delivers eight sessions of Cognitive Behavioural Therapy (CBT), along with between-session CBT exercises, meditation, and problem-solving tool.
MindBay uses Large Language Models (LLMs) trained on extensive datasets, enabling the generation of nuanced, context-specific responses in real time. Unlike earlier chatbots that relied on rigid rules or scripts, our tool offers a more personalised, precise and engaging experience, addressing key limitations of earlier AI-driven mental health interventions.

Clinical context

Before MindBay, GPs faced only two main first-line tools for mild-to-moderate depression or anxiety: (1) start an antidepressant - taken by 8.7 million people in England in 2023/24 despite common side-effects and patchy adherence - or (2) refer the patient to NHS Talking Therapies, where the average gap between first and second appointments exceeded three months and 1.76 million yearly referrals often received little more than review slots or self-help leaflets while they waited.
MindBay, a **Class I medical device** that delivers AI-supported, CBT-based conversations, is designed to **supplement - not replace - these established pathways**. A GP can generate an activation code through the electronic prescribing system to accompany medication or a Talking Therapies referral; clinicians can likewise issue a code at assessment so that patients on wait-lists gain immediate, guided CBT practice. Usage and symptom-change dashboards feed back to the referrer, supporting stepped-care reviews and helping teams prioritise follow-up. In this way, MindBay functions as a scalable, cost-effective **adjunct** that offers timely psychological support while preserving - and never substituting for - the clinician's judgment, pharmacotherapy, or face-to-face therapy.

Development lifecycle

The current phase of the product life cycle is the **initial feasibility and pilot stage.**
This document, as well as the Hazard Log and Clinical Safety Case Report, will be updated as a result of progress through subsequent phases of the development lifecycle. It will be specified how clinical risk activities are applicable at each particular lifecycle phase.

Clinical Risk Management (CRM) Governance Arrangements

The CRMP will be executed by the Clinical Safety Team. The list below identifies the key people responsible for clinical safety within our organisation. The Clinical Safety Team includes representatives from our top management. All members of the safety team integrate an awareness of clinical safety into every aspect of their work.

Clinical Safety Team
The list below identifies key people responsible for clinical safety within our organisation, making up the Clinical Safety team.
Clinical Safety team

Name	Role	Responsibilities
Paul Jewell	*Clinical Safety Officer*	*Create clinical risk management processes* *Review clinical risk management documentation* *Approve clinical risk management documentation* *Lead hazard identification reviews* *Lead regular, episodic clinical risk management reviews*
Taha Ouertani	*Product Manager*	*Product development identification of risk* *Product development identification of controls for named risks* *Communicate product development with CSO* *Communicate user feedback with CSO* *Join hazard identification reviews* *Join regular, episodic clinical risk management reviews*

Clinical Safety Officer
The Clinical Safety Officer is responsible for ensuring the clinical safety of MindBay Technologies products through the application of clinical risk management. The Clinical Safety Officer is a suitably qualified and experienced clinician who holds current registration with their relevant professional body and has had appropriate training for this role.

Name	Professional qualifications	Professional Body	Competency/Skills/Experience	Clinical Safety Training
Paul Jewell	Medical doctor, BMBCh, MRCP	GMC: 7515784	Medical doctor with over 8 years experience, NHS Digital Clinical Safety Officer training and certification	NHS Digital CSO course

Key responsibilities include:

- approval of the Clinical Risk Management Plan to confirm that the plan is appropriate and achievable in the context of the Health IT System development and modification;
- reviewing and approving of all safety documentation including Clinical Safety Case Reports and Hazard Logs;
- reviewing evidence in the Clinical Risk Management File to ensure it is complete and supports the Clinical Safety Case Report;
- escalating any unacceptable safety risks.

Delegation of authority
This table will note any delegation of authority (DOA) to allow for sign off and changes to this document and the Clinical Safety report in the absence of the named Clinical Safety Officer.

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

- Clinical Risk and Safety Meetings

The Clinical Safety Team will meet for Clinical Risk and Safety Meetings once **every six months**, to review the clinical safety approach, the hazard logs, mitigations and residual risks for the current software and potential future releases.
The Clinical Safety Team will also meet with Customer Organisations to ensure clinical safety has been assessed and mitigated in respect of DCB0160 with regards to deployment.
Each clinical safety team will maintain a Clinical Safety Incident Management Log.
All documents created as part of the our Clinical Safety Management System are maintained, version controlled and managed by our Clinical Safety Team, and authorised by the Clinical Safety Officer.

Clinical Risk Management Deliverables

Clinical Risk Management File
We will establish a Clinical Risk Management File (CRMF) for all of our safety related healthcare IT products. The purpose of the CRMF is to provide a central repository where all safety related information pertaining to the healthcare IT system is stored and controlled.
For each safety-related implementation of our products, the following deliverables will be produced:

1. Clinical Risk Management Plan (CRMP, this document)
2. Hazard Log (HL)
3. Clinical Safety Case Report (CSCR)
4. Safety Incident Management Log (SIML)

The deliverables will be kept up to date to reflect the scope of the live product. They will be subject to version control so that the status and most up to date version is clear and will be stored in the Clinical Risk Management File.

Clinical Risk Management Plan
We will establish a Clinical Risk Management Plan (CRMP) (this document) for each safety related healthcare IT product. 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.

Hazard Log
We will establish and maintain a Hazard Log (HL) for each safety related healthcare IT product. The HL is made available within the CRMF. The purpose of the HL is to manage the effective resolution and communication of hazard risk.

Clinical Safety Case
We will establish a Clinical Safety Case (CSC) for each safety related healthcare IT product.

Clinical Safety Case Report
We will issue a Clinical Safety Case Report (CSCR) for each safety related healthcare IT product. 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 made available within the CRMF.

Clinical Risk Management Plan Review process

This CRMP will be reviewed and updated periodically, as decided by our product and safety teams, and the Clinical Safety Officer, to ensure that:

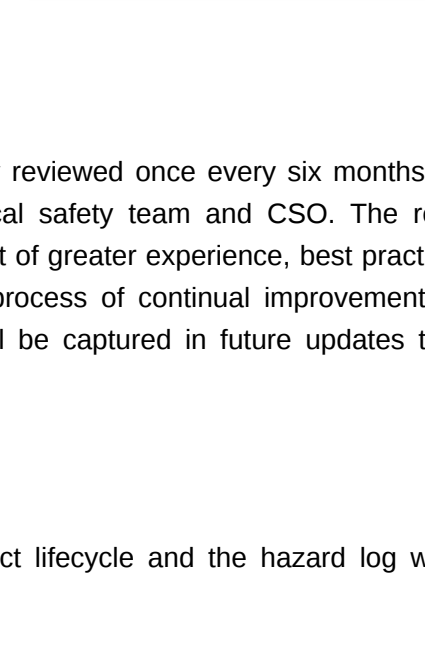
- changes in working practices are incorporated
- issues identified through an established internal audit programme are addressed
- the safety approach continues to adhere to the requirements of applicable international standards
- the system continues to protect the safety of patients in a complex and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

The current CRMP review frequency is: once every six months.
Review of the CRMP may be also triggered by a transition to the next phase in the Health IT System lifecycle, a change of resource or in line with existing governance arrangements. It may also be triggered by a modification of the product or in response to an incident, as outlined by our **Clinical Safety Change Management Procedure**, and our **Clinical Safety Incident Management Procedure**.
The CRMP will be maintained throughout the life of our health IT products.

Clinical Risk Management Activities

Clinical Risk Management Process

The purpose of the clinical risk management process, outlined in the adjacent diagram, is to identify and document known and foreseeable credible hazards that could impact on patient safety, related to our health IT products' **intended use**, in both normal and fault conditions. A hazard is defined as a condition or event in which harm to a patient could theoretically occur.
The clinical risk management process will also establish the controls which are already present or need to be put in place to mitigate the risk to acceptable levels. The clinical risk matrix (see Appendix) determines the risk score based on the severity and likelihood of an identified hazard.
The following diagram (right) sets out the overall Clinical Risk Management process.


Clinical Risk Management Plan
Clinical Risk Analysis
- Intended use
- Identification of hazards
- Estimation of risk(s)
Clinical Risk Evaluation
Clinical Risk Control
- Risk control analysis
- Implementation of control measures
- Residual risk evaluation
- Risks arising from control measures
Hazard Log
Evaluation of overall risk acceptability
Clinical Safety Case Report
Post Deployment Monitoring
- Incident management
- Change management

CRM Review Process
The clinical risk management process will be formally reviewed once every six months, with representatives including key stakeholders, the clinical safety team and CSO. The review examines whether any changes are needed as a result of greater experience, best practice or lessons learnt from previous releases to support a process of continual improvement. Any changes to the clinical risk management process will be captured in future updates to the Clinical Risk Management Plans.

Hazard Identification

Hazards can be identified at any stage of the product lifecycle and the hazard log will be continually maintained and updated as required.

Hazard identification methodology
A Structured What-If Technique (SWIFT) will be used to perform the hazards analysis. The Structured What-If Technique is a systematic method of hazard identification. The technique, carried out as a brainstorming activity, employs an analysis of potential deviations from the expected business process. The clinical or system business process is broken down into individual tasks. 'What If' questions will be tested against each task to generate ideas for hazards, causes and controls. Should the SWIFT technique be found to be inappropriate for the subject matter or additional rigour be required, other structured techniques can be employed such as Failure Modes and Effects Analysis (FMEA), Bow-Tie diagram or Fishbone diagram.

HAZID workshops
In line with best practice, to maximise hazard identification, when appropriate we will conduct hazard identification (HAZID) workshops to identify potential hazards associated with the deployment and use of our health IT products. These will be attended by representatives from multiple domains, including the development teams, product teams, safety and assurance teams and CSO. We will endeavour to ensure at least one key stakeholder or representative from the deploying healthcare organisation will also be in attendance, subject to availability.
Minutes of any HAZID workshops will be taken and a copy stored in the CRMF. If a healthcare IT solution is deemed not to be safe then this decision will be formally recorded.

Additional hazard identification
Hazards may be identified in other ways outside of HAZID workshops, during the development and use of our products such as:

- Discovery during design or use of a solution by ourselves or the deploying Healthcare Organisation;
- Testing of amended functionality;
- Ad hoc testing of live service functionality;
- Reporting of an incident or problem within the live service;
- Identification by a member of staff within the supplier or Healthcare Organisation

Our **Clinical Safety Change Management Procedure**, and our **Clinical Safety Incident Management Procedure** have been designed to enable new hazards to be identified and the HL to be updated as appropriate. All newly identified hazards will be recorded in the HL.

Hazard log
For each identified hazard, the following information will be defined and recorded in the Hazard Log:

- Hazard ID or number;
- Hazard name or description;
- Potential clinical impact – this will describe the effect of the hazard in the care setting and potential impact on the patient;
- Possible causes – these may be technical, human, error etc. A hazard may have a number of causes; and
- Controls – these are identified controls or measures that are in place and will remain in place post implementation that provide mitigation against the hazard.

Each Hazard will be discussed by the Clinical Safety team and any other appropriate people. They will perform the following tasks and record the outcome in the Hazard Log:

- Estimation of clinical risks;
- Clinical risk evaluation; and
- Clinical risk control option management.

Risk Analysis

For each identified hazard estimation will be made of the clinical risk. Clinical risk will be determined based on the description of patient harm, severity, causes and contributory conditions. The estimation process will follow that established by the safety processes defined in DCB0129. See Appendix for copies of the Risk Assessment Matrix, and definitions of Hazard likelihood and Hazard consequence.

The HL will be updated to capture the risk analysis.

Risk Evaluation

Each identified hazard will be evaluated and attributed a level of clinical risk according to the criteria set out in the Appendix. Together the hazards and their associated clinical risk will comprise the safety profile. A project may only proceed if the clinical risk associated with the identified hazards are acceptable.
A hazard will be deemed acceptable if:

- The Residual Clinical Risk is Low or Moderate
- The Residual Clinical Risk is Significant, but it can be evidenced that the hazard has been mitigated to, As Low As Reasonably Practicable, or (exceptionally);
- The Residual Clinical Risk is High or Very High but this can be justified based on a clinical risk-benefit analysis.

Should the Residual Clinical Risk be deemed Unacceptable, and this cannot be justified by the clinical benefits, the assessment will conclude that additional means of risk control must be implemented before the project can proceed.
The HL will be updated to capture the risk evaluation.

Risk Control

Where the initial risk evaluation is deemed unacceptable, further risk controls will be required. Adequate additional clinical risks controls will be identified, justified, implemented and verified. Details of the risk control measure and evidence of effective implementation will be captured in the HL.

Third Party Products

As part of the clinical risk management process, any third party products used in our health IT system or products will be identified and considered in the scope of hazard identification activities and subsequent risk assessment. Where none are used, there will be a positive declaration to this effect. Details of any third party products used and any associated risks will be outlined in the **Clinical Safety Case Report**.

Pre-deployment review

Prior to deployment, we will complete a formal review of the Health IT system and Hazard Log, which will be recorded in the **Clinical Safety Case Report**. The Health IT System configuration for the specific release will be specifically recorded in the **Clinical Safety Case Report**. The **Clinical Safety Case Report** will require approval by the Clinical Safety Officer prior to deployment. This will ultimately ensure that all of the requirements of the Clinical Safety standard have been addressed.

Post-deployment Monitoring

Incident Management

Post-deployment, we will maintain a process to collect and review reported safety concerns and incidents, and will assess the impact of any such information on the ongoing validity of the Clinical Safety Case. If gathered evidence undermines the safety case, appropriate corrective action will be taken. Any reported safety incidents will be assessed and resolved in a timely manner.
A record of safety incidents, including their resolution, will be maintained in the **Clinical Safety Incident Management Log**. Any reported incidents will be managed appropriately with requirement for CSO assessment if the severity dictates. These incident management procedures are detailed in our **Clinical Safety Incident Management Procedure**.

Change Management

Post-deployment, we will maintain a process to apply clinical risk management processes to any modifications or updates of the deployed health IT system. The application of this process will be commensurate with the scale and extent of the change and the introduction of any new clinical risks. Any changes will result in the issue of an updated **Clinical Safety Case Report** to support any modification to the health IT system that changes its clinical risk.

The change management procedure is currently defined in our **Clinical Safety Change Management Procedure**.

Clinical Safety Competency and Training

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

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 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.
Staff competency will be reviewed periodically, and records of staff competency will be maintained. All registered clinicians involved in safety roles shall, as a minimum, have completed an accredited training course.

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, and/or 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.

Audits

Overview
Audits shall be undertaken to ensure that projects are adhering to the defined safety requirements. We will maintain an audit trail of all versions and patches released for deployment.
Internal Safety Audits
We 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 internal quality management procedures.

Appendix

Hazard likelihood definitions

Likelihood Category	Interpretation
Very high	Certain or almost certain; highly likely to occur
High	Not certain but very possible; reasonably expected to occur in the majority of cases
Medium	Possible
Low	Could occur but in the great majority of occasions will not
Very low	Negligible or nearly negligible possibility of occurring

Hazard Consequence definitions

Severity Classification	Interpretation	Number of Patients Affected
Catastrophic	Death	Multiple
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Multiple
Major	Death	Single
	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term	Single
	Severe injury or severe incapacity from which recovery is expected in the short term	Multiple
	Severe psychological trauma	Multiple
Considerable	Severe injury or severe incapacity from which recovery is expected in the short term	Single
	Severe psychological trauma	Single
	Minor injury or injuries from which recovery is not expected in the short term.	Multiple
	Significant psychological trauma.	Multiple
Significant	Minor injury or injuries from which recovery is not expected in the short term.	Single
	Significant psychological trauma	Single
	Minor injury from which recovery is expected in the short term	Multiple
	Minor psychological upset; inconvenience	Multiple
Minor	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible severity	Single

Clinical Risk Management Risk Matrix

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				

Risk Matrix key - Acceptability

5	Unacceptable level of risk. Mandatory elimination or control to reduce risk to an acceptable level
4	
3	Undesirable level of risk Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical.
2	Acceptable where cost of further reduction outweighs benefits gained.
1	Acceptable, no further action required