Clinical Safety Case: Cyril

Author: Alison Mitchell-Hall
Date Drafted: 20/12/2023
Version: 0.1

Approval

The signatures below certify that this management system procedure has been reviewed and accepted, and demonstrate that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision.

	Name	Position	Date
Prepared by	Alison Mitchell – Hall	Chief Nurse & Strategy Director	20/12/2023
Reviewed by	Katy Longhurst	Chief Product Officer	12/01/2024
Approved by	Mike Jackson	Chief Executive Officer	22/01/2024

Amendment Record

This procedure is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual additions or omissions is given below:

Page No.	Context	Revision	Date

Company Proprietary Information

The electronic version of this procedure is the latest revision. It is the responsibility of the individual to ensure that any paper material is the current revision. The printed version of this manual is uncontrolled, except when provided with a document reference number and revision in the field below:

Document Ref. ______________________ Rev ________

Uncontrolled Copy □ Controlled Copy ✓ Date ________

Contents

Executive Summary

This document provides the clinical safety case to support implementation of Cyril, a remote patient monitoring system. The standard provides information models and implementation guidance which will be used by Barcode Data Healthcare Solutions to develop technical standards for structuring and coding to facilitate the sharing of information in support remote patient monitoring utilising the Cyril platform. The aim is to incorporate ISO27001 standards to facilitate better access and interoperability.

A total of 9 hazards have been identified associated with the implementation of Cyril and are recorded within the Hazard Log (Section 6). Evaluation of the initial risk associated with these hazards has led to a requirement to implement additional risk controls to reduce residual risk to a tolerable level. Provided that the risk controls and other mitigation recorded in the hazard log (Section 6) are successfully implemented, the residual risk associated with the implementation of Cyril is considered tolerable.

Introduction

In November 2016 NHS England published a new digital strategy which set out its ambitions to drive and deliver sustainable improvements in healthcare utilising technology to digitise services, connect them to support integration and, through these foundations, enable service transformation. The aim of the strategy is twofold:

To improve the safety of digital technologies in health and care, now and in the future

To identify and promote the use of digital technologies as solutions to patient safety challenges

In addition, delivering care to patients within the comfort and safety of their own homes (including care homes) has been enabled by NHSX through the launch of remote monitoring procurement dynamic purchasing system or DPS. The DPS will make it easier for NHS and social care organisations to select and use the right remote monitoring platforms for patients through a needs-based approach, which takes into consideration the preferences and capabilities of patients to manage their digitally enabled care in the home.

Purpose

The purpose of this Clinical Safety Case Report (CSCR) is to demonstrate that hazards associated with the implementation of Cyril have been identified and the associated risk evaluated. Where the initial risk was judged to be unacceptable, appropriate controls have been agreed to reduce residual risk to a tolerable level.

Scope

It should be noted that the scope of this CSCR is restricted to consideration of hazards that are directly associated with the implementation of Cyril. Hazards associated with the deployment of any supporting technical solution, software or other system are out of scope and safety cases for their development and deployment must be provided separately.

Cyril

Barcode Data Healthcare Solutions data platform solution, Cyril, is implemented for and hosted on AWS (Ireland Region) to leverage its comprehensive security and compliance measures, such as, data centre security, data protection and encryption, asset protection and resilience, environment separation, operational security, governance framework, etc. AWS provides its certification details at https://aws.amazon.com/compliance/iso-certified/, which includes ISO/IEC 27001:2022.

The development of the platform follows well-defined HealthCare Cloud Risk Framework and Digital Data Risk Model for workload risk classification and security impact analysis. The design of the platform follows AWS's Cloud Adoption Framework and AWS Well-architected Framework and apply Security by Design and Zero Trust principles to ensure rigorous security and resilience standards.

Security and compliance highlights:

- Shared responsibility model between Barcode Data Healthcare Solutions and AWS to ensure security and compliance requirements to be met.
- Follow AWS Well-architected Framework, especially the Security Pillar and Resilience Pillar to ensure data protection, resilience, and security controls.
- Deploy dedicated AWS Landing Zone and secure VPCs for each client..
- Apply data encryption in transition and data encryption at rest by default for data protection.
- Employ comprehensive tools, e.g. AWS WAF, AWS Shield, AWS Firewall, for Internet and Interface protection.
- Implement DevSecOps practice and tooling for automation and security testing at every stage of the SDLC.
- Joint responsibility and collaboration with AWS for Vulnerability management and system security patching.
- Employ protective monitoring and incident management process to ensure application health and service continuity.
- Implement role-based and policy-based access control with AWS IAM to ensure personnel security and secure user management
- Robust Identity and access management solutions for interface (API) access, 3rd Party Integration, and End user authentication.
- Implement Service Administration and Auditing capabilities, such as security logging, database activity monitoring, security & compliance alerts, etc.

The summary above provides some insights into the security posture of Barcode Data LTD's data platform. Auditing and certification are being built into the development plan of the platform. We are fully aware of the cyber security guidelines and best practices, in the context of Health Care domain, set by relevant authorities and agencies, such as ENISA, EHDS, UK NHS, etc.

Clinical Safety Management

Barcode Data Healthcare Solutions manages clinical safety through integration with Health Organisations and professional bodies. The Company gives particular consideration to the integration with the approval of Information Standards and the process by which incidents and risks are managed both internally and in partnership with our clients.

Barcode Data Healthcare Solution will seek to integrate with the existing suite of clinical devices where possible, in doing so will confirm devices in situ have compliance with ISO 13458:2016 and ISO 14971:2019. Any additional devices deployed by us will be compliant with these standards, as we deploy only those products that meet the standards outlined.

Hazard Identification and Risk Analysis

The first step to preventing harm to patients through the use of these standards is to ensure a good development process that results in standards fit for purpose. Activities that have been carried out to clarify and address this potential include:

Initial patient safety assessment

What could go wrong (hazards), how often (likelihood) and how bad could it be (severity)?

What are the hazard causes?

What risk controls/mitigation is already in place?

What (if any) additional risk controls should be put in place?

Agreement was also reached relating to the transfer of risk (where applicable) to external organisations e.g. those bodies responsible for implementing the standards.

Clinical Risk Evaluation

The scope of the patient safety assessment and subsequent hazard analysis is restricted to those hazards which relate directly to the implementation and use of Cyril and the requirements of DCB0129 and DCB0160 respectively.

Risk Evaluation Process

The clinical risk associated with each hazard was scored based on two factors; the severity/consequence of harm (if the hazard were realised) and the likelihood of occurrence of that harm. For each of these factors the presence or otherwise of existing risk controls/mitigation was considered.

Risk Estimation Matrix

An inherent risk rating represents the level of risk in the absence of a control environment and is arrived at after measuring the likelihood and the consequence of an event occurring. For each impact or risk that is identified, a risk evaluation is undertaken to assign a specific score in order to determine the correct level of action.

The criteria that were used for scoring are provided below. The values obtained for severity/consequence and likelihood were then applied to the following matrix to obtain an overall risk score from 1 to 5, where 5 represents the greater risk.

Risk severity is calculated by multiplying the likelihood by the consequences of risk. The resulting score is then used to prioritise the appropriate level of action.

Risk Severity

Likelihood of Occurrence (L)	Consequence Rating				
	Catastrophic	Major	Moderate	Minor	Negligible
Certain	25	20	15	10	5
Occasionally	20	16	12	8	4
Probable	15	12	9	6	3
Unlikely	10	8	6	4	2
Improbable	5	4	3	2	1

Likelihood

Score	Likelihood	Description
1	Rare	May only occur in exceptional circumstances
1	Rare	Will only occur in exceptional circumstances
2	Unlikely	Could occur during a specified time period
3	Possible	Might occur within a given time period
4	Likely	Will probably occur in most circumstances
5	Almost Certain	Expected to occur in most circumstances

Consequences/Severity

Score	Impact	Quality
1	Negligible	Non-compliance with standard or procedure that can be managed. No patient harm
2	Minor	Developed component or system may not receive approval through assurance process. Minor injury or illness requiring minor intervention
3	Moderate	Failure to manufacture component to meet design, specification, or standards. Moderate injury requiring professional intervention
4	Major	Failure of a major component or system leading to rejection. Major injury leading to long term incapacity/disability
5	Catastrophic	Catastrophic failure of a component to function in either temporary or permanent state. Incident leading to death

Risk Exposure Score

Score	Colour	Management Control Action (MCA)
1 to 4	Very Low	No mitigation, no action is required, the risk is ALARP. Monitor to ensure that the risk remains tolerable at this level.
5 to 8	Low	Maintain assurance that the risk remains tolerable at this level. Monitor and manage by routine procedures, unlikely to need specific application of resources (managers and key staff).
9 to 12	Medium	Tolerable if the cost of reduction would exceed the improvement gained. Mitigate through management by specific reviews and monitoring of procedures (Managers) but regular monitoring should occur.
13 to 15	High	Tolerable only if risk reduction is impractical or if cost is disproportionate to the improvement gained. Mitigate by implementing controls to reduce the risk to as low as is reasonably practicable. Where this cannot happen, continual monitoring should occur.
16 to 25	Very High	Intolerable, the risk cannot be justified, expect in extraordinary circumstances. Mitigate by ceasing all related activities.

Of the 9 hazards identified, 2 were initially scored greater than 3 and hence it was agreed that additional risk controls should be put in place.

Clinical Risk Control

Full details of each hazard, the potential consequences and risk controls/mitigation can be found in the attached hazard log however a summary of the risk reduction claimed is provided below:

Summary of Risk Controls and Mitigation			
Hazard	**Initial Risk**	**Risk Controls/Mitigation**	**Residual Risk**
Hardware Failure	6	• Sensors have a heartbeat, an alert will be triggered on Help Desk Dashboard If there is no streaming of live data • Staff training to manage routine issues e.g. battery replacement and sensor maintenance • Provision of spare hardware to clients at hubs • 24/7 Service Level Agreement in Place with Sensor Hardware Provider • KPI with hardware provider within 4hrs of failure • Development of chatbot for live support • 24hr helpdesk	3
User Issues/Understanding	6	• System has been designed to provide all Patient's key information at one click. • Clinical Data is transmitted in near Real Time to provide accurate view of the Patient. • Staff training during implementation • Provision of user guides • System User Guide • Website Chat Box • 24/7 Support • Named Point of Contact. • Webpage Q&A	3

Data Security Breach	2	• RDA database in AWS • MFA and data encryption • BCDHS only access pseudonymised data using unique identifier • Role based system access • Annual penetration testing • Monthly system audits • System access controls • Staff training on induction and annually • Business Policies • Data Protection Officer in post • System Access Controls	2
Lost Hardware	3	• Encrypted 2FA • Asset Register • Replacement process with agreed KPI • RFID asset tracking solution	3
Inappropriate management of FoI Requests	2	• Staff training on FoI on induction and annually • All requests for information forwarded to lead care provider • Safeguarding/criminal offence requests forwarded to Caldicott Guardian • Privacy Notice published on website	2
AWS Failure	3	• AWS data back up • Auto back up every 6hrs • Process for client notification • Business Continuity Plan	3
Cybersecurity Attack	3	• Sophos Anti-Virus Software • Staff training inc Phishing emails • Routine Phishing emails testing programme • Annual Penetration Testing	3
Power Failure	3	• Alert when live streaming stops • Process for client notification • Business Continuity Plan	3
Internet Failure	3	• Data continues to stream through router gateway • Data immediately updates once internet restored • Process for client notification • Business Continuity Plan • Provision of router gateway where no access to Wi-Fi	3

Summary of Risk Controls and Mitigation

On the basis that the risk controls and other mitigation identified in the above table are satisfactorily implemented, the residual risk associated with all 9 of the hazards scoring 3 or less and is hence considered broadly acceptable.

Tolerability of Residual Risk		
Hazard	**Residual Risk**	**Argument for Tolerability**
Hardware Failure	3	The severity of consequences associated with this hazard cannot be reduced, however the likelihood of harm has been reduced to the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
User Issues/Understanding	3	The severity of consequences associated with this hazard cannot be reduced, however the likelihood of harm has been reduced to the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
Data Security Breach	2	The severity of consequences associated with this hazard is low and the likelihood is the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
Lost Hardware	3	The severity of consequences associated with this hazard is low and the likelihood is the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
Inappropriate management of FoI Requests	2	The severity of consequences associated with this hazard and the likelihood are the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
AWS Failure	3	The severity of consequences associated with this hazard cannot be reduced, however the likelihood of harm has been reduced to the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
Cybersecurity Attack	3	The severity of consequences associated with this hazard cannot be reduced, however the likelihood of harm has been reduced to the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
Power Failure	3	The severity of consequences associated with this hazard cannot be reduced, however the likelihood of harm has been reduced to the lowest level possible within the framework. Hence the overall risk score cannot be reduced further
Internet Failure	3	The severity of consequences associated with this hazard cannot be reduced, however the likelihood of harm has been reduced to the lowest level possible within the framework. Hence the overall risk score cannot be reduced further

Hazard Log

A copy of the Hazard Log is attached below:

DCB 0129 Hazard Log (1).xlsx

Summary Safety Statement

A total of 9 hazards have been identified, associated with the implementation of Cyril and the associated standards, and are recorded within the Hazard Log.

Provided that the risk controls and other mitigation identified in the hazard log (Section 6) are successfully implemented, the residual risk associated with the implementation of] is considered tolerable.

This clinical safety report and hazard log has been reviewed by the Clinical Safety Officer to ensure that all risks, hazards, and strategies are addressed.

Quality Assurance and Document Approval

The clinical safety work undertaken to support development of this CSCR has been conducted in compliance with the NHS Digital CSMS. This report illustrates how the requirements of DCB0129 have been applied during the development of the standards in the context of an information standard, rather than a Health IT System.

Configuration Control / Management

Maintenance arrangements for the standards required will be in accordance with the Information Commissioners Office Standards and National Data Guardians 10 Data Security Standards.

Release Management

Every release that is delivered to a health organisation is accompanied by this clinical safety case report and hazard logs are reviewed to identify and mitigate against any new hazards identified with the new release. If a release does not have safety related issues, then a statement to that affect with evidence that the system has been tested satisfactorily will be provided.