Best-practice guidance for the in-house manufacture of medical devices and non-medical devices, including software in both cases, for use within the same health institution

Version Record

Version number	Date	Description
1.0	18/01/2021	First issue
2.0	22/07/2022	• Original Annex A dealing with software replaced by comprehensive guidance. • Update of Annex B regarding the UK regulatory situation. • Section 2.2.2 added dealing with the transfer of custom- made devices • Additional sub-section dealing with 'borderline' devices inserted at 4.1.3 and subsequent sub-sections renumbered. • Section 4.5.3 added dealing with useability • Section 4.10 added dealing with legacy devices • A new Section 6 'Where to go for further advice' inserted and following sections renumbered • Other relatively minor textual changes.
2.1	25/07/2022	• Broken web links updated
2.2	19/04/2024	• Update of section 1.2 and Annex B regarding development of UK MD regulations from 2024. • Reference made at 4.1.3 to NHS England Standards DCB 0129 (Manufacture) and DCB 0160 (Use) regarding Health IT Systems. • Update of section 4.7.1 regarding MHRA guidance on clinical investigations of IHMU devices. • Reference made to developing UK regulation on post-market surveillance. • Improvements in sentence construction and punctuation in various places. • Correction of three typos and one spelling error.

Background

Some types of clinical activity require health institutions to manufacture medical devices for their own use. Such devices are not at present required to comply with full regulatory requirements, because they are not 'placed on the market'.

This guidance document has been developed to provide scientific, engineering, technical, clinical and risk management staff with guidance on the regulatory issues and best-practice involved in the manufacture, management and use of these devices. These recommendations will help to minimise risk and maximise patient safety.

The principles and good practice in this guidance apply equally to the creation of safe and effective non-medical devices including non-medical health or other software within health institutions.

The document will be kept under review by the IPEM Engineering Policy and Standards Panel and updated as appropriate.

Key recommendations

See Section 4 for detailed discussion.

1. Determine whether the device under consideration meets the definition of a medical device or an accessory for a medical device.
2. Carry out manufacture of devices under a Quality Management System that has been set up and approved to comply with an external Standard such as ISO 9001 or ISO 13485. This will cover among other things:
    1) Control of design and development;
    2) Control of production;
    3) Control of documentation;
    4) Audit, both internal and external;
    5) A designated individual responsible for best-practice compliance. Note: many Clinical Engineering Departments have quality management systems in place with senior staff who have relevant technical knowledge plus an in depth understanding of clinical and regulatory implications. They are well placed to provide and support an individual to undertake this role (see 4.2.5).
3. In addition to establishing detailed specifications for device function and design, it is vital to determine the essential safety and performance requirements that the item must meet.
4. Undertake a formal risk assessment and risk management process as part of the quality management system.
5. Follow a systematic design and development process.
6. Establish and maintain detailed technical documentation.
7. Undertake appropriate clinical, technical, performance and safety evaluations.
8. Plan for ongoing support of the device.
9. Plan and undertake post deployment surveillance including appropriate clinical follow-up.
10. Review legacy in-house manufactured devices.

Date first published: 15/01/2021

Current version: as per Version Record above.

Review-by date: 30th June 2025

Drafted by: a Task & Finish group on behalf of the Engineering Policy and Standards Panel. See contributors in section 8 below and in section A11 of Annex A dealing with software.

Main document peer reviewed by: Dr George Dempsey, Professor Colin Gibson, Dr Keith Ison OBE, Mr Richard E. Stubbs, Professor Paul White and Mr Adam Chalkley.

See section A11 of the Software Annex A for peer reviewers of that Annex

This Edition approved by:

Dr Anna Barnes	IPEM President
Prof. Carl Rowbottom	Director, Professional & Standards Council
Dr Warren Macdonald	Vice President, Engineering
Mr Matthew Dunn	Vice President, Medical Physics

Policy Statements and Guidance provide expert advice from the Institute of Physics and Engineering in Medicine (IPEM) on a range of technical and scientific issues. This Guidance was endorsed by the IPEM President and the Vice Presidents for Engineering and Medical Physics, supported by the Deputy Chair of the Professional and Standards Council on 18th July 2022. It is made available under a Creative Commons copyright licence. Health institutions are free to make use of this expert advice under their own responsibility.

Best-practice guidance for the in-house manufacture of medical devices and non-medical devices, including software in both cases, for use within the same health institution

Contents

1 Introduction and context

1.1 Aims and scope of this document

The aim of this document is to provide best-practice guidelines for the in-house manufacture of products of any type that are not medicinal products (for which other regulations apply) and are intended to be put into use within the same health institution or other relevant organization, i.e. are not to be 'placed on the market'. Fundamentally, the guidance is about general medical devices and accessories for a medical device, both of which are defined terms, a key aspect of which is that the manufacturer intends them to be used for a medical purpose. The term medical device(s) will be used to include both.

Active implantable medical devices, for which the risk profile is much higher, are not considered in any detail though the same principles apply. In regulatory terms, such devices are now dealt with by the EU within the Regulation (EU) 2017/745 for all types of medical devices and in the UK by the current updated amendment of SI 2002 No. 618 (see below for a link to a consolidated PDF version).

In-vitro Diagnostic Medical Devices, the regulations for which are parallel but different, are not considered in this guidance.

Full definitions are given in Annex D. However, the principles set out in this document can and should[1] be applied to the manufacture of non-medical devices. Other UK regulations may then apply, and this is dealt with in section 4.1.2.

Most of the general guidance we present below is also applicable to software which is either part of a physical medical device, or is a medical device in its own right. However, there are specific issues that relate only to software and this is covered briefly in section 5. Annex A provides a comprehensive coverage of issues relevant to all software but particularly to medical device and health software, and contains a list of further references.

Our aim is to provide guidelines based on best engineering practice that are, in the first instance, largely independent of regulatory requirements for the reasons outlined below. It is our intention to update the document from time to time as the UK regulatory situation becomes clearer.

[1] We use the word *should* throughout in the sense of *strongly advise*.

We hope that this guidance may also encourage healthcare organizations to consider how best to align their approaches to the oversight of in-house medical device manufacturing and use throughout their organization, and assist their understanding and application of relevant legislation.

This document is primarily aimed at engineers, scientists, technical staff and clinicians engaged in activities requiring in-house device development, manufacture and use. It will also be of interest to risk managers and others concerned with clinical and organizational governance and patient safety.

The guidance is written in the context of the situation existing in the UK. We use the term Trust to include all NHS health institutions in all parts of the UK (most in Wales and Scotland are formally named Health Boards). The principles are, in our opinion, universal and so should also be applied in non-NHS UK health institutions, and could be applicable in other non-UK jurisdictions.[2]

1.2 UK Regulatory context

With final exit of the UK from the EU on 31st December 2020, and the postponement of the date of full application of the new *EU Medical Devices Regulation* (EU MDR) (European Parliament and Council, 2017) to June 2021, the EU MDR has not become retained EU law throughout the UK.

The regulations in force in January 2024 regarding the manufacture of medical devices to be placed on the market (based on the *EU Medical Devices Directive* (EU MDD)) are in the *UK Medical Devices Regulations 2002 — SI 2002 No 618* (The Medical Devices Regulations, 2002), in its most up to date July 2023 version. The amendments are complex, and a consolidated text up to date as of 12 January 2024 is available here: https://www.legislation.gov.uk/uksi/2002/618/contents

We will refer to the updated UK regulations, applicable from the July 2023 as the UK MDR 2002+.

The regulations make different provisions for Northern Ireland (NI) and for England, Wales and Scotland (GB). For GB, it does not alter the existing regulations in respect of there being no explicit regulatory requirements for medical devices that are not placed on the market. For NI, under the terms of the Northern Ireland Protocol, the EU MDR, and therefore Articles 5.4 and 5.5 (the so called health institution exemption - HIE) is applicable. We have set out these Articles in Annex C below.

This amendment to UK existing law in 2023 follows a consultation process carried out in 2021 and a considered response to that. The Government's plan, outlined in January 2024, is to develop new regulations, (particularly for GB) during 2024. No proposed date of coming into force is stated but three points are worth noting:

– a stated objective is to 'bring the essential requirements for medical devices being placed on the market in GB into greater alignment with those of the EU'.

– the core regulations will include new requirements for exempt in-house manufactured devices and custom-made devices.

– the stated transitional arrangements for the GB market, in summary, extend the validity of CE marked devices to 30 June 2028 for those compliant with the EU MDD and to 30 June 2030 for those compliant with the EU MDR.

Based on the consultation document to date, it seems likely that they will address the issue of devices manufactured and used only within the same health institution but the exact details are not certain at present. Hence the continued need

[2] In various places we make reference to formal Standards and have capitalized that word except where it is in a quote from another source. For simplicity we refer to them by their international prefix, either ISO or IEC. However the UK British Standards versions, available through BSI, will have the prefix BS EN …

for best-practice guidelines at this time.

We have expanded in Annex B on the UK regulatory context as it exists from the beginning of 2024 and will keep that Annex up to date as legislation develops.

1.3 In-house manufacture and use of medical devices within the same health institution

One reason for the need for this guidance is that many health institutions have departments that manufacture medical devices but only use them within the same organization. The MHRA guidance document Managing Medical Devices (v1.3 January 2021) makes three references to in-house manufactured devices but provided no further guidance other than including them in devices to be appropriately managed. However you should be aware that this MHRA guidance is under review as of January 2024.

Examples in outline of in-house manufacture from different clinical services would be:

Example 1: A medical device to monitor patient position during Intracranial Pressure (ICP) Monitoring

Body position is known to affect intracranial pressure readings and the only way to record this information was by relying on nursing staff to input the patient's position manually whenever they could throughout the 48 hr recording period. A system was developed to automatically integrate patient position and movement data into the ICP recording, allowing easy identification of ICP pressure events that were related to the patient's movement or posture. The system comprises a three-axis accelerometer that is attached to the patient's clothing via two press stud gel electrodes, and an electronic interface box.

Example 2: Glomerular Filtration Rate (GFR) calculation spreadsheet commonly used in Nuclear Medicine

A GFR audit organized by IPEM in 2013 (55 UK centres responded) estimated that about 15,000 GFR tests are performed each year in the UK and revealed that 78% of centres use a spreadsheet and 81% of centres developed their own software in-house for the purpose of calculating patients' GFR. See also in Annex A.

Example 3: Custom-made seating for wheelchair users

For the definition of a 'custom-made' medical device, see Annex D.

Some patients/service-users of posture and mobility services require custom-made seat devices to be fitted to their wheelchair. The requirement is to enable the patient to be seated appropriately and at the same time not to compromise the stability or safety of the wheelchair. Such seats are custom-made medical devices.

Example 4: Septal Button (a custom-made medical device)

A Maxillo Facial department in a regional burns and plastic surgery hospital manufacture custom-made silicone buttons used to obturate a nasal perforation. These are used to close a perforation (hole) in the nasal septum; a condition referred to as a nasal septal perforation (NSP).

Perforations can vary in size from a few millimetres to centimetres in diameter. The button friction fits the defect and has thin flanges to retain the button and allow insertion by the clinician / patient.

Example 5: Orthotic medical devices issued to patients by podiatrists

Podiatrists sometimes supply orthotics such as custom-made insoles, padding and arch supports to relieve arch or heel pain. The orthotic is put into the patient's shoe to realign the foot or take pressure off vulnerable areas of the foot.

We refer to this and similar clinical activity as 'in-house manufacture and use' (IHMU). Such activity is clearly not 'placing the device on the market', to use a concept and phrase from both the UK MDR 2002+ (based on the EU MDD) and the EU MDR. Thus neither regulations apply.

The legal issue is whether IHMU is 'putting into service', another defined term in both sets of regulations. The EU MDD and the UK MDR 2002+ for GB are both silent on this situation and the interpretation of 'putting into service' in the UK was and remains that this Directive did not cover such activity (https://www.gov.uk/government/publications/in-house-manufacture-of- medical-devices/in-house-manufacture-of-medical-devices).

The EU MDR clarified this and introduced explicit requirements for IHMU (as set out in Annex C below) which if followed, exempted such devices from full conformity assessment. However, as explained in section 1.2 above, the EU MDR will not be applicable in GB but will apply in NI as part of the Northern Ireland Protocol to the UK-EU exit agreement.

This guidance will provide some examples as to what activity clearly is 'in-house manufacture and use' and some of the less clear situations and will expand on best-practice details.

1.4 Best-practice and state of the art

The aim of this document is, as far as possible, to provide guidance which conforms to best-practice as understood in the UK and which follows relevant standards and regulations

Now that it is clear that EU MDR rules can be applied for placing on the market in UK until 2028 or 2030 (see Annex B below) they still have applicability. The UK had significant influence on the content and wording of these and they represent 'state of the art'. We have therefore not ignored EU MDR definitions where they can be appropriately applied.

The best we can do is provide well thought out best-practice guidance for the situation we know about now, and keep that up to date as the UK regulatory regime becomes clear.

2 Health Institutions

2.1 What constitutes a 'health institution'

The words 'health institution' appear twice in the UK MDR 2002+, in Part IV dealing with in-vitro diagnostic devices (IVDs); see Regulation 33.—(1)(a) and 33.—(2)(a). The term is not listed as a defined term, but the context indicates that the applicability of this section, which gives an exemption from the UK regulations for in-house IVDs, depends on there having been no transfer to another legal entity. There is no similar explicit exemption in Part II which deals with general medical devices.

In the EU MDR, a health institution is defined in Article 2(36) as … *an organisation the primary purpose of which is the care or treatment of patients or the promotion of public health*. The MHRA issued draft guidance on the health institution exemption for public consultation but never finalised it (MHRA, 2018). On 1st January 2021 they issued an updated version for Northern Ireland which states … *This includes hospitals, laboratories, local authorities and public health institutes supporting the health care system and/or addressing patient needs, but who may not treat or care for patients directly e.g. laboratories, local authorities and public health institutes.*

The key characteristic of a health institution is that it is a legal entity. It may be physically located in many places, all under common governance.

- Many organizations are clearly health institutions:
- NHS Trusts or Health Boards;
- Private hospitals.

Some are less clear:

- Charitable trusts with a healthcare purpose.
- Non-NHS wheelchair services.

- University laboratories providing a clinical service along side research work, for example clinical gait analysis.

Where there is any doubt, authoritative legal advice should be sought.

2.2 Placing on the market and transferring between organizations.

2.2.1 General medical devices

Again, there are situations were neither set of regulations is clear, though if commercial exploitation is foreseen, then different parts of the UK MDR 2002+ or the EU MDR come into play.

The key factor regarding whether the transfer of devices becomes 'placing on the market' seems to be whether the responsibility and control of a medical device manufactured in a heath institution (a legal entity) passes out of the control and responsibility of that legal entity.

For example, on that basis, if a Clinical Engineering workshop in a hospital which is part of Trust P works with Surgeon A (employed by Trust P) and makes a surgical instrument for their use in a different hospital also in Trust P, there is no 'placing on the market'.

However, suppose Surgeon A is asked to go and perform an operation in a hospital in Trust R and, with the approval of Trust P, takes this surgical instrument with them and returns it, would that be placing on the market?

Perhaps not legally, but there are significant governance issues. Furthermore, if something went wrong, the patient would sue Trust R, so arguably the control and responsibility have passed from Trust P to Trust R. Possibly a short term loan for a particular procedure would be acceptable but a long term loan for general use would not. Legal advice would be required and governance in some Trusts would not allow this scenario.

To continue this narrative, surgical colleagues in Trust R are so impressed with the instrument that they ask for one to be made for them. To do so would be 'placing on the market' and the HIE would not be applicable.

Suppose that the Clinical Engineering department in Trust P agree to pass on to Trust R all the design and manufacturing documentation for them to make one themselves under their own full responsibility and liability, taking account of their own environment and circumstances and following best-practice. That would probably not fall within the regulations because there is no transfer of a medical device but there would need to be an agreement between the Trusts and Trust P would need to ensure they were not carrying any ongoing liability.

A different unclear situation that would need careful consideration would be when staff from two different Trusts, or from a Trust and a university agree to work collaboratively on the development of a medical device for which they do not foresee commercial exploitation. The guidance for the application of Article 5.5 of the EU MDR in Northern Ireland (see the link to this guidance in 2.1 above) in the first paragraph of the 'Transfer of devices' section on page 10 is helpful here:[3]

> "*To transfer a device between health institutions each health institution will need to apply the exemption separately with each applying the requirements of the exemption including making a separate declaration. Documentation sharing between original and transfer health institutions will facilitate this process.*"
> (Note that not all of the issues mentioned are relevant under the UK MDR 2002+ regulations applicable at present in GB)

[3] By email, the following advice was received from a senior MHRA officer: "*Although there is no legal requirement, we would definitely support the application of our HIE guidance for the purposes of GB as well, whilst we review our GB legal requirements.*"

In the case of a Trust / university collaboration, for the health institution exemption to apply, the health institution would have to be leading and taking the responsibility, since a university is unlikely to meet the definition of a heath institution.

A sentence in the MHRA guidance on borderline product (see 4.1.2 below) largely clarifies in its section 20 the situation regarding a health institution sub-contracting the manufacture of a device to an external party.

"*Where the manufacture of an 'in-house' design has been sub-contracted to an external party by the user, this will still be considered to be 'in-house' provided that the product is not supplied to any third party.*"

(NB. We take the word 'user' to mean the health institution.)

Note that the design has been done in-house. The guidance for the application of Article 5.5 of the EU MDR in Northern Ireland expands on the issue of the control of sub-contractors on page 10. It would be reasonable to assume that parts for the device, designed or specified in-house but manufactured by a sub-contractor, would also be covered by this advice, as would the buying in of sub-assemblies such as power supplies.

2.2.2 Transfer of custom made devices

For the definition of a 'custom-made' medical device, see Annex D. Such devices are issued to individual patients, though usually the ownership remains with the health institution. A possible problem arises if the care of the patient transfers from one health institution to another.

The guidance for Northern Ireland referenced above, deals with this issue in the Transfer of Devices section:

"*Some devices made, distributed and used within a health institution have been issued to an individual patient and are essential to the continuity of patient care. These devices can be transferred between legal entities without the need for a further exemption by the second health institute. Examples include implanted devices, fitted prostheses, assistive technology devices (e.g. mobility or support devices) issued to patients or patient-transfer devices.*"

Best-practice would be clear communications between the health institutions and transfer of all the technical and maintenance files to the new health institution (retaining copies). Clinical records should also be transferred. However, sometimes patients/service-users do not tell the original health institution that they are moving, so there is no formal handover. Good-practice may then have to be put in place retrospectively, when the situation becomes clear.

2.3 Devices made for a research purpose or for 'proof of concept' of an idea

A clear part of the definition of a medical device is that its manufacturer must intend it to have a specific medical purpose. Thus, a product made in-house for or in support of a research study but which is not itself the subject of that study, is not a medical device, provided it is not intended to influence the clinical management of the patients involved in the research study. If it is being used with patients or volunteers, all the usual research ethics requirements including approval of the non-medical device must be complied with. Following this best-practice guide will ensure safety and assist in getting the necessary approvals.

It is important to note that should a subsequent decision be made to use the research device in routine clinical practice, then at that point it has been given a medical purpose and therefore becomes a medical device. These guidelines should be applied, and local governance mechanisms should include consideration of this scenario. Research device should not be allowed to simply drift into routine clinical use.

Also, as outlined above, if at some point in the research project, commercial exploitation of the device is foreseen, then other parts of Regulations become

applicable. Clinical evaluation and clinical investigation need to be controlled appropriately (see 4.7.1) in conjunction with ethical approval and MHRA consent.

A particular difficulty that requires careful thought is the status of devices at the 'proof of concept' stage of development, whether or not commercial development is contemplated. Even at this early stage technical documentation should have started.

It could be argued that devices made for such proof of concept or feasibility studies are not 'medical devices' (as defined under the regulations) since they do not yet have a proven medical purpose, and therefore the regulations do not apply.

However the proof of concept may require studies with human volunteers, particularly if the device is aimed at people with specific disabilities. The designers would not know if it was a viable system worthy of further work until it had been tried with the people for whom it was being designed. However, when investigations involving volunteers are needed to take an idea forward, ethical approval is required and this regulatory distinction is not necessarily understood. Additionally, basic safety is essential.

It seems that the ethical approval process requires a 'letter of no objection' from the MHRA for a clinical investigation of a device at the product evaluation stage, but does not require this for a product clearly at the stage of 'Basic Science involving human participants'. Health institutions should consider which approach is most relevant for their activities. Some more detailed guidance is set out at 4.7.1 below.

3 Manufacture

3.1 What constitutes 'manufacture'?

Manufacture in this context is broader than taking raw materials, components or sub-assemblies and bringing them together to make an identifiable 'thing'. Manufacture encompasses medical device design, development and production. In addition to the creation of novel devices it can include modifying a device, repurposing a device, bringing together a number of devices to form a system. Additionally, software that is either embedded in a medical device or that in itself meets the definition of a medical device must be included in 'manufacture'. Furthermore, software used to control or influence a medical device i.e. from another platform, is an 'accessory for a medical device'.

Note: An accessory for a medical device (as defined, see Annex D below) is to be treated as a medical device and therefore best-practice, as outlined for in-house medical device manufacturing, should apply.

For the purpose of this best-practice guide it is sensible to adapt the wording from the MHRA guidance issued for Northern Ireland.

Where any of the actions below are not explicit in a commercial medical device manufacturer's intended purpose or instructions for use (IFU), manufacturing a medical device by a health institution could include:

- the putting together of a device from raw materials or component parts,
- the complete rebuilding of an existing device and giving it a new identity,
- making a new device from used devices,
- fully refurbishing a device[4],
- development of software (which might include scripts, compiled code, web pages, spread sheets or apps etc.) that meet the definition of a medical device,
- assigning a medical purpose to a product that is not CE marked as a medical device even if the product is CE marked under a different Directive or Regulation, e.g. the Low Voltage Directive 2014/35/EU. The MHRA have provided guidance on off-label use.

[4] NOTE: this is a defined term in the EU MDR

- putting together combinations of medical devices and other equipment,
- deviations from the instructions for use (including maintenance instructions) that significantly alter the safety, performance or function of the device, or
- using an existing medical device for a different purpose from that intended by the original manufacturer. This would also be off label use.

In the context of rehabilitation engineering, the Rehabilitation Engineering Services Management Group (RESMaG) have put together a useful document that sets out various scenarios and gives advice to achieve compliance to the EU MDR. https://resmag.org.uk/hie/. It addresses specifically Article 5.5 in the EU MDR, now no longer relevant in full in GB, but the decisions whether a device or activity constitutes in-house manufacturing and use, and how to satisfy each EU MDR requirement are helpful.

4 Key aspects of in-house manufacture and use (IHMU) guidance

In developing this guidance, we have drawn up and expanded on nine key aspects that should be considered once you have made a clear and informed decision that your proposed activity is not 'placing on the market'.

These are dealt with in detail in the rest of this section but can be summarised as follows.

1) Determine whether the device under consideration is a medical device.
2) Carry out manufacture of devices under a Quality Management System that has been set up and approved to comply with an external Standard such as ISO 13485 or ISO 9001. For services with existing, well established ISO 9001 QMS, it is important to review the scope to ensure that all aspects of IHMU are included. A QMS based on either framework must cover among other things:
    a) Control of design and development;
    b) Control of production;
    c) Control of documentation;
    d) Audit, both internal and external;
    e) A designated individual responsible for best-practice compliance. Note: many Clinical Engineering Departments have quality management systems in place with senior staff who have relevant technical knowledge plus an in depth understanding of clinical and regulatory implications. They are well placed to provide and support an individual to undertake this role (see 4.2.5).
3) In addition to establishing detailed specifications for device function and design, it is vital to determine the essential safety and performance requirements that the item must meet.
4) Undertake a formal risk assessment and develop a risk management process as part of the quality management system.
5) Follow a systematic design and development process.
6) Establish and maintain detailed technical documentation.
7) Undertake appropriate clinical, technical, performance and safety evaluations.
8) Plan for ongoing support of the device.
9) Plan and undertake post-deployment surveillance including appropriate clinical follow-up.

4.1 Is the device that you are considering manufacturing a 'medical device'?

We have given both the current UK MDR 2002+ definition (based on the MDD but with improved English) and the EU MDR definition in Annex D. The words need to be read carefully and thoughtfully. Two key phrases in the preamble of the EU MDR are, '*intended by the manufacturer …*' and '*… for one or more of the specific medical purposes:*'

At the beginning of your project, as you document the requirements and detailed specification of the device you intend to design and manufacture you should set out clearly your intention and the purpose of the device. A key step at this stage is to be certain that your requirements cannot be met or cannot be met at the appropriate level of performance by a device that is on the market.

Cost may be a factor if what you want is, for example, a simple single parameter medical device when that parameter is only available in a costly multi-parameter device. However, the true cost of one-off in-house development can be significant.

Software applications running on non-medical device platforms such as smart phones or PCs can often be difficult to categorise as to whether they are medical devices or not. The MHRA have provided a PDF based app to assist in making this decision. https://www.gov.uk/government/publications/medical-devices-software-applications-apps#history. Note that this app references the EU MDD definitions; the risk classification of software under the EU MDR is stricter than under the EU MDD. Best-practice is to refer to the stricter classifications.

4.1.1 The device is a medical device

The UK MDR 2002+ are relevant but at present include no requirements for IHMU in GB. See section 1.2 above and Annex B (which we will endeavour to keep up to date) for an explanation of the current regulatory situation. For as long as there are no regulatory rules for IHMU in your jurisdiction, these best-practice guidelines will provide a solid, defendable platform for your development.

4.1.2 The device is a 'borderline' device

Some devices may on first consideration, seem to be to be a 'medical device' but it is very important to read the definition carefully and thoroughly. It is best to use the EU MDR definition. It has been developed from the EU MDD definition, based on experience and international discussions: software aside, it is unlikely that anything considered to be a medical device under that definition would not be so considered under the current UK-GB regulations based on the EU MDD

The MHRA have provided some very useful guidance, updated in June 2023 here: https://www.gov.uk/government/publications/borderlines-with-medical-devices

Note that section 2 of this guidance says:

> *"Although the UK MDR 2002 does not use the phrase 'medical purpose', medical devices are considered to be items intended to be used in a 'medical' context. Whether or not a product is considered to have a 'medical purpose' will be defined by the manufacturer's intention for the product as defined in their labelling, instructions for use and promotional material and its mode of action in conjunction with the definition of a medical device as stated in the UK MDR 2002.*
>
> *Note that not all equipment used in a healthcare environment or used by a healthcare professional will be considered to come within the definition of a medical device."*

Section 3 of this MHRA guidance goes on to give examples of products that are not normally considered to be medical devices and some that have "*a specific primary intended medical purpose*" and in its section 5, deals with which types of 'assistive technology products' should be considered as meeting the definition of a medical device.

4.1.3 The device is not a medical device

Other UK regulations may apply. A comprehensive list of other UK regulations is given on the Health and Safety Executive website here:https://www.hse.gov.uk/work-equipment-machinery/uk-law-design-supply- products.htm

The emphasis of all these regulations is on 'placing on the market' and CE or

UKCA marking of the particular type of non-medical device. The extent to which they apply to IHMU would need careful and thorough examination. All contain appropriate 'essential health and safety requirements', usually in their respective first Annex.

In respect of The Supply of Machinery (Safety) Regulations 2008 the pre- Brexit HSE guidance said:

> *In particular, they must be designed and built to meet the relevant essential health and safety requirements listed in Annex 1 of this Directive. This requirement applies to the manufacturers of machinery, even where it is for their own use. It also applies to those who modify existing machinery to such an extent it must be considered a new machine …*
>
> *The manufacturer … carries the full responsibility for the safety and conformity of the product. This duty must be met before the product is placed on the market or put into service. …*
>
> *Users who make machinery for their own use also have the full manufactures' responsibilities for CE marking and compliance with the Supply of Machinery (Safety) Regulations. This must be done before they put the machine into service for the first time.*

(our emphasis underlined)

The current guidance is less detailed but similar. In respect of the Electrical Equipment (Safety) Regulations 2016 it seems that there is not a requirement to CE mark IHMU products. There is no defined term 'put into service' and 'manufacturer' is defined as:

> *"manufacturer" means any person who—*
> *(a)* manufactures electrical equipment, or has electrical equipment designed or manufactured; and
> *(b)* markets that electrical equipment under that person's name or trade *mark;*

Further guidance is here: https://www.gov.uk/government/publications/electrical-equipment-safety-regulations-2016.

Having no IHMU requirement for electrical equipment seems a bit inconsistent with the general advice here: https://www.hse.gov.uk/work- equipment-machinery/manufacturer.htm

However, going back to our first link, https://www.hse.gov.uk/work-equipment-machinery/uk-law-design-supply-products.htm HSE point out that Section 6 of the Health and Safety at Work etc Act 1974 (HSW Act) applies to articles and substances for use at work where other more specific product safety law does not apply.

For software that is not a medical device, as a minimum, issues such as the General Data Protection Regulations and copyright would need to be considered. In addition, NHS England have published Information Standards DCB 0129 (Manufacture) and DCB 0160 (Use), which are mandatory for those providing services in England[5]. These mandate risk management activities for "Health IT Systems" defined as products used to provide electronic information for health or social care purposes, a broader definition than that in the EU or UK MDR. The risk management activities they contain are aligned to ISO 14971:2012 - *Medical Devices: Application of Risk Management to Medical Devices* (see section 4.4) so are aligned with the best-practice discussed.

This guidance cannot give definitive legal interpretation of these various regulations; only the courts can do that. However, following best-practice as outlined in these guidelines will substantially minimise the likelihood of adverse events.

[5] Section 250 of the Health and Social Care Act 2012

From here on this guidance will assume that the product being designed and manufactured is a medical device (within which we include accessories for a medical device – as defined). However, we suggest the guidance is equally relevant to the best-practice design and manufacture of a non-medical product, taking account of the different essential safety and performance requirements (see section 4.3) and different relevant Standards.

4.2 Have a Quality Management System (QMS) in place

Many departments have put in place formal quality management systems to cover the provision of their services. We believe that the first in the NHS was the MEMO organization in Bristol in the late 1980s. The adoption of QMS Standards has expanded very considerably since then and includes ISO 9001 in Radiotherapy applications and ISO 9001 or ISO 13485 in Clinical Engineering Departments.

A QMS provides a structured framework that helps to minimise risk, including risks to patients, by ensuring that actions and decisions are considered and documented and that lessons are learned. It also provides a systematic way to capture organizational actions taken to reduce risk and prevent harm.

ISO 9001 is the internationally recognised Standard for quality management systems; it is intentionally generic, to be adoptable by organizations irrespective of their industry sector, products, type of services, or size. The generality of ISO 9001 does however mean that key requirements in specialist sectors are not explicitly captured, and as such some sector-specific QMS Standards have evolved, particularly in high risk and highly regulated industries. The international QMS Standard for design and manufacture of medical devices is ISO 13485. See Annex F for further historic detail.

4.2.1 Which QMS framework to use

a) If you have no QMS in place and you manufacture or intend to manufacture in-house (in it broadest sense as in 3.2 above) and put into use medical devices, you should (and perhaps should already have started to) put a QMS in place.

You should use ISO 13485 as your framework. The title of the document makes its purpose clear: *Medical devices. Quality management systems—Requirements for regulatory purposes.*

The Introduction, section 0.1 General says:

> *This International Standard specifies requirements for a quality management system that can be used by an organization involved in one or more stages of the life-cycle of a medical device, including design and development, production, storage and distribution, installation, servicing and final decommissioning and disposal of medical devices, and design and development, or provision of associated activities (e.g. technical support).*

It is therefore clear that an ISO 13485 QMS can be developed to cover all aspects of the work of a Clinical Engineering, Rehabilitation Engineering, Medical Physics, Scientific Computing or Informatics department or a clinical department who are engaged in manufacture of (usually) custom-made devices, for example a Maxillo-facial or Podiatry Department.

b) If you have an ISO 9001 QMS in place and you manufacture or intend to manufacture medical devices in-house and put them into use, you should first check that your QMS scope includes and covers design, development and manufacture. If not, you should first extend the scope and put in place policies and procedures to cover all aspects of IHMU, using requirements taken from ISO 13485.

You may wish to develop and put in place a plan to convert the whole of your QMS to be based on ISO 13485. Many of your existing policies and procedures can readily be moved across into the new system. There is little point, as well as cost and complexity, in running an ISO 13485 system just for design, development and

manufacture alongside an ISO 9001 system for service provision, when the former can cover all activities.

4.2.2 Internal QMS management

Both ISO 13485 and ISO 9001 allocate specific responsibilities to *top management*. If you already have a QMS in place, the allocation of these responsibilities will have been decided but if not, you will need to decide at what level in the organization these should be set. Do not go too high up the chain of command, because the person concerned needs to be actively involved and have an understanding of the QMS and its operation.

The other requirement is to have a 'management representative' though this explicit requirement has gone from ISO 9001:2015. The role is more usually described as *quality manager* or *quality lead* and the basic role description is in ISO 13485 at 5.5.2. The person appointed to this role needs to be appropriately experienced and qualified. Familiarity with, and a thorough understanding of ISO 13485 would be required. Training in internal audit would be necessary and appropriate courses are available.

4.2.3 Certification of your QMS

Internal auditing of your QMS is a requirement of both ISO 9001 and ISO 13485. External auditing and certification of your QMS is good practice and should be considered best-practice for manufacture of higher risk medical devices i.e. above risk Class I as well as medical devices that are in Class I and require sterilization or have a measurement function or are reusable surgical instruments.

Certification of an organization's QMS by an external auditing body provides independent confirmation that the QMS meets the requirements of the Standard that has been adopted. This provides the organization with assurance of effective governance and compliance to the applicable legislation. The external auditors should be accredited to certify the particular Standard being audited. In the UK, the sole agency for accrediting certification bodies is the UK Accreditation Service (UKAS). For higher risk medical devices placed on the market, the certifying body must also be a legally designated Notified Body (NB) (or a UK Approved Body (UKAB) from 1st January 2021) that satisfies prescribed capability and specialist competency requirements.

A list of organizations accredited to certify ISO 13485 quality management systems can be found on the UKAS website at – https://www.ukas.com/find-an-organisation/?q=ISO+13485+quality+management+systems&country%5B%5D=87

Any of these certification bodies may suffice for departments (e.g. Podiatry or Occupational Therapy) that only ever make risk Class I medical devices. A pragmatic but advantageous approach for such departments within a Trust or Health Board would be for them to work together to put in place a single externally certified QMS that covers multiple services. Internal cross auditing would then help share ideas and ways of working across professional boundaries.

However, departments manufacturing medical devices of higher risk classifications should select a certification body whose designated scope is appropriate to the types of medical devices being manufactured. Also note that under the EU MDR much of the software meeting the requirements of a medical device has been re-classified from risk Class I to at least the higher Class IIa and this is likely to happen in new GB regulations.

4.2.4 The role of formal accreditation in health care systems

The independent regulator of health and social care in England, the Care Quality Commission (CQC), now uses accreditation schemes that relate to a particular service to inform their inspection activity and enable them to take a proportionate approach.

Recognised accreditation schemes such as the Quality Imaging Standard, Medical Laboratories (ISO 15189) and Improving Quality in Physiological Services Accreditation Scheme (IQIPS), demonstrate a higher level of inspection and audit through peer assessment of quality and competency.

IPEM has worked with BSI to produce a Standard, BS 70000:2017 against which departments can be formally accredited, and in partnership with UKAS and NHS England has produced a new accreditation scheme for Medical Physics and Clinical Engineering services, known as MPACE.
https://www.ukas.com/accreditation/about/developing-new- programmes/development-programmes/medical-physics-and-clinical- engineering-mpace/

BS 70000 has the full title *Medical physics, clinical engineering and associated scientific services in healthcare – Requirements for quality, safety and competence*. It is based on BS EN ISO 15189:2012 *Medical laboratories. Requirements for quality and competence*.

BS 70000 is described in its Foreword as an 'accreditation standard' but states that … Fundamental to accreditation to BS 70000 is the implementation of a formal quality management system equivalent to BS EN ISO 9001. It gives both ISO 9000 and ISO 13485 as normative reference Standards (i.e. other Standards that will be required to fulfil the requirements of the base Standard). In section 4.3 'Governance and risk management' at 4.3.1b)8) 'product development and manufacture', there is a note which states:

> *NOTE For medical devices development this should be consistent with BS EN ISO 13485 and BS EN ISO 14971. For IT networks incorporating medical devices this should be consistent with BS EN 80001-1.*

The decision to seek MPACE accreditation based on BS 70000 will be determined by senior level leadership in medical physics and clinical engineering, but it seems that if design, development and manufacture of medical devices is part of a department's work, ISO 13485 certification or equivalent will be needed.

4.2.5 Person responsible for best-practice compliance

In a health institution where there are unconnected departments manufacturing medical devices for internal use (and see 3.1 for what might constitute 'manufacture' – it is quite wide) the health institution should appoint an appropriately competent individual to be responsible for monitoring, advising and reporting at an executive level on best-practice compliance across the organization.

The MHRA guidance issued for Northern Ireland, where the EU MDR is being statutorily applied, has a paragraph in the Governance section as follows:

> *Health institutions should appoint the most appropriate competent and senior person(s) with relevant expertise to sign the declaration and take responsibility for regulatory compliance of exempted devices including the supervision and control of manufacturing, and surveillance over the lifetime of the device.*

Such a person would need to be appropriately qualified and experienced, and be able to understand and advise on details of the performance, the limitations and the clinical implications of the technology being deployed, as well as the overall regulatory and best-practice requirements. Suitably experienced senior clinical engineers and clinical scientists are well placed to meet these requirements across a wide range of devices and technologies.

As has been noted in 1.2 and explained in more detail in Annex B, although there are at present no specific medical device regulatory requirements for the in-house manufacture and use of any type of manufacture of medical devices in GB, other regulatory or civil law issues may apply which could constitute a risk to the organization.

Appointment of a suitably qualified and experienced person to take such a role in all jurisdictions would help health institutions to:

a) manage the risks around in-house manufacture and use, particularly as the new regulatory framework develops in GB post January 2024 (see section 1.2),
b) coordinate expertise and compliance monitoring across the organization, and
c) take the lead for the organization in working with the MHRA.

4.3 Find out which are the 'essential safety and performance requirements' relevant to the product being designed and manufactured

4.3.1 For medical devices

Two options are available for medical devices:

The UK MDR 2002+ regulations for GB point out to Annex I, the 'Essential Requirements' of the EU MDD for the relevant essential safety and performance requirements.

The more up to date and stricter 'General Safety and Performance Requirements' of the EU MDR are in Annex I of that regulation. These would represent best-practice as being 'state of the art' and are applicable in Northern Ireland.

It is important to note that in both sets of safety and performance requirements there are broad general requirements in the first section; points 1 to 6 in the EU MDD Annex I, and points 1 to 9 in Annex I of the EU MDR. These should all be considered and are applicable in almost all cases.

An Excel based app has been developed by the Rehabilitation Engineering Department in Swansea Bay University Health Board. This provides a checklist for the General Safety and Performance Requirements in Annex I of the EU MDR. The app has been made available with a suitable disclaimer under a Creative Commons copyright licence on an open part of the IPEM website.
https://www.ipem.ac.uk/media/h2qclyq5/gspr-swansea-checklist-ver-1-1.xlsx

4.3.2 For non-medical products

Consider the points made above in section 4.1.2. Work out which of the various categories your proposed product falls into and find the relevant essential safety and performance requirements which will either be directly in the UK regulation or will be signposted from there to the associated EU Directive or Regulation.

A recent example has been the in-house manufacture of non-medical device personal protective equipment (PPE).

4.4 Risk assessment and risk management

4.4.1 Fundamentals

The fundamentals of risk assessment and risk management are that you should have in your QMS a process which meets the requirement in ISO 13485, 7.1

… The organization shall document one or more processes for risk management in product realization.
Records of risk management activities shall be maintained …

Hazard identification, risk assessment and risk management are a feature of all the essential safety and performance requirements in UK legislation that we have looked at. See section 4.1 above.

The risk assessment process requires you to:

- identify possible hazards in general terms;
- identify actual and reasonably foreseeable hazardous situations around those hazards in your particular product;
- consider hazardous situations that might arise from ergonomic factors during the use of the medical or non-medical device;

- quantify or estimate the severity of the harm that those hazardous situations might cause;
- quantify or estimate the likelihood of the occurrence of those hazardous situations;
- decide and set an acceptable level of residual risk for each hazardous situation;
- apply risk reduction measures that will reduce the initial risks to the acceptable residual level in each case;
- for medical devices in particular, consider the benefit-risk ratio and demonstrate in your risk management file that the benefits of using the medical device outweigh the identified residual risks.

Remember, nothing is 100% safe. Safety is defined as '*freedom from unacceptable risk'* (ISO 14971:2019 subclause 2.26).

The general requirement for management of health and safety at work is to reduce risk to 'as low as reasonably practicable' (ALARP), which allows technical and economic considerations to be made when judging practicability. https://www.hse.gov.uk/managing/theory/alarpglance.htm. The ALARP principle is also introduced in some risk management Standards, such as ISO 14971.

You should note however that there is a more exacting requirement under regulations for medical devices; the EU MDD and the EU MDR require risk to be reduced 'as far as possible', which does not allow for economic consideration when judging risk acceptability. The EU MDR inserted an explanatory paragraph at Annex I.2

> *The requirement in this Annex to reduce risks as far as possible means the reduction of risks as far as possible without adversely affecting the benefit-risk ratio.*

Many medical devices, for example high frequency surgery equipment or hypodermic needles, do things to patients that would be completely unacceptable without taking account of the clinical benefit-risk ratio.

Among the hazards you should consider are any risks that might arise from poor useability of the product, inadequate instructions for use or reasonably foreseeable misuse.

4.4.2 Risk reduction steps and priorities

In reducing risk, you should apply measures in this order of priority:

1) eliminate or reduce risks as far as possible through safe design and manufacture;
2) where appropriate, take adequate protective measures, including adding alarms if necessary, in relation to risks that cannot be eliminated;
3) provide information for safety (warnings/precautions/contra-indications) and, where appropriate, training to users;
4) in your instructions for use (IFU) inform users of any residual risks.

4.4.3 Risk management Standards

For medical devices in particular, but applicable for other products, the relevant Standard is ISO 14971. The current edition of the EN version is published by BSI as BS EN ISO 14971:2019 *Medical devices — Application of risk management to medical devices*

The BSI Whitepapers series which you can sign up for here: https://www.bsigroup.com/en-GB/medical-devices/resources/whitepapers/ has an authoritative and useful guide (van Vroonhoven, 2020).

There is also a formal guidance document to ISO 14971, published by BSI as PD CEN ISO/TR 24971:2020 *Medical devices – Guidance on the application of ISO*

14971. (BSI 2020a) This is important because some of the very helpful informative annexes in the previous ISO 14971:2007 version have been moved to the ISO/TR 24971:2020 guidance document. An 'expert commentary' from BSI is also available (BSI 2020b)

4.4.4 Risk management documentation

In order to ensure ongoing compliance with necessary requirements, your risk management process needs to form part of your QMS.

A risk management file should be created for each medical or non-medical device and the results of your risk management deliberations and decisions included in this documentation.

For custom-made devices where the general characteristics, method of manufacture and application are common to a medical device 'family' with only the shape and size being different for each patient, it can be acceptable to have in place a generic risk evaluation which is referred to in the documentation for each device made. The generic evaluation should be considered in each case and patient notes should include any specific additional applicable details or conclusions.

4.4.5 Medical device risk classification

If you were to design and manufacture a medical device and place it on the market, your route to conformity assessment would depend on the risk classification of the said device. Both the parts of UK MDR 2002+ based on the EU MDD, and the EU MDR have an annex setting out a set of rules that enable the manufacturer to determine the risk classification; Annex IX in the EU MDD and Annex VIII in the EU MDR. The EU MDR rules are in some respects stricter and some types of device (particularly software, either embedded in a physical device or a medical device in its own right) have been moved to higher classifications.

In developing the risk management plan for your medical device, it would be best-practice to investigate which risk category it would fall into if marketed. A PDF based app that takes you through the rules from the EU MDR is available on the IPEM website pointed to in section 4.3.1 above.
https://www.ipem.ac.uk/media/z2gifmew/classification-document.pdf

4.5 Design and development

4.5.1 Design and development cycle

A simplified diagram of the design and development cycle is shown in Figure 1.

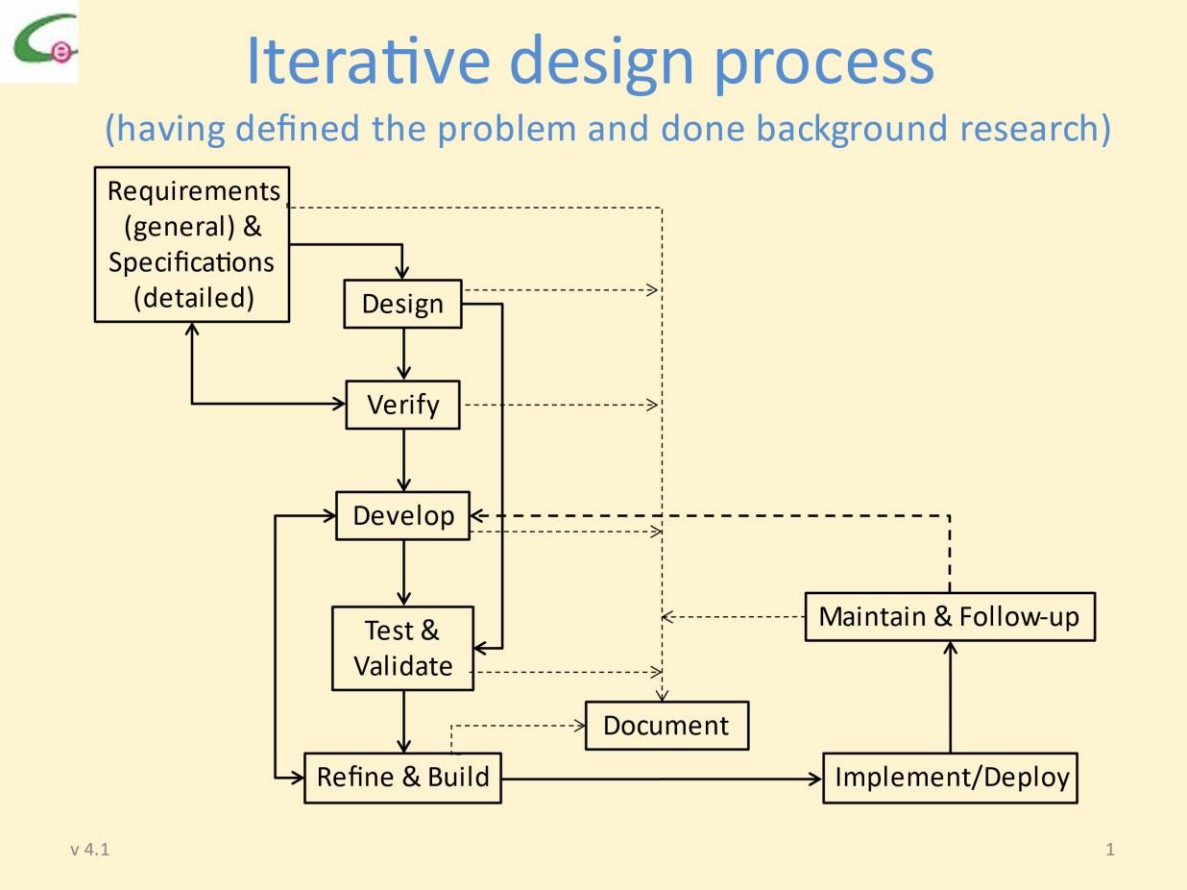

Figure 1: The iterative design process[6]

Note the emphasis on documenting all the steps in the process.

Note also that there is not consistent agreement about the terms Verify and Validate or about Requirements and Specifications.

- Double arrows indicate a potentially iterative part of the process. You may go round those loops more than once.
- The link between Design and Test & Validate is intended to show that at the design stage you should be thinking about what tests you will carry out to validate prototypes and/or final versions of your medical device or non-medical product.
- Implement/Deploy is the stage at which you put your device/product into use.
- Maintain & Follow-up covers both routine maintenance and post-deployment surveillance and appropriate clinical follow-up which may lead back into the Develop stage.

Subclause 7.3 of ISO 13485 covers the design and development process and makes clear which steps must be documented. 7.3.6 covers verification and 7.3.7 covers validation

Some further notes are in Annex E.

[6] Copyright J P McCarthy. Used with permission

This basic methodology is as valid for the development of software products as it is for hardware. We have included more details specific to medical device software in Annex A which has been further developed in this second edition of the guidance.

4.5.2 Essential safety and performance requirements

As part of the planning for your design, by which you intend to meet your requirements and specification, you need to take account of the essential safety and performance requirements that are applicable to the type of product that you are proposing to manufacture, medical device or non-medical product. See 4.3 above.

4.5.3 Human factors and usability engineering in medical devices

Human factors and useability engineering have increasingly come to be seen as significantly important in the design for safety of medical devices. The MHRA have produced guidance here, dated January 2021. HSE have general guidance here.

This document is written in terms of the UK MDR 2002+ regulation as applied in GB. The document also lists:

- EN 62366-1:2015 Medical devices, Part 1: Application of usability engineering to medical devices
- IEC/TR 62366-2:2016. Medical devices, Part 2: Guidance on the application of usability engineering to medical devices

And adds that … *these are not designated standards. However, the MHRA deems these latest versions best-practice and we therefore strongly recommend their use over previous versions.*

4.6 Technical documentation

Both the MDD on which the UK MDR 2002+ are based and the EU MDR require technical documentation to be generated and kept. The EU MDR sets out in Annex II the requirements for this technical documentation under six headings and says that the documentation should be *'… in a clear, organised, readily searchable and unambiguous manner …'*. This clarity is absent from the EU MDD.

The six headings are:

1) Device description and specification, including variants and accessories;
2) Information to be supplied by the manufacturer;
3) Design and manufacturing information;
4) General safety and performance requirements;
5) Benefit-risk analysis and risk management;
6) Product verification and validation.

These headings and the associated detail, taken in context and applied proportionately, are a particularly useful guide to the sort of documentation that should be generated and kept up to date for any in-house development and use. This has links to particular sections in ISO 13485 e.g. *Design and development files* at 7.3.10 and the requirement for a *Medical device file* at 4.2.3 which should be … *compatible with applicable regulatory requirements*.

4.7 Clinical evaluation

Clearly, this applies only if you are developing a medical device.

4.7.1 The need for a clinical evaluation

A *clinical evaluation* is a systematic and planned process to continuously generate, collect, analyse and assess the clinical data relevant to a medical device in order to verify its safety, performance and clinical benefits when used as intended. It starts before a design is finalised and continues as post-deployment surveillance and

clinical follow-up after a medical device has been put into use.

The objective of the initial clinical evaluation is to confirm that the relevant essential safety and performance requirements identified by the process set out in 4.3.1 have been met.

Both sets of medical device regulations, the UK MDR 2002+ and the EU MDR require a clinical evaluation to be carried out as part of the development of a medical device that is to be placed on the market. As noted above in section 1.2 and in detail in Annex B, the UK interpretation of the EU MDD does not cover IHMU. Additionally, the HIE as set out in Article 5.5 in the EU MDR does not explicitly call for a clinical evaluation of an IHMU device.

However, we consider, and the MHRA have indicated both in direct communications and in the guidance document for Northern Ireland (see the link in section 2.1), that a clinical evaluation (which may need to include a clinical investigation) and a report is a requirement for IHMU. This should be appropriate to the proposed benefits and proportionate to the risk classification. Without it you cannot be certain that your medical device is safe and effective. This report would form part of the device's documentation under your QMS.

For a simple device with general characteristics similar to already existing devices it may be sufficient to rely on previously published literature, trials, textbooks etc.

For custom-made devices where the general characteristics, method of manufacture and application are common to a device 'family' with only the shape and size being different for each patient it may be acceptable to have in place a generic clinical evaluation which is referred to in the documentation for each device made. Patient notes should include specific details applicable in each case.

Medical devices that are not custom-made will need a specific clinical evaluation. If your proposed device is innovative this can be complex and may require animal work followed by a *clinical investigation* of a protype – a systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of the device.

This is sometimes referred to as a *clinical trial,* but this is not the formal term. Clinical trial is the term used for medicinal products or vaccine trials, which almost always involve double-blind processes.

Ethical approval and local institutional research approval will be necessary for any clinical investigation. In addition, for a medical device where the intention is possibly to place it on the market, approval from the MHRA in the form of a 'letter of no objection' is required.

MHRA guidance on notifying them of intention to carry out a clinical investigation for medical devices, updated as of January 2024, has a section on Special circumstances for healthcare establishments.
This should be read in full but section 2 states:

> ***2. A healthcare establishment manufactures a medical device solely for use on its own patients within a clinical investigation and does not see the possibility of placing that device on the market.***
> *Because the device is being used in-house and will not be commercialised, a clinical investigation notification to the MHRA will not be required.*

If you decide that a clinical investigation is not required as part of your clinical evaluation of the proposed medical device, you should document your reasons for having come to that decision.

4.8 Device/Product Support

Before a newly manufactured medical or non-medical device is deployed into use you should give consideration to the support that should be in place and implement as appropriate. Some points below should have been dealt with in your consideration of the relevant 'essential safety and performance requirements'.

4.8.1 Labelling and Instructions for use

Both the UK MDR 2002+ (based on the EU MDD) and the EU MDR have explicit requirements for labelling and for the necessary instructions for use in their respective Annex I. The requirements are more detailed in the EU MDR. Some requirements may not be applicable, but all should be considered.

4.8.2 User training

Once again, the EU MDR is more explicit and detailed about user training so if you have used Annex I of this regulation as the basis for your design and development you should have already considered user training. If your device is a one-off novel medical device, you should consider the implications of this in your risk management plan. Similarly, if your device is to be issued to a patient, then suitable training and instructions should be provided.

4.8.3 Technical training

The people who have designed and manufactured the medical device may not be the people who are going to have the responsibility to support it technically into the future. Therefore, technical instructions and training for those who will be responsible should be part of the pre-deployment of the device(s).

4.8.4 Asset management

It is essential that IHMU devices are given an asset number (or batch number if appropriate) and included on the relevant databases that your health institution uses. In this way a full service history will be started, and this will feed back into post-deployment surveillance. For custom-made devices it will be necessary to link each device manufactured to the patient to whom it was issued.

In-house manufacturers should take account of government policy and MHRA guidance around application of Unique Device Identification (UDI) marking requirements as these develop.

4.8.5 Consumables and accessories

If your medical device requires consumables or particular accessories you will have considered the suitability and availability of these as part of your design process. You will have to be aware of any implications if the source of these were to change.

4.9 Post-deployment surveillance and clinical follow-up

Under the current regulatory regime in GB, there is no requirement to register a new IHMU device with the MHRA, though any problems that arise should be reported to the MHRA through the appropriate channels in your location: see https://yellowcard.mhra.gov.uk/medicaldevices

Once an in-house medical device has been manufactured and delivered to the clinical users it is not acceptable to then just forget about it. IHMU devices should be accepted onto the relevant medical equipment asset database in the same way as used for any new UKCA or CE marked devices, but additional surveillance should be initiated.

The Government is developing new regulations regarding post-market surveillance of medical devices, but it is not clear whether these will apply directly to

IHMU devices now or in the future. Never the less, post-deployment surveillance of IHMU devices is important and best-practice.

Surveillance is the monitoring of the performance and safety of a device following its deployment. Surveillance activities collect information on the device's effectiveness and on any problems arising with it, thereby informing any response actions that may need to be taken. The surveillance plan should be developed before the device is deployed. A range of appropriate methods of surveillance should be explored – potential stakeholders include clinical users, patients and technical support staff.

Two key elements of surveillance activities are vigilance and post deployment clinical follow-up.

Vigilance is the monitoring of incident data and includes the reporting of certain problems arising with a given medical device. The reporting and alert methods in the UK are overseen by the MHRA but these are implemented differently within England, Wales, Northern Ireland and Scotland. You must be familiar with and implement the system in place particular to your jurisdiction.

Clinical follow-up is the proactive collection and analysis of real-world clinical data, including the use of registries, against which the medical device's original clinical evaluation and risk-benefit assessment should be reviewed and revised as necessary. Such feedback can lead to future improvement opportunities.

4.10 Legacy IHMU devices

Devices previously manufactured in-house can legally remain in use provided they are not transferred to another legal entity. However, it would be prudent to review their condition and safety, and their clinical, technical and method of decontamination status. A risk assessment will lead to a decision whether they should continue in service, be modified in accordance with current best-practice, or be withdrawn.

This also applies to legacy devices in Northern Ireland.

5 Medical device software

As has already been noted, medical device software can either be embedded in and part of a physical medical device or be a medical device in its own right, running on a non-medical device platform such as a PC, tablet or smart phone.

All of the principles set out in section 4 above apply in general to medical device software. However, there are specific techniques of specifying, developing, testing and maintaining software and specific Standards that apply.

We have therefore devoted Annex A to the issue of medical device software with its own list of works cited. Annex A has been further developed in detail in this second edition of this guide.

6 Where to go for further advice

For further advice it is best to contact the MHRA (devices.regulatory@mhra.gov.uk or software@mhra.gov.uk); however, it is very important to provide a clear definition of what the intended purpose of the device is. The following are two examples where a clear and unclear question was asked of the MHRA.

6.1 Vague intended purpose: Nurse trolley

The MHRA responded to a question about whether a trolley which included CE-marked medical devices and IT equipment would be classed as a medical device.

The MHRA were unable to give a definitive answer due to the lack of information

and instead provided some guidance in their response. They stated that to determine if a product has a medical purpose as defined in the EU Medical Devices Directive (EU MDD) EEC 93/42 1993 (as amended) you should consider not only the device itself but any intended uses implied in the accompanying documentation or instructions for use. They added that software that performs calculations or interpretations of captured data to aid or replace a clinician's own calculations are medical devices.

The MHRA also provided some examples of software that is not considered a medical device; this included hospital record systems that are used for "archiving/retrieving patient records/images without intended changes."

The MHRA added that any products used on the trolley that are already on the market for non-medical purposes would not require conformity assessment marking as a medical device. This would apply to data transmission devices, or digital cameras and microphones that the trolley and its equipment may make use of.

Finally, the MHRA stated that unless you are placing the whole trolley and all its components on the market as a single product then the trolley would likely not require conformity assessment marking.

6.2 Well defined intended purpose: Nursing pressure sore assessment tool

The MHRA responded to a question on whether a pressure sore assessment tool would be a medical device. A piece of software based on a paper form for diagnosing skin assessments was to be developed under the EU MDR.

The MHRA gave a clear answer in response to this question as they were given substantial information in order to make their decision. They stated that under the EU MDR the "*digitalised version of a risk assessment form for pressure area assessment, which will be used by a healthcare professional to inform clinical decisions on diagnosis, treatment and prevention of pressure ulcers*" would be a class IIa medical device.

The reasoning given by the MHRA was that this would be a piece of software that will be used to make a decision in a diagnostic or therapeutic process (Annex VIII of the EU MDR, Chapter III, Rule 11).

At the time the advice was given, the MHRA added that as The Medical Devices (Amendment etc.) (EU Exit) Regulations 2019 No. 791 will mirror the "*key elements*" of the EU MDR and EU In vitro Diagnostic medical devices Regulation (2017/746) as far as possible then the software would still be a medical device under the new legislation. BUT, note that the quoted 2019 S.I. No. 791 has itself been amended and the reference to mirroring the EU MDR is no longer assured and is the subject of the ongoing consultations.

7 Works Cited

BSI, 2020. PD CEN ISO/TR 24971:2020 *Medical devices – Guidance on the application of ISO 14971.*

BSI, 2020. PD CEN ISO/TR 24971:2020 ExComm *Expert Commentary for PD CEN ISO/TR 24971:2020. Medical devices. Guidance on the application of ISO 14971.*

European Parliament and Council, 2017. *REGULATION (EU) 2017/745 on Medical Devices as amended by Regulation 2020/561.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0745-20200424
[Accessed 15 January 2024].

MHRA, 2018. *Draft guidance on the health institution exemption (HIE) — IVDR and MDR.* [Online]
Available at: https://www.gov.uk/government/consultations/health-institution-exemption-for-ivdrmdr
[Accessed 15 January 2024].

The Medical Devices Regulations, 2002. *S.I. 2002/618.* [Online]
Available at: https://www.legislation.gov.uk/uksi/2002/618 [Accessed 15 January 2024].

van Vroonhoven, J., 2020. *Risk management for medical devices and the new ISO 14971,* London: BSI.

8 Contributors

The following people contributed to the production of this document with input also from the peer reviewers named on the introductory pages:

Michael Ayers, Alison Bray, Crina Cacou, Patrick Carena, Geoff Charles-Edwards, Gerard Dean, George Dempsey, Geoff Harbach, Foteini Katsiouli, James Leighs, Helen Nelson, Adam Partlow, Rebecca Nix, Lorna Tasker, Sarah Ward, Peter Watson

The following were also involved:

Sharon Allen, Paul Lee, Keith Fawcett, Paul Hewett, Simon Hook, Craig Smith, Mark White.

Lead author and editor: Justin McCarthy

Rebecca Nix and Adam Chalkley reviewed & contributed to the Edition 2.2 changes.

9 Annexes

Annex A	Medical Device and Health Software
Annex B	UK Regulatory situation as of April 2022
Annex C	MDR Articles 5.4 and 5.5
Annex D	Definitions of 'medical device', 'accessory for a medical device' and 'custom-made device'
Annex E	Notes on the Engineering Design Process
Annex F	The history of ISO 13485

Annex A Medical Device and Health Software

A0 Introduction

The aim of this annex is to highlight specific issues pertinent to the development of in-house software, not covered in the main guidance document. For convenience the annex structure follows that of section 4 of the main guidance document, which in turn follows the medical device lifecycle. The annex is not intended to be read in isolation. The remainder of this section (A0) will briefly outline what should be considered as software, and why a separate annex is required. Section A1 will then look at when software should be considered a medical device. Section A2 will review Quality Management Systems (QMS) pertinent to software in-house manufacture and use (IMHU). Section A3 will deal with essential safety requirements and useability issues regarding software.

Sections A4, A5 and A6 will then look at more practical risk management, design and development and documentation for software. Finally, sections A7, A8 and A9 will review differences in clinical evaluation, support and post-deployment surveillance relevant to software.

There are a number of national and international standards that are applicable to these sections, these are briefly summarised in Table A1 for reference. We have not dated these Standards and you should always use the most up to date version.

Table A1: Summary of key standards and which sections they are most applicable to: please note many are applicable throughout.

Key International Standards	**Sections**
ISO 13485 *Medical devices — Quality management systems — Requirements for regulatory purposes*	A2
ISO 14971 *Medical devices — Application of risk management to medical devices* ISO-TR 24971 *Medical devices — Guidance on the application of ISO 14971*	A4
ISO/IEC 15026 *Systems and software engineering – Systems and software assurance*	A5, A6
ISO 16142-1 *Medical Devices – Recognized essential principles of safety and performance of medical devices*	A3
IEC 60601-1. *General requirements for basic safety and essential performance*	A3
IEC 62304 *Medical device software — Software life cycle processes" — Amendment 1*	A2, A5, A6
IEC 62366-1 *Medical devices - Application of usability engineering to medical devices*	A3, A4, A5
IEC 80001-1 *Application of risk management for IT-networks incorporating medical devices. Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software*	A8
IEC 80002 *Medical device software*	A5, A6
NHS Digital Information Standards	**Sections**

DCB0129: *Clinical Risk Management: its Application in the Manufacture of Health IT Systems*	A5
DCB0160: *Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems*	A5

A0.1 The Need for a Software Annex

Software can be defined as a set of instructions and data that tells computer hardware how to work. This is a broad definition and it covers a wide range of uses, from code written in a low level programming language to formulae in a spreadsheet or a *functional document* (as defined in MHRA 2021a). This wide definition means that some of the activities that Medical Physicists and Clinical Engineers (MPCE) undertake using computers could be considered as in-house manufacture and use (IHMU) of Software. The nature of MPCE work means that some of this software will meet the definition of a Medical Device and thus best-practice and medical device regulation will need to be considered. This may also apply to the work of other clinical and technical staff within the NHS and to the development of 'Health IT Systems' where the requirements of DCB0129 and DCB0160 apply (see A4.1.1 below). Indeed, the clinical context means that following best-practice is recommended for all IHMU within a healthcare institution.

Software engineering has a number of factors that differentiate it from other forms of engineering, e.g. mechanical or electrical. Primarily, software is readily changeable or mutable; code can be reworked and extended almost limitlessly. This means that mistakes and bugs can quickly be fixed, but it also encourages a trial-and-error style of development, which may just as quickly create new errors. This is at odds with the planned development that is required by medical device regulation, and therefore more discipline is required by developers. As a code base becomes larger and more complex, and especially when multiple authors are involved, changes in one area can have unexpected consequences elsewhere, i.e. the code becomes brittle. Unless the code has been subject to thoughtful planning that includes robust change control processes, verification and validation, it can be difficult to maintain and become unsafe.

This mutability means that software has a lower barrier to entry than more traditional engineering fields, as the only resource generally required is time, with ubiquitous tools like Microsoft Excel available within most schools, businesses and hospitals. Programming, especially for modelling, is generally taught as part of most physics and engineering degree programmes, but the principles of software engineering are often not included.

Once written, software can be readily reproduced, shared and distributed, at negligible material cost. Snippets of code from popular support forums (e.g. Stack Overflow) can be copied and pasted into spreadsheets or programs, providing rapid solutions for problems. Open Source software, distributed by individuals or groups, can be integrated into more complex packages providing general solutions to common issues. This is extremely beneficial, but also has a range of associated risks to those assimilating the third-party software in their solution. Although the code may itself be excellent, there are no guarantees that it will be documented or supported, and the quality of testing is at the whim of the contributor.

Finally, software is generally installed on computers that run many other programs and which are connected to an internal and/or external network.

Software is often designed to run on a wide variety of different hardware and for multiple operating systems. This lack of isolation means that programs need to be developed with consideration of this complex environment, and especially considering aspects such as cybersecurity and information governance, as well as basic

interoperability issues. The adoption of general-purpose networks, on which many systems rely, also means that there is a wide range of stakeholders involved, including corporate IT and outsourced services.

These factors provide many of the key benefits of software over more traditional engineering approaches, but also introduce a number of challenges to applying best-practice. The development of software in line with best-practice requires a disciplined software engineering approach, and those writing software for medical purposes should have the appropriate skills and training. More importantly, departments undertaking software projects should ensure the competence of developers and make sure they are able to fully support and resource the development. This applies not only during a project's initial implementation but to the continued maintenance of the software throughout its useful life. In-house manufacture should never be viewed as a cheaper alternative to procurement. If an alternative is available on the market then there needs to be a justifiable reason, such as performance, why it is not purchased in preference to IHMU.

A1 Is it a Medical Device?

The definition of a medical device can be found in Article 2 of EU Medical Devices Regulation 2017/745 (EU MDR), and section 2.—(1) of UK Medical Devices Regulations SI 2002 No. 618 (as amended) (UK MDR 2002+). The current (July 2023) UK regulations are based on EU Medical Device Directive (Refer to Annex D for full text of the current definitions). In both cases, the key consideration is the intended use of the software as defined by the manufacturer, i.e. the person or institution that is making the software available for use. It is not enough to state that a device is not a medical device, when it clearly performs a function consistent with the definition. If an institution uses an uncertified device for a medical purpose, they are taking on complete liability if something goes wrong.

The medical device definition is broad, and software used in a healthcare setting often falls within a grey area where it is challenging to determine whether or not it meets the definition and falls within scope of the regulations. For that reason, extensive guidance has been produced both in the UK and EU. The reader is directed to the original guidance documents which are well-written and cover a wide range of use-cases. However, the key questions a manufacturer should consider when deciding whether or not software meets the medical device definition can be summarised as:

- Is the software performing an action on data other than storage, archive, communication, loss-less compression or simple search? Software that only performs one or more of these listed actions is less likely to meet the definition of a medical device
- Is the action for the benefit of individual patients? Software that is only used for audit is unlikely to meet the definition
- Is the action for a medical purpose, as defined in the UK MDR / EU MDR?

There is a subtle difference in the medical device definition between the current UK MDR 2002+ and the EU MDR. Specifically, the EU MDR formalises the inclusion of devices where the intended purpose is for the "prediction and prognosis" of disease as per existing guidance (MEDDEV 2016). This more advanced concept of diagnostics is likely to apply to devices which include software, rather than hardware devices on their own.

In addition to meeting the definition of a medical device, software may meet the narrower definition of an in-vitro diagnostic (IVD) medical device, for example, when the software is processing data from an IVD medical device. Additional requirements

for IVDs apply, outlined in the regulations associated with in vitro diagnostic medical devices.

IVDs are outside of the scope of this best-practice guide.

A1.1 Key guidance in determining whether or not software falls within scope of the regulations

The documents below cover both EU and UK guidance on what is a medical device. These can be helpful regardless of whether or not the software is being produced solely for GB or the UK.

The MHRA have produced an interactive tool for manufacturers providing guidance on whether or not a piece of standalone software meets the definition of a medical device. This guidance is in the context of the current UK MDR 2002+ and is frequently updated. (MHRA 2021a)

The EU Medical Devices Co-ordination Group (MDCG) has produced guidance on the qualification and classification of a medical device in the context of the EU MDR (MDCG 2019, 2021b)

There is also an infographic summarising the decisions required to determine whether software is a medical device. (MDCG 2021a)

The EU borderline devices document provides a broad list of examples of both hardware and software applications. These examples have been collated from across the EU and illustrate how EC law has been applied by individual member states to borderline cases. (EC 2019)

A1.2 Software modifications: is it now a Medical Device?

Software modifications can be easy to make, and a subtle change or the addition of a simple feature (e.g. adding a calculator to an application for managing electronic health records) can result in a piece of software which previously did not meet the definition of a medical device now falling under the scope of the regulations. It is therefore essential to consider the medical device definition at all stages of the project lifecycle including post-release, and particularly when decisions about feature changes are being made.

A1.3 Medical Device Accessories

Some software fulfil their medical purpose in conjunction with other medical devices. These are classed as *accessories for a medical device*, and need to be considered with the same rigour as a standalone medical device. See Annex D for the formal definitions of *accessory for a medical device* in the EU MDR and of an *accessory* in the EU MDD. For example, if a commercial software medical device uses a plug-in or pipeline architecture, then development of third-party plug-ins or pipeline 'steps' should be considered as producing an *accessory*.

A1.4 Common "Grey Areas"

A1.4.1 Are Spreadsheets, PDFs and other functional documents medical devices?

It is possible that software which is not a medical device can produce functional documents that are classified as a medical device. Examples of this include spreadsheets, image processing software, PDFs, text documents with macros, and other files that have automation. Microsoft Excel is not a medical device; its intended use is the production of spreadsheets. Spreadsheets can be used to create calculators that can have medical applications; such as calculating doses, clinical metrics, such as Glomerular Filtration Rate (section 1.3) or Modified Early Warning Score), or comparing measures to a reference set and warning when out of expected ranges. If an organization created a spreadsheet with a medical purpose, then that spreadsheet

is a medical device, even though Microsoft Excel is not. In this instance the organization is the manufacturer of a medical device which is a spreadsheet.

A1.4.2 Is Artificial Intelligence (AI) a medical device?

If the intended use of the Artificial Intelligence (AI) meets the definition of a medical device and is implemented in software, the AI should be treated as Software as a Medical Device. There may be additional requirements for AI, and standards are currently in development; this is a rapidly changing field.

A1.4.3 Adapting and modifying existing medical devices

Software which is a medical device may have the capability to be adapted and modified. If the change is within the intended use of the software as outlined by the manufacturer, then this is simply adapting the device as intended. However, if an organization modifies the device outside of the manufacturer's intended usage this would make the organization a manufacturer of a medical device as they have changed the intended purpose (off-label use). Two examples of this are discussed below illustrating different vendors' approaches.

RayStation is a Treatment Planning System (TPS) used in radiation therapy. It has the ability to be adapted through the use of scripting via Python. This is an intended feature and its use is outlined by the manufacturer of the device for automating processes by chaining together various actions native to the TPS, i.e. invoking only RayStation scripting API functions. If the script goes beyond this and calculates new derived metrics, not provided by the TPS, on which treatment decisions are based or if it removes decisions from the user then the script should be considered as a separate medical device. If the script is for data mining, i.e. not for the benefit of an individual, then it would not be a medical device. The manufacturer also provides training on scripting.

The Siemens Symbia SPECT imaging systems have imaging software supplied with them. It has the ability to be modified through the use of IDL scripting to produce your own visualisations. However, this is not within the intended use as described by the manufacturer in their documentation or marketing material. If an organization were to produce scripts that create visualisations of imaging data, they would have modified the software and become the manufacturer of the modified medical device.

A2 Quality Management Systems for Software

A2.1 QMS for Software – Highlighting the differences

The overarching principles for the application of a Quality Management Systems to medical devices (described in the main report, section 4) are equally applicable to software. However, historically, QMS standards were aimed at the development of hardware projects, and the nature of software design, development and manufacture can be quite different. This offers both challenges and opportunities when it comes to developing software under a QMS.

The current MHRA (2021b) guidance for the Northern Ireland Healthcare Institution Exemption (HIE) states that ISO 13485 *Medical devices - Quality management systems - Requirements for regulatory purposes* is considered an appropriate quality management system. It also states that:

> *The minimum requirement for qualifying QMS is a standard appropriate for the scope of products to be covered by the exemption. Essential elements of an appropriate standard include selection of devices, management, use and record keeping for the lifetime of the device. Additional elements include design, manufacturing, performance review and the need to conform to applicable laws*

(including IVDR or MDR) and harmonised to the IVDR / MDR.

Selection of devices should include the justification of in-house manufacture over procurement. The EU MDR requires this justification to be based on the clinical requirements not being met, at an appropriate level of performance, by any available device on the market (Annex C).

A2.2 Implementing a QMS for software development

A QMS defines a set of interlinked processes which, when adhered to, give assurance over the consistency of the end product or service. BS EN 62304:2006+A1:2015 *Medical device software - Software life-cycle processes* has been harmonised to the EU MDD and provides guidance on a minimum set of processes which should be established. Specifically, any QMS for software should include documentation of processes for:

- Software Planning
- Requirements analysis
- Architectural and detailed design
- Unit implementation and verification
- Integration and integration testing
- System testing
- Software release
- Maintenance Plan
- Risk management
- Change Control
- Post market surveillance

A core principle of quality systems is the process of internal and external audit. All processes should establish what records will be generated as a by-product, and ultimately used to evidence conformity during audit. Appendix C of BS EN 62304:2006+A1:2015 illustrates how it can be used to satisfy the requirements of ISO 13485.

It is recognised that many medical physics and clinical engineering departments may already be working under an ISO 9001 accredited QMS. If software development is being integrated under an existing QMS, consider documenting processes and work instructions specifically for the design, development, manufacture and release of software, where those processes are not adequately described by the original procedures. Useful guidance on the application of ISO 9001 to software projects can be found in BS ISO/IEC/IEEE 90003:2018 *Software engineering. Guidelines for the application of ISO 9001:2015 to computer software*.

A2.2.1 Leveraging modern software development practices within a QMS

Implementing a QMS can add-in overheads and slow down device development. This may be a particular concern to software teams using agile approaches. Although an initial reading of IEC 62304 may indicate that a waterfall approach is preferred, it does not specify a particular lifecycle model. Useful guidance has been produced by the Association for the Advancement of Medical Instrumentation (AAMI) demonstrating how agile practices may be adopted to show adherence to BS EN 62304 (AAMI TIR45:2012 *Guidance On The Use Of AGILE Practices In The Development Of Medical Device Software*). To summarise, in order to effectively implement agile practices, careful consideration must be given to when non-software design outputs (*i.e.* documentation) is generated.

Modern software development practices can offer advantages in operating a QMS that are not available to hardware devices.

Specifically:

- Automated testing
  - Unit, integration and system testing should, wherever possible, be performed automatically with only the minimum set of manual tests required for verification / validation of requirements performed.
- Continuous integration / continuous delivery systems
  - The use of automated testing instead of manual testing allows for continuous integration and delivery systems, providing a robust verification / validation of the software being released
- Integrated customer feedback / post market surveillance
  - Possibilities for integrated bug reporting and rapid feedback to developers
  - Possibilities for rapid delivery of updates / changes
- Documentation
  - Potential for auto-generating documentation – inline
  - Generation of release records and verification records via continuous delivery systems
- Improved traceability
  - Change control records via software versioning systems (Git, SVN etc.)
  - Release records via continuous delivery systems
  - Potential for capturing user requirements functionally and linking directly to User Acceptance Testing

A2.3 Implementing a QMS for software use and management

An appropriate QMS must also cover the use of the software, which should include how it will be managed and supported. Currently there are no appropriate QMS specifically covering medical device usage, however most institutions use a QMS for their clinical processes.

IT service management standards, for example the ISO/IEC 20000 series *Information technology – service management* or ITIL® (AXELOS 2019), may be useful when defining how to support a medical device during routine operation. These define general IT processes such as inventory, change management, configuration management, and problem and incident management. Similarly ISO 27001 *Information Security Management* may be beneficial to meeting essential requirements (see section A3.1 below). Their use may improve communication with corporate IT through a shared vocabulary.

Standards specific to medical devices include BS EN IEC 80001-1 *Application of risk management for IT-networks incorporating medical devices. Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software*, which is covered in more detail in section A8, and ISO 81001:2021 *Health software and health IT systems safety, effectiveness and security*. ISO 81001 is an emerging standard, aiming to cover all software and systems used within a healthcare context, incorporating the entire system and data lifecycle, from development to decommissioning. It highlights key points in the lifecycle where responsibility is transferred between stakeholders, to help improve communication.

A2.4 Competence

The QMS should include processes to ensure that the skills, training and experience of members of a development and support team are sufficient when considering the nature of the project being undertaken and the risks involved. This requirement is by no means unique to software development but, with the ready availability of varying development tools and deployment technologies, it can be

relatively easy and tempting for a developer to stray beyond the limits of their knowledge and safe practice.

A2.5 Software QMS specific considerations

A2.5.1 Organizational versus Departmental development activity:

The ubiquitous nature of IT hardware and hence the availability of potential development platforms, such as spreadsheets, means development may occur outside of your management structure. It may be unrealistic to eliminate such development routes and hence a means may need to be established to capture and manage such development activity.

You may also need to consider how your life cycle management processes fit in with your IT department's management processes.

Research activities may be left out of scope for clinical QMS, however following the same development procedures will aid integration of the software into clinical pathways or clinical trials later, and is considered best-practice.

A2.5.2 Modification of medical devices via in-built configuration tools

As discussed in section A1.3, many medical devices have facilities by which, a trained end user could essentially develop a new medical device as a macro or script that runs on the existing device. Such modifications, their classification and management will need to be handled under the quality management system so that they can be used safely and legally.

A2.5.3 Use of software as a development tool

Any tools used within your QMS will need to be documented, validated and managed this will include:

- Development environments
- Version control software (including cloud hosted repositories)
- Build automation tools, especially those connected to package repositories
- Testing tools/platforms
- Programming languages: versions, style guides, library management

A2.5.4 Use of SOUP (Software Of Unknown Provenance)

It is likely that software being developed will rely on existing libraries or components developed from outside your QMS. These will need to be managed and risk assessed accordingly, keeping in mind that these components will need to be tested, validated and supported. When using software outside of its intended purpose (including software licensed as research only) you are taking on the responsibilities of the manufacturer. Further guidance on incorporating SOUP within a project can be found in BS EN 62304.

A3 Essential Safety Requirements for software

A3.1 Specific clauses

As noted in the main guidance, the General Safety and Performance Requirements (GSPR) set out in Annex I of the EU MDR are regarded as best-practice; however the regulations have not been retained as UK law due to Brexit (see Annex B). The EU MDD Essential Requirements therefore are still mandated by the UK MDR 2002+. Both contain requirements specifically aimed at software, which are summarized in Table A2, although there are other general requirements that will apply. EU MDD Annex I, Essential Requirements 1-6 and the EU MDR Annex I, GSPR 1-9 apply to all medical devices, whereas the rest may or may not be applicable.

ISO 16142-1 *Medical Devices – Recognized essential principles of safety and performance of medical devices* Part 1 Tables B.1 and B.2 provide a detailed

breakdown on which standards are applicable to the EU MDD essential requirements.

In the EU MDR GSPR, additional requirements applicable to software are frequently linked to information security. For in-house manufacture, if the software being developed will store personal data then the Data Protection Act (DPA 2018), which implements the EU General Data Protection Regulations (GDPR), will apply, and these sections must therefore be considered.

Information Security should therefore be considered throughout the development process. The EU MDR GSPR calls for risks of the interaction of software and the wider IT environment to be considered, BS EN IEC 80001-1 provides guidance on the application of risk management for IT-networks incorporating medical devices, this will be considered further in section A8.1

Good cyber security practice, especially as part of data protection, includes regular patching of systems to ensure that newly discovered vulnerabilities are mitigated. For all but the most trivial programs, a framework is generally used when producing a new application (e.g. Django for Python or .NET for C#). The framework provides the non-scientific code required, for example user interfaces, web services, user access control and security. The decision over which framework to use therefore usually introduces the first SOUP, and its maintainability should be considered along with other constraints such as ease of development and features. This includes decisions over whether a commercial or open source framework is used, whether commercial support is available if open source, if not how often is it patched or updated, and who contributes to the project (e.g. companies).

Table A2: Excerpts from EU MDR and MDD highlighting changes between GSPR and Essential Requirements for Software.

EU MDR Annex I, GSPR	**UK MDR – EU MDD Annex I, Essential Requirements**
14.2 Devices shall be designed and manufactured in such a way as to remove or reduce as far as possible: (d) the risks associated with the possible negative interaction between software and the IT environment within which it operates and interacts;	
14.5. Devices that are intended to be operated together with other devices or products shall be designed and manufactured in such a way that the interoperability and compatibility are reliable and safe.	
15. Devices with a diagnostic or measuring function	
15.1. Diagnostic devices and devices with a measuring function, shall be designed and manufactured in such a way as to provide sufficient accuracy, precision and stability for their intended purpose, based on appropriate scientific and technical methods. The limits of accuracy shall be indicated by the manufacturer.	
15.2. The measurements made by devices with a measuring function shall be expressed in legal units conforming to the provisions of Council Directive 80/181/EEC (1).	
17. Electronic programmable systems — devices that incorporate electronic programmable systems and software that are devices in themselves.	

EU MDR Annex I, GSPR	UK MDR – EU MDD Annex I, Essential Requirements
17.1. Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.	12.1. Devices incorporating electronic programmable systems must be designed to ensure the repeatability, reliability and performance of these systems according to the intended use. In the event of a single fault condition (in the system) appropriate means should be adopted to eliminate or reduce as far as possible consequent risks.
17.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.	12.1.a) For devices which incorporate software or which are medical software in themselves, the software must be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification.
17.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).	
17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access, necessary to run the software as intended.	
18.8. Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorized access that could hamper the device from functioning as intended	
23.4. Information in the instructions for use	
(f) where applicable, information allowing the healthcare professional to verify if the device is suitable and select the corresponding software and accessories;	
(ab) for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.	

A3.2 Usability Engineering

The EU MDR GSPR and the EU MDD Essential Requirements both state that ergonomics of a medical device should be considered when performing risk assessment (Table A3 below).

Table A3: Excerpts from EU MDR and MDD highlighting requirements for ergonomics to be considered

EU MDR Annex I, GSPR	**UK MDR – EU MDD Annex I, Essential Requirements**
5. In eliminating or reducing risks related to use error, the manufacturer shall: (a) reduce as far as possible the risks related to the ergonomic features of the device and the environment in which the device is intended to be used (design for patient safety), and (b) give consideration to the technical knowledge, experience, education, training and use environment, where applicable, and the medical and physical conditions of intended users (design for lay, professional, disabled or other users).	1. The devices must be designed and manufactured in such a way that, when used under the conditions and for the purposes intended, they will not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their intended use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety. This shall include: — reducing, as far as possible, the risk of use error due to the ergonomic features of the device and the environment in which the device is intended to be used (design for patient safety), and — consideration of the technical knowledge, experience, education and training and where applicable the medical and physical conditions of intended users (design for lay, professional, disabled or other users).
14.6. Any measurement, monitoring or display scale shall be designed and manufactured in line with ergonomic principles, taking account of the intended purpose, users and the environmental conditions in which the devices are intended to be used.	

For software, this relates to the usability of the User Interface (UI), and how it can be developed to minimise the chance of user errors, especially when patient harm can result. IEC 62366-1 Part 1: *Application of usability engineering to medical devices* provides guidance on how this can be achieved within an ISO 14971 risk management framework. Usability should consider characteristics of the user, tasks and environment, so the UI requirements may differ for software used in a stressful ICU compared to a patient device used at home. The interface should be reviewed for opportunities for use error, and the consequences of these errors should be determined, with controls implemented to minimise the risk of these occurring. Summative testing should be performed by users to replicate these scenarios. Usability should also be considered throughout the software lifecycle (installation/deployment, use, upgrade and decommissioning) to minimise the risk of harm. Residual use error risks should then be included in the user documentation.

A4 Risk Management of Software

The following provides a general focus on the main considerations for the application of risk management to software medical devices and is not designed to replace any of the afore mentioned standards. The reader is encouraged to obtain access to the standards and training to support their knowledge, understanding and application of ISO 14971.

A4.1 Relevant Standards

Section 4.4 of the main guidance document, *Risk assessment and risk management,* outlines the general approach to the design and development of medical devices. Although ISO 14971 and ISO 13485 apply to both hardware and software, the approach to medical device software risk management has some specific considerations and requirements. Specifically, when developing a software medical device, whether embedded or as standalone medical device software, the risk management approach must integrate the IEC 62304, 4.2 risk management approach in order to demonstrate conformity. All of clause 14 in IEC 60601-1 will also apply to embedded software within a hardware medical device.

Additionally, as discussed in section A3.2, the adoption of a usability risk management process (IEC 62366-1) and consideration of information security standards (IEC 27002, IEC 80001-1, IEC 81001-5-1, IEC 82304-1) would ensure comprehensive risk management is in place.

A4.1.1 NHS Digital Clinical Risk Management Information Standards

The NHS Digital Information Standards DCB0129 *Clinical Risk Management: its application in the manufacture of Health IT Systems* and DCB0160 *Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems* are published under section 250 of the Health and Social Care Act 2012 and are mandatory in England. They state that:

> *[These Information Standards] apply to all Health IT Systems including those that are also controlled by medical device regulations, though the requirements defined in [these Information Standards]* are broadly consistent wit*h the requirements of ISO 14971*.

Whilst they reference the EU MDR they do not include IEC 62304, IEC 62366, IEC 60601-1 or ISO 13485.

A4.2 IEC 62304 Software safety classification

The IEC 62304 software safety classification scheme is intended to be used to determine which processes should be followed for the development and maintenance of software. The risk of the software is used as the input for determining the classification, and the various clauses of the Standard are then conditional on the class (summarised in IEC 62304, Annex A.2).

Figure A1 shows the process for assigning a software safety class, and the classes are:

Class	Outcome
A	No injury or damage to health is possible
B	Non-serious injury is possible
C	Death or serious injury is possible

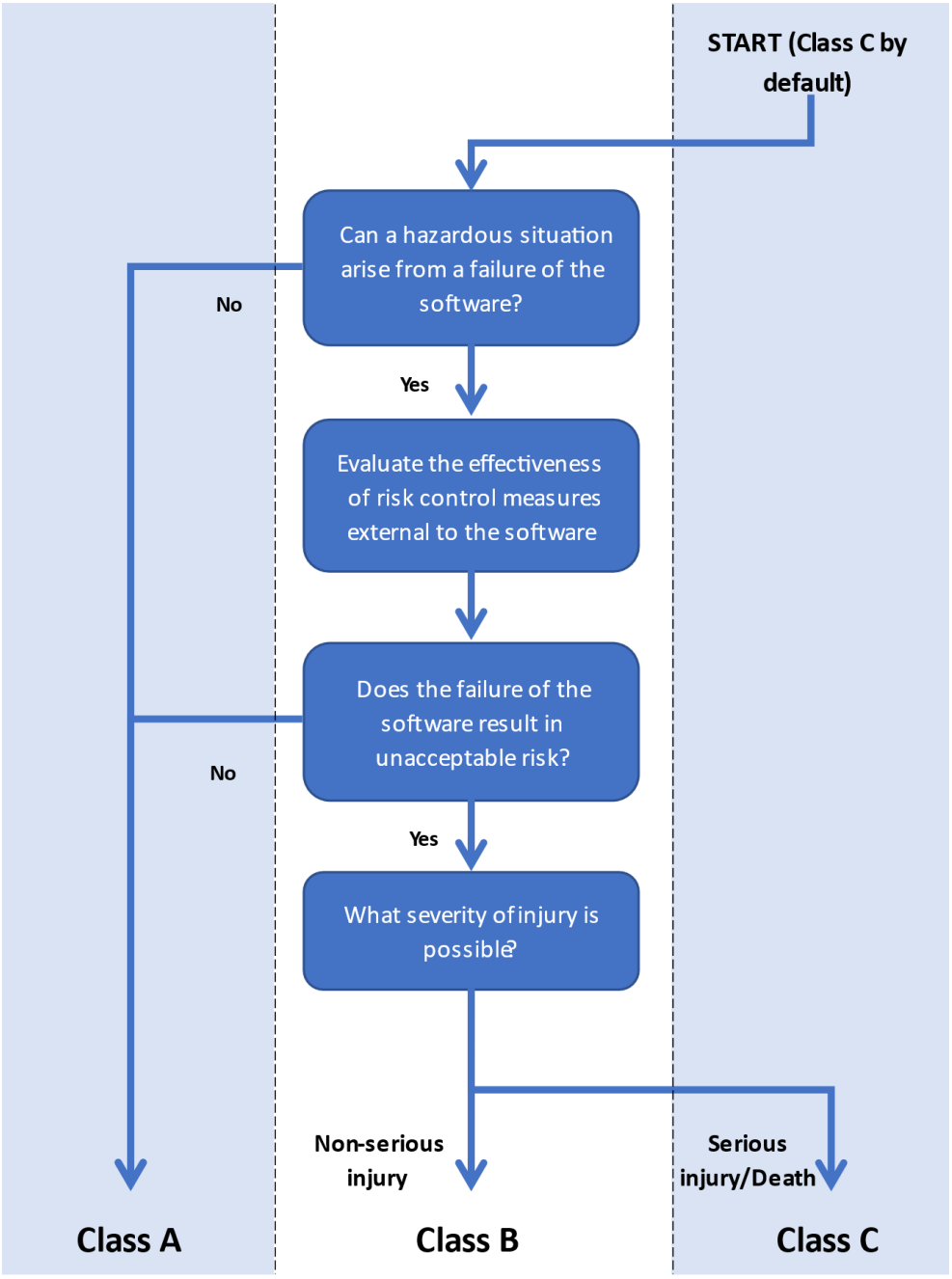

Figure A1: The process for determining the IEC 62304 software safety class

The probability of software failure shall be assumed to be 1 for the purposes of determining the safety class, and therefore only risk controls external to the software system shall be considered. These risk controls may reduce the probability of harm. The risk of the failure of a risk control may also need to be considered. (Adapted from Figure 3 in ISO 62304)

The risk here is a worst-case-scenario in which the software system can contribute to a hazardous situation leading to injury (patient, operator or other people). The more serious the potential outcome (i.e. Class C) the more rigorous the development and maintenance processes should be, for example in validation (section A5.2) and documentation (section A6.2).

Risk is generally calculated by considering both severity and likelihood, however there is no consensus on how to determine the probability of software failure. In-line with the worst case estimation therefore, a probability of 1 should be assigned. If the software is part of system where for hardware components the probability can be determined, then these likelihoods can be included when determining the safety class. The risk is calculated after the effectiveness of any risk control measures is evaluated, and the classification can be changed by adding controls in the system architecture. These controls must be external to the software, but can include hardware or independent software systems, as well as procedural controls.

A software system may be decomposed into further software items with different software classifications to the whole system, and each software item may be further divided. Where the classification of the 'child items' differ from that of the parent item, the manufacturer must provide a rationale for explaining why and how the parent/child items are segregated. This provides a method of focusing effort on safety critical software items.

IEC 62304, B.4.3 provides further guidance, by stating that before the end of the software architecture design process, risk management should be aimed at *architectural risk controls* that reduce the opportunity for software failure to cause harm, or add subsystems to protect against harm. After the architecture has been developed, the risk management approach is to use processes (development, testing etc.) that are aimed at reducing the probability of a software item failing.

The software safety classification must not be confused with the UK/EU MDR classification of devices (I, IIa, IIb and III) which are based on their intended purpose and inherent risks, although they are likely to be correlated.

A4.3 Software Risk Management

IEC 62304, 7 outlines the overall process for the risk management of medical device software, in accordance with ISO 14971. The requirements vary with the assigned software safety class. A risk management plan detailing risk management activities should be included within the software development plan (IEC 62304, 5.1.7). Special reference is made to the inclusion of risk management for Software of Unknown Provenance (SOUP). All risk management activities shall be recorded in a Risk Management File (ISO 14971, 4.5).

DCB0129/DCB0160 specifically require that a Hazard Log and a Safety Incident Management Log are included in the risk management file, and a Clinical Safety Case must be developed to evidence the software is safe for release

A4.3.1 Competence

ISO 14971 requires that clinical risk management tasks should be performed by individuals with appropriate education, training, skills and experience, with records of competence maintained. This will include competence for medical device risk management, software development and clinical use. These tasks may be better carried out by a group, each contributing different expertise. DCB0129 and DCB0160 call for a Clinical Safety Officer (CSO) to be nominated by top management. The CSO must ensure that the processes defined in the information standards are applied. They must be suitably qualified and hold current registration with an appropriate, relevant professional body.

A4.3.2 Software Risk Analysis

Risk management starts with the identification of software items that could contribute to a hazardous situation, based on an ISO 14971 compliant risk analysis. For these items, any potentially causative mechanisms in the software item should be identified. Typical considerations sited in IEC 62304 are:

- Functional specification issues
- Software defects
- Software of Unknown Provenance (SOUP) failure or erroneous results
- Hardware or Software issues leading to unpredictable software operation
- Reasonably foreseeable misuse

Care must be taken when using SOUP to ensure a clear understanding of any known anomalies for the version of SOUP used in the medical device software. These should be reviewed to ensure a hazardous situation is not triggered by a chain of events initiated by an anomaly (IEC 62304, 7.1.3).

All identified potential contributions to a hazardous situation and sequences of events that could cause a hazardous situation must be documented in the Risk Management File.

A4.3.3 Risk controls

Risk Controls should be implemented for all the identified potential contributions to a hazardous situation; these shall also be documented in the Risk Management File. The risk control measures can be implemented in hardware, software, working environment or user instruction (IEC 62304, 7.2). Having a clear and documented understanding of the impact or pathway of a potential hazardous situation to the software item and to the specific cause and related control measure and its verification is essential. With the potential of a software item contributing to a hazardous situation (Safety Classes B and C only) the means of controlling and reducing the risk of harm should be specified, including what it does and how well it does it (IEC 60601-1, 14.7), documented, and the method verified. Use of risk control methods where their reliability is known are preferred.

A4.3.4 Risk Control Verification

Risk controls need to be verified i.e. tested to ensure that they function as intend, and the results of this verification needs to be recorded in the risk management file. For class B and C software, the risk management process should be iteratively repeated to ensure that failure of the risk control measure cannot lead to a hazardous situation. For these classes, traceability in the documentation should be clear from hazardous situation to software item; software item to software specific cause; software cause to risk control; and risk control to verification result.

A4.4 Risk management of software changes

Irrespective of the safety classification of the medical device software, any changes (including those to SOUP) must be analysed to understand the impact on safety and performance and to determine if additional risk controls are required (IEC 62304, 7.4). Changes may impact the classification of software items, the individual and overall residual risk and any requirement for revalidation, additional or modification of controls. As part of an impact analysis, consider how the change may impact:

- The risk assessment
- The overall safety classification
- Requirements for verification and validation

Special care should also be taken to ensure the software is validated for the intended operating systems and infrastructure in which the software is deployed,

including impact on cybersecurity risks.

A4.5 Legacy Software

The development of a system may also include the use of legacy software. This is medical device software that has been legally placed on the market or put into service in-house, but there is insufficient evidence that the current version of IEC 62304 was used in its development. A risk management process can be used an alternative to applying a completely new development lifecycle for the legacy software. This shall include assessing existing post market surveillance; considering how the software will be integrated; verifying if existing risk controls in the legacy software are sufficient; and identifying and controlling any specific hazardous situations arising from the use of the legacy software. A gap analysis should then be performed on the complete lifecycle, based on the safety classification that would be given to the legacy software, and these gaps should be closed.

The manufacturer must document the version of the legacy software used and a rationale for its continued use.

A5 Design and Development of Software

A5.1 Development Lifecycle

Terminology here is from IEC 62304, although these overlap with DCB0129 and DCB0160. IEC 62304 is considered state of the art as required by the MHRA; however the NHS Digital standards provide additional useful practical guidance. All stages should be completed by undertaking a review process, involving all stakeholder representatives identified in this section, including appropriate Clinical Risk Analysis, Evaluation and Control, e.g. by involvement and sign-off by your organization's Clinical Safety Officer (CSO) if you're following DCB0129 and DCB0160. At all stages of the process the software and version must be uniquely identified to allow cross referencing of documentation and product.

A5.1.1 Implementation models

The notes in this section outline the important elements of a Software Development Life Cycle (SDLC) for medical service software development and use; however, this is not an exhaustive list. To aid in the implementation of these steps, there are many models/methodologies available such as the linear "Waterfall" model, the V-model (Figure A2), iterative models (section 4.5.1) and Agile (Figure A3) development.

Ultimately, it is most important that you define a process that works for your team and application, taking into account of the associated clinical risk and all the stages.

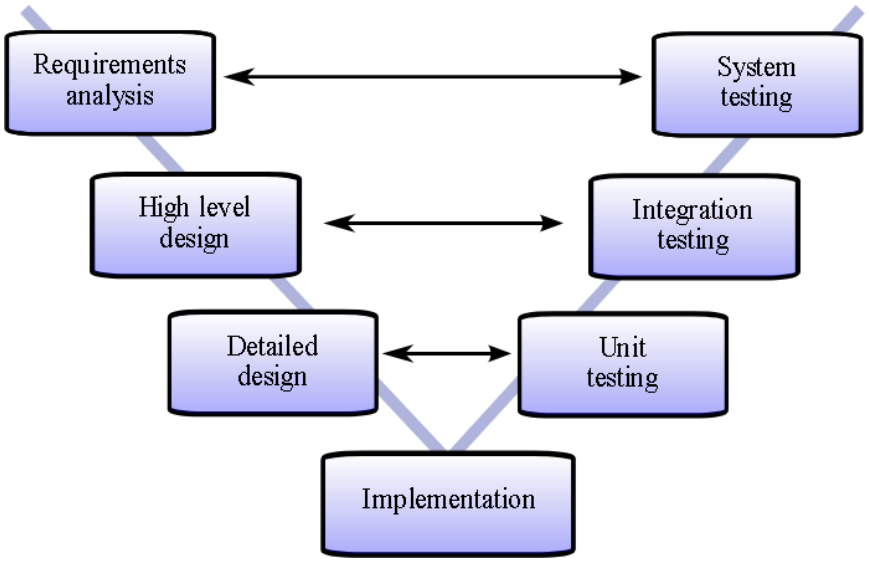

Figure A2: The V-model, which is similar to the Waterfall model, but has a strong emphasis on testing against each level of the device design (Bruyninckx 2008).

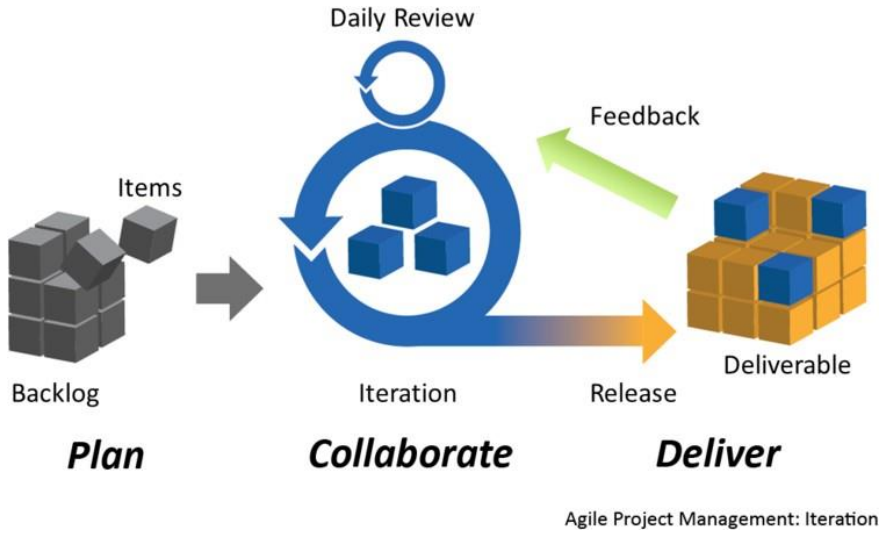

Figure A3: The Agile development model, which iterates towards an end-goal, with a strong emphasis on continuous feedback from end-users and less-detailed designs early-on in the lifecycle. Items here refer to software requirements, with each iteration containing planning, developing, testing and release. (Planbox 2012).

A5.1.2 Stage 1: Software Development Planning

This is a vital section of the Software Development Life Cycle (SDLC) that can reduce the likelihood of major reworks required much later in the process. A number of preliminary factors should be considered here, including developing an understanding of the background to the clinical 'problem', developing a justification for undertaking the work, and assessing associated risks. The following questions should be answered:

1. What is the clinical application and what is the current situation in this area?
2. Why do we need this new software?

3. Why can we not purchase something already CE-marked and on the market? As per EU MDR Article 5(5c), you must be able to evidence that there are no CE-marked devices already on the market that meet your requirements. It is almost always more sensible to procure than develop your own.
4. Do we have sufficient and appropriate resource to safely complete this development in a sensible timeframe? Experience of previous software projects is likely to lead to better estimates of the time required which are otherwise subject to pre-implementation optimism.
5. Who are the product owners and service (usually clinical) representatives? Also identify any other relevant stakeholder group representatives and get their support.
6. What are the hazards and what are their associated likelihoods and severities? Produce a high-level hazard log that's consistent with your adopted Clinical Risk Management System (section A4.1). It is important to note here that the Hazard log is a live document throughout the lifecycle and its primary aim is to ensure risks to patients are reduced as far as possible without adversely affecting the risk-benefit ratio.
7. How will the solution be verified and validated?

A5.1.3 Stage 2: Software Requirement Analysis

Following the definition of the problem and confirmed stakeholder support, the solution needs to be defined in detail. In this stage, the device requirements should be defined to a level of detail proportionate to the level of risk. For example, if complex image-analysis software is to be developed which will produce diagnostic reports, which will be used to determine patient treatments, the risk is high and the software requirements should be defined to a relatively high level of detail.

For all risk levels, this stage should involve fleshing-out a summary of the software to be developed. This should include a definition of the intended scope of use of the software, where it is to be used and who are its users. It should also detail any interfaces and interactions with other components or systems, for example if it is part of a medical device system or designed to process data. Any assumptions and exclusions should be detailed.

Functional requirements should be detailed covering for example user stories and required algorithms, as relevant for the intended use and associated risk level. Non-functional requirements should also be described, to a level of detail useful for the device being developed, covering items such as deployment method, user interface, accessibility, performance, security and data protection impact assessments.

A5.1.4 Stage 3: Software Design

Software design is the process of planning how the software will be implemented to achieve the requirements. The level of detail required will vary considerably with the complexity and risk of the system being designed. IEC 62304 breaks the process down into architecture design and detailed design. Architectural design considers software items to be developed and items external to them, including SOUP, and the interfaces between them. Segregation of these items is used to manage risk (section A4.2). Detailed design is planning how the individual software units (modules, classes, functions, procedures etc.) make up a software item. A minimum set of design documentation should be specified depending on safety class (see section A6).

An often-overlooked element of good software development is User Interface (UI) design. It is important to follow a design procedure otherwise even the most advanced software can be left unused. For this stage, ensure a design system (e.g.

NHS Digital's Design System) is available to the project team, with design principles and design language visible, and evidence that the current design has been developed in line with it. Poor UI design can also lead to clinical risks, and so should be risk assessed for possible use errors in line with IEC 62366-1 (section A3.2).

A5.1.5 Stage 4: Software unit implementation and verification

It is often tempting to directly start programming the software, but it's vital to conduct this implementation in a well-organized and structural manner. Ideally, this should begin by considering test planning, thinking about how are you are going test that you have met your requirements. This should be done to a level of detail that is proportional to the risks involved, and to a level that is useful in this context. This is covered in detail in section A5.2.

Software units are then implemented, documented and source-controlled, and ideally traceable directly to requirements; unit tests should be written where appropriate and ideally by someone other than the developer. In most cases (apart from lowest risk if agreed), define all tests and pass criteria, and verify each software unit produced. Where relevant, development requirements should be linked to risks highlighted in the hazard log. A remote version control system should be in place throughout i.e. somewhere other than on the developer's machine, to avoid loss of work and facilitate team-working.

During development, it is important to undertake code peer review or 'pair-programming'. The reviewer, or co-author, should look for practical steps that could be taken to improve the implementation, documentation and testing.

This stage should also include compilation of software documentation, comprising information about software setup for both users and developers, instructions for use and ideally evidence that at least the minimum essential requirements (section A3) are met.

A5.1.6 Stage 5: Software System Testing (Verification and Validation)

Testing is a vital element of any software development lifecycle, but even more so in medical device software. Test planning should begin early in the cycle, prior to development work, it is important to ensure traceability between requirements and tests, and to ensure that requirements are defined in sufficient detail to be testable. For software units, Test Driven Design is a just-in-time approach, where unit tests are designed and programmed just prior to source code development. Depending on the complexity of the software system, further testing will include Integration, System and User Acceptance Testing (section A5.2.5) as well as Clinical Validation Testing (section A7). Clinical validation is intended to prove that the device will have a positive impact on the clinical pathway in which it will sit, both for patient safety and for overall patient outcomes. The outcome of this testing will form part of the evidence required for the Clinical Safety Case Report and Hazard Log as detailed in DCB0129 and DCB0160.

This stage should be completed by undertaking a review process, involving all stakeholder representatives identified in this section. This is likely to include a review of the software documentation, including the outputs of the testing stage, instructions for use (IFU), technical manual, and evidence that the General Safety and Performance Requirements of the EU MDR have been met.

A5.1.7 Stage 6: Software Release

Once approved for release by the CSO and all stakeholder representatives, an appropriate deployment procedure should be followed ensuring any reported issues can easily be linked to software version(s) deployed. The deployment procedure should consider the archiving of documentation, creation of release notes, safety case

report if appropriate, and handover to the team who will support it. It must also consider the training for users and the support team.

A passive surveillance system should be in place to appropriately receive and act on feedback from users and other stakeholder groups (e.g. a Corrective Actions and Preventative Actions CAPA process) to ensure that the issue is resolved, and appropriate action is taken to prevent similar issues in future. An active surveillance system should also be in place to gather issues and usage information, e.g. from logs, end-users, reporting clinicians, and other stakeholders, which should be reviewed regularly on a defined timescale. It is likely that the outcomes of the above surveillance will occasionally involve changes to the device. A process should be defined to enable looping back into new cycle of SDLC as required, with level of detail determined by clinical risk.

A5.2 Software Testing

A5.2.1 If you're planning to build it, you must plan to test it!

Testing methods are one of the key differences in developing software compared to hardware. This section will give more practical guidance on the software testing steps described in section A5.1.

The testing of medical device software can be viewed as similar to commissioning a new treatment technique or introducing new clinical equipment. In both cases the aim is not to pass a test, but to find problems and then fix them. Only by finding problems and fixing them does quality improve. No system should fail because it was not suitably tested, and documentation should be available to show this.

It is important that adequate time should be given to testing within software development and care should be taken in estimating the amount of time required at the planning stage. Various estimates suggest that typically 50- 75% of project time should be allocated to testing (including debugging and fixing). This is often something of a shock for many inexperienced developers, for whom it is tempting to believe that testing is merely a formality tacked onto the end of the programming phase. To this end testing should be considered as early on in the project as possible. Testing plans and specifications should follow immediately after user, architecture and component design decisions. If you're planning to build it, you must plan to test it.

Testing should be independent of development, to ensure that the software is viewed from a fresh perspective without foreknowledge of how any controls should work. This should be built into the testing plan. The test plan needs to consider the scope of the testing, which will be based on the risk of the device, and needs to ensure that the software both functions correctly (verification) and meets the users' requirements (validation). The test specification will then detail which strategies will be employed to achieve this.

A5.2.2 Verification and Validation

When designing your tests, it is important to be aware of the difference between validation and verification; both of these are equally important.

Table A4: Definition and examples for the terms verification and validation.

	Verification	Validation
Definition	The Verification process determines that the *"product is built right".*	The Validation process determines that the *"right product is built".*
Example	Modified Early Warning Score (MEWS) is correctly calculated.	User wants MEWS calculated, and not some other metric e.g. National Early Warning Score (NEWS).

A5.2.3 Scoping: Testing requirements under IEC 62304

The scope of testing should be based on the risk assessment of the medical device software. As discussed earlier in section A4.2, IEC 62304 identifies three safety classes for medical device software and explicitly states that testing requirements should be based on this classification. High risk class devices (Class C) require full testing, including testing against specific acceptance criteria outlined in IEC 62304, 5.5.4. It should be noted that where verification is required, it is also necessary to evaluate the verification process.

Table A5: Testing requirements for various IEC 62304 Software Safety Classes.

Type of Test	Relevant IEC 62304 Clause	Class A	Class B	Class C
Software unit implementation and verification	5.5.1 (unit implementation)	X	X	X
	5.5.2, 5.5.3, 5.5.5 (establish verification process, unit acceptance criteria, unit verification)		X	X
	5.5.4 (additional software acceptance criteria)			X
Software integration and integration testing	All requirements		X	X
Software System Testing	All requirements	X	X	X

A5.2.4 Independence of testing and peer review

Testing should be independent of development, to ensure that the software is viewed from a fresh perspective; this should be built into the testing plan.

Code (peer) review is a related software quality assurance method, where a second programmer checks the code for bugs, compliance to local coding style guides and general legibility. This may also be performed as pair-programming. Static Code Analysis tools can help improve the efficiency of detecting bugs or inefficiencies. In

small software teams resourcing this independence of testing is often seen as a barrier, however having multiple people familiar with the code base improves the resilience of the service to staff turn-over.

A5.2.5 Types of Testing

Software testing can be classified in a range of different ways such as by development stage (unit, integration and system) or by end point (usability, compatibility, security, compliance) these will be described below, this list is not exhaustive. IEC 62304 defines tests primarily by stage.

A5.2.5.1 Unit Testing

A unit test involves testing a small block of code for which the functional specification can be clearly defined and easily understood. This code module (typically a subroutine, class or function) is tested in isolation (i.e. independent of the rest of the system, which may not necessarily even exist yet). This isolation helps enormously in error investigation – clearly, the module at fault is the one being tested. Unit testing should catch the majority of the errors in your code for relatively little effort. It cannot (by definition) identify problems caused by interactions of the unit under test with the remainder of the system (that is the responsibility of integration testing) but finding and fixing unit-level errors first will greatly simplify that task.

Test Driven Design is the practice of creating unit tests prior to implementing functional code, to ensure that the implementation is testable, and that all units are included.

The unit will typically be tested in a simple 'test frame'. A test frame is a piece of software designed to provide an interface to the unit under test which (from the unit's point of view) provides a simulation of the environment in which it will run in the final system. At its simplest, it provides a set of suitable (section A5.2.6) test input values to the unit under test, runs it, and records or displays the output(s) it returns. If we are interested we can measure the time taken to execute an individual module directly and use this to lead optimisation efforts.

Keep the test frame as simple as possible to reduce the effort required to maintain it – since it is software in its own right it deserves the attention to design, development, review, testing, version control etc. you would accord to any other software.

A5.2.5.2 Integration Testing

Integration testing takes two or more modules which have successfully completed unit testing and tests them in combination. The procedure for running an integration test is much the same as for a unit test. A test frame is written to supply the planned test data, and record the output generated.

Pay particularly careful attention to software and test frame version arrangement when integration testing. The scope for possible test setups increases as more versions and modules become available and the number of combinations increases.

Integration testing also includes the testing of SOUP software items. These tests must verify the function of all software risk controls introduced to mitigate issues that might arise from the anomalous behaviour of the SOUP.

A5.2.5.3 System Testing

System tests should be designed to walk through typical use cases of the software. This also includes verifying that interfaces to other devices (hardware or software) function as specified. To this end it may be useful to develop test scripts

that walk a user through a variety of use cases to demonstrate that the software meets the user requirements. As with unit and interface testing, system tests can be automated depending on the nature of the user interface and the platform used.

Your system test processes should reference your test data. Test data should be sufficient to allow you to complete the steps outlined in your test scripts and you should ensure that you either have a record of the correct results or are able to obtain the correct results from an alternative method. You should also be ready to add new data sets to your test data especially for edge or error cases where your software initially does not behave as expected or produces an error. This process of building up test sets could form part of your surveillance process as described in section A9.

One argument against use of test scripts is that it forces the user to operate the software in a set way and may result in you missing failures that could arise from a user performing operations that are allowed by the software but not considered by the developers. This can be somewhat mitigated against by predicting any deviations and covering them in additional test scripts, or though the less structured approach of allowing an end user free reign on the system and ask them to record any bugs encountered.

A5.2.5.4 Usability Testing

If your software has a user interface you will need to consider and document usability requirements under a usability engineering plan and test your software to provide evidence that these requirements have been met (IEC 62366-1). Usability covers whether the end user is able to operate the software safely rather than whether the software operates. Things to consider might be labelling, feedback to the end user including error and warning display, control layout in response to different screen sizes, responsiveness of controls, use of colour, use of language and terminology (NHS Digital 2019).

A5.2.5.5 Compatibility/Portability Testing

This is closely linked to usability and needs to be considered as early in the project process as possible. Ensuring that your software will work on as many operating systems and platforms as possible is desirable but may increase your testing overhead. For example, consider the user requirement "Must work on modern web browsers" – this would imply compatibility and hence assurance of that compatibility across a wide range of browser software.

A5.2.5.6 Security Testing

Ensuring secure behaviour of controls and processes e.g. sanitization of text inputs, blanking of password entry, encryption of passwords, security of sensitive data, should be captured in your functional requirements. Specific testing to ensure that security functionality is met will depend on the software technology and target operating system. The overall security will be highly dependent on the system on which your software will be deployed, so make sure that requirements for the host system relating to network connectivity, folder permissions, means of access, compatibility with anti-virus software are clear and can be tested as part of deployment testing.

A5.2.5.7 Compliance Testing

Having developed your software under an appropriate quality management system with reference to all applicable regulatory requirements, it is important that you demonstrate that your software and its design and development processes have met those requirements – all aspects have been verified.

A5.2.5.8 Accessibility Testing

Ensuring that accessibility functions, for example font sizes, speech generation, colour palettes and contrast options work correctly with your application (World Wide Web Consortium 2008, NHS Digital 2019).

A5.2.5.9 Performance and Stress Testing

Testing to ensure the performance of the software is acceptable, within given constraints of time and other resources. Performance should be validated under load, to ensure that it continues to function as expected.

A5.2.6 Test Design Techniques

There are a number of techniques which can be helpful in identifying test conditions and cases to ensure adequate test coverage for the code being developed. The following non-exhaustive list is based on ISO 29119-4 *Software and systems engineering - Software testing - Part 4: Test techniques.* Not all will be required or applicable for each project.

- Specification-based test design techniques (Black Box)
    - Equivalence partitioning
    - Classification Tree Method
    - Boundary-value analysis
    - Syntax testing
    - Decision table testing
    - Cause-effect graphing
    - State transition testing
    - Scenario testing
    - Random testing
- Structure-based test design techniques (White box)
    - Statement Testing
    - Branch Testing
    - Decision Testing
    - Modified Condition Decision Coverage (MCDC) Testing
    - Data Flow Testing
- Experience-based test design techniques
    - Error Guessing

A5.2.7 Automation of testing

As software changes, it is important to repeat the testing, this is known as regression testing. Automating tests introduces an initial overhead, but it helps to ensure that these repeat tests can be performed and reported quickly and consistently. The use of automation needs to be balanced against the maintenance requirements of any test framework or software developed as a result.

Your version control software may have easily deployable mechanisms to ensure that unit testing is performed and passes with each release (known as Continuous Integration). It can also be used to ensure that any operations introducing new code or changes to existing code can be reviewed before they are accepted into a release. Automated tools may also be benefited for static code analysis and for ensuring your code conforms to your style guide.

A6 Technical Documentation

A6.1 Technical documentation for software development

The purpose of documentation is to communicate to all stakeholders that a medical device is safe and effective; meeting the essential requirements or GSPR.

The documentation should aid the use, development and maintenance of the device, and also be sufficient for external validation, for example audit by the MHRA. It needs to cover the intended purpose of the device, and the design and performance data used to verify and validate this purpose. Higher level documentation in the QMS (section A2) is required to cover the manufacturing facilities and processes (e.g. software lifecycle and associated tools) used to develop all software devices within the scope of the QMS.

For software, the technical documentation is required to cover all stages within the development lifecycle (section A5.1). Given that software can be easily developed by those who do not ordinarily manufacture physical medical devices and that the range of software types can lead to uncertainty about what technical documentation is required, some additional detail and examples are given in this section. It is intended that the provided examples (supplied in a ZIP folder at https://www.ipem.ac.uk/media/xorhkjft/documentationexamples_rc2.zip could be adapted to suit the specific context within which the software is being developed.

A6.2 Risk-based documentation

The required documentation will vary depending on the risk of the associated project and this is supported by the details associated with each risk category in IEC 62304. Consequently, a low-risk project will not require as many design documents as a high-risk one. This is demonstrated by the summary of required documentation in Table A6. It should be noted that some of the documentation in Table A6 is likely to be shared between software projects, and these should be within in the QMS. For example, the software lifecycle specified by a department's software development policy could be used for all software developed within the department. This may mean that development and maintenance plans would not need to be created for each individual software project.

Table A6**:** Summary of documentation required by IEC 62304 for each software risk category

Documentation	**IEC 62304 Risk Category**		
	A	B	C
Software development plan	x	x	x
Software maintenance plan	x	x	x
Software requirements	x	x	x
Medical device risk analysis	x	x	x
Software architecture		x	x
Detailed design of each software unit and interface			x
Validation plan for software unit implementation		x	x
Validation plan of software integration		x	x
Record of software system testing	x	x	x
Identification of hazards and control measures	x	x	x
Archive of software and documentation	x	x	x
Record of change requests	x	x	x
Record of problem reports	x	x	x

A6.3 Storing and organizing documentation

The tools used for storing and organizing technical documentation are important to facilitate easy search and audit. Existing systems used within the QMS may be sufficient for the local context. However, it may be beneficial to consider tools that are specific to software development. These tools often include features such as integration with the version control code repository and the ability to track bugs and assign them to specific release versions or commits.

It is important that whatever system or tools are used, the documentation for all of the software is quickly and easily identifiable and that the documentation provides the full story of the software over the entire lifecycle (including post release).

A6.4 Barriers to implementation

The introduction of additional documentation, particularly for software types such as Excel Spreadsheets, can be a barrier for compliance with a new software development process. It is therefore important to have a lean approach to documentation such that all of the necessary requirements are fulfilled but is not excessive for the context and the risk specific to the software in question.

Additionally, if the creation of documentation can be automated or re-used in parts, this should be encouraged in order to improve uptake and compliance. The timing of updating documentation can be specified (for example you might release documentation with each release as opposed to each build). It may also be acceptable to complete some design documentation retrospectively after initial prototypes have been created.

A6.5 Documentation examples

Below are brief details of technical documentation that may be beneficial within your software lifecycle/context. The list of documents below is not exhaustive or chronological; nor is it expected that every context will require all of the documentation in this list.

- **Software development policy:** This document will detail the lifecycle(s) that should be followed within your organization for developing software. It should detail all of the documentation that should be produced and at what stage.
- **Style guide:** The style guide can be used by the institution to ensure consistency in coding styles. The guide can cover aspects such as naming conventions for variables/functions/classes etc. and the use of comments within the code. Consistency and accessibility for user interfaces can also be improved by using GUI style guides such as the NHS Digital's Design System.
- **Justification document:** The justification document helps identify that there is sufficient need for the software and that the resources are available to develop and maintain it. This is also a good opportunity to record the results of an options appraisal or market search (for example, the options may be: "do nothing", "develop in-house solution" or "purchase commercial solution") whereby the chosen option is justified. The purpose of the software needs to be identified.
- **Medical device assessment:** This document is a formal assessment of whether the software could be considered a medical device and the class of device that it would be. This could be incorporated into other documentation such as the justification.
- **Risk assessments/hazard log:** The hazard log is an on-going document that should be completed throughout the development lifecycle and will help

guide the design and identify if any additional controls are required. This document will form a key part of the Risk Management File for the device.

- **Software requirements specification:** This should specify all of the functional and non-functional requirements of the software to meet the needs and can detail requirements relating to aspects such as security, interfaces with other devices, user interfaces etc.
- **Software-specific design documentation:** This will be software specific but might include architectural designs using UML diagrams, data dictionaries for databases and user interface sketches.
- **Verification/validation evidence:** An auditor should be able to easily identify the evidence for why the software functions as expected, and that the design meets the needs of the original request. The exact evidence will differ depending on the software and the planned validation/verification process.
- **User documentation:** The exact form of user documentation will vary depending on the software and the context. But as a minimum, it must identify the version, purpose, scope and limitations of the software.
- **Clinical safety report:** The clinical safety report is the summary document that makes the case for why the software is safe and effective for clinical release. It should summarise and link to the evidence. An auditor should be able to take the clinical safety report for the software and identify all of the information they need to conclude on the safety and efficacy of the software.

A7 Clinical Evaluation

As discussed in the main document, Clinical Evaluation is the systematic, planned and continuous process of generating, collecting, analysing and assessing clinical data pertaining to a device to verify its safety and performance, including clinical benefit. Whilst clinical evaluation is not specifically mandated for IHMU under the current UK or EU MDR, a clinical evaluation report is required by the MHRA (2021a) Health Institution Exemption guidance for NI. It is considered best-practice to perform an evaluation, proportionate to risk/benefit, in order to demonstrate that a device is safe and effective.

The EU Medical Device Coordination Group (MDCG 2020) provides guidance on the clinical evaluation of software. Clinical Evaluation should compile three components to demonstrate Clinical Association, Technical Performance and Clinical Performance. Clinical association is the background and underpinning science to any medical device software, for example a systematic literature review. Technical performance relates to the software's accuracy and reliability; this may be demonstrated by unit, integration and system testing as described in section A5.2. Finally clinical performance demonstrates that the software achieves its intended clinical benefit, in the intended conditions, target populations and environments. It should also consider usability of the device, so should involve all stakeholders. This final stage is generally the additional requirement for medical device software over general good software development practice.

Clinical Evaluation does not end at the release of the medical device software; it should form part of post-deployment surveillance (section A9). With future software releases, the need for further clinical evaluation should be reviewed and documented.

A8 Device/Product Support

The main body of this guidance highlights four specific areas as part of support: Labelling and Instructions for use, User Training, Technical Training and Asset management. These areas are all pertinent to software and should be considered. As noted previously in section A3.1, technical training and instructions for use should include IT and data security considerations needed to run the software as intended, such as minimum requirements concerning hardware, IT network characteristics and IT security measures, including protection against unauthorised access.

Asset management of software needs to include recording the version of software installed on each system to enable effective post-deployment surveillance (section A9). It will also help to ensure that changes to the software are deployed uniformly. Centralisation, for example developing the software as a web application, greatly simplifies this process but is not always possible.

For medical device software, as with all software, the maintenance phase will be the longest. Software will often be used within an institution after the original developers have moved on. The software is likely to need to be modified, either to meet the changing needs of the service or due to changes in the IT environment. Design decisions made during the creation of software can therefore have long term consequences on its maintainability. Institutions and departments therefore need to ensure that the knowledge of those involved in supporting and maintaining the software is captured and ensure problem, change and configuration management processes are in place (IEC 62304, 6, 8, 9; ISO/IEC 20000-1, 8.2.6, 8.5, 8.6). This new functionality may change the software into something that would be considered a medical device, or increase its potential class and so must be reassessed.

A8.1 BS EN IEC 80001-1: Application of risk management for IT-networks incorporating medical devices

The BS EN IEC 80001-1 standard, and nine accompanying Technical Reports (designated by BSI as PD IEC/TR 80001-2-x), were developed in recognition that medical devices are often attached to general purpose IT networks within a hospital, and that an overriding risk management policy is needed. The 2011 version of IEC 80001-1 did not gain wide adoption, and a revised version was released in September 2021. This later version extends the remit of IEC 80001-1 to include all networked health software and health IT systems, and is aligned with the emerging ISO 81001-1 *Health software and health IT Systems safety, effectiveness and security*. It is no longer tightly coupled to ISO 14971 *Medical devices — Application of risk management to medical devices*, instead using ISO 31000 *Risk Management*, although it is intended to work alongside any existing organizational risk management process.

The standard recognises that for networked medical devices a single group may not be responsible for the risk management of the device, so there is need for top level management oversight and a controlled, inclusive process.

Responsibility Agreements are suggested to ensure transparent inclusion of all involved stakeholders, a *Responsible, Accountable, Informed and Consulted* (RACI) Chart is suggested (IEC/TR 80001-2-6) to highlight the different groups, and identify when and how they need to be involved for different tasks during an application's lifecycle. Assurance cases (IEC/TR 80001-2-6) are required to demonstrate the risks identified and controls implemented.

From a manufacturer perspective, the standard suggests (IEC/TR 80001-2- 2) that implementing institutions request specific information from suppliers to inform the network risk management process, for example the Manufacturer Disclosure

Statement for Medical Device Security (MDS2: NEMA 2019) questionnaire. The use of standardized questionnaires reduces the work for vendors, compared to answering individual queries from customers, and ensures transparency and good coverage of potential issues. Whilst there is no requirement to do so for IHMU, working through an MDS2 will help guide the risk management of networking a medical device.

In practice, the implications of this can be seen when using corporate IT resources as part of the IHMU of software. For example developing an application that utilises a central IT login service (e.g. Microsoft Active Directory or LDAP) removes the need for users to remember two passwords, ensures passwords conform to the institution's Information Governance password policy, centralises account deactivation when users leave the institution and allows IT to audit login activity (MSD2: Person Authentication (PAUT) Question 2). By doing this however the application's availability is now dependent on the IT infrastructure and network. Network interruptions will mean the application is unavailable, and changes by IT may also require changes to the software. This risk and benefits of doing this therefore needs to be carefully considered during the development of the software.

A9 Post deployment surveillance

As discussed in the main document, surveillance consists of vigilance for errors and clinical follow-up, to ensure that the device continues to maintain clinical performance (section A7).

A9.1 Vigilance

Bug tracking software (for example Bugzilla or JIRA) is commonly used as part of software maintenance, and provide good integration with source code version control repositories. Their use should be reflected in the QMS, although additional institutional reporting may be necessary depending on clinical impact. Where software of unknown provenance (SOUP) has been used, whether commercial or open source, vigilance extends to ensuring that risks caused by newly discovered vulnerabilities in them are mitigated, either by patching the system and re-releasing or ensuring they do not propagate to the medical device. Practically, this can be achieved by monitoring repositories such as the Common Vulnerabilities and Exposures (CVE) for new issues that may impact frameworks and libraries that may be used by the software. NHS Digital also provides alerts of risks found within the Health and Social Care Network (HSCN), which may exploit these vulnerabilities (NHS Digital 2021).

A9.2 Clinical Follow-up

Medical device software can record a lot of information, in databases and logs; this provides an excellent opportunity to ensure that data is captured to monitor clinical performance as well as user errors and bugs. To maximise the benefit, this needs to be planned from the start of the software development project and reflected in the software requirements. Logging can help developers understand the interaction of users with the software, to help them improve the efficiency of the UI for future upgrades, and can monitor software usage to flag when a system is moving towards obsolescence.

A10 Works cited in Annex A

AXELOS (2019). *ITIL Foundation, ITIL 4 edition.* TSO, England. ISBN: 9780113316083

Bruyninckx, H. (2008). *V model from structured system design.* GNU Free Documentation Licence. Accessed: 19/10/2021. Available at: https://commons.wikimedia.org/wiki/File:V-model.svg

BS EN 60601-1:2006+A2:2021. *Medical electrical equipment. General requirements for basic safety and essential performance.*

BS EN 62304:2006+A1:2015. *Medical device software. Software life-cycle processes*

BS EN 80001-1:2021. *Application of risk management for IT-networks incorporating medical devices. Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software.*

BS EN 82304-1:2017. *Health Software – Part 1: General requirements for product safety*.

BS EN ISO 14971:2019+A11:2021. *Medical devices. Application of risk management to medical devices.*

BS ISO/IEC/IEEE 90003:2018. *Software engineering. Guidelines for the application of ISO 9001:2015 to computer software.*

BSI ISO/IEC 12207:2017. *Systems and software engineering – software lifecycle processes.*

ISO 16142-1:2016. *Medical devices — Recognized essential principles of safety and performance of medical devices — Part 1: General essential principles and additional specific essential principles for all non-IVD medical devices and guidance on the selection of standards.*

DCB0129:2018. *Clinical Risk Management: its Application in the Manufacture of Health IT Systems*. NHS Digital. Accessed 19/10/2021. *Available online at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems*

DCB0160:2018. *Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems*. NHS Digital. Accessed 19/10/2021. Available at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems

European Commission (2019). *Manual on borderline and classification in the community regulatory framework for medical devices. Version 1.22.* Accessed: 19/10/2021. Available at: https://ec.europa.eu/docsroom/documents/35582

European Parliament and Council, (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation.* Accessed 19/10/2021. Available at; http://data.europa.eu/eli/reg/2016/679/oj

European Parliament and Council, (2017). *Regulation (EU) 2017/745 on Medical Devices as amended by Regulation 2020/561*. Accessed: 19/10/2021. Available at: http://data.europa.eu/eli/reg/2017/745/2020-04-24

IEC 60601-1-6:2013+A2:2020. *Medical electrical equipment. General requirements for basic safety and essential performance. Collateral standard. Usability*

IEC 62366-1:2015+A1:2020. *Medical devices. Part 1: Application of usability engineering to medical devices*

ISO 9001:2015. *Quality management systems — Requirements*

ISO 13485:2016 *Medical devices — Quality management systems — Requirements for regulatory purposes.*

ISO 31000:2018. *Risk management — Guidelines*

ISO 81001:2021. *Health software and health IT systems safety, effectiveness and security - Part 1: Principles and concepts.*

ISO/IEC 20000-1:2018. *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC/IEEE 29119-4:2015. *Software and systems engineering — Software testing — Part 4: Test techniques*

MDCG (2019). *MDCG 2019-11: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.* Medical Device Coordination Group. Accessed 19/10/2019. Available at: https://ec.europa.eu/docsroom/documents/37581

MDCG (2020). *MDCG 2020-1: Guidance on clinical evaluation (MDR) / Performance evaluation (IVDR) of medical device software.* Medical Device Coordination Group. Accessed: 19/10/2021. Available at: https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2020_1_guidance_clinic_eva_md_software_en.pdf

MDCG (2021a). *Is your software a Medical device? Decision steps to assist qualification of Medical Device Software*. Medical Device Coordination Group. Accessed: 19/10/2021. Available at. https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_mdcg_2021_mdsw_en.pdf

MDCG (2021b). *MDCG 2021-24 - Guidance on classification of medical devices*. Accessed 28/03/2022. Available at: https://ec.europa.eu/health/latest-updates/mdcg-2021-24-guidance-classification-medical-devices-2021-10-04_en

MEDDEV (2016) *MEDDEV 2.1/6 July 2016: Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices*. Accessed 17/02/2022. Available at: https://www.medical-device-regulation.eu/wp-content/uploads/2019/05/2_1_6_072016_en.pdf

MHRA (2021a). *Medical devices: software applications (apps).* The Medicines and Healthcare products Regulatory Agency. Accessed 19/10/2021. Available at: https://www.gov.uk/government/publications/medical-devices-software-applications-apps

MHRA (2021b). *MHRA guidance on the health institution exemption (HIE) – IVDR and MDR (Northern Ireland).* The Medicines and Healthcare products Regulatory Agency Accessed: 19/10/2021. Available at: https://www.gov.uk/government/publications/mhra-guidance-on-the-health-institution-exemption-hie-ivdr-and-mdr-northern-ireland

NEMA (2019). *Manufacturer Disclosure Statement for Medical Device Security. ANSI/NEMA HN 1-2019. 100382.* National Electrical Manufacturers Association. Published 08/10/2019, Accessed 09/05/2021. Available at: https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security

NHS Digital (2019). *NHS Digital Service Manual: Design System*. Accessed 19/03/2022. Available at; https://service-manual.nhs.uk/design-system

NHS Digital (2021). *Cyber and data security*. Accessed: 19/10/2021. Accessed: 19/10/2021. Available at: https://digital.nhs.uk/cyber

PD IEC/TR 62366-2:2016. *Medical devices – Part 2: Guidance on the application of usability engineering to medical devices*.

PD IEC/TR 80001-2-1:2012. *Application of risk management for IT-networks incorporating medical devices. Step-by-step risk management of medical IT-networks. Practical applications and examples*.

PD IEC/TR 80001-2-2:2012. *Application of risk management for IT-networks incorporating medical devices. Guidance for the disclosure and communication of medical device security needs, risks and controls*.

PD IEC/TR 80001-2-3:2012. *Application of risk management for IT-networks incorporating medical devices. Guidance for wireless networks*.

PD IEC/TR 80001-2-4:2012. *Application of risk management for IT-networks incorporating medical devices. Application guidance. General implementation guidance for healthcare delivery organizations*.

PD IEC/TR 80001-2-5:2014. *Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems.*

PD IEC/TR 80001-2-8:2016. *Application of risk management for IT-networks incorporating medical devices Part 2-8: Application guidance - Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*.

PD IEC/TR 80001-2-9:2017. *Application of risk management for it-networks incorporating medical devices. Application guidance. Guidance for use of security assurance cases to demonstrate confidence in IEC TR 80001-2-2 security capabilities Standards*.

PD IEC/TR 80002-1:2009. *Medical device software. Guidance on the application of ISO 14971 to medical device software.*

PD IEC/TR 80002-3:2014. *Medical device software – Part 3: Process reference model of medical device software life cycle processes (IEC 62304).*

PD ISO/TR 17791:2013. *Health informatics. Guidance on standards for enabling safety in health software.*

PD ISO/TR 80001-2-6:2014. *Application of risk management for IT-networks incorporating medical devices – Part 2-6: Guidance for responsibility agreements.*

PD ISO/TR 80001-2-7:2015. *Application of risk management for IT-networks incorporating medical devices - Part 2-7: Application Guidance - Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*.

PD ISO/TR 80002-2:2017. *Medical device software - Part 2: Validation of software for regulated processes*.

Planbox 2012*. Agile Project Management by Planbox*. Creative Commons Attribution-Share Alike 3.0 Unported license. Available at: https://commons.wikimedia.org/wiki/File:Agile_Project_Management_by_Planbox.png

The Data Protection Act, 2018, S. I. 2018/12. Available at: https://www.legislation.gov.uk/ukpga/2018/12

The Medical Devices Regulations, 2002. S.I. 2002/618. [Online] Available at: https://www.legislation.gov.uk/uksi/2002/618

NHS Digital (2019). *NHS Digital service manual: Accessibility guidance for Testing*. Accessed: 21/10/2021. Available at: https://service-manual.nhs.uk/accessibility/testing

World Wide Web Consortium (2008). *Web Content Accessibility Guidelines (WCAG) 2.0*. Accessed: 21/10/2021. Available at: https://www.w3.org/TR/WCAG20/

A11 Contributors and Acknowledgements

Section		Lead Author(s)
A0	Introduction	A. Chalkley[a]
A1	Is it a Medical Device?	A. Partlow[b] and C. Tarbert[c]
A2	QMS for Software	C. Tarbert[c] and J. Moggridge[d]
A3	Essential Safety requirements of Software	A. Chalkley [a]
A4	Risk Management of Software	D. Jennings[e]
A5.1	Design and Development: SDLC	J. Leighs[f] and M. Guy[f]
A5.2	Design and Development: Testing	J. Moggridge[d] and A. Green [a]
A6	Technical Documentation	J. Kirby[g]
A7	Clinical evaluation	A. Chalkley [a]
A8	Device/Product support	A. Chalkley [a]
A9	Post-deployment surveillance	A. Chalkley [a]

Affiliations

a. University Hospitals Birmingham NHS Foundation Trust
b. Cardiff and Vale University Health Board
c. Greater Glasgow and Clyde
d. University College London Hospitals NHS Foundation Trust
e. Belfast Health and Social Care Trust
f. University Hospital Southampton NHS Foundation Trust
g. Newcastle Hospitals NHS Foundation Trust

Peer Reviewers

E. Claridge, M. Drinnan, P. Ganney, D. Grainger, J. McCarthy

Annex B UK Regulatory situation as of January 2024

The current regulations in force regarding the manufacture of medical devices to be placed on the market in the UK are in the UK Medical Devices Regulations 2002 (SI 2002 No 618, as amended from time to time since) (The Medical Devices Regulations, 2002).

Prior to Brexit, these were based on the three EU medical devices Directives for Active Implantable Devices, General Medical Devices (the EU MDD) and In-vitro Diagnostic Devices. The new EU Medical Devices Regulation (EU MDR) (European Parliament and Council, 2017) was also in force in the UK until 31st December 2020 (but not mandatory) but did not become directly applicable retained EU law after that date because its date of full application was postponed by the EU until a date after the end of the Brexit transition period on 31st December 2020.

In September 2020 the MHRA produced guidance on regulating medical devices from 1st January 2021 and updated this in a version dated 8th February 2024, Regulating medical devices in the UK. This set out the situation from that date in respect of both GB (England, Wales and Scotland) and of Northern Ireland.

The Government also produced a new Statutory Instrument (SI) that further amends the UK MDR 2002; The Medical Devices (Amendment etc.) (EU Exit) Regulations 2020 which came into affect on 1st January 2021 at the end of the implementation period as part of the EU withdrawal agreement. There is also a draft Explanatory Memorandum.

A key feature of this S.I. was that unlike the Medical Devices (Amendment etc) (EU exit) Regulations 2019 which it further amended in part, this new Amendment Regulation 2020 does not bring in requirements which were clearly based on the EU MDR and IVDR (but worded in a UK context) for the whole of the UK. However, because of the Northern Ireland Protocol which was agreed with the EU as part of the Withdrawal Agreement, Northern Ireland (NI) would continue to apply the provisions of the EU MDR, whilst Wales, Scotland and England (GB) would continue to apply the amended UK MDR 2002 based on the old EU MD Directives.

An explanatory memorandum issued with this 2020 S.I. says at 7.16 …

Any devices that are in conformity with EU legislation (MDD, AIMDD, IVDD, MDR, IVDR) can continue to be placed on the market in GB until 30 June 2023. This is to provide manufacturers with time to adjust to future GB regulations that will be consulted on and published at a later date.

The final sentence of this paragraph is significant. It was clear that these 2020 amendments to the earlier version of the UK MDR 2002, and the allowance for CE marking, are in effect a stop-gap measure whilst the UK government drafts new stand- alone medical devices regulations to take effect after 30th June 2023.

Between September and November 2021, the MHRA initiated the promised consultations on proposed changes to the regulatory framework for medical devices in the United Kingdom (UK) based, at least in part, on concerns voiced that developing and bringing into force new regulations, and having manufacturers able to implement them, by June 2023 risked supply problems. IPEM submitted a considered response to this consultation exercise.

The nature of the questions asked in the consultation document appeared to indicate that some form of alignment with the EU MDR is contemplated (perhaps similar essential safety and performance requirements and similar device classification rules) and that a regulated but permitted 'health institution exemption'

from full conformity assessment of in-house manufactured and used devices is likely to be included.

In June 2023, the Government used the Medical Devices (Amendment) (Great Britain) Regulations 2023 (S.I. 2023 No.627) to further amend the Medical Devices Regulations 2002. The most significant result is in summary, to extend the validity of CE marking of medical devices to 30 June 2028 for devices with a certificate of conformity under the EU MDD and to 30 June 2030 for devices with a certificate of conformity under the EU MDR. It is a little more complicated for IVDs.

MHRA propose to consult on new draft regulations in 2024 with the objective of them coming into force in 2025 – presumably with a transition period to 2030.

In the meantime, they are working on putting into place additional, strengthened requirements for post market surveillance as a new S.I.

See https://www.gov.uk/government/publications/implementation-of-the-future-regulation-of-medical-devices/implementation-of-the-future-regulations

It is now possible to access a consolidated version of the UK MDR 2002+ on the Legislation.gov website: https://www.legislation.gov.uk/uksi/2002/618/contents Make sure the 'Latest Available' button is selected under 'What Version', Click the 'Print Options' button, then click the pdf option under 'The Whole Instrument', to get a PDF version

We have referred to these amended UK regulations as the UK MDR 2002+.

In-house manufacture and use (IHMU): historic context

The EU MDD and the UK MDR 2002 were both silent on IHMU and the interpretation in the UK was, and remains, that this Directive did not cover such activity. Other EU member states took a different view and the EU Commission did not agree with the UK interpretation but as a Directive, different interpretations in different jurisdictions are possible. Consequentially in the UK as a whole, until 1st January 2021 there was no mandatory regulatory framework around IHMU for general medical devices. As of January 2024, this remains the case for GB but in NI, the provisions in the EU MDR 2017 should be followed – see below.

The MHRA and it predecessors had from time to time produced some guidance but have not kept accessible the more detailed one (which is undated) (MHRA, n.d.). A more recent guidance document is from 2014 (MHRA, 2014). There is also the very recent on line guidance linked to above.

IPEM produced a detailed document in its Report series in 2004 (Wentworth, 2004). This is a particularly useful document in its basic concepts though it concentrated on medical electrical devices and most of the supporting documents and Standards referred to have now been long updated. Nevertheless it is well worth consulting.

The EU MDR 2017 explicitly dealt with IHMU, clearly brought it within the new Regulation in Article 5.4 and then mandated a set of requirements in Article 5.5 which if followed, exempted the health institution from full conformity assessment for such medical devices. The MHRA have referred to this as the 'health institution exemption' (HIE). The full text of Articles 5.4 and 5.5 are given in Annex C. However, as explained above, the EU MDR has not become applicable in GB.

Key message

The key messages as far as in-house manufacture and use is concerned are that for Northern Ireland, the EU MDR Article 5.5 must be applied from 2021 and the MHRA have provided a guidance document. In GB, for the time being, the UK

2002 MDR+ apply with no explicit regulatory requirements for IHMU. However other health and safety regulations may apply in some circumstances, and these 'best-practice' guidelines will be useful even in the Northern Ireland context as will the NI guidance document in the GB context.

IPEM will continue to engage in the MHRA consultation process and promote the introduction of specific but proportionate regulatory requirements for in-house manufacture and use.

References

European Parliament and Council, 2017. *REGULATION (EU) 2017/745 on Medical Devices as amended by Regulation 2020/561.* [Online]
Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02017R0745-20230320
[Accessed 2024-01-17].

MHRA, 2014. *In-house manufacture of medical devices.* [Online]
Available at: https://www.gov.uk/government/publications/in-house-manufacture-of-medical-devices/in-house-manufacture-of-medical-devices
[Accessed 2024-01-17].

MHRA, n.d. *Bulletin 18: The Medical Devices Regulations: Implications on Healthcare and other Related Establishments,* London: MHRA.

The Medical Devices Regulations, 2002. *S.I. 2002/618.* [Online]
Available at: https://www.legislation.gov.uk/uksi/2002/618
[Accessed 2024-01-17].

Wentworth, S. (Ed), 2004. *Safe Design, Construction and Modification of Electromedical Equipment,* York, UK: Institute of Physics and Engineering in Medicine

Annex C EU MDR Articles 5.4 and 5.5

5.4. Devices that are manufactured and used within health institutions shall be considered as having been put into service.

5.5. With the exception of the relevant general safety and performance requirements set out in Annex I, the requirements of this Regulation shall not apply to devices, manufactured and used only within health institutions established in the Union, provided that all of the following conditions are met:

(a) the devices are not transferred to another legal entity,

(b) manufacture and use of the devices occur under appropriate quality management systems,

(c) the health institution justifies in its documentation that the target patient group's specific needs cannot be met, or cannot be met at the appropriate level of performance by an equivalent device available on the market,

(d) the health institution provides information upon request on the use of such devices to its competent authority, which shall include a justification of their manufacturing, modification and use;

(e) the health institution draws up a declaration which it shall make publicly available, including:

  (i) the name and address of the manufacturing health institution;

  (ii) the details necessary to identify the devices;

  (iii) a declaration that the devices meet the general safety and performance requirements set out in Annex I to this Regulation and, where applicable, information on which requirements are not fully met with a reasoned justification therefor,

(f) the health institution draws up documentation that makes it possible to have an understanding of the manufacturing facility, the manufacturing process, the design and performance data of the devices, including the intended purpose, and that is sufficiently detailed to enable the competent authority to ascertain that the general safety and performance requirements set out in Annex I to this Regulation are met;

(g) the health institution takes all necessary measures to ensure that all devices are manufactured in accordance with the documentation referred to in point (f), and

(h) the health institution reviews experience gained from clinical use of the devices and takes all necessary corrective actions.

Member States may require that such health institutions submit to the competent authority any further relevant information about such devices which have been manufactured and used on their territory. Member States shall retain the right to restrict the manufacture and the use of any specific type of such devices and shall be permitted access to inspect the activities of the health institutions.

This paragraph shall not apply to devices that are manufactured on an industrial scale.

Annex D Definitions of 'medical device', 'accessory for a medical device' and 'custom-made device'

From the UK MDR 2002 Regulation 2.—(1) as amended in 2008, and current at January 2024

"medical device" means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnosis or therapeutic purposes or both and necessary for its proper application, which—

(a) is intended by the manufacturer to be used for human beings for the purpose of-
  (i) diagnosis, prevention, monitoring, treatment or alleviation of disease,
  (ii) diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
  (iii) investigation, replacement or modification of the anatomy or of a physiological process, or
  (iv) control of conception; and

(b) does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, even if it is assisted in its function by such means,

and includes devices intended to administer a medicinal product or which incorporate as an integral part a substance which, if used separately, would be a medicinal product and which is liable to act upon the body with action ancillary to that of the device;

From the UK MDR 2002 Regulation 5.—(1) as amended in 2008, and current at January 2024

"accessory" means an article which, whilst not being a medical device, is intended specifically by its manufacturer to be used together with a medical device to enable it to be used in accordance with the use of the medical device intended by its manufacturer.

"custom-made device" means a relevant device that is—

(a) manufactured specifically in accordance with a written prescription of registered medical practitioner, or other person authorised to write such a prescription by virtue of his professional qualification, which gives, under his responsibility, specific characteristics as to its design; and

(b) intended for the sole use of a particular patient,

but does not include a mass-produced product which needs to be adapted to meet the specific requirements of the medical practitioner or professional user.

From the EU MDR Article 2

For the purposes of this Regulation, the following definitions apply:

(1) 'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
  — diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
  — diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

— investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
— providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,

and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices:

— devices for the control or support of conception;
— products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point.

(2) 'accessory for a medical device' means an article which, whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s);

(3) 'custom-made device' means any device specifically made in accordance with a written prescription of any person authorised by national law by virtue of that person's professional qualifications which gives, under that person's responsibility, specific design characteristics, and is intended for the sole use of a particular patient exclusively to meet their individual conditions and needs.
However, mass-produced devices which need to be adapted to meet the specific requirements of any professional user and devices which are mass-produced by means of industrial manufacturing processes in accordance with the written prescriptions of any authorised person shall not be considered to be custom-made devices;

Additional informative note:

Article 1(2) of the EU MDR refers to a list in Annex XVI of groups of products without an intended medical purpose to which "the Regulation shall also apply".

The list includes "high intensity electromagnetic radiation (e.g. infra-red, visible light and ultra-violet) emitting equipment intended for use on the human body, including coherent and non-coherent sources, monochromatic and broad spectrum, such as lasers and intense pulsed light equipment, for skin resurfacing, tattoo or hair removal or other skin treatment."

These and the other types of products listed are now also covered by the EU MDR.

Annex E Notes on the Engineering Design Process

Modified in red from http://www.sciencebuddies.org/engineering-design-process/engineering-design-process-steps.shtml

A0.1.1.1 Key Info

- The engineering design process is a series of steps that engineers follow to come up with a solution to a problem. Many times the solution involves designing a product (like a machine or computer code) that meets certain criteria and/or accomplishes a certain task.
    - This process is different from the Steps of the Scientific Method, which you may be more familiar with. If your project involves making observations and doing experiments, you should probably follow the Scientific Method. If your project involves designing, building, and testing something, you should probably follow the Engineering Design Process. If you still are not sure which process to follow, you should read Comparing the Engineering Design Process and the Scientific Method.
- The steps of the engineering design process are to:
    - Define the problem;
    - Do background research;
    - Specify the requirements;
    - Brainstorm solutions;
    - Choose and verify the best solution;
    - Devise validation tests;
    - Do development work;
    - Build a prototype;
    - Test (validate) and redesign as necessary.
- Engineers do not always follow the engineering design process steps in order, one after another. It is very common to design something, test it, find a problem, and then go back to an earlier step to make a modification or change to your design. This way of working is called **iteration**, and it is likely that your process will do the same!

Note

verification asks the question 'Is the design proposal a true reflection of the requirements set out in the design specification?' Therefore, it comes in at a fairly early stage of the process.
ISO 13485 7.3.6 says:

Design and development verification shall be performed in accordance with planned and documented arrangements to ensure that the design and development outputs have met the design and development input requirements.

validation asks the question, 'Does the final product meet the original design specification?' Validation tests should be devised and agreed as an earlier part of the design process.

ISO 13485 7.3.7 says:

Design and development validation shall be performed in accordance with planned and documented arrangements to ensure that the resulting product is capable of meeting the requirements for the specified application or intended use.

Annex F The history of ISO 13485

ISO 13485 started off in the late 1990s with the title *Quality systems. Medical devices. Particular requirements for the application of EN ISO 9001*. Although it became a stand alone Standard it remained closely aligned to ISO 9001 as that Standard was developed and revised. This was the case up to and including the 2012 Edition which was structurally aligned with the 2008 4th Edition of ISO 9001.

The 5th Edition of ISO 9001 in 2015 brought this Standards into line with the common High Level Structure that ISO had introduced in 2012 for management system Standards such as ISO 14001 (Environmental management systems), ISO 45001 (Occupational health and safety) and ISO/IEC 27001 (Information security management systems).

The revision of ISO 9001 was a considerable restructuring with a less prescriptive, more risk based approach, perhaps suitable to its very wide applicability. In parallel and over the same time period, ISO 13485 was also being updated but its structure was not at this time brought into line with the High Level Structure and the 2016 issue remained aligned with the structure of the 2008 4th Edition of ISO 9001.

As part of a scheduled review of ISO 13485 in 2018 there was pressure from ISO on its relevant Technical Committee, TC 210, to structurally revise ISO 13485:2016 to bring it into line with the High Level Structure as had happened with ISO 9001:2015. This was not accepted by the national member bodies including BSI, in considerable part because ISO 13485:2016 (still structurally aligned with ISO 9001:2008) was widely used in a medical device regulatory context in many jurisdictions including the EU. Additionally and significantly, the Food and Drugs Administration (FDA) in the USA had decided to adopt ISO 13485:2016 as the QMS framework for US manufacturers.

It is probable that ISO 13485 will be aligned with the ISO High Level Structure at its next revision but will remain the clear QMS Standard of choice for medical device manufacture and management.

The first NHS organization to put in place a formal QMS is thought to be the MEMO organization in Bristol and the second (or maybe third) was the Bioengineering Unit in Cardiff. (McCarthy & Hicks, 1991). Both were certified to ISO 9002 (i.e. did not include design and manufacture and covered service only). The adoption of QMS Standards has expanded very considerably since then and includes ISO 9001 in Radiotherapy applications and ISO 9001 or ISO 13485 in Clinical Engineering and Rehabilitation Engineering Departments.

Many departments now include design and development in the scope of their QMS and an increasing number are using the ISO 13485 framework.

Reference

McCarthy, J. & Hicks, B., 1991. Quality in healthcare: Application of the ISO 9000 standard. *Int. J. Health Care Quality Assurance,* 4(16), pp. 21 - 25.