Helsedirektoratet

Report on quality assurance: Use of artificial intelligence in health and care services

Først publisert: 23. mai 2025
Last revised date: 23. mai 2025

Innhold

Foreword

The national coordination project *Better Use of Artificial Intelligence* (AI) was carried out from 2019 to 2023 as part of the National Health and Hospital Plan 2019–2023. During this work, a need was identified for clearer frameworks on how to ensure the quality of AI systems to support their safe and effective use in the health and care sector.

As a result, the subproject *Frameworks for Quality Assurance* was initiated in August 2023, following an initiating phase conducted in close dialogue with the health sector, including workshops held in spring 2023. The subproject is now part of the *Joint AI Plan for the Health and Care Services 2024–2025*. This report presents the work completed to date. Further communication, updates, and development of guidance materials will be carried out in line with the priorities of the Joint AI Plan.

The following health agencies have contributed to the work: The Norwegian Directorate of Health / Directorate for e-Health, The Norwegian Medicines Agency / The Norwegian Medical Products Agency, The Norwegian Institute of Public Health, and The Norwegian Board of Health Supervision, joined later by The Directorate for Radiation Protection and Nuclear Safety. Representatives from The South-Eastern Norway Regional Health Authority (South-Eastern Norway Regional Health Authority) and Sykehuspartner Hospital Trust have also participated. The work has been led by The Norwegian Directorate of Health.

A user panel was established, consisting of potential external users of the guidance materials, and in addition, experts in the field. The panel included representatives from Haukeland University Hospital, Akershus University Hospital, Vestre Viken Hospital Trust, Bærum Hospital, LIVV Health, the Centre for Patient-Centered Artificial Intelligence (Senter for pasientnær kunstig intelligens) at the University Hospital of Northern Norway, DNV, Norwegian Computing Center, Sykehusinnkjøp, the National Centre for E-health Research, Stavanger Municipality, Drammen Municipality, Trondheim Municipality, Bergen Municipality, and the Norwegian Association of Local and Regional Authorities (KS – kommunesektorens organisasjon).

The expert network Artificial Intelligence in the Norwegian Health Services (KIN) has provided continuous and valuable contributions through professional input and discussion.

Oslo, 18th December 2024

Executive summary

This report is intended to support organizations planning to acquire an AI system, ensuring that such systems can be used safely and effectively. It outlines the key considerations organizations must address to assess whether an AI system is trustworthy when procuring, implementing, and using AI in health and care services.

The US National Institute of Standards and Technology (NIST) characterises trustworthy AI as follows: *Valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed* [1].

In 2019, the European Union published ethical guidelines describing three core components of trustworthy AI that should be upheld throughout a system's lifecycle:

> (1) it should be legal, complying with all applicable laws and regulations, (2) it should be ethical, ensuring adherence to ethical principles and values, and (3) it should be robust, both from a technical and social perspective, as AI systems, even with good intentions, can cause unintended harm [2].

This report describes the current legal framework, outlining what is required by applicable regulations and, in part, what is considered good practice. However, AI is a rapidly evolving field, with new legislation on the horizon. The more specific boundaries between the EU's regulations on medical devices, data protection and artificial intelligence need to be clarified. In the time to come, updated guidance material will be necessary as knowledge and new regulations take shape.

AI systems can take different forms: a stand-alone application on a PC or mobile application, a web service, or components integrated into clinical systems or electronic health records.

With this in mind, the report presents some overarching aspects that organizations must consider. We have structured these into six phases covering procurement, implementation and use of AI.

Legal framework: Adopting AI systems involves assessments related to clinical responsibility, data protection, information security, access to health data, data management and automated decision-making processes.

Health legislation contains obligations and rights for health and care services and patients. Key principles are the right to health care, the requirement for medically sound services and health professionals' duty of confidentiality. The processing of health information is also covered by the General Data Protection Regulation (GDPR), which imposes several requirements for the data controller. The Equality and Anti-Discrimination Act is also relevant [3]. The Medical Devices Regulations regulates manufacturers' responsibilities for ensuring the safety of medical devices, including those that incorporate or consist of AI [4]. The Artificial Intelligence Act aims to ensure that products and systems that utilise AI are safe to use [5]. The regulations impose requirements on both manufacturers and users of AI (which may be the health and care services). It is also important to identify and apply any relevant domain specific regulations when procuring, validating, and implementing AI systems.

Risk management: While AI has the potential to enhance healthcare delivery, it also introduces new challenges. Without adequate risk assessment, AI systems may produce, reinforce, or perpetuate unjust or undesirable outcomes for individuals, health services, or society, potentially compromising patient safety.

Validation: Prior to implementation, AI models must be quality assured, and this may include clinical validation. In this report, clinical validation means confirming that the AI model performs as intended, for a specific intended purpose [6]. If the intended purpose of an AI model is to detect fractures on X-rays, it must be validated precisely for that use case.

Ethical principles: AI systems must be both safe and ethically acceptable. The European Commission's expert group has proposed seven ethical principles, which are also reflected in the Norwegian government's AI strategy [7]. The strategy emphasizes that AI must be based on ethical principles, ensure transparency, and respect human rights and democratic values [8]. At the same time, it may be ethically questionable not to use AI systems if they can provide better quality, streamline services and thus free up resources for other important tasks.

Six phases for the procurement, implementation and use of AI
This report is divided into six phases that an organization can use as a starting point when considering the procurement and implementation of an AI system. The phases are briefly described in the list below. While many of the phases involve similar quality or risk-related topics, these are addressed with increasing depth and specificity. For low-risk AI applications, the organization does not need to address all aspects in the same detail. As new information emerges, it may be necessary to revisit earlier phases and update or repeat parts of the process.

AI fact sheets: In-depth information on selected topics covered in the report can be found in the AI fact sheets published on the inter-agency information site on AI in healthcare [9].

[1] Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov), page 12 and Trustworthy and Responsible AI | NIST: Characteristics of trustworthy AI systems include: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed.

[2] European Commission: Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI, Publications Office, 2019, https://data.europa.eu/doi/10.2759/346720

[3] Act on Equality and Prohibition of Discrimination (Equality and Anti-Discrimination Act) – Lovdata

[4] Medical device regulations – Norwegian Medical Products Agency (dmp.no)

[5] The EU adopted a law on artificial intelligence (the AI Regulation) in 2024. https://www.iso.org/obp/ui/

[6] https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en In the ISO 9000:2015 standard "Quality Management System - Fundamentals and vocabulary", "validation" is defined as: "Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled."

[7] Ethics guidelines for trustworthy AI | Shaping Europe's digital future (europa.eu) and

[8] Nasjonal strategi for kunstig intelligens (regjeringen.no)

[9] AI fact sheets will be published on Kunstig intelligens – Helsedirektoratet

Introduction

The *National Health and Collaboration Plan 2024–2027* emphasizes that AI can play a key role in ensuring the sustainable development of Norway's healthcare system. AI and other labor-saving technologies are expected to help maintain the quality of services in the coming years while also contributing to reduced waiting times [10].

This report reflects the state of knowledge as of the turn of the year 2024/2025. Given the rapid pace of development in the field of AI, the report will not be continuously updated to reflect emerging knowledge.

The work presented here stems from the subproject *Frameworks for Quality Assurance* and reflects the status at the end of 2024. As AI continues to evolve, new EU legislation is on the way that will influence how AI is used in Norway. In the time ahead, updated guidance materials will be needed as both knowledge and regulatory frameworks continue to develop. Communication, revisions, and further development of supportive tools will be carried out in accordance with the priorities of the *Joint AI Plan* [11].

The report describes the legal framework, the mandatory requirements and, to some extent, the best practices for ensuring that AI systems used in health and care services are trustworthy. The European Union identifies three components that a trustworthy AI system should meet throughout its lifecycle [12]:

1. It should be legal, in compliance with all applicable laws and regulations.
2. It should be ethical and ensure compliance with ethical principles and values.
3. It should be robust, both from a technical and social perspective, as AI systems, even with good intentions, can cause unintended harm.

Trustworthy AI is characterised by the US National Institute for Standardization and Technology (NIST) as follows: *Valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed* [13].

This report uses the definition of an AI system as described in the **AI Act**, which defines an AI system as:

> ...a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments [14].

An AI system can take different forms: standalone applications on a PC or mobile device, web services, components of specialist clinical systems, or modules embedded in electronic health record systems.

AI also has inherent characteristics that make quality assurance more complex than for traditional IT systems. When procuring, implementing, and using AI, organizations must consider several critical factors, including:

- **The black-box problem:** AI models, especially those based on deep neural networks, can be difficult to interpret. In some cases, their logic and data may be inaccessible due to commercial restrictions. This lack of explainability can undermine trust and hinder use among healthcare professionals and may in turn affect patients' right to understand how their health information is processed [15].
- **Bias:** are systematic errors that occur in AI systems due to biases in the training data. AI models reflect the data they are trained on and must be representative of the population the AI model will be used on. The data can also represent discrimination in society. Bias can cause AI models to provide incorrect, biased or discriminatory content [16]

- **Hallucination**: Generative AI models create content based on the data the model is trained on. This content may appear to be true and correct but may be untrue or fabricated. This presents a specific risk that organizations should be aware of when deploying such systems in healthcare settings.

Goals and target group

This report has been developed to support organizations planning to acquire an AI system, helping to ensure its safe and effective use. The goal is to provide guidance on identifying, assessing, and managing the risks associated with the procurement, implementation, and operation of fully developed AI systems in the healthcare sector. It highlights key issues that organizations should pay particular attention to assess whether an AI system can be considered trustworthy.

The target audience for the report includes individuals involved in assessments and decisions related to planning, acquiring, implementing, and managing AI systems in health and care services. The report may also be relevant for staff in organizations that use AI, suppliers of AI systems, and health authorities.

Delimitations

The report is limited to the procurement of fully developed products. It therefore does not cover in-house development of AI systems. Issues related to AI systems that are continuously learning are not specifically addressed. These are relevant topics for further work in the subproject.

Generative AI models are not dealt with separately, but another sub-project in the Joint AI plan will focus on assessing the risks associated with large language models and how to ensure that the use of language models is adapted to Norwegian conditions [17].

Relevant sources for the introduction

- A buyer's guide to AI in health and care (digital.nhs.uk) – NHS Transformation Directorate (england.nhs.uk)
- What is AI? Can you make a clear distinction between AI and non-AI systems? – OECD.AI
- Norwegian Digitalisation Agency: Guidance for responsible development and use of artificial intelligence in the public sector (digdir.no)
- *Adoption of AI in healthcare* is a comprehensive white paper, prepared by DNV in an international collaboration, describing what to consider in the procurement of artificial intelligence-based tools and can be read here: https://www.dnv.com/Publications/how-do-i-turn-this-on-what-to-consider-when-adopting-ai-based-tools-into-cli
- *The National Institute of Standards and Technology* (NIST) has published a risk management framework for AI (NIST AI RMF 1.0), which describes how to work systematically with risk management of AI systems: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (PDF) NIST also has an article on explainable AI: Four Principles of Explainable Artificial Intelligenc (PDF)
- The "Ethical Guidelines for Trustworthy Artificial Intelligence" (digital-strategy.ec.europa.eu) prepared by an expert group appointed by the European Commission mentions three main principles for responsible artificial intelligence, namely legal, ethical and safe artificial intelligence. The same principles are reflected in the government's national strategy for artificial intelligence (regjeringen.no) from 2020 and in Digital Norway of the future - national digitalisation strategy 2024-2030 (regjeringen.no)
- GENERATING EVIDENCE FOR ARTIFICIAL INTELLIGENCE-BASED MEDICAL DEVICES: A FRAMEWORK FOR TRAINING, VALIDATION AND EVALUATION (WHO , 2021) (PDF)

- The Code of Conduct for information security and data protection (Normen) has published an article on security risks in systems that use artificial intelligence and how to set security requirements for suppliers of such systems: Normen (Norwegian)
- FDA: U.S. Food and Drug Administration (fda.gov)
- ISO/IEC 22989 Artificial intelligence concepts and terminology (zip.) establishes a terminology for AI and describes concepts in the field of AI and Standard Norge | standard.no. ISO/IEC 22989:2022
- Built-in discrimination protection: A guide to detecting and preventing discrimination in the development and use of artificial intelligence (ldo.no)

[10] Meld. St. 9 (2023–2024) (regjeringen.no)

[11] Felles KI-plan for trygg og effektiv bruk av KI i helse og omsorgstjenesten 2024 - 2025

[12] European Commission: Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI, Publications Office (data.europa.eu/, 2019

[13] Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) (PDF), page 12 and Trustworthy and Responsible AI | NIST: Characteristics of trustworthy AI systems include: valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed.

[14] Article 3 of the AI Act (translated) (eur-lex.europa.eu)

[15] More about the black box problem: https://www.helse-nord.n o /499f60/siteassets/documents-and-blocks/research/strategy-for-artificial-intelligence-in-health-north-2022-2025/s

[16] See also: Ordliste for kunstig intelligens (teknologirådet.no)

[17] Joint AI plan for the safe and effective use of AI in the Norwegian health and care services 2024 - 2025 – Helsedirektoratet

Phase 1: Describe the challenge and assess whether AI is the solution

The purpose of this phase is to:

- Create a well-defined problem description
- Assess potential risks
- Assess expected benefits

Describe the need the AI system should address

> Defining and clarifying the organisation's needs is essential for identifying relevant AI systems that can address the challenge. For example, if you want to acquire an AI system that is to be used for one or more medical purposes involving human subjects, it may be classified as a medical device (see phase 2) [18]. It must also be clear who will use the AI system and who or what it will be used on. Similarly, the level of autonomy with which the system will operate must be considered. It must be assessed whether an AI-based solution is both feasible and appropriate. If the problem can be addressed more effectively, simply, or cost-efficiently using a non-AI approach, this should also be mapped and evaluated.
>
> [18] Medical devices are defined in Article 2 (1) of the MDR and include software which, according to the manufacturer, is intended to be used on human beings for, inter alia, the following specific medical purposes: diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease. Kvalifisering av medisinsk utstyr (dmp.no)

Overall risk assessment using an AI system

> Providers of AI systems are generally required to carry out comprehensive risk assessments before placing their products on the market. Healthcare organizations that adopt AI systems must conduct their own internal risk assessments, taking into account how an AI system might impose a risk in interaction with their existing systems, procedures, and staff.
>
> Even if there is insufficient information early in the process to conduct a full risk assessment, it is still crucial to identify any potential significant negative consequences. These could ultimately outweigh the intended benefits. Relevant assessment points include:
>
> - whether it fulfils the requirement for sound health care services
> - how it will impact the organization's expertise and comptence
> - whether it will lead to overuse of healthcare services
> - whether it will affect patient safety
> - whether it could introduce discriminatory outcomes [19]
> - whether it could pose a risk to data privacy
>
> Procuring an AI system that has already been adopted successfully in similar organizations will generally be less risky than acquiring a completely unknown AI system.

[19] It can be difficult to detect discrimination if you don't have the necessary data, see Heart Room for Ethical AI (datatilsynet.no), a sandbox project with Ahus. See also Built-in discrimination protection: A guide to detecting and preventing discrimination in the development and use of artificial intelligence (ldo.no)

Overall benefit assessment

The three prioritization criteria (benefit, resource use and severity) for the health service in Norway also apply to AI. A cost-benefit analysis can help determine whether an AI system is the right solution and whether investment is justified.

An estimate may include costs associated with:

- Investments to be able to deploy the AI system
- Testing and validation
- Implementation
- Training
- Usage (personnel, license and unit price)
- System management

These costs should be weighed against the expected benefits, such as increased patient safety and improved use of resources. Examples of potential benefits include:

Quality

- Increased diagnostic accuracy or faster diagnostics: Provides more precise diagnoses and shorter time from examination to treatment.
- Optimization of treatment: Improved treatment regimen, correct dosing and increased personalized care.
- Improved treatment outcomes: Faster recovery, fewer side effects, complications, relapses and hospital readmissions compared to current treatment.
- Better training and communication: More effective training for patients, carers and healthcare professionals.
- Customized information and decision support for patients and relatives: Empowering patients and relatives to take an active role in their care.
- Better collaboration: Strengthened collaboration between stakeholders, both internally within the organization, between the municipal and the specialist health service, and across sectors.

Economy

- Task- or labor-saving: Reducing manual work through automation of tasks.
- Administrative efficiency: Automation of administrative tasks such as contract management, logistics and resource allocation.
- Improved documentation: Faster and more accurate clinical documentation, including medical coding.
- Shorter waiting times: Quicker turnaround in, for example, radiological assessments or patient discharge, freeing up system capacity.

Development

- Research and innovation: Analyzing large datasets to identify new patterns and drive innovation.
- Better prognostic tools: Improving the ability to predict treatment outcomes and reduce risk.
- Technology and process development: Enhancing existing systems and introducing new solutions to strengthen healthcare delivery.

Involve the right expertise

All phases of procuring, implementing, and using AI systems in healthcare should be approached with interdisciplinary collaboration.

To clarify responsibilities, involvement and planning, a responsibility matrix, often referred to as a RACI matrix, can be a useful tool for procurement teams [20][21]. Such a matrix is used to describe different levels of involvement and responsibility that different roles should or can have, depending on the task.

Table 1
The table is an example of a RACI matrix for a procurement process. It shows which roles can be part of a procurement team and what responsibilities they have. R: Responsible (performs the task, can be shared between several roles/people), A: Accountable (has the final responsibility, there can only be one per phase), C: Consulted (someone who is consulted before the final decision is made, requires two-way communication) and I: Informed (someone who is only informed of the decision, one-way communication)

Role	Phase 1 Describe the challenge and assess whether AI is the solution	Phase 2 Map AI systems on the market	Phase 3 Assess your organization's ability to adopt an AI system	Phase 4 Procure an AI system	Phase 5 Implement and quality assure an AI system	Phase 6 Operate and manage an AI system
Project management	I	RA	A	R	A	
User and/or domain expertise (e.g. clinician)	RA	R	R	C	C	C
IT/enterprise architect	I	R	R			
Subject-specific expertise (e.g. radiation protection)	C	C	R	R	R	C
Ethical competence	C		C			C
Citizen/patient/service recipient	I		I		I	
Legal expertise	C	C	C	C	C	C
Privacy, information security		C	C	R	R	R
Data management			R	C	C	C
Analytical expertise		R	I	I	R	C
Procurement expertise		C		R		
Solution architect			C	R	C	
Test lead		I	I	C	I	

Operations and management			C		C	R
AI superuser (for example, an "AI radiologist" or "AI medical physicist")					C	R
System manager (IT supplier)	C	I	C	C	I	A
System owner (business management)	C	I	C	A	I	I

For a more detailed description of the roles, see AI fact sheet 0 [22].

[20] RACI: Responsible, accountable, consulted and informed. Template for responsibility matrix | Anskaffelser.no, Eksempel ansvarsmatrise (xlsx) (live.com)

[21] Role and responsibility matrix (ks.no)

[22] AI fact sheets will be published on Kunstig intelligens

Relevant sources for phase 1

- Artificial intelligence – Norwegian Directorate of Health
- Guidance for responsible use and development of artificial intelligence | Digdir

Phase 2: Map AI systems on the market

The purpose of this phase is to map currently available AI systems to determine whether any of them:

- have an intended purpose that matches the need defined in Phase 1
- comply with applicable regulations
- demonstrate acceptable performance and quality

Identify current AI systems

As of 1 November 2024, no centralised overview of available AI systems exists. The EU will establish a database of high-risk AI systems [23]. In addition, the EUDAMED database for medical devices is currently under development, but it will only provide a comprehensive overview once its use becomes mandatory [24]. This is expected to occur in 2026. The U.S. Food and Drug Administration's (FDA [25]) also maintains a public registry of medical devices with AI functionality, which may be a useful reference [26].

In the field of radiology, a dedicated website offers an overview of AI systems, including CE-marked systems including their classification and the applicable regulatory framework [27][28]. This site also provides additional documentation, such as peer-reviewed studies and information on FDA approvals.

As part of the early stages of procurement, it may be beneficial for the organisation to initiate an early market dialogue [29] to gain insight into available AI systems [30]. To verify regulatory compliance for medical devices, procurement teams should consider requesting key documentation from the manufacturer, such as the declaration of conformity, EC certificate, and instructions for use [31].

[23] The European Commission, in co-operation with the Member States, will establish a database for high-risk AI systems in accordance with Article 71 of the AI Act. The database will contain detailed information about the registered AI systems, including, among other things, the intended purpose, description of data used and the system's operational logic (Annex VIII of the AI Act).

[24] EUDAMED will consist of six modules related to: Operator Registration, Unique Device Identification (UDI) and Device Registration, Notified Bodies and Certificates, Clinical Investigations and Performance Studies, Vigilance and Market Surveillance. EUDAMED database (ec.europa.eu)

[25] FDA: U.S. Food and Drug Administration (fda.gov)

[26] Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices | FDA

[27] AI for radiology database: Radiology (healthairegister.com)

[28] CE marking (standard.no) The marking means that the product is considered to fulfil the requirements of the authorities set out in a directive or regulation.

[29] RFI; request for information

[30] Request for information, a non-binding market survey to increase our own expertise about what the market offers and what we want to demand. Håndbok for planlegging og gjennomføring av tidlig markedsdialog i offentlige anskaffelser (PDF)

[31] A declaration of conformity for medical devices is a statement from the manufacturer that a medical device fulfils the requirements of the EU regulations for medical devices and thus receives a CE mark.

Regulations governing the use of AI systems

The regulations for medical devices are particularly important for AI systems in the healthcare sector. In addition, the forthcoming AI Act introduces key principles and will impose requirements on both manufacturers and users (e.g. healthcare organisations) of high-risk AI systems [32]. Although the AI Act has not yet entered into force in Norway as of 2024, it may be appropriate for organisations to begin considering its requirements now, particularly when planning to procure high-risk systems. The Personal Data Act and the general health legislation also provide important frameworks for the use of AI systems [33].

Intended purpose

The intended purpose of an AI system, i.e. the purpose for which the system is designed to be used, determines which regulations apply [34]. *General-purpose AI models (GPAI models*) [35] do not have a specific intended purpose on their own, but they can be incorporated into systems that has a medical purpose. They fall under specific regulations in the EU regulation for AI.

Under the Medical Device Regulations, AI systems are considered medical devices if they are intended for use on human beings for the purpose of diagnosing, preventing, monitoring, predicting, prognosing, treating or alleviating disease [36][37]. Other types of AI systems, such as those used for logistics or shift scheduling, do not typically fall under medical device regulations. However, AI systems like electronic health record systems may include additional functions that could result in their classification as medical devices. The EU Medical Device Coordination Group (MDCG) [38] has published guidance documents to assist in determining when software qualifies as a medical device under EU law [39].

- **If the intended purpose is medical, the following applies:**
  - The AI system is considered a medical device, and the organisation must procure a CE-marked device [40]. The equipment must fulfil the documentation requirements set out in the Medical Devices Regulation.
  - The AI system will generally be considered a high-risk system in accordance with the AI Act and must comply with the requirements set for these systems when the Act enters into force [41].
- **If the intended purpose is not medical, the following applies:**
  - The AI system is considered a high-risk system under the AI Act if the intended purpose is listed in Annex III and must fulfil the requirements therein when it enters into force [42]. This applies, for example, if the AI system influences an individual's right to receive public benefits or health services [43]. In this case, public service providers are required to conduct a Fundamental Rights Impact Assessment (FRIA) [44].
- **If the AI system is intended to interact directly with natural persons**, the following applies, with some exceptions:
  - The AI Act requires transparency: The AI system must be designed and developed so that affected individuals are informed that they are interacting with an AI system [45].

- **Additionally, the organisation must assess whether the AI system may fall under other product legislation** [46]. The section Alignment of product legislation on EU's website for the New legislative framework provides an overview of relevant product categoreis [47].

The legislation for medical devices [48]

The Norwegian laws and regulations on medical devices implement the EU Medical Devices Regulations (MDR and IVDR). If an AI system is to be used for a medical purpose, a medical device must be procured. While similar systems may be available on the market under other regulations, they do not meet the safety requirements for medical devices.

- **Medical devices** can only be marketed, distributed, or put into use when the devices comply with the fundamental requirements for safety and performance in accordance with the regulations, have undergone **conformity assessment**, and bear the **CE mark**, as outlined in § 7 of the Regulation on the use of medical devices (Håndteringsforskriften). This regulation require that the organisations ensure that medical devices are suitable for their intended use and that they are used in accordance with the manufacturer's enclosed instructions for use.

Risk classes for medical devices

The extent of the conformity assessment required under the Medical Device Regulation depends, among other factors, on the risk class of the medical device [49].

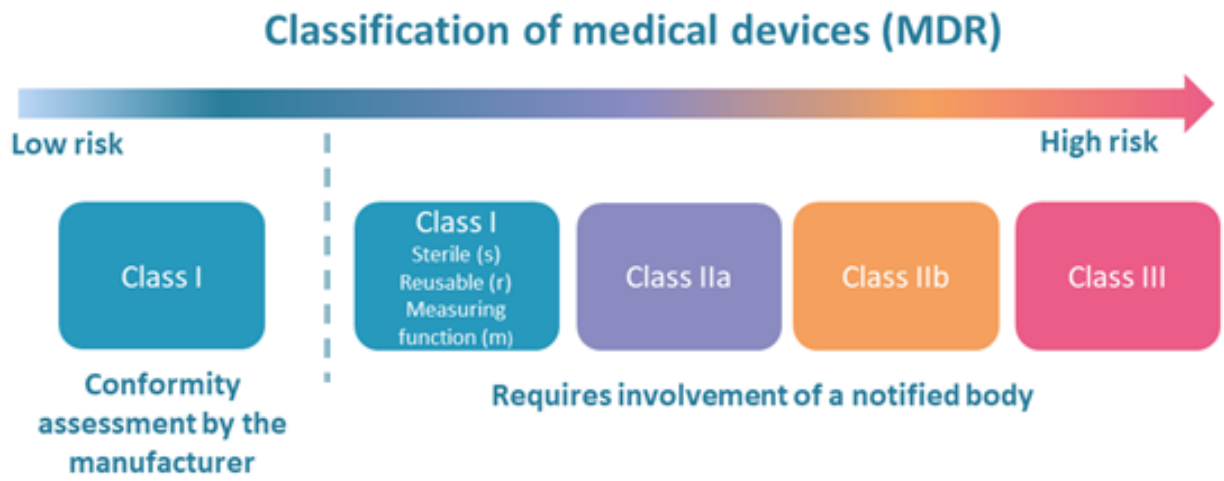

Figure 1: Retrieved from the website of the Norwegian Medical Products Agency

Medical devices are classified into four risk classes (I, IIa, IIb and III) based on the level of risk associated with their intended use. For most types of class I devices, manufacturers may self-declare conformity. For class IIa, IIb and III devices (as well as equipment in classes Ir, Is and Im), a certificate from a notified body is required. An overview of classification rules can be found on the Norwegian Medical Products Agency website [50].

Medical devices intended for in vitro diagnostics (IVD) have their own classes (A, B, C and D) [51]. A certificate from a notified body is required for IVD equipment in classes B, C and D

Manufacturer responsibility

If a medical device is used for a purpose other than that stated in the declaration of conformity, or if the organisation modifies the device in a way that may affect compliance with the applicable requirements, the organisation assumes the legal obligations of a manufacturer under the MDR. This includes full responsibility for ensuring that the AI system meet all applicable safety and regulatory standards [52].

An example of this from diagnostic radiology [53]:

- An AI system developed for use in adults cannot automatically be used on children (ages 0–18). Children are not simply “small adults,” and special expertise is required to assess whether the AI system is safe for paediatric use and whether its performance on children is comparable to that on adults. If the system was CE-marked for adult radiology, but is intended to be used for children, it must be tested for the new age group through a clinical trial. In such cases, the organisation takes on manufacturer responsibility for the AI system.

Healthcare institutions may develop medical devices for internal use. The Norwegian Medical Products Agency's website provides guidance on the applicable requirements [54].

Transitional arrangements

Some medical devices currently on the market are still regulated under the previous EU regulations [55]. Transitional provisions have been introduced to bridge the gap between old and new regulations and to avoid shortages in the European market. For details, refer to the DMP’s website [56].

Clinical trial of an AI system that is not CE marked

If no suitable CE-marked alternative exists, or if an unmarked AI system is considered appropriate, organisations must apply for approval to conduct a clinical trial. Applications should be submitted to both the Norwegian Medical Products Acency(DMP) and the Regional Committees for Medical and Health Research Ethics for Clinical Trials (REK KULMU) [57].

FDA approval

Medical devices that are approved by the US Food and Drug Administration (*FDA*) [58], but have not undergone EU conformity assessed and do not carry the CE mark, cannot legally be used in Norway or elsewhere in the EU/EEA. They should therefore not be procured for clinical use. Manufacturers sometimes offer different models or versions of their devices for the U.S. and European markets. In such cases, it is important to ensure that the version being procured is the CE-marked model intended for use in the EU/EEA.

The AI Act

The purpose of the AI Act is to promote and increase the use of human-centred and trustworthy AI systems, while ensuring a high level of protection of health, safety and fundamental rights, including key democratic values, such as the rule of law and the environmental sustainability, against harmful effects that may result from AI systems. At the same time it aims to support innovation.

The AI regulation was published on 7th July 2024 [59], and its various provisions will enter into force **gradually** over time [60]. The Norwegian government has stated its intention to ensure that the AI Act is incorporated into the **EEA Agreement** as swiftly as possible [61].

To support compliance, the European Commission has mandated the development of harmonised European standards. These will provide technical specifications to help manufacturers and users meet the requirements set out in the regulation [62].

A key principle of the AI Act is that risk classification is based on the system's intended use, not solely on the technical characteristics of the AI system itself. As a result, the same AI model may be considered limited risk in one application, but high risk in another, depending on the context in which it is deployed.

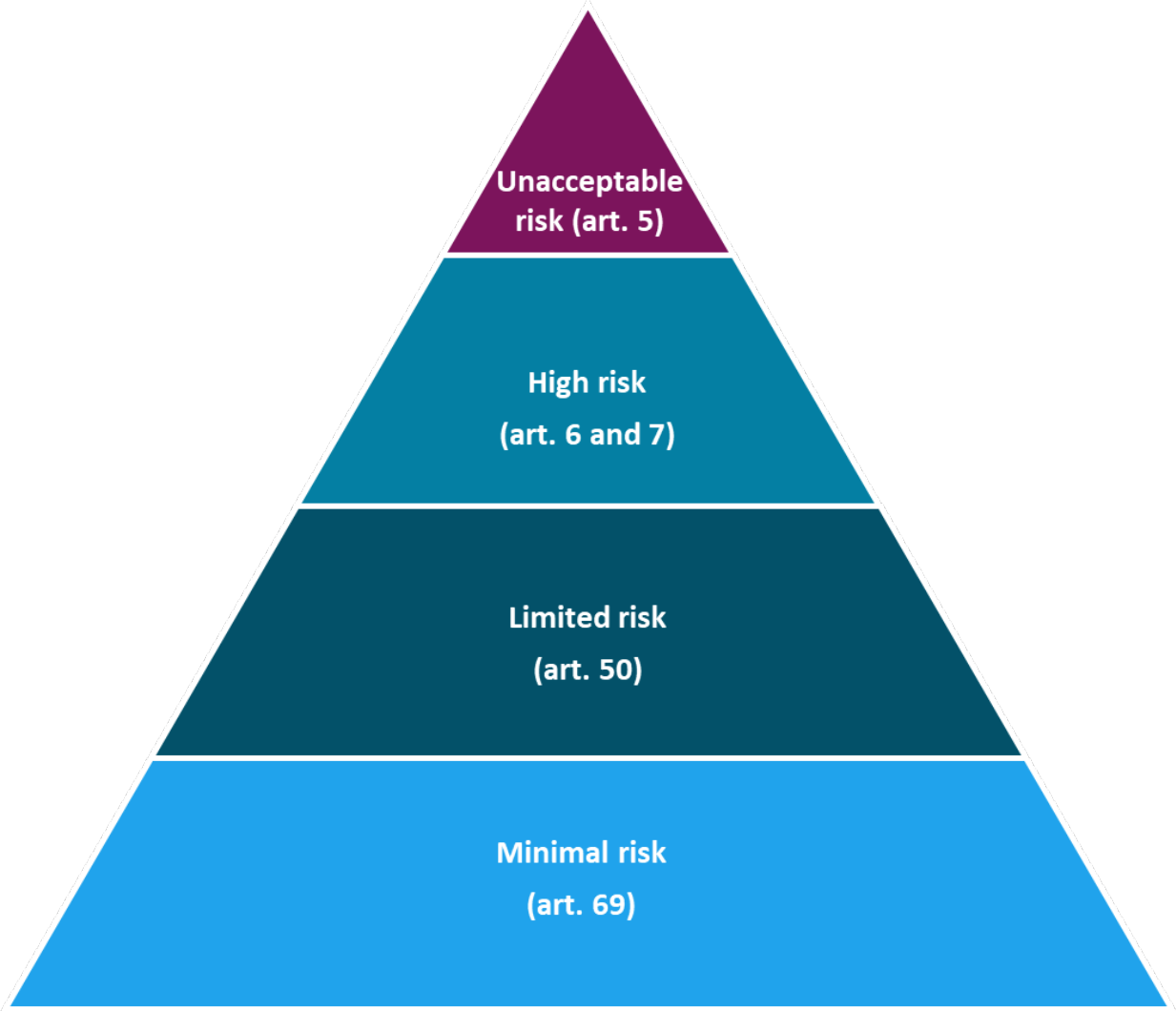

Figure 2: Risk classes in the AI Act

High-risk AI systems

The AI Act describes two categories of high-risk AI systems

Regulated products: Annex I of the AI Act

If there is a requirement for third-party certification of a product or safety component in a product that is already regulated by one of the EU regulations mentioned in Annex I, among others:

- Medical Device Regulation (MDR)
- In Vitro Diagnostic Device Regulation (IVDR)
- Machinery Directive, Toys Directive etc.

Regulated uses: Annex III of the AI Act

Stand-alone systems such as:

- Biometric identification, emotion recognition
- Critical infrastructure
- Education and vocational training
- Recruitment and working conditions
- Access to basic welfare services
- Law enforcement authorities
- Migration, asylum, border control
- Democratic processes and the work of the courts

Under the AI Act, an AI system may be classified as high-risk in two ways: If it is part of a regulated product category (e.g. medical devices) or if it is used for a regulated purpose [63].
The specific requirements for AI systems that are, or form part of, medical devices will apply from 2nd August 2027 [64]. For high-risk systems used for purposes listed in Annex III, the requirements will come into force on 2nd August 2026.

The AI Act outlines a number of mandatory requirements for high-risk AI systems, including:

1. Risk management system (article 9)
2. Data and data management (article 10)
3. Technical documentation (article 11)
4. Logging (article 12)
5. Transparency and information to users of the system (article 13)
6. Human oversight (article 14)
7. Accuracy, robustness and cybersecurity (article 15)

Article 11 provides detailed requirements for the technical documentation that must be maintained for each high-risk AI system, and this is further elaborated in Annex IV of the AI Act [65]. While these provisions will not be legally binding in Norway until the regulation enters into force, this is documentation that suppliers will have to prepare as parts of the AI Act become applicable in the EU. They can already serve as a **useful reference** in the procurement process.

The concepts of *transparency* and *human oversight* (as described in Articles 13 and 14 of the AI Act) may be unfamiliar elements in the procurement process. A *transparent* AI system is designed in a way that makes it possible to understand how the AI model was developed. It should also be clear to users that they are interacting with an AI system. When users are aware that the system employs AI, they can take this into account when interpreting and applying the information it provides. *Human oversight* of an AI system may involve some form of human supervision or the ability to intervene when necessary. Users should not be entirely dependent on the system for making critical decisions. Ensuring effective human oversight requires, among other things, appropriate competence and training [66].

AI systems with limited risk

AI systems classified as limited-risk are not subject to the same stringent requirements as high-risk AI systems. However, they must still comply with certain obligations—most notably, that the systems are transparent, and that AI-generated content is labelled in a machine-readable format [67]. Organisations adopting such systems are also required to ensure that personnel responsible for operating or using the AI systems have adequate competence and training.

General Purpose AI Models (GPAI)

General Purpose Artificial Intelligence (GPAI) models [68] can be used either directly, such as ChatGPT and Gemini, or they can be customised and/or fine-tuned by other manufacturers for a specific purpose. Manufacturers relying on GPAI models must ensure they have sufficient documentation about the underlying model in order to demonstrate the quality and compliance of their own product.

Although the GPAI models do not have a specific intended purpose in and of themselves, they are still regulated under the AI Act if they meet certain criteria outlined in Article 51 [69]. Suppliers of GPAI models are, among other things, required to ensure that downstream users understand the models well enough to use them responsibly and lawfully in their own products and to meet their legal obligations [70]. If a GPAI model is considered to pose systemic risk, additional and stricter requirements apply [71]. Examples of systemic risk include the AI system's potential to influence elections, critical infrastructure and emergency preparedness. Suppliers of GPAI models with systemic risk must, among other things, conduct model evaluations to identify, and continuously assess and reduce systemic risks through risk management, post-deployment monitoring, and collaboration with relevant stakeholders. Serious incidents and possible corrective actions must be reported immediately to the European Commission and national competent authorities.

Pending the development of harmonised standards, the European Commission has launched a first draft of guidelines for GPAI models [72].

Other relevant regulations

AI liability directive

The European Commission has proposed an AI Liability Directive concerning non-contractual civil liability in cases where damage is caused by an AI system. The directive lays down common rules for the burden of proof in relation to high-risk AI systems, enabling claimants to better substantiate liability claims [73].

Automated decisions

The General Data Protection Regulation (GDPR) contains several provisions related to automated individual decision-making, particularly Article 22, which concerns decisions made without human intervention. These provisions apply when AI systems make such automated decisions or are involved in fully automated data processing. Under the GDPR, individuals have the right not to be subject to a decision based solely on automated processing, including profiling, if the decision produces legal effects or similarly significant impact [74]. There are exceptions to this right, but in such cases, individuals are entitled to additional safeguards, such as the right to human review of the decision [75]. The GDPR also requires transparency and explainability regarding the logic underlying automated decisions, as outlined in Articles 13, 14, and 15 [76]. In Norway, provisions regarding automated decision-making are also included in Section 11 of the Patient Records Act (lovdata.no) and Section 21-11a of the National Insurance Act (lovdata.no), which permit the issuance of regulations allowing automated decisions in more invasive cases.

Rules on access to and use of health information

Under Norwegian law, health information is protected by a duty of confidentiality, and all processing of personal data must have a legal basis under Article 6 and Article 9 of the GDPR for the processing of health information [77].

A data controller is required for all processing of personal and health data [78]. The data controller is responsible for ensuring that the processing of personal and health data complies with applicable regulations. This includes ensuring that health data is processed lawfully, and that adequate information security and internal control measures are in place.

The GDPR provides the framework for the duties and responsibilities of the data controller and establishes the possibility of sanctions if these obligations are not met. Among the most important responsibilities are ensuring the lawful processing of health data, as well as maintaining satisfactory information security and internal governance.

The data controller may enter into an agreement with a data processor regarding the processing of personal data, a data processing agreement. This is relevant when another party is to process data on behalf of the controller. The data processor may only process the data in accordance with the agreement with the data controller.

See more about confidentiality and access to health information for validation in phase 5.

Radiation protection regulations

The introduction of AI systems may impact the use of radiation-emitting equipment or other areas related to radiation safety, such as decision support systems used to assess the justification for radiological examinations. Many of the relevant AI systems are used in radiology and radiotherapy. The radiation protection regulations impose strict requirements, including risk assessments, quality assurance and control of the systems and expertise among those operating them [79].

[32] REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (eur-lex.europa.eu)

[33] Act relating to the processing of personal data (Personal Data Act) - Lovdata

[34] Definition of "intended purpose" in the AI Act art. 3 no. 12 Article 3 Definitions (eur-lex.europa.eu) \and MDR art. 2 no. 12 (EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2017/745 (PDF))

[35] There is no official Norwegian translation. In this report, we rely on the Danish translation of the AI Regulation, which uses the term "AI-model til almen brug".

[36] Medical Devices Act - Lovdata

[37] See also the EEA supplement on medical devices here. EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2017/745 (PDF)

[38] Medical Device Coordination Group Working Groups - European Commission

[39] Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR (health.ec.europa.eu)

[40] Handling regulations: Regulations on the handling of medical devices (lovdata.no)

[41] Systems are categorised as high-risk systems if: 1) it is included as a safety component in a product or the system itself is a product regulated by the regulations listed in Annex I and 2) must undergo third-party certification in accordance with the regulations in Annex I of the AI Act. Article 6.1 of the CI Regulation: Classification rules for high-risk AI systems (eur-lex.europa.eu)

[42] Article 6.2 of the AI Act: Classification rules for high-risk AI systems (europa.eu)

[43] Point 5 b and c in Annex III of the AI Act

[44] Article 27 of the AI Act

[45] Article 50 of the AI Act

[46] Requirements for products in Norway | Directorate for Civil Protection (dsb.no)

[47] New legislative framework (single-market-economy.ec.europa.eu)

[48] The Norwegian Medical Products Agency (DMP) is the technical and supervisory authority for medical devices in Norway and administers the product regulations for medical devices.[17] Further information can be found on DMP's website.

[49] Classification - Norwegian Medical Products Agency (dmp.no)

[50] Klassifiseringsregler (dmp.no)

[51] Klassifisering av medisinsk utstyr (MDR) (PNG)

[52] See MDR and IVDR article 16

[53] AI models developed for use on adults cannot easily be used on children. See Use of Artificial Intelligence in Radiology: Impact on Paediatric Patients, a White Paper From the ACR Pediatric AI Workgroup (jacr.org)

[54] Egentilvirkning av medisinsk utstyr i helseinstitusjoner (in-house) (dmp.no)

[55] The Medical Devices Regulation (MDR) entered into force on 26 May 2021 and repealed Directive 93/42/EEC on other medical devices and Directive 90/385/EEC on active implantable medical devices with certain exceptions. The In Vitro Diagnostic Medical Devices Regulation (IVDR) entered into force on 26 May 2022 and repealed Directive 98/79/EC on in vitro diagnostic medical devices.

[56] Read more about transitional arrangements on the DMP website.

[57] Clinical trials subject to application - Norwegian Medical Products Agency (dmp.no)

[58] U.S. Food and Drug Administration (fda.gov)

[59] Regulation - EU - 2024/1689 - EN - EUR-Lex (europa.eu)

[60] Article 113 of the AI Act

[61] Digital Norway of the future - national digitalisation strategy 2024-2030 (regjeringen.no) p. 67

[62] Register of Commission Documents (ec.europa.eu)

[63] The categories are described in Annexes I and III of the AI Act, respectively. The European Commission has the authority to amend the list of regulated uses in Annex III according to specified criteria, as set out in Article 7 of the AI Act.

[64] Article 113 of the AI Act and Annex III: High-Risk AI Systems Referred to in Article 6(2) (artificialintelligenceact.eu)

[65]Technical documentation referred to in Article 11(1) (eur-lex.europa.eu)

[66] Article 26 (2) of the AI Act on: Obligations of deployers of high-risk AI systems (eur-lex.europa.eu)

[67] Article 50(1)(2) of the AI Act: Transparency obligations for providers and deployers of certain AI systems (eur-lex.europa.eu)

[68] Article 3 (3) of the AI Act defines 'general-purpose AI model' as follows: means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;

[69] Chapter V of the AI Act: GENERAL-PURPOSE AI MODELS (eur-lex.europa.eu)

[70] Article 53 of the AI Act: Obligations for providers of general-purpose AI models (eur-lex.europa.eu)

[71] Article 55 of the AI Act: Obligations of providers of general-purpose AI models with systemic risk (eur-lex.europa.eu)

[72] First Draft of the General-Purpose AI Code of Practice published, written by independent experts (europa.eu)

[73] AI-ansvarsdirektivet (regjeringen.no)

[74] Artikkel 22.Automatiserte individuelle avgjørelser, herunder profilering (lovdata.no)

[75] Rettar ved automatiserte avgjerder (datatilsynet.no)

[76] General Data Protection Regulation: Avsnitt 2 Informasjon og innsyn i personopplysninger (lovdata.no)

[77] Read more about this on the Norwegian Directorate of Health's website on artificial intelligence: Regulations for the development of artificial intelligence – Norwegian Directorate of Health

[78] Controller is defined in the GDPR as a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes of the processing of personal data and the means by which it is to be carried out or as laid down in Union or national law, cf. Article 4(7). see also section 2(e) of the Patient Records Act, which refers to the definition in the GDPR with regard to who is responsible for the processing of health information in treatment-related health registers, including in patient records.

[79] Forskrift om strålevern og bruk av stråling (strålevernforskriften) (lovdata.no)

Assessing the quality of an AI system

An important part of the mapping conducted in Phase 2 is to gain an overview of the performance, security, and cost-effectiveness of the AI system. This forms the basis for more specific assessments and planning in the next phase.

Performance of an AI system

The performance of an AI system is closely linked to how the model has been developed and the quality of the data it has been trained on. If the training data contains systematic bias, the AI model may produce unfair or unreliable results. AI models are often highly flexible and may memorise training data without being able to generalise to new, unseen data. It is therefore essential that the model's performance is tested on independent data that has not been included in the training.

The manufacturer may have validated their solution to varying extents. There should be documentation available that explains how the technical validation was performed, which data sets were used and whether the AI model was tested on independent datasets. Under the MDR, manufacturers of CE-marked devices are required to document system performance. While there is no general requirement for clinical validation for AI models, such validation may be required for higher-risk medical devices (particularly class IIb and III). In these cases, clinical testing may be necessary [80]. MDCG's report provides guidance on the clinical evaluation of software as a medical device [81]. Article 61 of the MDR addresses clinical evaluation of medical devices, while Article 62 outlines the general requirements for conductiong clinical investigations.

For more information, refer to later phases of this report as well as AI fact sheets 3 and 2, which address validation and performance, respectively [82].

Security of an AI system

As part of Phase 2, an overall assessment should be conducted to determine whether available AI systems on the market meet acceptable security standards.

The Code of Conduct for information security and data protection (Normen) is a helpful tool for safeguarding information security and privacy in the health and care sector. It is technology-neutral and includes, among other things, dedicated articles on the use of artificial intelligence [83].

Evaluation of method and knowledge base

If a health technology assessment (HTA) has already been conducted for the AI system prior to procurement, it can provide valuable insights. Full HTAs offer a robust foundation for decision-making, as they are based on thorough scientific methodology and may include a comprehensive impact assessment. Given that AI remains a relatively new field, few full HTAs have been completed for AI systems so far.

Health Technology Assessment (HTA)

A *Health Technology Assessment* (HTA) is an interdisciplinary process that evaluates the efficacy, safety, ethics, organisational impact, cost-effectiveness, and budgetary consequences of introducing or phasing out a technology in the healthcare system [84][85].

The *New Methods* system (Nye metoder) is Norway's national framework for determining which treatment methods may be offered within the specialist health service. The Norwegian Institute of Public Health and the Norwegian Medical Products Agency perform HTAs on behalf of the Ordering Forum for New Methods (Bestillerforum for nye metoder) [86]. The Norwegian Radiation and Nuclear Safety Authority (DSA) assists in the HTA if the method uses radiation or may have an impact on the medical use of radiation. A national strategy is currently being developed to guide the further evolution of the New Methods system [87]. Additionally, a working group has been appointed to propose a framework, objectives, and criteria for assessing medical devices within the system.

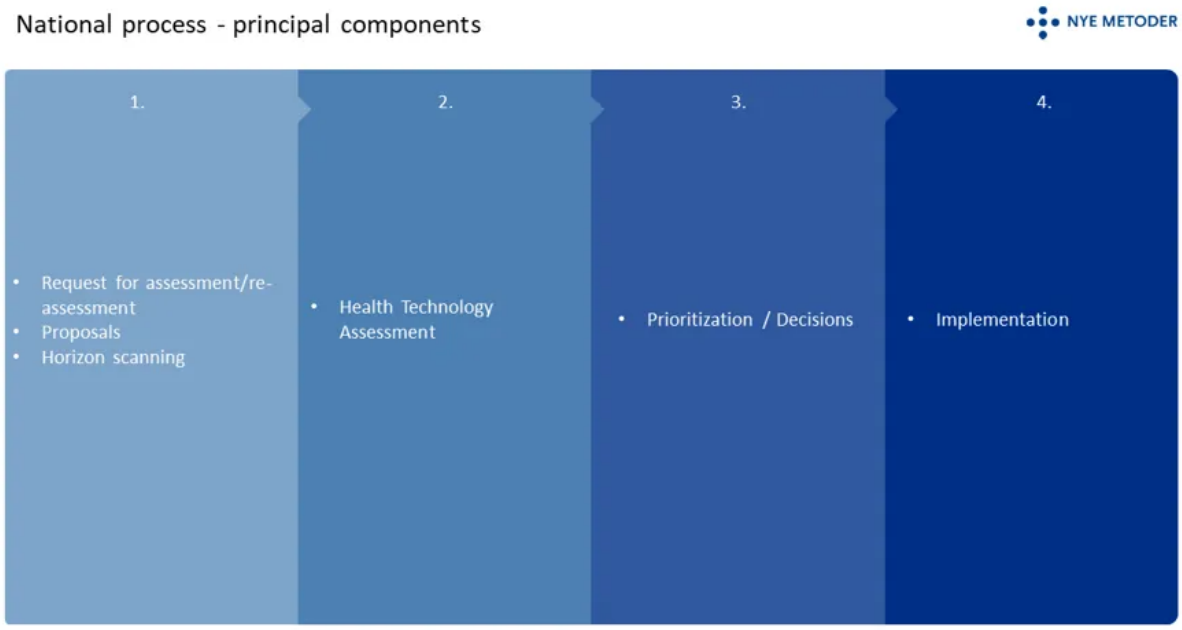

Figure 3 : Process map for New methods [9]

Minimethod assessments

Many decisions are made at the local level, where mini-HTAs may be relevant. A mini-HTA is a simplified version of the national HTA and is tailored for use in both hospitals and municipalities. The NIPH is responsible for mini-HTAs and provides guidance as well as a national database of all completed and ongoing assessments on its website [88]. The database also includes contact persons for previously completed mini-HTAs.

According to the Radiation Protection Regulations, any new method that involves or affects the use of radiation must undergo a generic justification assessment. Method assessments that address radiation safety aspects are generally considered sufficient documentation in this context [89].

Lessons learnt from peer-reviewed publications

Peer-reviewed articles provide an independent description of the technology and offer documentation of its effectiveness, including evaluations of clinical utility. While the CE marking confirms that the product meets regulatory requirements for safety and performance, peer-reviewed literature can serve as an important complementary source of evidence.

Experiences from users of comparable AI systems

Systematic experience-sharing is valuable when new technologies are being introduced. Organisations should consider contacting others that have gained practical experience with similar AI systems. For example, user experiences related to interfaces and realised benefits are often best understood by consulting actual users in other healthcare institutions or countries. Suppliers may also be able to provide references to other organisations that have implemented their AI systems.

[80] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2017/745 (PDF)

[81] MDCG 2020-1 Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software (PDF)

[82] AI fact sheets will be published on Kunstig intelligens – Helsedirektoratet

[83] Security risks in artificial intelligence systems - what do we know and what can we do? - eHealth

[84] Method assessments - FHI

[85] What is health technology assessment? - NIPH

[86] Method assessment (nyemetoder.no)

[87] Strategi for Nye metoder 2023-2028 (nyemetoder.no)

[88] Background: Why do we have New Methods? (nyemetoder.no)

[89] Mini-method assessment (minimetodevurdering.no)

[90] See in particular section 39 Eligibility: Forskrift om strålevern og bruk av stråling (strålevernforskriften) (lovdata.no)

Relevant sources for phase 2

- The e-health reference catalogue provides an overview of mandatory and recommended standards for health and care services, as well as other requirements documents such as technical specifications. Currently, there are no mandatory or recommended standards in the reference catalogue that deal specifically with AI. However, the European Commission has asked the European standardisation organisations CEN and CENELEC (ec.europa.eu) for European standards to support the implementation of the AI Regulation. Eventually, these will also be harmonised for Norwegian conditions and included in the reference catalogue.
- The European Medical Device *Coordination Group* (MDCG) is composed of national experts and the establishment of the group is regulated in the MDR (Articles 103-108). Among other things, they have published guidance on
  - qualification and classification of medical device software (health.ec.europa.eu)
  - on clinical evaluation/performance evaluation of software (health.ec.europa.eu)
  - on the qualification of software and hardware combinations (health.ec.europa.eu) and
  - on cybersecurity for medical devices (health.ec.europa.eu)

- The Norwegian Directorate of Health is currently (1 October 2024) assessing the degree of normalisation for a guide and standard (SN-CEN TS/ISO 82304-2:2021) for quality assurance of non-medical e health apps. This will be useful to use if the organisation is going to use an AI system for health and wellbeing that will not be used for medical purposes.
- A report published by the UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA), among others, provides guidelines for the secure development of AI systems, and these can be used to see what a supplier can be expected to do to manage information security risks in the systems they develop: Guidelines for secure AI system development (ncsc.gov.uk)
- The Open Worldwide Application Security Project (OWASP) has created an overview of how to handle privacy during the development of an AI system: OWASP AI Security and Privacy Guide | OWASP Foundation
- In addition, an article on artificial intelligence in the health service (tidsskriftet.no) was published in the Journal of the Norwegian Medical Association in October 2023, which provides useful guidance.
- New methods: Home (nyemetoder.no), Strategy for New Methods 2023-2028 (nyemetoder.no).
- The Norwegian Institute of Public Health's page on mini-method assessments: Mini-method assessment (minimetodevurdering.no)
- The Norwegian Institute of Public Health's product portfolio in New methods: Changes to the product portfolio (PDF).
- Experiences with testing of ISO 42001 at AHUS (linkedin.com)
- Act on Equality and Prohibition of Discrimination (Equality and Discrimination Act) (lovdata.no)
- Report from the Equality and Anti-Discrimination Ombud: Built-in discrimination protection (ldo.no)
- Ahus, final report: Heart space for ethical AI (datatilsynet.no). Report from the Danish Data Protection Agency's regulatory sandbox
- Norwegian Directorate of Health: Circular for the regulations for the development of artificial intelligence.
- How to get ChatGPT regulatory approved as a medical device - Hardian Health
- Crafting an intended purpose in the context of software as a medical device (SaMD) - GOV.UK (www.gov.uk)
- Medical devices and artificial intelligence (dmp.no)
- Guidance and regulations - Norwegian Medical Products Agency
- Clinical evaluation and performance evaluation - Norwegian Medical Products Agency
- The EU is in the process of establishing a database of CE marked products (ec.europa.eu)
- Relevant harmonised standard: ISO13485 - Quality system for medical (advisera.com)

Phase 3: Assess your organization's ability to adopt an AI system

The purpose of this phase is to

- Identify and evaluate the organisation’s human and technical capabilities
- Develop a sound decision basis and plan for the procurement of an AI system

Human factors

As with the introduction of any other technology, human factors play an important role in determining whether an AI system will function effectively in practice in the organisation. AI systems are socio-technical in nature, meaning they are influenced by the interaction between medical technology, clinical practice and human factors, including the behaviour and decisions of patients and healthcare professionals [91]. The benefits and risks associated with an AI system will vary depending on the context and how it is used [92].

Ethical assessments and guidelines

An organisation’s norms, values, and behavioural culture form the foundation for the ethically responsible use of AI. In the specialist health services, clinical ethics committees are available and may be consulted as needed. In the municipal sector, KS (The Norwegian Association of Local and Regional Authorities) collaborates with the Centre for Medical Ethics to support municipalities in navigating ethical questions in healthcare. The organisation may also have internal policies or ethical guidelines that restrict or govern the use of AI, for example, prohibiting the use of AI for specific purposes.

Some ethical questions that may arise include:

- How will patients respond to knowing that decisions affecting their care are informed by an AI system and not solely by a human professional?
- Is the system fair? Does it support equitable access to health and care services, regardless of diagnosis, location, financial situation, gender, country of origin, ethnicity, or individual life circumstances? Does it promote equality in quality and outcomes across different patient groups?

Organisational leadership

It may be beneficial to consider implementing an AI management system, such as ISO/IEC 42001 Management system for artificial intelligence (standard.no). This standard can help organisations identify and reduce risks associated with the implementation of AI.

The organisation should assess the changes that the introduction of an AI system will bring to existing work processes. This ensures that leadership is well-informed about how the deployment of an AI system will impact staff and the services provided.

This assessment may include:

- Identifying affected stakeholders and their expectations, including:
    - Potential changes in workload and/or routines for healthcare personnel during and after implementation
- Assessing the need for resources and training for those who will both use and manage the AI system, including:
    - How to handle the system's limitations
    - Whether new roles, responsibilities, or collaborations are required
    - Whether there is a need for skills development or capacity building
- Planning for unanticipated situations and their consequences, such as temporary cost increases if:
    - An existing system needs to run in parallel with the new AI system
    - The AI system experiences temporary downtime

When the AI Act enters into force, organisations that intend to implement certain types of high-risk AI systems will be required to conduct a *Fundamental Rights Impact Assessment* (FRIA) [93]. This assessment is intended to help identify any potential adverse impacts the AI system may have on fundamental rights. Based on the findings, the organisation must implement appropriate measures to safeguard those rights and ensure compliance with the other requirements of the AI Act.

Users of the AI system

The Health Personnel Act requires that healthcare professionals provide safe and responsible care, and it is essential that they possess the necessary qualifications and competence to use the AI system as intended. They must feel confident that the AI system will effectively support their work processes and should therefore be involved in the procurement process. Their engagement, ownership, and expertise are crucial for ensuring acceptance and proper use of the AI system. It is important to identify their needs for training and support during the implementation process, as well as any resistance to changes in work routines.

How the use of AI as decision support impacts the competence of those using the system is also an important consideration. The organisation must ensure that the competence of healthcare professionals using AI is maintained over time, in line with the Regulations on Management and Quality Improvement in the Health and Care Services [94]. It may be relevant to establish mechanisms to address this, such as routines that help healthcare personnel avoid or reduce the risk of automation bias—that is, an overreliance on AI tools that may undermine professional judgement and the quality of care.

The AI Act will introduce requirements for transparency, including the need for AI systems to be interpretable, and for it to be clear to users that they are interacting with an AI system [95]. In addition, under the AI Act, employers will be obligated to inform employees when AI systems are introduced in the workplace [96].

Individuals the AI system will be used on

AI systems are often used to provide advice or decision support that directly concerns citizens, patients, and other service recipients. The organisation should plan how to provide clear and appropriate information to these groups, recognising that the use of AI may generate both enthusiasm and scepticism.

The use of an AI system can lead to perceptible changes in how a service is experienced—by citizens, healthcare personnel, patients, and service users alike. Transparency and clear communication about the goals and purposes of AI use, and how it supports healthcare delivery, may be essential to building public trust in the use of AI in health and care services.

- A survey from the United Kingdom found that nine out of ten adults viewed the use of AI for cancer detection positively. However, 56% were concerned about relying too heavily on technology rather than professional judgement, and 47% were worried about the difficulty of determining responsibility when something goes wrong [97].

Norway's National AI Strategy also emphasises that transparency includes the right to know when one is interacting with an AI system. Individuals have the right to be informed when they are interacting with an AI system [98].

Under the Patients' and Users' Rights Act, patients have the right to participate in decisions about their care and to receive information about the content of their healthcare, including potential risks [99]. The GDPR requires that individuals are informed about how their personal data is processed. Organisations should consider informing individuals which health data is shared with the AI system and for what purposes [100].

The organisation should assess whether changes to internal work processes are needed to safeguard patients' rights when implementing an AI system. A user advisory committee may be consulted in this process.

[91] "A Human-Centered Evaluation of a Deep Learning System Deployed in Clinics for the Detection of Diabetic Retinopathy" (dl.acm.org)

[92] Artificial Intelligence Risk Management Framework (AI RMF 1.0) (PDF)

[93] Article 27 of the CI Regulation. A FRIA shall include, among other things, a description of the processes in which the AI system will be used, the time period and frequency of use, persons or groups that may be affected, specific risks of harm, description of human supervision and other risk mitigation measures, and handling of complaints.

[94] Regulations on management and quality improvement in health and care services - Lovdata

[95] Article 13 of the AI Act.

[96] Article 26 of the AI Act

[97] Ada Lovelace Institute and The Alan Turing Institute, How do people feel about AI? A nationally representative survey of public attitudes to artificial intelligence in Britain (2023). Available at: How do people feel about AI? (2023) (adalovelaceinstitute.org)

[98] Nasjonal strategi for kunstig intelligens (PDF)

[99] Chapter 3 of the Patient and User Rights Act

[100] General Data Protection Regulation art. 13 and 14

Technical factors

Several technical factors are important to ensure that the AI system functions properly within the organization's infrastructure. It must be well integrated into the workflow, fit the environment in which it will

be used, and be easy to use. It is important to remain open to making significant changes and thinking innovatively, such as prioritizing the establishment of efficient infrastructure to ensure good workflow, rather than merely improving existing but limited systems.

Data management, quality and compatibility

Those responsible for the organisation's information governance are important in the mapping process and must be involved. The organisation should plan for holistic information management. The guide *Getting your own house in order* from the Norwegian Digitalisation Agency

can be useful in both mapping and planning [101]. The organisation should have assessed the requirements that will apply to the processing of data in the AI systems and whether the organisation's data meets these requirements. This applies, for example, to requirements for data quality, data format and structure, encryption, compression, data labelling and storage methods.

Integration of the AI system

When assessing whether an AI system is suitable for the organisation, it must be clarified which interfaces the organisation uses for integration with local processing systems and electronic health record systems, as well as which open standards these interfaces comply with. Effective data handling and interoperability between systems are essential for ensuring efficient processes.

Storage, processing power and infrastructure

The AI system must be evaluated in light of any technical infrastructure requirements the organization may have, for example, regarding processing capabilities, storage, network, monitoring tools, security, and software licenses. It should be assessed whether changes to the technical infrastructure are needed for testing, implementation, and ongoing operations.

Evaluate test environments

Test environments may be necessary when procuring AI systems, as they enable the organization to conduct quality assurance in a controlled setting. Requirements for test environments during the various phases should be clearly defined, including the technical infrastructure needed, whether the supplier is expected to provide (parts of) the test environment, and the need to test integration with existing systems.

Both initial and ongoing operational costs associated with the test environments should be estimated. The supplier must specify whether additional costs will be incurred for access to their own test environments, or for using the AI system within the organization's test environments — for example, additional licensing fees.

[101] Guide to keeping your house in order | Digdir

Planning the Procurement

The mapping conducted so far has provided insight into which AI systems are available, as well as the human and technical factors the organization must consider when procuring a system. This knowledge helps update the risk assessments and benefit analyses, ensuring that the organization has a solid basis for decision-making regarding whether to proceed with the procurement of an AI system.

Update benefit analyses

Where possible, the organisation should evaluate the potential benefits of the AI system using an approach similar to a health technology assessment, based on the available evidence. A health economic evaluation, comparing costs with expected health outcomes, is a key component in the decision-making process for whether to invest in an AI system. The assessment should include the following elements:

- The benefits provided by the AI system, whether clinical, administrative, research-related, or other
- The resources required to implement and use the AI system
- The risks associated with the introduction of an AI system

The estimated use of the solution, such as the number of users or number of examinations, may affect the cost. The introduction of AI systems can also lead to increased use of, for example, diagnostic methods. Therefore, an assessment of potential increases in total healthcare costs due to increased service utilization should be conducted.

By conducting and documenting relevant baseline measurements, for instance, the amount of time healthcare personnel currently spend on specific tasks, these measurements can serve as a reference point in the ongoing assessment of benefits.

Updating risk assessments and planning security measures

Information security and data protection relate to the entire system and its use, not just the AI model itself. Within the organization, the AI system will be part of a larger whole, operated, managed, and used within an environment that includes multiple other systems, established workflows, organizational culture, and existing competencies. The Code of Conduct for information security and data protection and the NIST framework for AI risk management can be useful tools in assessing whether requirements for information security and data protection are adequately addressed [102]. Based on the results of the risk assessment, the organization should plan appropriate measures needed to be implemented to ensure sound risk management for safe service delivery, both during the implementation phase and throughout the AI system's regular operation [103].

Planning clinical validation

The organization should assess whether additional clinical validation is necessary before or in connection with the implementation of an AI system it plans to procure. The market mapping conducted in Phase 2 can serve as a basis for evaluating the extent and scope of validation that the organization itself must carry out. For further details on validation, see AI Factsheet 2 [104]

In some cases, it may be sufficient to test the solution on a small sample of the organization's own data before putting the product into operation, followed by quality control measures to detect any errors. In other

cases, it may be appropriate to conduct prospective studies, such as randomized controlled trials, to validate the AI system within the intended workflow.

It may also be advisable to plan a pilot [105] phase before the AI system is deployed in other parts of the organization. Conducting a pilot can help reduce risks by allowing corrections to be made before the consequences become significant, prior to any potential scaling. It is important that healthcare institutions ensure that such validation does not constitute clinical investigation without seeking approval in accordance with the MDR.

[102] Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov)

[103] Regulations on management and quality improvement in health and care services - Lovdata aims to contribute to professionally sound health and care services, quality improvement and patient and user safety, and that other requirements in health and care legislation are complied with.

[104] AI fact sheets will be published on Kunstig intelligens – Helsedirektoratet

[105] A pilot is a limited trial or test project in an organization, as close as possible to actual day-to-day operations. The purpose is to identify potential problems, assess effectiveness, and understand the consequences of the new system in a smaller and controlled setting.

Experience sharing and research

The organization may consider whether it is appropriate to conduct accompanying research during the implementation of the AI system or other forms of research to contribute to experience sharing. If so, it is necessary to establish contact with relevant research groups, define the objectives and scope of the research, and secure funding for the work. This aspect should be considered before the tender documents for the procurement are announced. Clinical research must be approved by the Regional Committees for Medical and Health Research Ethics (REK), and clinical investigations of medical devices must be approved by the Norwegian Medical Products Agency (DMP).

Example: Northern Norway Regional Health Authority has financed an accompanying research project at the Norwegian National Centre for E-health Research (NSE) on the benefits and values of introducing commercial AI solutions in the field of radiology in Northern Norway Regional Health Authority.

Relevant sources for phase 3

- Regulations on management and quality improvement in health and care services (lovdata.no) aim to contribute to professionally sound health and care services, quality improvement and patient and user safety, and that other requirements in health and care legislation are complied with . The Norwegian Directorate of Health has produced a guide to the regulations: Ledelse og kvalitetsforbedring i helse- og omsorgstjenesten
- Article from the Code of Conduct on security risks in systems that use artificial intelligence: Normen (Norwegian)
- The Code of Conduct's guide to risk management: Risikostyring for informasjonssikkerhet og personvern

- Report from NSE on privacy-enhancing technologies: Personvernfremmende teknologier for bruk av kunstig intelligens i helse- og omsorgstjenesten (ehealthresearch.no)
- A report published by the UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA) and others provides guidelines for secure AI system development: Guidelines for secure AI system development (ncsc.gov.uk)
- The Open Worldwide Application Security Project (OWASP) has created an overview of how to handle privacy during the development of an AI system: OWASP AI Security and Privacy Guide | OWASP Foundation
- Report from the Norwegian Data Protection Authority on artificial intelligence and privacy, including recommendations for good privacy protection in the development and use of AI: Kunstig intelligens og personvern (datatilsynet.no)
- The Directorate of Health's guide on Management and quality improvement in health and care services
- Current standard: ISO SO/IEC FDIS 42001: Information technology - Artificial intelligence - Management system (online.standard.no)

Phase 4: Procure an AI system

The purpose of this phase is to procure an AI system and will primarily include:

- Requirement specification
- Announce a call for tenders
- Evaluate offers
- Enter into an agreement with the selected supplier

Consider collaboration on the procurement of AI systems

> The organization should assess the appropriate scale for the procurement. Various factors may indicate that a local procurement process is preferable. For example, an AI system may be so specialized that it would only benefit a few users within a specific organization. In other cases, it may be advantageous for the organization to collaborate with other municipalities or hospitals on the procurement, or the procurement may be suited for a regional process. Imaging diagnostics, such as radiology, is standardized and performed across many institutions, making it suitable for procurement on a larger scale.
>
> In some cases, framework agreements may already exist that the organization can utilize. A framework agreement simplifies the procurement process for those entitled to use it. Therefore, it may be desirable to establish a framework agreement if one is not already in place within the organization.

Procurement regulations

> Procurement is regulated by laws and regulations; guidance is available at anskaffelser.no. Here, relevant laws, regulations, and guidelines can be found, including how to calculate the value of a procurement and which threshold values apply for selecting the appropriate procurement procedure. The ability to modify an already concluded contract is also regulated. As the rules of the AI Act come into force, it will become increasingly important to determine the risk classification of an AI system. This will affect the requirements the organization must set for the supplier, as well as the requirements the organization must comply with under the AI Act as a user of the AI system.
>
> There will primarily be three types of AI system procurements in the health and care sector: AI for clinical use, AI for administrative use, and AI for use in research and innovation.

Specific provisions for research and innovation

If the procurement is carried out as part of a research or innovation project, the Public Procurement Regulations contain specific provisions that allow exceptions from the obligation to publish such contracts

[106][107]. According to Article 2 no.6 of the AI Act, the regulation does not apply to AI systems and models, including their outputs, that are developed and used solely for research and development purposes. However, the rules of the AI Act will apply if the AI system is placed on the market.

[106] For the implementation of innovation and development projects, see: Finn riktig metode for gjennomføring av innovasjon- og utviklingsprosjekter (anskaffelser.no)

[107] For exceptions for R&D contracts, see: Unntak for enkelte FoU-kontrakter (anskaffelser.no)

Procurement procedure

The choice of procurement procedure affects the time required, the use of resources, and the opportunities for dialogue with suppliers during the procurement process. In a market characterized by rapid technological development, the need for quality assurance must be weighed against the risk of acquiring outdated solutions if processes take too long. The organization's familiarity with the market for the product or service to be procured will influence the choice of procurement method and form the basis for the competition strategy. *Competitive dialogue* can be a relevant and flexible procurement procedure for AI systems if it is unclear from the outset which solution is best suited. In a prequalification phase, the number of suppliers allowed to participate can initially be limited based on their expertise and experience, followed by a dialogue phase where the requirements specification can be adapted in collaboration with the suppliers [108].

- For example, South-Eastern Norway Regional Authority's procurement of a framework agreement for AI platforms was carried out as a competitive dialogue [109].

In many organizations, there are established procedures for conducting procurements. For example, Oslo University Hospital Trust has described such a procedure in its electronic handbook system for the procurement of medical technical equipment, known as the "eHandbook." [110]

[108] Competitive dialogue | Anskaffelser.no

[109] Qualification: Framework agreement KI platforms for the South-Eastern Norway Regional Health Authority | Doffin, Database for Public Procurement

[110] eHandbook - Collaboration model for MTU-ICT in OUS (ous-hf.no)

Pricing models

AI systems have various pricing models, which may change more frequently than those for more mature products. Pricing models may include one-time costs, maintenance and upgrade costs, and/or usage-based costs. The pricing model may also be scalable, meaning that costs depend on the level of usage. If the AI supplier operates with a fixed base price, the previously conducted assessments of intended use and benefit analyses will be valuable. This enables the organization to ensure that the procurement is cost-effective.

Agreements

Please refer to Statens standardavtaler (SSA) (anskaffelser.no) for standard agreements used in public procurement of, for example, software and IT solutions.

A procurement process typically includes a main contract accompanied by a Service Level Agreement (SLA) and appendices such as the requirements specification.

The SLA defines responsibilities and response times in the event of operational issues or system errors. It specifies who is responsible for what, how errors should be handled, and should also include a plan for version updates. The contract may also allow for further development of the AI model.

If the supplier is to process personal data on behalf of the organization, a data processing agreement must be established [111]. The supplier may not use the organisation's data for its own purposes, for example for research or improvement of the AI system, unless explicitly agreed upon. It is important to clarify this during early supplier dialogue and ensure it is reflected in the contract.

[111] The Norwegian Directorate of Health's template and guide to standard data agreements

Requirements specification

The groundwork established in earlier phases forms the basis for developing the requirements specification for the procurement. If an early market dialogue was conducted during Phase 2, it will have provided insight into available products and their capabilities and limitations.

A requirements specification is a detailed document outlining the specific requirements the system must meet. It is important to consider the appropriate level of detail; overly specific requirements may limit the range of potential solutions. It can be useful to formulate user stories and allow suppliers to propose how the needs can be met, or alternatively to provide a detailed description of how the AI system should be configured and operate.

The organization must require the manufacturer to provide documentation that enables a thorough assessment of the AI system’s performance, trustworthiness, and safety before the contract is signed.

The upcoming AI Act includes requirements for AI systems classified as limited or high risk. It is advisable to take these into account when specifying requirements, in addition to other regulatory obligations [112]. We refer to phase 2. Article 11 of the AI Act, along with Annex IV, describes in more detail what documentation is required for a high-risk AI system [113][114].

The requirements specification contains requirements that are divided into different groups:

1. General requirements
2. Functional requirements
3. Technical requirements
4. Safety requirements

General requirements

General requirements may include that the supplier must address ethical and societal considerations related to the AI system [115].This can include requirements for safeguarding fundamental human rights, such as health and safety, as well as environmental and sustainability considerations. AI systems consume substantial amounts of energy, both for data storage and for training and operating large AI models. As of January 1st, 2024, an amendment to the Regulation on Public Procurement requires that environmental and climate considerations must be weighted at a minimum of thirty percent in all procurements, including those of AI systems, where environmental impact is relevant. All AI systems should contribute to fulfilling the United Nations Sustainable Development Goals.

Under the AI Act, high-risk AI systems will also be required to be designed in a way that ensures transparency and human oversight. The organization may request that the supplier describe the training and testing methods used. Requirements for quality management systems and logging, as outlined in the AI Act, may also be included. For medical devices, monitoring is a mandatory supplier obligation in accordance with the MDR.

Functional requirements

Users of the AI system should define functional requirements, for example, how the user interface should work, and how the AI system's output should be presented to the end user. It may also be necessary to require explainability, interpretability, and transparency for those who will be using the AI system.

Data quality is a particularly important consideration in AI procurements, as the data used to train AI models directly affects system performance, reliability, and fairness Requirements should be set for the supplier to explain which data [116] were used during development, both for training and validation, and on what legal basis the data were processed under the GDPR. The AI Act includes data quality requirements. Article 10 sets out obligations for data and data handling in high-risk AI systems. Training, validation, and testing data must meet quality criteria, they must be relevant, sufficiently representative, and, as far as possible, free of errors and complete in relation to the intended use [117].

There should also be requirements for documentation of the AI system's performance and quality in actual use, for example, how clinical evaluation or testing has been conducted, on whom, and with what equipment.

Technical requirements

The AI system must be compatible with the organization's infrastructure. Requirements should therefore be set for descriptions of data flow and data formats that will be processed and exchanged between the AI system and other systems. Requirements may also include the scalability of the AI system in terms of number of users or usage volume, as well as any need for test environments. Reference is often made here to the organization's internal standard documents, or to equivalent international or Norwegian standards and technical certifications.

AI models can be deployed either locally on the organization's own servers or in the cloud. When using cloud solutions, it is important to define requirements in accordance with current national recommendations.

Safety requirements

Most organizations in the health and care sector are required to comply with the The Code of Conduct for information security and data protection (Normen). The measures described in the Code of Conduct, which are important for securing digital systems in general, are also important in the protection of AI systems.

The organization must require that the supplier has considered the special challenges and threats associated with AI systems. The Code of Conduct has published an article on security in AI systems and MITRE ATLAS™ provides an overview of known threat scenarios targeting AI systems.

The European Union Agency for Cybersecurity (ENISA) identifies the following threats in the AI lifecycle

- **Evasion:** AI systems can often be tricked in new ways, for example by the attacker using special input values (*adversarial examples, prompt injections*)
- **Poisoning:** Attacker influences training data or the AI model so that the behavior of the system is affected in a chosen direction.
- **Information leakage**: An attacker can extract information about the AI model, such as configuration, parameters and training
- **Compromised components in the AI system**: Attacker compromises a component, for example by exploiting vulnerabilities in open-source libraries used by the AI system.
- **AI system failure**: The entire AI system fails, for example by an error or by an attacker managing to take down the AI system

[112] Obligations of providers and deployers of high-risk AI systems and other parties (europa.eu)

[113] Art. 11 Technical Documentation - EU AI Act (euaiact.com)

[114] Annex IV: Technical Documentation Referred to in Article 11 (1) - EU AI Act (euaiact.com)

[115] Artificial intelligence and ethics - SN-ISO/IEC TR 24368 (standard.no)

[116] How data is selected, the origin of the data and the processes when the data originated. What equipment has been used to collect data. For example, which camera equipment has been used in the development of an AI model for image interpretation. How the data is labelled, whether it is correct, complete and appropriate for the purpose for which it is to be used.

[117] Article 10 of the AI Act (eur-lex.europa.eu)

Rating of the suppliers

During the procurement process, both suppliers and the proposed AI systems are evaluated based on the requirements set out in the tender documents.

The supplier's value chain should be assessed, including all levels from manufacturer to supplier, any subcontractors involved, and how robust this value chain is. This involves considering ethical issues, as well as risk and vulnerability factors.

Organizations should consider how such developments could affect them, what actions might be required in such cases, and whether any preventive measures can be taken. It may also be advisable to regulate in the contract whether the agreement can be transferred to another supplier.

Rating the offered AI systems

Testing AI systems with the organization's own data can be a way of assessing the suitability of the AI system in this phase. This allows for technical testing related to data flow and infrastructure compatibility, as well as evaluating the AI model’s performance using the organization's own data.

It may also be relevant to consider a retrospective validation process at this stage. If the suppliers permit this, it is important to ensure that all vendors are treated equally in accordance with procurement regulations [118]. See Phase 5 for legal grounds for data processing and exceptions to confidentiality requirements regarding the use of data from the organization’s medical records. If validation is desired but not feasible before the contract is signed, the organization may consider including a contractual provision allowing for termination if the AI system does not perform as expected when validated with the organization's own data.

[118] As also described in phase 2, a situation where a solution has been fully tested (including integrations) from a single supplier before initiating a competition phase could create challenges in terms of conducting a procurement that fulfils the requirement for equal treatment in the procurement regulations. In such situations, it is necessary to equalise any advantages that a supplier may have gained, which in such cases often means that the procurement process can take quite a long time, because the other suppliers must also have the same knowledge base and should have the opportunity to showcase their solutions in a similar way before a contract is awarded.

Relevant sources for phase 4

- Standard data processing agreement for use in the health and care sector, with guide
- Guide to the use of cloud services for the processing of health and personal data
- How to use the Code of Conduct's requirements in procurement
- Use of data processor (The Code of Conduct's fact sheet 10)
- Information security and privacy for providers
- Guide to rights in the processing of health and personal data

Phase 5: Introduce and quality assure an AI system

The purpose of this phase is to ensure quality in the implementation process by:

- Conducting a new risk assessment
- Implementing necessary measures
- Testing and validating the AI system

New risk assessment

In addition to standard assessments conducted when introducing standard ICT systems, such as *Data Protection Impact Assessm*ent (DPIA) and Risk and Vulnerability Assessment, this phase may require an AI-specific impact assessment to dentify other and unique risks related to AI [119].

A DPIA will often be required when using AI, as it constitutes a new and innovative technology (in accordance with the GDPR [120]. When the AI Act enters into force, organizations providing services to the public will be required to conduct a Fundamental Rights Impact Assessment (FRIA) for high-risk AI systems used in areas that may affect human rights [121].

A Fundamental Rights Impact Assessment (FRIA) is a detailed analysis of:

- The organization's processes
  - How will the AI system be used in practice?
- Time period and frequency
  - How long and how often will the system be used?
- Affected individuals
  - Which categories of individuals or groups are likely to be affected?
- Specific risks
  - What risks of harm may arise for the affected individuals?
- Measures for human oversight
  - How will you ensure human control and monitoring of the system?
- Measures to manage risk
  - What measures will be implemented to minimise or eliminate the identified risks?

The purpose of a FRIA is to protect fundamental rights, strengthen trust in AI, and prevent adverse outcomes.

An AI impact assessment may include (but is not limited to) issues related to patient safety, fairness, transparency, explainability, cybersecurity, information security, privacy, financial impact, accessibility and human rights, and the potential for malicious use of the system [122]. There may be some overlap between such an AI impact assessment, DPIA and FRIA. It may therefore be appropriate to conduct these assessments in parallel. There are several sources of information on how to conduct an impact assessment, and various templates [123] 124] [125].The Danish Data Protection Agency has published a template intended for a privacy impact assessment when using personal data in AI systems [126].

The National Institute of Standards and Technology has published a risk framework for artificial intelligence Information Technology Laboratory AI Risk Management Framework (nist.gov). This framework can be used to build a structure for managing risks associated with artificial intelligence and provides an overview of the different types of risk that should be considered.

These assessments form the basis of the organisation's risk management plan and determine which additional measures must be implemented beyond those described in the AI system's user maual [127] [128].

[119] Companies must comply with the requirements of the Personal Data Act and the General Data Protection Regulation, cf. Lov om behandling av personopplysninger (personopplysningsloven) (lovdata.no)

[120] GDPR article 35: Data protection impact assessment (eur-lex.europa.eu)

[121] Fundamental rights impact assessment (FRIA), Article 27 of the AI Act

[122] See also ISO/IEC 42001:2023: Management system for artificial intelligence.

[123] AI and data protection risk toolkit | ICO

[124] Government of the Netherlands: AI Impact Assessment

[125] RAI Institute: Artificial Intelligence Impact Assessment (AIIA) - GOV.UK

[126] New templates for conducting impact assessments (datatilsynet.no)

[127] Regulations on the handling of medical devices - Lovdata

[128] Article 26 of the AI Act

Implement technical and organizational measures

The organization must implement appropriate technical and organizational measures based on previous assessments. Some measures that may be relevant for the implementation of AI systems include:

- Technical adaptations and integrations: Existing systems must be adapted to the new AI system and new workflows. The organization may consider implementing constraints in the AI system to ensure it is used within the scope for which it was developed and validated [129]. An example could be an AI system that has been developed and validated only for adults. If a user inputs data for a child and age is included in the input, the AI system could notify the user that applying the system to this patient falls outside its intended use.
- Training: Before the system is put into use, the organization must ensure that relevant user groups receive training and understand the AI system’s functions, limitations, and ethical considerations. Users must be aware of the applicable incident reporting procedures, including which authority or reporting system to use if errors or incidents related to the AI system are identified during use, to

ensure that such issues are detected and addressed. Existing incident management systems within the organization should be used as the basis for this [130]. This should also ensure compliance with the AI Regulation's requirement for human oversight.

[129] See "intended purpose" in phase 2

[130] Regulations on the handling of medical devices - Lovdata

Testing of the AI system

Once adaptations and integrations have been completed, they must be tested. The testing should cover both the AI system itself and the overall environment it will operate within, ensuring that the AI system produces the expected outputs. This involves testing functionality, security, robustness, workflow and testing of integrations throughout the workflow. CE-marked medical devices have a defined intended purpose, and the healthcare organization must follow the manufacturer's instructions before the system can be put into use.

Organizations often have established procedures for how testing should be conducted. There are various terms used for different testing methods, some of which may overlap. The tests should be formalized and included in the agreement with the vendor, specifying the responsibilities of each party, which errors are acceptable to the organization, and a plan for resolving any identified issues.

Clinical validation

Any organization operating within the health and care sector is required to provide professionally sound health and care services and to ensure good patient safety [131]. Therefore, the AI system should be tested using representative data from the organization to ensure the quality of its accuracy, precision, and reliability. The fact that an AI system is CE-marked does not necessarily mean that it will perform well in practice on the organization's specific patient population, equipment, or examination protocols.

The term *validation* can have several meanings depending on the context. Validation of AI models refers to the process of evaluating a model's performance and provides a measure of how well the model generalizes to unseen data.

Terms commonly used in relation to AI include *internal validation*, which is performed by the developer; *external validation*, which is carried out by an independent party; *technical validation*, which takes place during the development process; and *clinical validation*, which is conducted in a clinical setting after the AI model has been fully developed.
Validation can be performed either *retrospectively*, using previously collected data, possibly gathered for a different purpose, or *prospectively*, using data from a real-world use setting.

The *black box* problem with AI refers to the challenge that advanced AI models, especially those based on deep neural networks, can produce results without clearly explaining how those results were derived. This lack of transparency and explainability fundamentally conflicts with the core principles of evidence-based medical diagnostics and treatment. In addition, the internal logic of the model is often inaccessible to the organization for commercial reasons [132]. The organisation must therefore ensure that the AI system is

safe to use. Given the difficulty in explaining how an AI model functions, clinical validation using the organization’s own data remains a key method for assessing how well the system performs within the target patient population.

Validation using representative datasets is performed for detecting potential biases in an AI model early in the process, enabling the organization to address any weaknesses before the system is deployed in clinical practice. If an AI model fail to provide adequate performance for a population group, the organisation must develop a plan to ensure that appropriate care is provided to this group [133].

The extent of clinical validation required depends on several factors, including how the AI model was trained, the nature of the training data, and the intended clinical application. When an organization adopts an AI system that has already been implemented and validated in another institution with a similar patient population, identical equipment, and comparable clinical protocols, the scope of additional clinical validation may be limited. Conversely, if the AI system is intended to operate with a high degree of autonomy, more comprehensive clinical validation will be necessary. Validation of AI systems should be risk-based and be repeated, either in full or in part, whenever the supplier releases updates or new versions of the AI system.

Kortesniemi et al. have recently published an article in the field of radiology outlining practical approaches for testing AI systems prior to clinical implementation [134]. The methods presented in the article may also prove useful for other clinical specialties.

Regulations governing access to data for validation

The healthcare organization is responsible for conducting the clinical validation and will typically act as the data controller for the data used in this process. Health data must be handled in accordance with confidentiality regulations. While consent from individual patients can serve as a legal basis for data use, this is often impractical or unfeasible when large volumes of data are involved.

As a data controller, the organisation must have a legal basis for processing and an exemption from the duty of confidentiality if patient data from medical records is to be used for purposes other than direct patient care (§ 20 of the Patient Records Act [135]) in the organisation's clinical validation process. Internal quality assurance aimed at verifying that the quality of care remains equivalent or improves with the use of the AI system may provide such an exemption under the statutory exception found in the Health Personnel Act § 26 [136].

This legal basis may also apply to collaborating organizations, provided there is a formal agreement as described in Section 9 of the Patient Records Act [137]. If multiple organizations have jointly procured an AI system and there is a need to share information between them, the exemption provision in the Health Personnel Act § 29 may be relevant, allowing for the use of data for quality assurance purposes [138][139]. A formal exemption decision provides both an exception to the duty of confidentiality and a legal basis for the use of health information from patient records and other treatment-related health registers for purposes such as developing, testing and using clinical decision support tools, as well as quality assurance.

It is often necessary or appropriate for the supplier of the AI model to play a role in the validation process conducted within the healthcare organization. As a rule, the supplier will be a data processor for the organization in this situation, in that it processes data on behalf of the organization. In such cases, the

GDPR requires that a data processing agreement will be established between the organization and the supplier for this purpose [140]. This agreement must be in place before any processing of personal data begins, see also phase 4 regarding contractual arrangements.

Assessment of the AI system's performance will be part of the validation process, refer to AI fact sheet 3. For further description of validation, see AI fact sheet 2 [141].

[131] Regulations on management and quality improvement in health and care services – Lovdata

[132] Strategi for kunstig intelligens i Helse Nord for 2022-2025 (PDF)

[133] Algorithms, artificial intelligence and discrimination : An analysis of the possibilities and limitations of the Equality and Anti-Discrimination Act (PDF)

[134]Testing process for artificial intelligence applications in radiology practice – ScienceDirect

[135]Act relating to the processing of health information in connection with the provision of health care (Patient Records Act) – Lovdata

[136] Act relating to Health Personnel, etc. (Health Personnel Act) (lovdata.no)

[137]Act relating to the processing of health information in connection with the provision of health care (the Patient Records Act) – Chapter 2: Patient records and other treatment-related health registers - Lovdata

[138] More information about section 29 in the Norwegian Directorate of Health's circular to the Health Personnel Act: Duty of confidentiality and right to information – Norwegian Directorate of Health

[139] Read more about how to apply for an exemption: Application for exemption from confidentiality – Norwegian Directorate of Health

[140] How to create a data processing agreement | Datatilsynet

[141] AI fact sheets will be published on Kunstig intelligens – Helsedirektoratet

Handover with operational and management plan

The handover of the AI system involves transferring responsibility to those who will operate and manage the system.

It is essential to clearly define responsibilities related to both the technical and security aspects of the AI system, as well as those concerning clinical operations. The use of AI systems may require the organization to establish new roles and responsibilities not previously encountered, particularly related to human oversight, performance monitoring, and managing data quality throughout the AI system’s lifecycle. Procedures must also be developed for how to log and address system malfunctions and unexpected performance issues.

> Before the AI system is handed over to the operational team, testing and training must be completed, and all roles and responsibilities must be clearly assigned and in place.

Relevant sources for phase 5

> - The Code of Conduct describes organizational and technical measures that are considered suitable for achieving satisfactory information security and privacy in the sector.
> - Template and guidance for completing a Data Protection Impact Assessment (DPIA)
> - Guide to risk management in information security and privacy
> - NSE has published a knowledge summary on the use of privacy-preserving artificial intelligence technologies in healthcare: Kunnskapsoppsummering om bruk av personvernbevarende teknologier for kunstig intelligens i helse- og omsorgstjenesten (ehealthresearch.no)
> - ISO/IEC 42001 Management system for artificial intelligence (standard.no)
> - EPIC has launched a free (open source) tool for local validation of AI models: AI validation software suite (fiercehealthcare.com). This can be used both in organizations that use EPIC and in organizations that use other systems.
>   - GitHub main link: GitHub - epic-open-source/seismometer: AI model evaluation with a focus on healthcare

Phase 6: Operating and managing an AI system

The purpose of this phase is to ensure that:

- A quality management system is in place for the AI system [142]
- The AI system is monitored throughout its lifecycle regarding safety, stability, performance and the quality of its outputs

[142] To the extent necessary, adapted to the size of the business and risk conditions.

Roles and responsibilities

> The organisation's management holds the overall responsibility for ensuring compliance with, among other things, requirements for quality assurance of the health service, cf. Regulations on management and quality improvement in the health and care service [143]. The AI Act requires providers and users to have a quality management system in place for high-risk AI systems, cf. Article 17 [144]. As the AI Act will gradually enter into force, the organization must prepare itself to comply with the new regulations. Existing management systems should therefore be expanded to include quality management for AI systems. The *AI Management System Standard (ISO/IEC 42001)* can serve as a useful tool for leadership [145].
>
> The operation and use of AI systems may require the creation of new roles and responsibilities to ensure safe and effective implementation. If the organization has acquired a high-risk AI system, several areas must be addressed in accordance with the AI Act:
>
> - The AI system, like medical equipment, must be used in accordance with the supplier's instructions for use [146]
> - Human oversight
> - Transparency and information to users of the system (applies to all AI systems)
> - Monitoring the AI system in operation, including management of logs and deviations
>
> *Human oversight* is described in Article 14 of the AI Act as a requirement for high-risk AI systems. It mandates that such AI systems must be developed in a way that allows for human control of the system. This includes understanding the capabilities and limitations of the AI system, enabling a human to override outputs, monitor performance, detect and manage deviations, as well as understanding how its use can lead to automation bias [147] [148]. This role must be assigned to a person with the necessary competence, support, and authority.
>
> - At Vestre Viken Hospital Trust, for example, designated AI physicians (AI radiologists) have been appointed with specific expertise in the AI system used in clinical practice.
>
> In larger organizations, it may be appropriate to establish an interdisciplinary group with both operational and strategic responsibility to ensure efficient system management and governance. This can be a helpful organizational structure for discussing system performance, identifying areas for improvement and risks, and providing a clear framework for decision-making and communication. An example of a group with personnel with broad expertise and clear responsibilities:

- Daily operations: Operations Manager, Systems Manager and IT personnel who play key roles in ensuring continuous and stable operations, technical responsibility for performance, infrastructure and security. Will coordinate technical updates, logging maintenance and integration with other systems.
- Domain expertise for relevance: Clinical expertise and/or super-user is essential to ensure that the AI system works as expected. They need to be the link between technical and clinical teams by translating clinical needs into technical requirements. They can provide training and support to other users of the AI system and report deviations or limitations.
- Compliance and risk: Professionals in privacy, information security and legal affairs are more central to overall management than to day-to-day operations. Will ensure patient trust and compliance with legislation and agreements.
- Information management: Responsibility for keeping your own house in order. Good information management will ensure that data used by the AI system is accurate, relevant and of high quality. This helps to manage and avoid data bias and data drift.
- Strategic management: The system owner has overall responsibility for ensuring that the system delivers value and complies with the organization's goals and regulations.

Reference is also made to the RACI matrix in phase 1 and AI fact sheet 0.

[143] Regulations on management and quality improvement in health and care services - Lovdata

[144] Article 17 of the AI Act: Quality management system (eur-lex.europa.eu)

[145] Artificial intelligence management system - ISO/IEC 42001 (standard.no)

[146] For example, if the organization makes significant changes to the AI system or does not use it in accordance with the instructions for use, the organization will assume the role of manufacturer and will be obliged to comply with the requirements imposed on manufacturers under both the Medical Devices Regulation and the CI Regulation. Cf. Article 16 of the MDR and Article 25 of the CI Regulation.

[147] Article 14 of the AI Act: Human oversight (eur-lex.europa.eu)

[148] A tendency to automatically trust or over-rely on the results of an AI system (automation bias) that provides decision support.

Monitoring

Monitoring of AI systems requires a multidisciplinary approach that includes technical, clinical, and safety-related aspects. The organization should identify and implement measures to enable the detection and investigation of changes in system behavior [149].

AI systems rely on robust technical infrastructure, which must be continuously monitored to protect against threats that could affect system stability and reliability. Clinical monitoring ensures that the AI system fulfils its intended clinical purpose and provides value to healthcare professionals and patients. Security incidents may have direct clinical consequences, such as misdiagnosis or incorrect treatment, that can endanger patient health and safety.

Cyber security, information security and data protection

AI systems may involve new or more complex technologies compared to what the organization is accustomed to. As knowledge about AI system security is still developing, it should be expected that understanding of security risks, and best practices for managing them, will evolve over time. The threat landscape is dynamic, and it may be necessary to regularly update risk assessments and implement new security measures. The EU Medical Device Coordination Group (MDCG) [150] has published a guidance document that can support cybersecurity assessments for medical devices [151]. Additional resources related to AI security are referenced in phase 4 [152][153][154].

Security testing must be considered for new versions. This includes assessing whether security testing procedures need to be adapted, for example, when new functionalities are implemented. It is essential to conduct regular security testing even if no changes to the AI system have been made. This makes it possible to detect newly emerging risks, such as the discovery of new vulnerabilities or unauthorized changes to the system. AI systems may pose unique security challenges due to specific requirements related to their monitoring and logging.

These risks can be managed through established routines for regular assessments and a structured plan for staying up to date on security threats associated with the type of AI technology the system relies on.

Performance monitoring

Like any other medical device or treatment, AI systems in use must be monitored. The AI Act will require continuous monitoring of high-risk AI systems, as well as mandatory reporting of serious incidents [155].

If the AI system is intended to function with a high degree of autonomy in the organization, this will require more extensive monitoring. AI systems and their operational contexts are often complex, which can make it difficult to detect and address errors as they occur.

Model drift is particularly important to monitor and refers to the deterioration of an AI model's performance due to changes in data or in the relationship between input and output variables. This includes tracking changes in input data, patient populations, or system outputs. Model drift can negatively impact the system’s performance, resulting in poor predictions or incorrect decisions [156]. There are various causes of model drift, and the AI system must be continuously monitored for these.

For a clinical decision support system based on AI, monitoring may include:

Technical measures for performance monitoring:

- AI systems are sensitive to the input data they receive, and control mechanisms should therefore be in place, for example, to ensure that data is complete and of the correct and expected quality and format.
- Monitoring of technical stability and robustness.
- Validation of new model versions using a fixed test dataset. Updating the test dataset when needed.
- Monitoring changes in input data and workflows and assessing their impact on model performance.
- Implementing performance monitoring mechanisms, such as tracking accuracy and bias.

Clinical measures for performance monitoring:

- Reporting errors, deviations and limitations in the use of the AI system. This includes both misuse of the AI system and issues related to its output.
- Conducting periodic validations against clinical datasets to detect potential errors that may be difficult to identify during routine use.
- Performing quality control by recording discrepancies between the AI model's predictions and actual clinical outcomes, and evaluating whether the system's recommendations or decisions align with clinical standards and professional guidelines.

[149] The Code of Conduct's documents, including Security risks in artificial intelligence systems - what do we know and what can we do?

[150] Medical Device Coordination Group Working Groups - European Commission (health.ec.europa.eu)

[151] MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices (health.ec.europa.eu)

[152] Security risks in artificial intelligence systems - what do we know and what can we do?

[153] MITRE ATLAS™

[154] Multilayer Framework for Good Cybersecurity Practices for AI (enisa.europa.eu)

[155] Requirements for the organization in Article 26 of the AI Act: Obligations of deployers of high-risk AI systems (eur-lex.europa.eu)

[156] What Is Model Drift (imb.com)

Logging and incident management

For medical devices, the supplier or manufacturer is obligated to monitor AI systems that are CE-marked under the Medical Device Regulation (MDR), even after they have been deployed (*post-market surveillance*). This includes responsibility for collecting and evaluating feedback from users of the device. The purpose is to ensure continued regulatory compliance, maintain safety and performance standards, and identify any need for immediate corrective actions [157].

The AI Act will impose similar requirements for high-risk AI systems, and users are also expected to contribute to fulfilling these obligations [158]. The organization must ensure that the AI system's automatic logs are retained and properly managed [159]. This post-market surveillance provides systematic documentation of performance and safety issues observed during operational use, supporting error correction and system improvement. Regular reporting to relevant authorities may be required. The designated authority for AI system market surveillance in Norway has not yet been determined [160].

Adverse events

It is essential to establish clear procedures for where and how incidents should be reported once the AI system is in use. The organization should ensure that its internal incident reporting systems are adapted to support reporting of AI-related incidents, whether clinical or technical, to capture all AI relevant events.

Incidents in the health and care service can be reported through melde.no. Patients can also use this to report adverse events. Alternatively, patients can contact HelseNorge.no directly.

Incidents that are classified as serious adverse events must be reported. For AI systems, the organization is obligated to report serious incidents that pose a risk to the supplier without delay, in accordance with Article 26(5) of the AI Act.

The Organisation for Economic Co-operation and Development (OECD) has established a global incident monitoring database for reporting AI-related adverse events: AI Incidents Monitor (oecd.ai)

Quality improvement

An effective quality management system enables the organisation to monitor the AI system so that declines in model performance or other adverse events can be identified in a timely manner. This allows the organisation to manage deviations, learn from them, and implement necessary corrective actions. Such actions may include requesting updates from the supplier, phasing out the existing AI system, or procuring a new one. Continuous quality improvement may also involve adjusting workflows, training, communication, or other operational routines.

[157] Including articles 83 of the Medical Devices Regulation (MDR): REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (PDF)and Article 78 of the Regulation on in vitro diagnostic medical devices: REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (PDF)

[158] Article 72 of the AI Act on aftermarket surveillance: Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems (eur-lex.europa.eu)

[159] Article 26 of the AI Act on business requirements: Obligations of deployers of high-risk AI systems (eur-lex.europa.eu)

[160] The Norwegian Agency for Public Management and Financial Management (DFØ) recommends that The Norwegian Communications Authority should be the national supervisory body, market surveillance authority and act as a point of contact with the EU regarding the AI Act. Why should Nkom be responsible for AI? (cw.no)

Benefit realization and experience sharing

Throughout the procurement, implementation and testing, the organization will gain a stronger basis for conducting the cost-benefit analysis. This analysis forms the foundation of the benefits realization plan, including specific and measurable outcomes.

The introduction of an AI system often leads to changes in how work is organized. The organization should monitor whether the AI system is being used as intended and whether the benefits of new workflows are being realized.

- An example of a new workflow: At Vestre Viken Hospital Trust, patients who receive a "no fracture" result from an AI analysis are sent home immediately, instead of waiting at the emergency department for a radiologist to review the images. As a result, radiologists no longer speak with patients where no fracture is detected, unlike previous practice.

During the governance phase, the organization can systematically measure and document the quality and outcomes of the AI system, including through statistics and reports. This information serves to track progress toward the expected benefits. If the anticipated benefits are not achieved, the organization should assess the underlying causes, identify corrective actions, and implement the most appropriate and effective measures. In many cases, the principles of benefits realization for AI systems are similar to those applied to other systems [161].

The organization's experience with implementing an AI system can provide valuable insight for others—both nationally and internationally. Results from the implementation and any accompanying research may benefit other institutions and should be published and shared. Sharing quantitative data on realized benefits can support others in conducting cost-benefit assessments of AI systems. An effective way of communicating qualitative benefits is through interviews with healthcare professionals who use the AI system, or testimonials from citizens, patients, or service recipients who have received faster or improved care. Likewise, negative lessons learned should also be shared to help others avoid making similar investments without achieving the desired outcomes. Organizations that collect data such as patient-reported outcome measures (PROMs) and patient-reported experience measures (PREMs) can also contribute valuable knowledge [162].

As quality assurance of AI-based systems becomes increasingly relevant across the health and care sector, this is an area where experience-sharing has great potential to strengthen future efforts.

[161] The Agency for Public Management and Financial Control has produced a general guide to benefit realisation (dfo.no) that may be useful.

[162] PROM; Patient-Reported Outcome Measure and PREM; Patient-Reported Experience

Relevant sources for phase 6

- AI Act: REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (eur-lex.europa.eu)
- Regulations for management and quality improvement, with guidance, provide a good basis for assessing results for AI systems in the same way as for other health services (Norwegian): Ledelse og kvalitetsforbedring i helse- og omsorgstjenesten
- Normen (The Code of Conduct for information security and data protection) describes organizational and technical measures that are considered suitable for achieving satisfactory information security and privacy in the sector: Normen
- The European Union Agency for Cybersecurity (ENSIA) proposes a cybersecurity best practice framework for AI: Multilayer Framework for Good Cybersecurity Practices for AI (enisa.europa.eu)
- The Code of Conduct points out the following threats with artificial intelligence: Sikkerhetsrisiko i systemer som benytter kunstig intelligens – hva vet vi, og hva kan vi gjøre?
- ISO/IEC 42001:2024: Management system for artificial intelligence: Ledelsessystem for kunstig intelligens – ISO/IEC 42001 (standard.no)
- ISO/IEC 22989:2023: Concepts and terminology for artificial intelligence (ISO/IEC 22989:2022): NS-EN ISO/IEC 22989:2023 (standard.no)