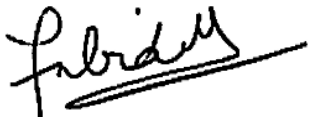
Birmingham and Solihull Mental Health NHS Foundation Trust

Clinical Safety of Digital Health Solutions Policy

Policy number and category	**C 31**	**Clinical**
Version number and date	**2**	**November 2023**
Ratifying committee or executive director	**Trust Clinical Governance Committee**	
Date ratified	**December 2023**	
Next anticipated review	**December 2026**	
Executive director	**Executive Medical Director**	
Policy Lead	**Clinical Safety Officer**	
Policy author (if different from above)	**Clinical Safety Officer**	
Exec Sign off Signature (electronic)		
Disclosable under Freedom of Information Act 2000	**Yes**	

POLICY CONTEXT

The Clinical Safety of Digital Health Solutions Policy is a policy that provides a framework that supports compliance with the Health and Social Care Act 2012 Section 250. More specifically it relates to NHS England Standards DCB 0129 and 0160.

The policy is a Clinical Risk Management framework that identifies the need to apply risk assurance processes to the procurement, deployment, maintenance, updates/upgrades and decommissioning of Clinical Systems, or systems deemed to be in scope of the policy where there is a potential to cause harm to service users.

POLICY REQUIREMENT (see Section 2)

All systems within scope of the policy must be risk assured through the processes outlined in Section 2 of this policy. Prior to the procurement of any system, the potential system should be triaged to determine whether it falls within scope of this policy.

Activities and processes within this policy are a co-ordinated effort between appropriate teams/functions and the Clinical Safety Officer. The role of the Clinical Safety Officer is to ensure that policy is being followed, and to approve hazards, incidents and clinical safety reports.

CONTENTS

1 INTRODUCTION

1.1 RATIONALE

1.1.1 This policy was previously referred to as Clinical Safety of Health IT Systems, it has been renamed to encompass a wider scope of systems and technologies.

1.1.2 The following two standards, relating to clinical safety, are accepted for publication under Section 250 of the Health and Social Care Act 2012 by the Data Coordination Board (DCB). In line with current DCB practice, each standard comprises:

- A specification, which defines the requirements and conformance criteria to be met by the user of the standard - how these requirements are met is the responsibility of the user.
- Implementation guidance, which provides an interpretation of the requirements and, where appropriate, defines possible approaches to achieving them.

1.1.3 Compliance with DCB 0129 and DCB 0160 is mandatory under the Health and Social Care Act 2012.

1.1.4 Software as a Medical Device (SaMD) is considered a type of medical device that is subject to regulatory oversight by the Medicines and Healthcare products Regulatory Agency (MHRA). Like other medical devices, SaMD must comply with the UK Medical Devices Regulations, which align with international standards and guidelines. The software is intended to be used for one or more medical purposes, such as diagnosis, monitoring, or treatment, without being part of a hardware medical device. As a regulated entity, SaMD must meet specific requirements for safety, effectiveness, and quality to be legally marketed and used in the UK healthcare system.

1.1.5 In the UK, Software as a Medical Device (SaMD) is regulated under the UK Medical Devices Regulations 2002, as amended by post-Brexit regulations, and is overseen by the Medicines and Healthcare products Regulatory Agency (MHRA). The regulations align with international standards like ISO 13485 and ISO 14971 for quality and safety.

1.1.6 The Clinical Safety of Digital Health Solutions Policy provides a framework for which Birmingham and Solihull Mental Health NHS Foundation Trust (BSMHFT) will operate under to ensure that compliance with DCB 0160 is achieved and maintained.

1.2 SCOPE OF POLICY

1.2.1 This policy is addressed to those persons in the Trust who are responsible for ensuring the safety of Digital Health Solutions through the application of risk management.

1.2.2 This is a Trust wide policy and applies to all staff, service users, volunteers, visitors and contractors regardless of location, inclusive but not limited to prison services.

1.2.3 In the deployment, use, modification or decommissioning of a Digital Health Solution, the scope of the standard and this supporting guidance includes:

- all clinical functionality which could potentially cause harm to patients.
- operational use and potential misuse of the clinical functionality and its potential to cause harm to patients.
- environmental considerations
- organisational procedures

1.2.4 This standard applies to all Digital Health Solutions including those that are also controlled by medical device regulations though the requirements are broadly consistent with the requirements of ISO 14971.

1.2.5 Whilst it is not possible to list all systems believed to be in scope, due to the volume, the following represent examples of systems that would fall in scope of this policy; Rio, EPMA, Inpatient Portal and IAPTUS.

1.2.6 Out of Scope of Policy

- Systems, technology and/or equipment that do not meet the definition of a Digital Health Solution e.g., Microsoft Office, Windows 10.
- Interdependent systems, technology and/or equipment required for the Digital Health Solution to successfully execute its functioning, unless meeting the definition of a Digital Health Solution within its own right e.g., Blackberry Enterprise Service.
- Information Governance, financial reporting, and statistical reporting tools E.g., Insight, Eclipse etc
- Medical Devices not defined as Software as a Medical Device.

1.3 PRINCIPLES (BELIEFS)

1.3.1 The Trust positively supports individuals with learning disabilities and ensures that no-one is prevented from accessing the full range of mental health services available. Staff will work collaboratively with colleagues from learning disabilities services and other organisations, in order to ensure that service users and carers have a positive episode of care whilst in our services. Information is shared appropriately to support this.

2 POLICY (WHAT)

2.1.1 All Digital Health Solutions MUST be included within the Information Asset Register.

2.1.2 A Clinical Safety Officer (CSO) should be nominated for the Trust. The Clinical Safety Officer will be responsible for ensuring the safety of a Digital Health Solution in the Trust through the application of the clinical risk management process. The nominated Clinical Safety Officer needs to satisfy the requirements set out by NHS England.

2.1.3 All solution within scope of the policy must be risk assured through the processes outlined in this section of the policy. Prior to the procurement of any system, the potential solution should be triaged to determine whether it falls within scope of this policy.

2.1.4 The procurement, update or decommissioning of any system within the Trust, should be approved via the Systems Strategy Group.

2.1.5 During procurement, individuals requesting new Digital Health Solutions MUST request a Digital Technology Assessment Criteria Tool to be completed by prospective suppliers / vendors, this should be reviewed by relevant subject matter experts to ensure compliance with relevant regulations and standards is evidenced.

2.1.6 During the full lifecycle of any system and/or technology within the scope of this policy, individuals MUST follow the Trust's Risk Management Policy.

2.1.7 All individuals involved in any activity outlined within this policy will receive training commensurate with the role and/or responsibilities.

2.1.8 Where there is evidence of the activities outlined in this policy and the below procedures are not being completed as expected, this MUST be Eclipsed. There should also be consideration for whether this constitutes an entry in the Trust's risk register. Furthermore, the Nominated CSO should be made aware.

2.1.9 The roles and responsibilities of personnel supporting the clinical risk management activities will need to be documented in the Clinical Risk Management File.

3 PROCEDURE

3.1.1 This section details procedures within the context of clinical safety of Digital Health Solutions which are required to ensure compliance with Standard DCB 0160.

3.2 INTELLIGENT PROCUREMENT

3.2.1 Risk to patient safety can be considerably reduced through intelligent procurement. A formal framework for procurement should therefore be an integral component of clinical risk management. Examples would be the inclusion of safety impacting requirements in procurement contracts placed on the supplier of the Digital Health Solution.

3.2.2 The Trust should:

- ensure that the supplier has assessed the clinical risks associated with the Digital Health Solution to be deployed is compliant with DCB 0129.
- request that the supplier's safety documentation is provided as this will form as key input into the Trust's own clinical risk management activities.
- request that a supplier agrees to implement new or updated standards that are applicable to the Digital Health Solution that is to be deployed.

3.2.3 The Trust may procure and deploy a Digital Health Solution from a Supplier which is not DCB 0129 compliant. In this situation the Digital Health Solution may not be supported by accompanying clinical risk management or safety documentation which may result in:

- an increased risk to patient safety
- the Trust having to produce the safety material that should have been provided by the supplier.

3.2.4 The Trust, as a result of conducting its own clinical risk assessment, may decide that the benefits of deploying a Digital Health Solution which does not satisfy the requirements of DCB 0129 outweigh any associated risk to patient safety. The deployment of a non DCB 0129 compliant Digital Health Solution would have to be authorised by executive lead.

3.2.5 As part of the procurement process the Trust will need to review the list of standards and identify which are applicable to their deployment and ensure that the Digital Health Solution is compliant with these standards. Such compliance could be achieved through inclusion in procurement contracts. Where a Digital Health Solution is non-compliant a defensible reason for non-compliance must be provided.

3.3 THIRD PARTY PRODUCTS

3.3.1 Many Digital Health Solutions are reliant on the use of third-party products. Such products can introduce a variety of risks particularly where a Digital Health Solution is reliant upon it or interoperates with it. Risks may also arise when software updates or patches are applied to

these products. Such products are, however, unlikely to have been risk assessed for health applications by the original supplier.

3.3.2 Where third party products and health software interact, the Trust will need to ensure that its own clinical risk management process takes this into account.

3.3.3 Suppliers who are compliant with DCB 0129 are required as part of their clinical risk assessment activities to consider any third-party product incorporated into their Digital Health Solution. The Trust should:

- confirm that any third-party product used has been considered in the Supplier's safety documentation.
- review the extent of the Supplier's contractual responsibilities for risk control both for original supply and for updates and patches which may be passed to the Trust through them. In this situation there should be a requirement for the Supplier to maintain the associated Clinical Safety Case Report and provide updates highlighting changes in the level of risk.

3.4 CLINICAL RISK MANAGEMENT FILE

3.4.1 All clinical risk documentation needs to be subject to configuration control so that any subsequent changes can be tracked.

3.4.2 The purpose of the Clinical Risk Management File is to provide a physical or logical repository of all records and documents that are produced by the clinical risk management process and required by this standard. If the documents are referenced from the Clinical Risk Management File, then they must be capable of being retrieved.

3.4.3 Consideration should be given to ensuring adequate back-up or archiving procedures are in place to guarantee that the Clinical Risk Management File and the artefacts it contains, or references remain preserved and recoverable throughout the life of the Digital Health Solution, including decommissioning.

3.5 CLINICAL RISK MANAGEMENT PLAN

3.5.1 The purpose of the Clinical Risk Management Plan is to document and schedule the clinical risk management activities to support the safe deployment, maintenance and decommissioning of the Digital Health Solution.

3.5.2 The Clinical Risk Management Plan SHOULD:

- define and describe the Digital Health Solution and the clinical context in which it will be used.
- state the relevant procedures, policies and resources required to ensure effective and efficient clinical risk management.
- adhere to the Trust's quality improvement and project management processes and requirements!
- define all the phases of the Digital Health Solution lifecycle and quantify which clinical risk activities are applicable at a particular phase.
- specify the criteria that are to be used to estimate the clinical risk and evaluate the acceptability of the clinical risk.

- identify key roles of responsibility and authority for each clinical risk activity. Additionally, it needs to identify what other resources are required to support the activity, e.g., reviewer, subject matter expert, test analyst, etc.
- define those members of staff who are able to approve the safety documentation.
- record under what circumstance or periodicity the plan should be reviewed. Triggers could be at a transition to the next phase in the Digital Health Solution lifecycle, a change of resource or in line with existing governance arrangements. The motivation for review is to maintain an up to date and effective plan and to support a process of continual improvement.

3.5.3 The extent of the Clinical Risk Management Plan needs to be commensurate with the scale and clinical functionality of the Digital Health Solution whilst addressing the clinical risk management activities specified within this standard.

3.5.4 The Clinical Risk Management Plan needs to be approved by the Clinical Safety Officer prior to use.

3.5.5 The Clinical Risk Management Plan forms part of the Clinical Risk Management File.

3.5.6 Please refer to appendix 2 to establish full documentation requirements relating to Clinical Safety.

3.6 GOVERNANCE

3.6.1 The Trust wide Systems Strategy Group will maintain authority to:

- Approve/Decline procurement of Systems and Technology that are considered in scope of this policy.
- Approve/Decline Requests for Change to current Systems and Technology that are considered in scope of this policy.
- Approve/Decline the Decommissioning of current Systems and Technology that are considered in scope of this policy.

3.6.2 Individuals will be required to provide a paper and appropriate assurance documentation for the procurement of any Systems and Technology to the Systems Strategy Group.

3.6.3 Where a decision has been made, a rationale will be provided by the Systems Strategy Group for that decision and advice on how to progress.

3.6.4 Individual project, programme and systems groups/boards may develop proposals independently; however, proposals must be presented in the form of a paper to the Systems Strategy Group for a decision to be made.

3.7 TRAINING

3.7.1 It is the responsibility of individuals undertaking activities associated with this policy to ensure that they have received and maintained the appropriate level of training commensurate with their role.

3.7.2 For the purposes of simplicity, there will be three levels of training: Level One, Two and Three

3.7.3 The levels of training are broken down as follows:

Level	Type	Whom

One	Digital Clinical Safety - Essentials – e-Learning Package provided through Trust e-Learning Platform	Anyone within the Trust that wants to learn more about the requirements
Two	Digital Clinical Safety – Intermediate Awareness – e-Learning Package provided through e-Learning for Healthcare Platform	Staff working within any function where the management of a system forms part of their role, ICT Functions and Programme Management staff
Three	Digital Clinical Safety - Practitioner – 1 Day workshop run by NHS England.	Clinical Safety Officer (Statutory Requirement), Heads of ICT and Programme Management Office Functions and individuals responsible for overall compliance and accountability for risk.

3.7.4 It will be the responsibility of individuals undertaking training to keep up to date with regulatory changes, these will be communicated through policy changes and Trust communications channels by the Clinical Safety Officer, their deputy, and/or the Systems Strategy Group.

4 RESPONSIBILITIES

POST(S)	RESPONSIBILITIES	REF
Executive Medical Director	The Executive lead remains responsible for authorising the deployment of a Digital Health Solution. Within the Clinical Risk Management Plan, the executive lead will need to specify those individuals who are able to approve the clinical risk management documentation. As a minimum this will be the Clinical Safety Officer.	
Deputy Director of ICT / CIO	The Deputy Director of ICT / CIO remains responsible for the overall portfolio of ICT and Strategic Development. They will form part of the Systems Strategy Group.	
Chief Clinical Information Officer (CCIO)	The CCIO remains responsible for the overall clinical leadership of digital systems and technology. They will chair the Systems Strategy Group.	
Head of ICT	The Head of ICT will remain responsible for ensuring collaboration between ICT Staff and Clinical Leadership to enable appropriate standards to be applied and systems and	

	technology to meet compliance with all assurance requirements.	
Clinical Safety Officer	The Clinical Safety Officer (CSO) will be responsible for • approval of the Clinical Risk Management Plan to confirm that the plan is appropriate and achievable in the context of the Digital Health Solution deployment, modification, and decommissioning. • ensuring that clinical risk management activities are completed in accordance with the Clinical Risk Management Plan • the review and approval of all safety documentation including Clinical Safety Case Reports and Hazard Logs • the review of evidence in the Clinical Risk Management File to ensure it is complete and supports the Clinical Safety Case Report • providing a recommendation to executive lead regarding whether the Digital Health Solution is safe to deploy. • raising any unacceptable safety risks to executive lead.	
All Staff	All staff will be responsible for reporting any incidents or issues relating to Trust systems and technology. To remain up to date with relevant systems training and regulatory changes. See 3.7 (Training)	
ICT Staff	All ICT Staff will have responsibility to ensure they have understanding commensurate with own role and responsibilities.	
Service, Clinical and Corporate Managers/Directors	Service, Clinical, and Corporate Managers/Directors will be responsible for providing subject matter expertise relevant to specific systems and technology to help ensure that systems and technology are clinically directed.	
ICT Managers	Will be responsible for ensuring that their staff have knowledge and skills commensurate with role and responsibilities and will be responsible for ensuring that staff within the team have appropriate training and qualifications relevant to the scope of this policy.	
Policy Lead	The policy lead will be responsible for ensuring that the policy remains contemporary, and that any changes in	

	legislation, regulations and/or standards are appropriately reflected within policy amendments and cascade to appropriate stakeholders.	

5 DEVELOPMENT AND CONSULTATION PROCESS

CONSULTATION SUMMARY		
Date policy issued for consultation		July 2023
Number of versions produced for consultation		1
COMMITTEES OR MEETINGS WHERE THIS POLICY WAS FORMALLY DISCUSSED		
WHERE ELSE PRESENTED	**SUMMARY OF FEEDBACK**	**ACTIONS / RESPONSE**

6 REFERENCE DOCUMENTS

6.1 RELEVANT LEGISLATION, POLICIES, PROCEDURES AND PROCESSES

- This policy may have interdependencies on the below legislation and Trust policies, procedures, and processes. It is therefore advisable to consider them in relation when ensuring overall compliance with this policy.
- This policy should also be reviewed on any updates to the below legislation and Trust policies, procedures, and processes.

6.2 LEGISLATION

- Computer Misuse Act 1990
- Data Protection Act 2018 and General Data Protection Regulation
- Equality Act 2010
- Freedom of Information Act 2000
- Health and Safety Act at Work 1974
- Health and Social Care Act 2012 (Specifically Section 250)
- National Health Service Act 2006
- Regulation of Investigatory Powers Act 2000
- The Copyright, Designs and Patents Act 1988
- The EU Regulation on In Vitro Diagnostic Devices 2017/746
- The EU Regulation on Medical Devices 2017/745

6.3 TRUST POLICIES

- C 25 Duty of Candour
- C 41 WHAT Handover Policy
- C 42 Internet Access Policy
- C 58 Learning from deaths
- CG 01 Policy Development and Management
- CG 09 Business Continuity Policy
- CG 20 Remote Working and Remote Access Policy
- IG 02 ICT Policy
- IG 09 Registration Authority Policy
- HR 05 Professional Registration
- RS 01 Risk Management Policy
- RS 02 The Reporting, Management and Learning from Incidents policy
- RS 16 Health and Safety Policy
- RS 19 Diagnostic and Therapeutic Equipment
- SFI 01 Standing Financial Instructions

6.4 PROCUREMENT REGULATIONS

- Public Contract Rules 2015
- Future Operating Model
- Standing Financial Instruction – Waivers
- Procurement Strategy

7 BIBLIOGRAPHY

No bibliographical information to add to section.

8 GLOSSARY

TERM	DEFINITION
Clinical Safety Officer (previously referred to as Responsible Person)	Person in a Trust responsible for ensuring the safety of a Digital Health Solution in that organisation through the application of clinical 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	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 Trust will conduct clinical risk management of a Digital Health Solution.
Clinical Risk Management Process	A set of interrelated or interacting activities, defined by the Trust, to meet the requirements of this standard with the objective of ensuring clinical safety in respect to the deployment of Digital Health Solutions.
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 Digital Health Solution.
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 Digital Health Solution's lifecycle.

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 Digital Health Solution.
Trust	Organisation within which a Digital Health Solution is deployed or used for a healthcare purpose.
Digital Health Solution	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 Supplier to customers.
Issue	The process associated with the authoring of a document. This process will include reviewing, approval and configuration control.
Likelihood	Measure of the occurrence of harm.
Lifecycle	All phases in the life of a Digital Health Solution, from the initial conception to final decommissioning and disposal.
Supplier	Person or organisation with responsibility for the design, manufacture, packaging or labelling of a Digital Health Solution, assembling a system, or adapting a Digital Health Solution 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.
Patient	A person who is the recipient of healthcare.
Patient Safety	Freedom from harm to the patient.
Post-Deployment	That part of the lifecycle of a Digital Health Solution after it has been manufactured, released, deployed and is ready for use by the Trust.
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 Digital Health Solution delivered to a Trust by the Supplier 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 patient's receiving healthcare.
Safety Incident Management Log	Tool to record the reporting, management and resolution of safety incidents associated with a Digital Health Solution.
Severity	Measure of the possible consequences of a hazard.
Third Party Product	A product that is produced by another organisation and not by the Digital Health Solution Supplier. Examples include operating systems, library code, database and application servers and network components.
Executive	Person or group of people who direct(s) and control(s) the Trust and has overall accountability for a Digital Health Solution.

9. AUDIT AND ASSURANCE

ELEMENT TO BE MONITORED	LEAD	TOOL	FREQ	REPORTING COMMITTEE
System Registry	CSO	TBD	Contemporaneously	System Strategy Group
Eclipse Incidents	CSO	TBD	Contemporaneously	System Strategy Group
Clinical Safety Case Reports	CSO	TBD	Contemporaneously	System Strategy Group
Systems awaiting procurement, update, decommissioning	CSO	TBD	Contemporaneously	System Strategy Group
Training Records	Relevant Managers	TBD	Contemporaneously	System Strategy Group
Hazard and Incident Logs	CSO	TBD	Contemporaneously	System Strategy Group

10 APPENDICES

APPENDIX 1 - Equality Impact assessment
APPENDIX 2 - Clinical Risk Management Activities and Documentation Process Map
APPENDIX 3 - Hazard Log
APPENDIX 4 - Clinical Safety Case
APPENDIX 5 - Clinical Safety Case Report (s)
APPENDIX 6 - Safety Incident Management Log
APPENDIX 7 - Software as a Medical Device (SaMD)

10.1 APPENDIX 1 – EQUALITY ANALYSIS SCREENING FORM.

Title of Proposal	**Clinical Safety of Digital Health Solutions Policy**		
Person Completing this proposal	**Shaun Kelly**	**Role or title**	**Chief Nursing Information Officer / Nominated Clinical Safety Officer**
Division	**Corporate**	**Service Area**	**Programme Management Office**
Date Started	**24th July 2023**	**Date completed**	**24th July 2023**
Main purpose and aims of the proposal and how it fits in with the wider strategic aims and objectives of the organisation.			
• To provide a risk assurance framework around the procurement, deployment, usage, maintenance, updating/upgrading and decommissioning of Health Information Technology Systems within the scope of the policy. • To ensure that patient safety is considered in the full lifecycle of Health Information Technology Systems within the scope of the policy. • To ensure that identified hazards and risks associated with the Digital Health Solutionss are mitigated and that the risks and hazards are reduced as low as practicably possible. • To ensure compliance with the Health and Social Care Act 2012 Section 250 and to ensure that the standards as determined by NHS England and the Data Co-ordination Board (DCB) are adhered to.			
Who will benefit from the proposal?			
• Service Users will benefit from this policy in an indirect way as it ensures that the systems and technology that support the delivery of care and treatment are risk assured, this in turn allows for reduction / elimination of the likelihood that any malfunction could lead to harm.			

Does the policy affect service users, employees or the wider community? **Add any data you have on the groups affected split by Protected characteristic in the boxes below. Highlight how you have used the data to reduce any noted inequalities going forward**
• The policy aims to improve the safety of systems and technology within scope, positively impacting service users, employees, and the wider community.
Does the policy significantly affect service delivery, business processes or policy? **How will these reduce inequality?**
• The policy has minimal impact on service delivery, business processes and policy. No negative or positive impact to reductions in inequality are expected.
Does it involve a significant commitment of resources? **How will these reduce inequality?**
• This policy does not require a significant commitment to resource. No negative or positive impact to reductions in inequality are expected.
Does the policy relate to an area where there are known inequalities? (e.g. seclusion, accessibility, recruitment & progression)
• This policy does not directly relate to an area where there are known inequalities, however the approach taken should have a positive impact on digital accessibility.
Impacts on different Personal Protected Characteristics – *Helpful Questions:*

Does this proposal promote equality of opportunity? *Eliminate discrimination?* *Eliminate harassment?* *Eliminate victimisation?*	*Promote good community relations?* *Promote positive attitudes towards disabled people?* *Consider more favourable treatment of disabled people?* *Promote involvement and consultation?* *Protect and promote human rights?*

Please click in the relevant impact box and include relevant data

Personal Protected Characteristic	No / Minimum Impact	Negative Impact	Positive Impact	Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.
Age	**No Impact**			
Including children and people over 65 Is it easy for someone of any age to find out about your service or access your proposal? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability	**No Impact**			
Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				
Gender	**No Impact**			

This can include male and female or someone who has completed the gender reassignment process from one sex to another Do you have flexible working arrangements for either sex? Is it easier for either men or women to access your proposal?				
Marriage or Civil Partnerships	**No Impact**			
People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?				
Pregnancy or Maternity	**No Impact**			
This includes women having a baby and women just after they have had a baby Does your service accommodate the needs of expectant and post-natal mothers both as staff and service users? Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?				
Race or Ethnicity	**No Impact**			
Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees What training does staff have to respond to the cultural needs of different ethnic groups? What arrangements are in place to communicate with people who do not have English as a first language?				
Religion or Belief	**No Impact**			
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? When organising events – Do you take necessary steps to make sure that spiritual requirements are met?				

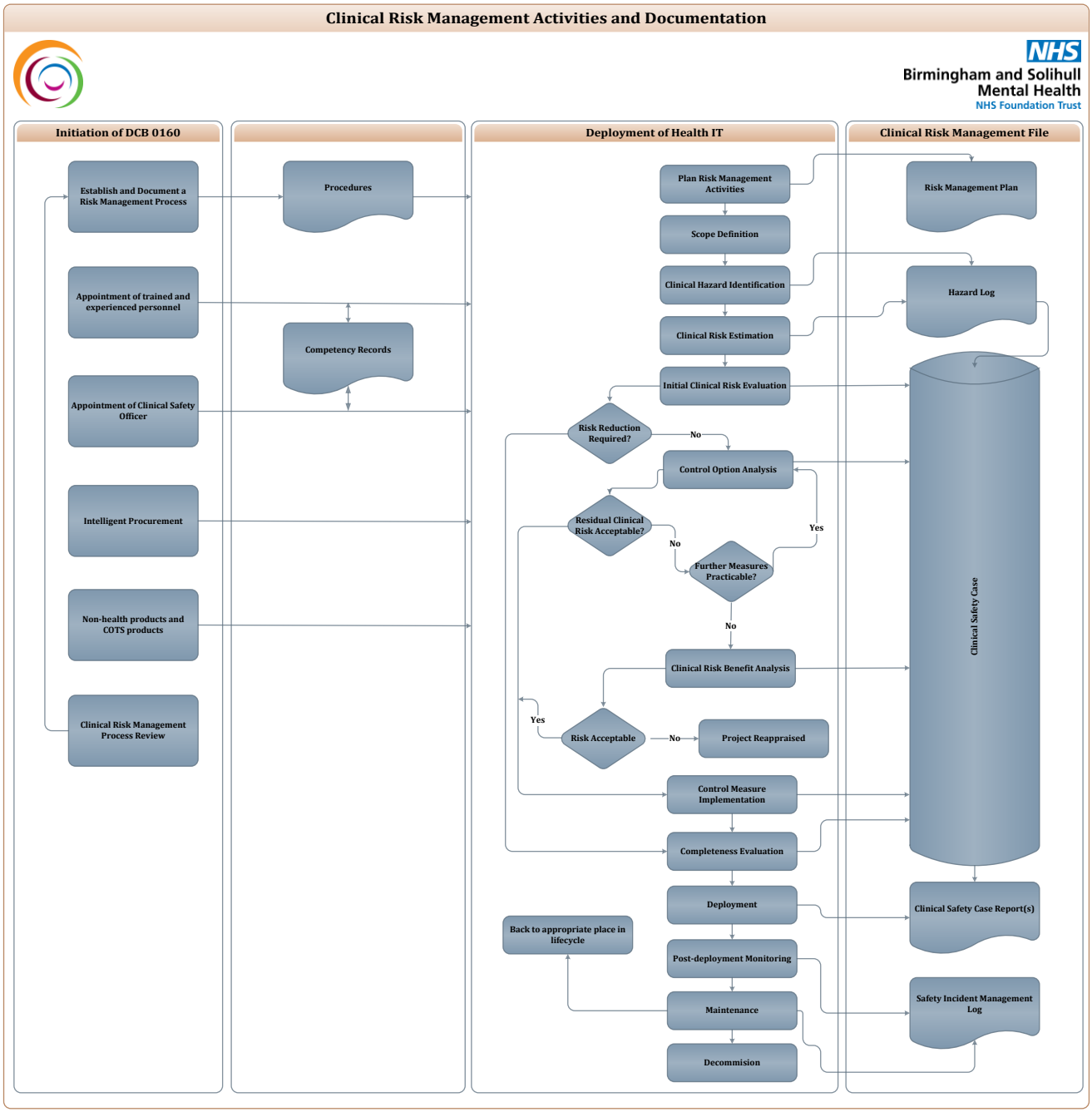
Sexual Orientation	**No Impact**			
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples? Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?				
Transgender or Gender Reassignment	**No Impact**			
This will include people who are in the process of or in a care pathway changing from one gender to another Have you considered the possible needs of transgender staff and service users in the development of your proposal or service?				
Human Rights	**No Impact**			
Affecting someone's right to Life, Dignity and Respect? Caring for other people or protecting them from danger? The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)				

	Yes	**No**		
What do you consider the level of negative impact to be?	**High Impact**	**Medium Impact**	**Low Impact**	**No Impact**
				No Impact

If the impact could be discriminatory in law, please contact the **Equality and Diversity Lead** immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required. If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the **Equality and Diversity Lead** before proceeding. If the proposal does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the **Equality and Diversity Lead.**
Action Planning:
How could you minimise or remove any negative impact identified even if this is of low significance?
• There has been no identified impact within the associated domains.
How will any impact or planned actions be monitored and reviewed?
• There has been no identified impact within the associated domains; however this will be reviewed on an ongoing basis. These domains will be considered in the full lifecycle of systems and technology.
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.

• During the full lifecycle of systems and technology, the associated domains will be considered to ensure that systems and technologies do not negatively impact individuals with protected characteristics,
Please save and keep one copy and then send a copy with a copy of the policy to the Senior Equality and Diversity Lead at **bsmhft.edi.queries@nhs.net**. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis

10.2 APPENDIX 2 – CLINICAL RISK MANAGEMENT ACTIVITIES AND DOCUMENTATION PROCESS MAP



The above process map provides a visual overview of Clinical Risk Management Activities and Documentation required by NHS England to ensure compliance with DCB 0160 and the Health and Social Care Act 2012 Section 250.

10.3 APPENDIX 3 – HAZARD LOG

10.3.1 The Hazard Log is a mechanism for recording and communicating the on-going identification and resolution of hazards associated with the Digital Health Solution. It is organised so that it enables a systematic approach to the management of hazards and supports the effective collation of safety case evidence. Such on-going revisions will:

- incorporate new hazards, when identified.
- record the mitigation of defined hazards through the implementation of clinical risk control mechanisms.
- reference supporting evidence.
- record the status of actions.

10.3.2 Whilst the Hazard Log is a living document and continues to be updated during the lifecycle of the Digital Health Solution, a base-lined version is to be issued with each Clinical Safety Case Report.

10.3.3 Each version of the Hazard Log MUST be reviewed and approved by the Clinical Safety Officer to signify that the clinical safety information recorded is accurate and appropriate.

10.3.4 An example Hazard Log template is presented at Table 2. It is not prescriptive or definitive but illustrates how, reading from left to right, a well-structured Hazard Log supports effective clinical risk management and promotes the collection of relevant evidence in a timely manner. Table 2 summarises the entries that are recorded in each column of a Hazard Log.

10.3.5 Table 2 – Hazard Log Entries

FIELD	DESCRIPTION
Hazard number	A unique number for the hazard
Hazard name	A short descriptive name for the hazard
Hazard description	A short description of the hazard
Potential Clinical Impact	Description of effect of hazard in the care setting and potential impact on the patient
Possible Causes	Possible cause(s) that may result in the hazard. These may be technical, human error, etc. Note: a hazard may have multiple causes
Existing Controls	Identification of existing controls or measures that are currently in place and will remain in place post implementation that provide mitigation against the hazard, i.e. used as part of initial Hazard Risk Assessment

INITIAL HAZARD RISK ASSESSMENT	
Severity	The severity of the hazard as defined in Table 7
Likelihood	The likelihood of the hazard as defined in Table 8
Risk Rating	The derived risk rating from the combination of likelihood and severity according to Table 9
ADDITIONAL CONTROLS	
Design	Identification of design features or configurations implemented in the Digital Health Solution in order to provide mitigation against the hazard.
Test	Identification of testing to be completed in order to provide mitigation against the hazard
Training	Identification of training to be implemented in order to provide mitigation against the hazard.
Business Process Change	Identification of any Business Process Changes implemented in order to mitigate against the hazard
RESIDUAL HAZARD RISK ASSESSMENT	
Severity	The severity of the mitigated hazard as defined by Table 7
Likelihood	The likelihood of the mitigated hazard as defined by Table 8
Risk Rating	The derived mitigated risk rating from the combination of likelihood and severity according to Table 9
ACTIONS	
Summary	Summary of the action being taken with regard to mitigation of the hazard or individual causes
Owner	The owner of the action
Hazard Status	The status of the hazard: • 'Open' not all clinical risk management actions, owned by the Supplier, in respect of this hazard, have been completed. • 'Transferred' all clinical risk management actions owned by the Supplier, in respect of this hazard, have been completed but not all actions, owned by the deploying Trust, have been completed. • 'Closed' all clinical risk management actions in respect of this hazard have been completed.

10.4 APPENDIX 4 – CLINICAL SAFETY CASE

10.4.1 The Clinical Safety Case is a structured argument which is supported by a body of relevant evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment. The argument provides an explanation of how the supporting evidence can be interpreted as indicating that the Digital Health Solution exhibits an adequate degree of safety, e.g. by demonstrating compliance with requirements or sufficient mitigation of identified hazards.

10.4.2 The supporting evidence is the result of observation, analysis, testing or simulation that provides information from which system safety can be claimed.

10.4.3 Parallels can be drawn between a Clinical Safety Case and legal proceedings:

- presentation of a defence (argument) without evidence is unfounded; how does the defence hold?
- presentation of evidence without a legal argument is unexplained; what is the meaning of the evidence?

10.4.4 The Clinical Safety Case should not be thought of as a physical issued document but rather the intellectual planning that needs to be considered and undertaken in order to establish the safety argument and generate the supporting evidence. Every effort should be made to establish the safety argument as soon as practical in the lifecycle. This will ensure that resource and effort is directed efficiently to generate relevant evidence. If consideration of the safety argument is left until later in the lifecycle it may become difficult to explain how the available evidence supports claims over the safety of the Digital Health Solution. Such an approach may result in gaps or lack of evidence which may result in additional work, delays and increased costs.

10.4.5 The Clinical Safety Case will evolve during the lifecycle of the Digital Health Solution and is to be reviewed to ensure that it continues to provide sufficient confidence in the safety of the Digital Health Solution.

10.4.6 The relationship between the Clinical Risk Management File, the Clinical Safety Case and the Clinical Safety Case Report can be understood by considering a filing cabinet analogy:

- the filing cabinet itself can be thought of as the Clinical Risk Management File, i.e., the repository in which relevant information is stored.
- the organisation, indexing and cross referencing of the information within the filing cabinet can be thought of as the Clinical Safety Case, i.e., the planning and structure.
- the retrieval of information from the filing cabinet can be thought of as the Clinical Safety Case Report, i.e., presentation of information that has previously been organised to support a safety position at any point in time. It is permissible for this presentation to be incomplete at a point in time. For example, it may not be possible to present evidence at an early iteration of the report, but it should be possible to present the need for that evidence.

10.5 APPENDIX 5 – CLINICAL SAFETY CASE REPORT (S)

10.5.1 The Clinical Safety Case Report is the physical document that summarises all the key elements of the Clinical Safety Case and references all supporting material in a clear, comprehensible and concise format. It serves to communicate the Clinical Safety Case to the end users and Executive but also where appropriate to other bodies such as regulators.

10.5.2 As the underlying Clinical Safety Case continues to evolve during the Digital Health Solution lifecycle, then there is a need to issue Clinical Safety Case Reports in support of key milestones.

10.5.3 Typically, a Clinical Safety Case Report will be issued at:

- Pre-Deployment: The supplier's Clinical Safety Case Report will be a key input to support the transition to live use of the Digital Health Solution. The scope of the Clinical Safety Case Report will extend to cover both normal and abnormal modes of system operation including associated recovery procedures. Human factors and the possibility of user error will be important considerations. Hazards identified in the Supplier's Clinical Safety Case Report and any assumptions made about clinical use will need to be considered in the specific deployment. The integration and the interaction of the Digital Health Solution with other systems will also need to be considered from a clinical risk perspective.
- Post Deployment: If assumptions made at pre-deployment about the intended use or operating environment are not realised during use then the Clinical Safety Case will need to be re-examined and the effect on the Digital Health Solution re-documented in a Clinical Safety Case Report. Similarly, if the anticipated benefit of clinical risk control measures is not realised then the Clinical Safety Case will need to be re-examined and the effect on the Digital Health Solution re-documented in a Clinical Safety Case Report.
- Maintenance: If during use, the Digital Health Solution is subjected to any change or modification or if its operating environment or clinical use is changed then the Clinical Safety Case Report needs to be re-evaluated and re-issued as appropriate. In practice this will involve undertaking clinical risk analysis, evaluation and control activities on the changes introduced and also on new or impacted interfaces within the system.
- Decommission: Here the focus of the clinical risk management process will be to identify, analyse, evaluate and control those hazards associated with removing the Digital Health Solution from service rather than preserving the level of clinical risk associated with its use. Consideration needs to extend to include any clinical risk associated with retaining any clinical capability, existing interfaces with any other retained and integrated system, preservation and migration of health information and back-up or recovery requirements.

10.5.4 A single Clinical Safety Case Report may be maintained; being re-issued in accordance with local configuration control procedures, or individual standalone Clinical Safety Case Reports may be issued.

10.5.5 The Clinical Safety Case Report is the primary vehicle for presenting a statement of the clinical safety of the Digital Health Solution. It therefore needs to be a readable document rather than simply a listing of the Clinical Safety Case or the content of the Clinical Risk Management File.

10.5.6 It needs to provide the reader with:

- a summary of all the relevant knowledge that has been acquired relating to the clinical risks associated with the Digital Health Solution at that point in the lifecycle
- a clear and concise record of the process that has been applied to determine the clinical safety of the Digital Health Solution
- a summary of the outcomes of the assessment procedures applied
- a clear listing of any residual clinical risks that have been identified and the related operational constraints and limitations that are applicable.

10.5.7 The structure of a Clinical Safety Case Report will reflect the organisation of the underlying Clinical Safety Case, which in turn will be influenced by the requirements of this standard. An example structure is provided in Table 6 but should not be considered to be prescriptive or definitive.

10.6 APPENDIX 6 – SAFETY INCIDENT MANAGEMENT LOG

10.6.1 The Trust needs to establish and use a Safety Incident Management Log to support the effective communication, resolution and archiving of safety related incidents. The log should be used during the deployment, use, maintenance or decommissioning of a Digital Health Solution. A Safety Incident Management Log could either be kept for a specific Digital Health Solution or as a single central log.

10.6.2 The Safety Incident Management Log should serve to provide a common portal to all Trust staff so that they have an up-to-date view of the status and management of both current and historical safety incidents associated with a Digital Health Solution. Use of the log needs to be limited to record only those incidents that result or have the potential to result in a clinical risk.

10.6.3 The Safety Incident Management Log should record the following parameters:

- Reference Number: Unique identifier
- Reported by: Name and contact details of person reporting the incident
- Reported Date: Date on which the incident was reported
- Incident Summary: Narrative of incident including as much detail as is available, for example, prevailing conditions, causes and observed effects including any harm that occurred
- Clinical Risk Assessment: Determination of clinical risk by considering severity of the incident, the likelihood of re-occurrence and known mitigation for relevant hazards
- System Configuration: Details of system affected
- Journal: Record of work conducted, including date and time, to resolve the incident. This entry would also identify any permanent risk control measures introduced to prevent re-occurrence. Should include “who” “when” and “what”
- Made Safe Date: Date at which the incident was made safe through the introduction of short-term risk controls
- Closed Date: Date at which the incident was resolved through the introduction of permanent risk control measures
- Cause: Summary of root cause analysis conducted.

10.7 APPENDIX 7 - SOFTWARE AS A MEDICAL DEVICE (SAMD)

Software as a Medical Device (SaMD) in the United Kingdom is a category of standalone software applications designed to perform one or more medical functions without being integrated into a hardware medical device. These applications are subject to regulatory oversight by the Medicines and Healthcare products Regulatory Agency (MHRA) and must comply with the UK Medical Devices Regulations 2002, as amended by post-Brexit regulations.

Appropriate Criteria for SaMD in the UK:

1. Medical Purpose: The software must serve a specific medical function, such as diagnosis, treatment, monitoring, or prevention of medical conditions.

2. Standalone Functionality: SaMD in the UK operates independently and does not require a specific hardware interface to perform its medical functions.

3. Regulatory Compliance: SaMD must adhere to the UK Medical Devices Regulations 2002 and any subsequent amendments. It is overseen by the MHRA, which provides specific guidelines for software used in healthcare.

4. Quality and Safety Standards: The software must align with international standards like ISO 13485 for quality management systems and ISO 14971 for risk management to ensure it meets both local and global quality and safety benchmarks.

5. Clinical Validation: Clinical evidence must be provided to demonstrate that the SaMD performs as intended for its specified medical purpose in a UK healthcare setting.

6. User Interface: The design of the user interface should consider the needs of the end-users, whether healthcare professionals or patients, to ensure effective and safe usage.

7. Data Security: SaMD must comply with UK data protection laws, including the Data Protection Act 2018, to ensure the secure handling of sensitive medical information.

8. Post-Market Surveillance: Continuous monitoring and updates are mandated to ensure ongoing efficacy, safety, and security of the SaMD.

9. Interoperability: The ability to integrate with other healthcare systems, devices, or software in the UK healthcare ecosystem is often considered a beneficial feature.

By meeting these criteria, SaMD in the UK can be considered a regulated medical device, subject to specific requirements for development, marketing, and post-market surveillance to ensure it meets the standards for patient safety and efficacy.