hscic Health & Social Care Information Centre

Document filename: CRM Middleware Implementation Guidance			
Directorate / Programme	Solution Design Standards and Assurance	**Project**	Clinical Risk Management
Document Reference		**NPFIT-FNT-TO-TOCLNSA-1307.01**	
Director	Rob Shaw	**Status**	Approved
Owner	Stuart Harrison	**Version**	1.0
Author	Ian Dugdale	**Version issue date**	06.06.2013

Clinical Risk Management: Middleware Implementation Guidance

Document Management

Revision History

Version	Date	Summary of Changes
0.1	19.09.2012	First draft
0.2	03.10.2012	Revised following review by Safety engineers appraisal.
0.3	19.10.2012	Revised following review by Safety engineers appraisal.
0.4	13.11.2012	Revised following review by Safety engineers appraisal.
0.5	22.01.2013	Revised following review by Safety engineers appraisal.
0.6	21.05.2013	Revised following review by Clinical Safety Officers and external appraisal.
1.0	06.06.2013	First issue

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	HSCIC Safety Engineers	22.01.2013	0.5
	HSCIC Clinical Safety Officers	21.05.2013	0.6
Gareth Butt	Quicksilva Technical Director	21.05.2013	0.6

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Rob Shaw	Programme Director	05.06.2013	1.0
Dr Maureen Baker	Clinical Director of Patient Safety	22.05.2013	1.0
Stuart Harrison	Lead Safety Engineer	22.05.2013	1.0

Related Documents:

These documents provide additional information and are specifically referenced within this document.

Ref	Doc Reference Number	Title	Version
1.	ISB 0129 Amd 39/2012	Clinical Risk Management: its Application in the Manufacture of Health Systems – Specification http://www.isb.nhs.uk/documents/isb-0129	2.0
2.	ISB 0160 Amd 38/2012	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems –	2.0

		Specification http://www.isb.nhs.uk/documents/isb-0160	
3.	NPFIT-FNT-TO-TOCLNSA-1300.02	Clinical Risk Management: its Application in the Manufacture of Health Systems – Implementation Guidance	2.0
4.	NPFIT-FNT-TO-TOCLNSA-1293.03	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Implementation Guidance	3.0
5.	NPFIT-ELIBR-AREL-DST-0406.03	ITK 2.0 Spine Mini Services Logical Interface Overview	2.0

Glossary of Terms

Term	Abbreviation	What it stands for
Clinical Safety Officer (referred to as Responsible Person in DSCN 18/2009)	CSO	Person in a Health Organisation \ Manufacturer's organisation responsible for ensuring the safety of a Health IT System in target organisation through the application of risk management.
Clinical risk		Combination of the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk analysis		Systematic use of available information to identify and estimate a risk.
Clinical risk control		Process in which decisions are made and measures implemented by which clinical risks are reduced to, or maintained within, specified levels.
Clinical risk estimation		Process used to assign values to the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk evaluation		Process of comparing a clinical risk against given risk criteria to determine the acceptability of the clinical risk.
Clinical risk management	CRM	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.
Clinical Risk Management Plan		A plan which documents how the Health Organisation \ Manufacture's organisation will conduct clinical risk management of Health IT Systems.
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 life cycle of the Health IT System.
Clinical Safety Case Report		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.

Term	Abbreviation	What it stands for
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		Repository to record the results of the clinical risk analysis and clinical risk evaluation.
Health Organisation	HO	Organisation within which health software is deployed or used for a health 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.
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.
Manufacturer		Person or organisation with responsibility for the design, manufacture, packaging or labelling of a Health IT System, assembling a system, or adapting a Health IT System before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party.
Middleware		Software that mediates between disparate applications across heterogeneous computing platforms. Allowing them to interact by providing interfaces, transformations, routing of data and the orchestration of business process flows. http://www.middleware.org/ For more information
Patient		A person who is the recipient of healthcare.
Patient safety		Freedom from harm to the patient.
Post-deployment		That part of the life cycle of the Health IT System after it has been manufactured, released, deployed and is ready for use by the Health Organisation.
Procedure		Specified way to carry out an activity or a process.
Process		Set of interrelated or interacting activities which transform inputs into outputs.
Release		A specific configuration of a Health IT System delivered to a Health Organisation by the Manufacturer as a result of the introduction of new or modified functionality.
Residual clinical risk		Clinical risk remaining after the application of risk control measures.
Safety incident		Any unintended or unexpected incident which could have, or did, lead to harm for one or more patients receiving healthcare.

Term	Abbreviation	What it stands for
Safety Incident Management Log		Tool to record the reporting, management and resolution of safety related incidents associated with the Health IT System.
Top Management		Person or group of people who direct(s) and control(s) the Health Organisation and has overall accountability for the Health IT System.

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1 Introduction

1.1 Background

This document provides useful Clinical Risk Management guidance for Manufacturers or Health Organisations developing and using, Middleware (messaging systems) as defined below. The guidance supplements the Clinical Risk Management implementation guidance for both Manufacturers [Ref. 3] and Health Organisations [Ref. 4]. Which support compliance to the safety standards ISB0129 [Ref. 1] and ISB0160 [Ref. 2] respectively. There are example generic hazards provided that can help inform decisions and assessments in complying with these standards.

Middleware definition: (also known as integration, messaging engines or services) In the context of Health IT Systems, mediates between disparate Health IT systems across heterogeneous computing platforms. Allowing them to interact by providing interfaces, transformations, routing of data and the orchestration of business process flows. It usually doesn't have much if any visible "front-end" of its own other than for configuration / monitoring purposes.

Table 1 Middleware definition

It sets out the scope of Clinical Risk Management within the context of ‘Middleware’ compliance. It may also be applicable for ITK standard accreditation processes. This document:

- outlines the scope of assurance activities for Manufacturers
- outlines the scope of assurance activities for Health Organisations
- details generic hazards provided to assist manufacturers in developing hazard logs and safety cases
- may indicate the amount of effort and resourcing any organisation must undertake in the implementation of a clinical risk management process.

It is intended as a supplement to:

- ISB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems – Implementation Guidance [Ref. 3]
- ISB 0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Implementation Guidance [Ref. 4].

For illustrative purposes Figure 1 sets out a pictorial overview showing the boundaries of Middleware assurance responsibilities, of a typical Health IT system, comprising disparate systems connected via Middleware.

1.2 Audience

The primary audience are the Clinical Safety Officers of Middleware Manufacturers seeking to demonstrate compliance ISB 0129 [Ref. 1] and Health Organisations seeking to demonstrate compliance ISB 0160 [Ref. 2].

2 Scope

2.1 In scope

The guidance is limited to Risk Management of Middleware as defined in section 1.1. Clinical risk control measures appropriate in this case will be largely system design, verification and validation. Use of administrative, implementation procedures and user training controls may be limited to system configuration hazards.

The scope of risk management for manufacturers of Middleware should as a minimum extend to the boundaries that the Middleware can influence the processing or flow of data. Health Organisations should apply risk management to the Middleware and all connecting Health Systems. This will be explained further in sections 3 and 4

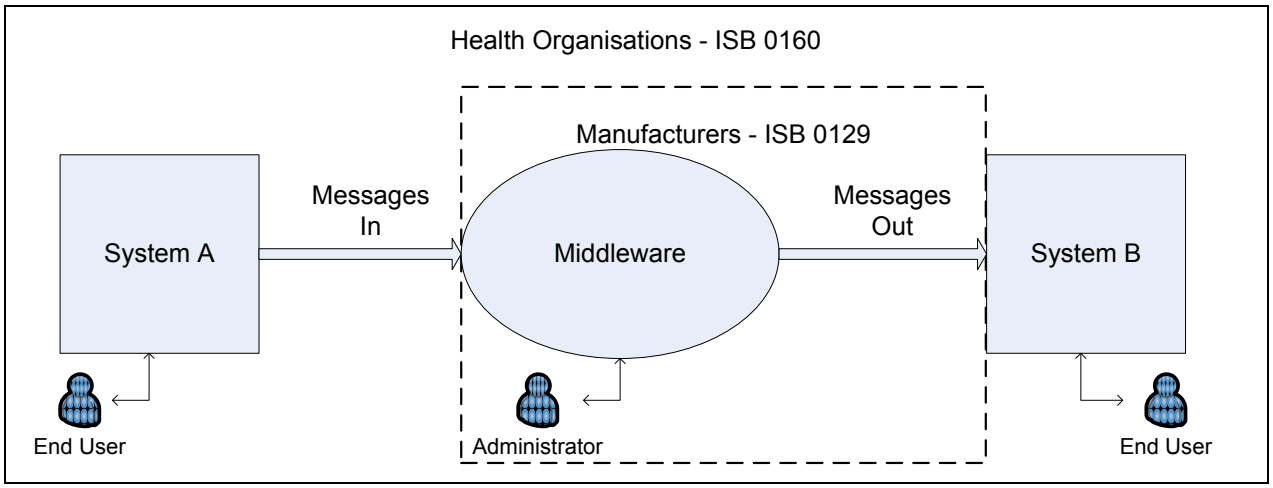

Figure 1 Pictorial overview showing the boundaries of Middleware assurance responsibilities, of a typical Health IT system, comprising disparate systems connected via Middleware.

2.1.1 Out of scope

Clinical functionality, front end application interfacing beyond the definition of middleware is out of scope.

2.2 Assumptions and Constraints

The following assumptions have been identified that apply to manufacturers:

- successful completion of the projects technical assurance criteria, this provides essential mitigation to hazards identified
- implementation of message validation rules, this provides essential mitigation to hazards identified
- IT Systems that are to be integrated by the middleware are functioning correctly. The risk assessment does not need to extend to cover failure or malfunction of any such systems

The following assumptions have been identified that apply to Health Organisations:

- holds sufficient Quality Assurance of interconnecting Health IT Systems and services
- cognisance of possible wider implications of local decisions and avoid making risk-based judgements without fully involving other organisations who may be affected [shared systems / nationally connected]
- data quality is a wider issue and not specifically within the scope of this guidance paper. Although the importance of good data quality assurance activities will provide essential mitigation to hazards.

3 Middleware Guidance for Manufacturers

The primary audience are the Clinical Safety Officers of Middleware Manufacturers seeking to demonstrate compliance ISB 0129 [Ref. 1].

This section provides guidance to support the interpretation of the requirements presented in ISB 0129 Version 2 [Ref. 1]. It is aimed at those persons in Manufacturer's organisation who are responsible for ensuring the safety of Health IT Systems through the application of clinical risk management. It considers areas that may need further explanation for Middleware systems to that given in ISB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems – Implementation Guidance [Ref. 3].

3.1 Scope Definition

ISB 0129	4.2.1	The Manufacturer MUST define the clinical scope of the Health IT System which is to be delivered.
	4.2.2	The Manufacturer MUST define the intended use of the Health IT System which is to be delivered.

Clinical scope is the extent of the functionality that is provided within the Health IT System that can be used to support or influence the administration of healthcare to a patient. The Middleware Manufacture must consider all message interactions, non functional, and configuration requirements of their Middleware Health IT system, in both normal and fault conditions. Figure 2 provides a pictorial overview showing the boundaries of Middleware Manufacturers responsibilities in demonstrating compliance ISB 0129 [Ref. 1].

Clinical functionality, front end application interfacing beyond the definition of middleware including end to end testing is out of scope.

Intended use is the definition or explanation of the functionality of Middleware and how it will be used, in terms of existing business processes or within new business process.

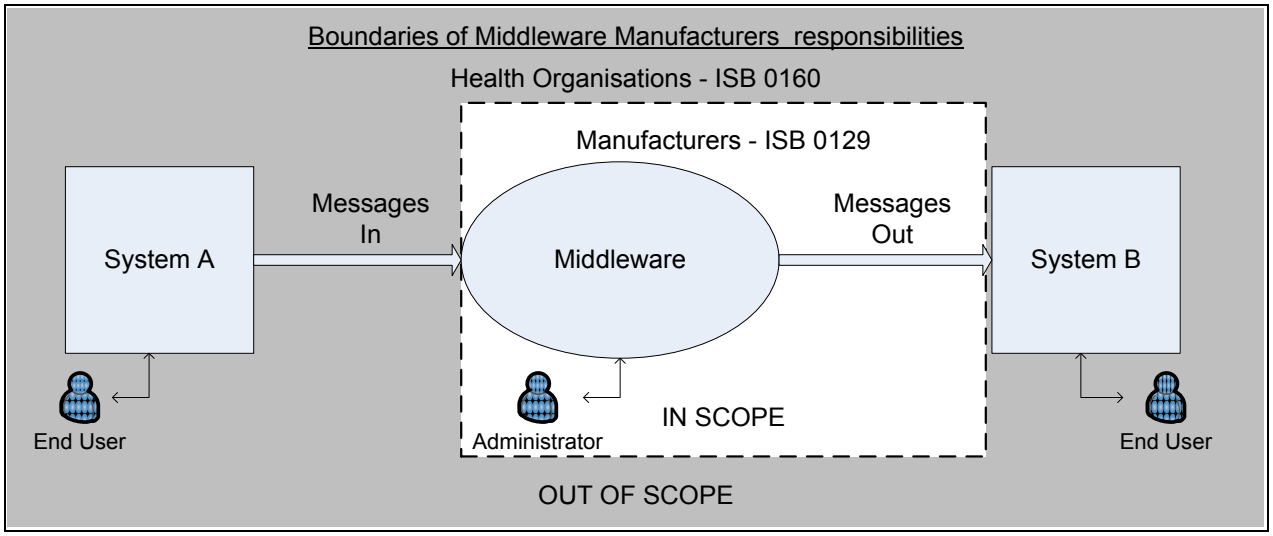

Figure 2 Pictorial overview showing the boundaries of Middleware Manufacturers' responsibilities, in assuring a typical Health IT system, comprising disparate systems connected via Middleware.

3.2 Identification of hazards to patients

ISB 0129	4.3.1	The Manufacturer MUST identify and document known and foreseeable hazards to patients with respect to the intended use of the Health IT System in both normal and fault conditions.
	4.4.1	For each identified hazard the Manufacturer MUST estimate, using the criteria specified in the Clinical Risk Management Plan: • the severity of the hazard • the likelihood of the hazard • the resulting clinical risk.

The Manufacturer will need to undertake and document hazard identification activities in order to reveal and document potential hazards to patients.

In order to identify pertinent Middleware hazards the following three key areas should be considered:

- message interactions
- non functional; performance messaging volumetric, stability
- configuration options.

A hazard workshop is strongly recommended to support identification of hazards to patients. It is of primary importance that recognition is given to both the clinical and technical aspects of the Health IT System. In the case of middleware end users may not be directly exposed to Middleware. However it is important that workshop attendees include Clinical Safety Officers and relevant subject matter experts from the Manufacturer and Health Organisation with appropriate experience to identify hazards and conduct risk assessments. Middleware messaging, performance and configuration options in both normal and fault conditions should be considered in Clinical Hazard identification activities.

Many techniques exist for hazard identification and an appropriate technique will need to be chosen depending on the application and the available expertise. Example hazard identification techniques are presented in [Ref. 3, Appendix B]. A method that focuses on information flow within a system such as HAZID may be appropriate for Middleware systems [Ref. 3, Appendix B.2].

Generic hazards and associated controls/mitigations derived from similar Health IT Systems, are listed in Appendix A.

3.3 Clinical Risk Evaluation

3.3.1 Risk Control Option Analysis

ISB 0129	6.1.1	The Manufacturer MUST identify appropriate clinical risk control measures to remove any unacceptable clinical risk.

In the case of Middleware of the five options discussed in [Ref. 3] [summarised as design, verification and validation, procedures, training, warnings] design, verification and validation are most appropriate.

A reduction in risk can be achieved through the application of one or more of the following mechanisms, listed in order of preference:

- changes to the design or the inclusion of protective measures in the Health IT System
- product verification and validation (for example, testing). A testing programme should address each of the hazards and thus provide a practicable demonstration that the claimed risk reduction has been achieved
- administrative and implementation procedures
  Note: For Middleware this may be limited configuration functionality only
- user, operator and other stakeholder training and briefing
  Note: For Middleware this may be limited configuration functionality only
- information for patient safety, including warnings.
  Note: For Middleware this may be limited configuration functionality only.

3.4 Delivery, Monitoring and Modification

ISB 0129	7.3.1	The Manufacturer MUST apply their clinical risk management process to any modifications or updates of the deployed Health IT System.
	7.3.2	The application of this process MUST be commensurate with the scale and extent of the change and the introduction of any new clinical risks.
	7.3.3	The Manufacturer MUST issue a Clinical Safety Case Report to support any modification to the Health IT System that changes its clinical risk.
	7.3.4	The Manufacturer MUST maintain an audit trail of all versions and patches released for deployment.

If Middleware functionality is modified, deleted or extended adherence to change management processes are essential to accurately define the scope, limitations or mitigations that support the clinical safety of each release.

Whenever a Middleware system is modified, a suitable and sufficient clinical risk analysis, commensurate with the scale, complexity and extent of the modification (itself established by risk analysis), should be undertaken. This will establish what, if any, new clinical risks have been introduced and their potential impact upon interconnected systems. Where it is not possible to gather all stakeholders to attend a formal hazard workshop they must be fully consulted. This will ensure that:

- no unacceptable clinical hazards are introduced as a result of a modification
- the basis of assessment of other parts of the Middleware system is reviewed and reassessed if it has changed
- potential impact upon interconnected systems is understood and communicated appropriately.

NOTE: The extent of the repeated clinical risk analysis will depend on the extent and the nature of the product modification. However, even apparently minor modifications can result in substantial clinical risks to both Middleware itself and interconnected systems thus, whatever the extent of the clinical risk analysis undertaken, it will need to be executed formally, rigorously and with due process.

4 Middleware Guidance for Health Organisations

The primary audience are the Clinical Safety Officers of Health Organisations seeking to demonstrate Middleware compliance to ISB 0160 [Ref. 2].

This section provides guidance to support the interpretation of the requirements presented in ISB 0160. It is aimed at those persons in Health Organisations who are responsible for ensuring the safety of Middleware Health IT Systems through the application of clinical risk management. It considers areas that may need further explanation specific to Middleware systems to that given in ISB 0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Implementation Guidance [Ref. 4].

A review of the Manufacturers Health IT system Safety Case[s] can inform the Health Organisations own Clinical Risk Management.

4.1 Scope Definition

ISB 0160	4.2.1	The Health Organisation MUST define the clinical scope of the Health IT System which is to be deployed.
	4.2.2	The Health Organisation MUST define the intended use of the Health IT System which is to be deployed.
	4.2.3	The Health Organisation MUST define the operational environment and users of the Health IT System which is to be deployed.

Clinical scope is the extent of the functionality that is provided within the Middleware that can be used to support or influence the administration of healthcare to a patient.

Intended use is the definition or explanation of the functionality of Middleware and how it will be used, in terms of existing business processes or within new business process.

In addition to any contribution to the Middleware Manufacturers Clinical Risk Management activities discussed in Section 3, Health Organisation must consider the wider impact of middleware upon all interconnected systems, within the operational environment. End to end testing is the responsibility of the Health Organisation. Figure 3 provides a pictorial overview showing the boundaries of Health Organisations responsibilities in demonstrating compliance ISB 0160 [Ref. 2].

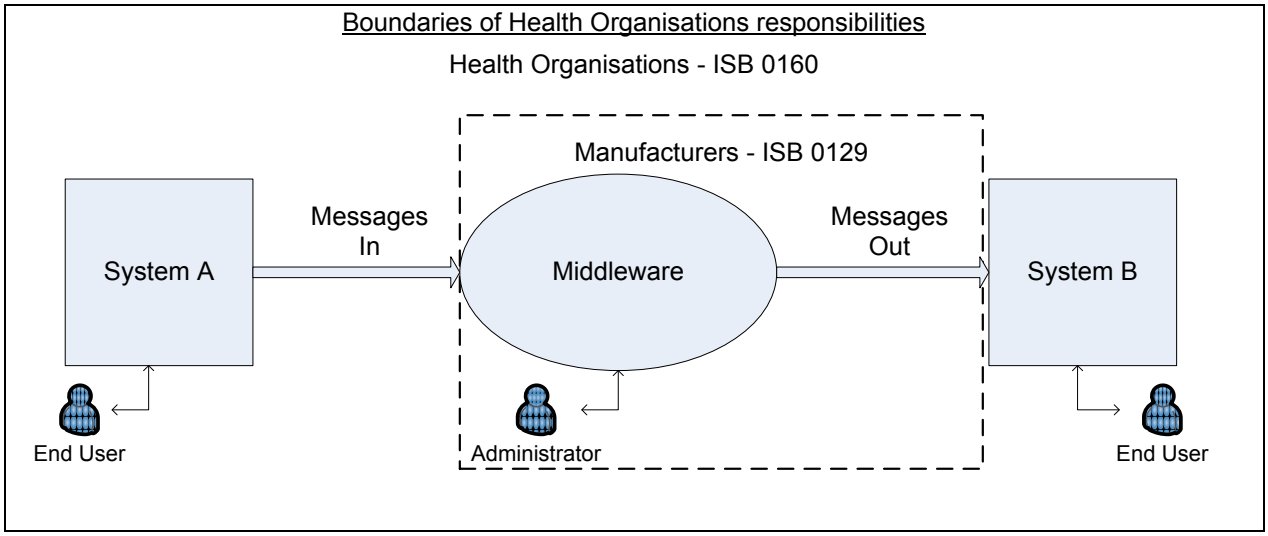

Figure 3 Pictorial overview showing the boundaries of Health Organisations responsibilities, in assuring a typical Health IT system, comprising disparate systems connected via Middleware

4.2 Clinical Risk Control

The Health Organisation is responsible for ensuring all Health IT Systems that are to be integrated by the middleware are functioning correctly. Impact assessments should be completed upon all interconnecting systems and Hazards identified in the Manufacturer's Clinical Safety Case Reports and any assumptions made will need to be considered in the specific deployment.

4.3 Implementation and completeness of Clinical Risk controls measures

ISB 0129	6.3.1	The Health Organisation MUST implement the clinical risk control measures identified in section 6.1.1.
	6.3.2	The Health Organisation MUST verify each clinical risk control measure implemented under 6.3.1.
	6.3.3	The Manufacturer MUST verify the effectiveness of each clinical risk control measure implemented under 6.3.1.
	6.4.1	The Health Organisation MUST ensure that the clinical risks from all identified hazards have been considered and accepted.

Health Organisations should consider the impact to patient safety of deployment and use of the of the Middleware system. They should complete their own Clinical Risk Management activities informed by Middleware Manufacturers and interconnected Health IT systems Safety Cases and consider:

- controls and mitigations identified and transferred to and from the Middleware system to interconnected Health IT systems or the Health Organisation
- local business processes and infrastructure consider.

The results of these activities will need to be recorded in the Health Organisations Clinical Safety Case Report.

4.4 Delivery, Monitoring and Modification

ISB 0160	7.1.1	The Health Organisation MUST assess any local customisations prior to deployment.
	7.1.2	The Health Organisation MUST undertake a formal review of the Health IT System prior to its deployment to ensure that all of the requirements of this standard have been addressed.
	7.1.3	The results of this review MUST be recorded in the Clinical Safety Case Report.

If Middleware functionality is modified, deleted or extended adherence to change management processes are essential to accurately define the scope, limitations or mitigations that support the clinical safety of each release.

Whenever a Middleware system is modified, a suitable and sufficient clinical risk analysis, commensurate with the scale, complexity and extent of the modification (itself established by risk analysis), should be undertaken. This will establish what, if any, new clinical risks have been introduced and their impact upon all interconnected systems. Where it is not possible to gather all stakeholders to attend a formal hazard workshop they must be fully consulted. This will ensure that:

- no unacceptable clinical hazards are introduced as a result of a modification
- the basis of assessment of other parts of the Middleware system is reviewed and reassessed if it has changed
- the impact upon interconnected systems is understood and communicated appropriately.

NOTE: The extent of the repeated clinical risk analysis will depend on the extent and the nature of the product modification. However, even apparently minor modifications to Middleware or interconnected Health IT systems can result in substantial clinical risks to all such Health IT systems thus, whatever the extent of the clinical risk analysis undertaken, it will need to be executed formally, rigorously and with due process.

Appendix A Generic Middleware Safety Hazards

Generic hazards derived from similar Health IT Systems under both normal and fault conditions are provided as a starting point only and are not to be considered definitive. They are presented in a consistent form providing a hazard name, description, potential clinical impact, possible cause(s) and possible control(s). They can be modified and include additional hazards and or causes specific to the middleware system under assessment.

Hazard assessments are not provided and should be completed collaboratively by the Manufacturer and Health Organisation from the results of a hazard workshop such as that described in section 3.2 above and Clinical risk analysis sections of Ref. 3 and 4.

A.1 Service is unavailable or access denied.

A.1.1 Hazard Description

Messaging between two or more systems fails. Failure to access the required data could contribute to a delay in clinical care until alternative sources of information are identified.

A.1.2 Potential Clinical Impact

Failure of the Middleware would adversely impact a Health Organisation ability to gain access to data stored on disparate systems. This may require the Health Organisation to revert to alternative means of communication with the potential for a delay in clinical care.

A.1.3 Possible Causes and Potential Controls / Mitigations

Possible Causes	Potential Controls / Mitigations
System inappropriately denies End point access due to a failure of or modifications to configure access permissions	• access to configuration functionality must be restricted to those with appropriate authority • ensure authorised users are adequately trained.
Failure of the hardware/software components, or system unavailability during cutover i.e. during or resulting from upgraded from one version to another. Should unforeseen circumstances occur, this period of unavailability could be extended	• messaging between the system and interconnecting systems will be tested to ensure that messages and transport comply with requirements • Middleware system performance monitoring is required. • Health Organisation should ensure contingency and disaster recovery processes and procedures are in place • user training to ensure users are familiar with contingency and disaster recovery

A.2 Messaging error

A.2.1 Hazard Description

Data in inbound or outbound messages is incorrect, absent, is sent to the wrong destination or not delivered. A message could contain invalid data or be in an invalid format (e.g. subtle corruption such as the omission of a numerical digit).

A.2.2 Potential Clinical Impact

Failure to correctly/fully communicate messages to a health care provider could contribute to a delay in care whilst a health care provider attempts to obtain information via alternative methods. May cause confusion if sender duplicates messages.

A.2.3 Possible Causes and Potential Controls / Mitigations

Possible Causes	Potential Controls / Mitigations
Data in inbound or outbound messages is incorrect, absent, corrupt or is sent to the wrong destination during the transport of the message.	• System performance monitoring • In/out bound message validation against agreed criteria • Reliable messaging, acknowledgement messages to source notifying them of either delivery success or failure, and details of the recipient. • The messaging between the system and interconnecting systems will be tested to ensure that the messages and transport comply with requirements.
Message corrupted or altered in transport due to transmission system error	• System performance monitoring • In/out bound message validation against agreed criteria • Reliable messaging, acknowledgement messages to source notifying them of either delivery success or failure, and details of the recipient. • The messaging between the system and interconnecting systems will be tested to ensure that the messages and transport comply with requirements.
Complete failure of message delivery.	• System performance monitoring • Reliable messaging, acknowledgement messages to source notifying them of either delivery success or failure, and details of the recipient. • The messaging between the system and interconnecting systems will be tested to ensure that the messages and transport comply with requirements.

A.3 System performance inadequate

A.3.1 Hazard Description

Poor response times from the system itself or its external dependencies.

A.3.2 Potential Clinical Impact

Poor performance of a system could result in the system not being suitable for use in the clinical environment in which it was intended. This may require the health care provider to revert to alternative means of communication with the potential for a delay in clinical care.

A.3.3 Possible Causes and Potential Controls / Mitigations

Possible Causes	Potential Controls / Mitigations
Lack of capacity or, anticipated volumes of data throughput exceed design estimations	• Performance estimates to allow for future message volume growth • System architecture allows for a degree of redundancy and throttling • Performance between the system and interconnecting systems will be tested to ensure requirements are met. • Failover testing will be carried out to prove failover capabilities and restoration of the system. • System performance monitoring • Health Organisation should ensure contingency and disaster recovery processes and procedures are in place. • Training, ensuring users are familiar with contingency and disaster recovery plans.
Excessive demand e.g. recovery after a period of downtime.	• Performance requirements to allow for foreseeable peak demands • System architecture allows for a degree of redundancy and throttling • Performance between the system and interconnecting systems will be tested to ensure requirements are met. • Failover testing will be carried out to prove failover capabilities and restoration of the system. • System performance monitoring • Health Organisation should ensure contingency and disaster recovery processes and procedures are in place. • Training, ensuring users are familiar with contingency and disaster recovery plans.

Possible Causes	Potential Controls / Mitigations
Local network or associated networks experiencing poor performance	• System architecture allows for a degree of redundancy and throttling • Health Organisation should ensure contingency and disaster recovery processes and procedures are in place. • Training, ensuring users are familiar with contingency and disaster recovery plans. • System performance monitoring

A.4 Modification to system and interconnecting system

A.4.1 Hazard Description

Changes made to systems may introduce unexpected defects in existing System.

A.4.2 Potential Clinical Impact

Failure to correctly/fully communicate messages to a health care provider could contribute to a delay in care whilst a health care provider attempts to obtain information via alternative methods. This could contribute to inappropriate delay in clinical care.

A.4.3 Possible Causes and Potential Controls / Mitigations

Possible Causes	Potential Controls / Mitigations
System configuration changes, upgrades, bug fixes or maintenance releases	• Access to configuration functionality must be restricted to those with appropriate authority. • Ensure authorised users are adequately trained. • Local change management, to include impact assessment to interconnecting systems before approval • All systems to be deployed to a test environment for local testing and only moved into live environment once proven to work as expected and signed off. • Appropriate training given to include where to seek assistance regarding each interconnecting system, if required. • Rollback, processes and procedures to restore to a previous version • System performance monitoring • Failover testing will be carried out to prove failover capabilities and restoration of the system • Health Organisation should ensure contingency and disaster recovery processes and procedures are in place. • Training, ensuring users are familiar with contingency and disaster recovery plans.

Possible Causes	Potential Controls / Mitigations
Interconnecting system configuration changes, upgrades, bug fixes or maintenance releases.	• Local change management, to include impact assessment to interconnecting systems before approval • All systems to be deployed to a test environment for local testing and only moved into live environment once proven to work as expected and signed off. • Appropriate training given to include where to seek assistance regarding each interconnecting system, if required. • Rollback, processes and procedures to restore to a previous version • System performance monitoring • Failover testing will be carried out to prove failover capabilities and restoration of the system • Health Organisation should ensure contingency and disaster recovery processes and procedures are in place. • Training, ensuring users are familiar with contingency and and disaster recovery plans.

A.5 Patient data error in interconnecting systems

NOTE: Out of scope for Middleware Manufacturer noted here for Health Organisation only

A.5.1 Hazard Description

Local or National (e.g. Patient Administration System [PAS] or national Patient Demographic Service [PDS]) data may be missing, incorrect, incomplete, out of date or corrupt.

A.5.2 Potential Clinical Impact

A Health Organisation may act on inaccurate information. If not detected, this may lead to a patient experiencing a delay in clinical care, delay in contacting a patient requiring clinical care or clinical decisions being made on incorrect information.

Duplicate patient records may be created if the national equivalent of a local record cannot be found.

A.5.3 Possible Causes and Potential Controls / Mitigations

Possible Causes	Potential Controls / Mitigations
Failure to identify duplicates of patients in local master patient Index.	• Health Organisation performs data cleansing exercise prior to go live. • Health Organisation data quality policies and procedures.

Possible Causes	Potential Controls / Mitigations
Missing, incorrect, incomplete, out of date or corrupt local data resulting in inability to identify patient or misidentification.	• Health Organisation performs data cleansing exercise prior to go live. • Health Organisation data quality policies and procedures.
Inconsistency of patient record identifiers between interconnecting systems	• Health Organisation performs data cleansing exercise prior to go live. • Health Organisation data quality policies and procedures.
Data incorrectly entered into national records e.g. PDS multiple active (non end-dated) address records exist.	• Out of scope for Middleware Manufacturer noted here for information only