SAHPRA
South African
Health Products
Regulatory Authority

SAHPRA Head Office
Building A
Loftus Park
2nd Floor
Kirkness Str
Arcadia
0083

COMMUNICATION TO STAKEHOLDERS

Issue No.: MD08-2025/2026
5 August 2025

REGULATORY REQUIREMENTS OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING (AI/ML) ENABLED MEDICAL DEVICES

INTRODUCTION

This communication is intended to provide industry stakeholders with the regulatory requirements of Artificial Intelligence and Machine Learning (AI/ML)-enabled medical devices in South Africa.

The South African Health Products Regulatory Authority (SAHPRA) recognises the transformative potential of AI/ML enabled Medical Devices & *in vitro* Diagnostics (IVDs) in healthcare. While SAHPRA has not commenced with product registration of medical devices and IVDs as per regulation 8 of the general regulations for medical devices including IVDs *(Regulation No. 1515 published in Government Gazette No 40480 on 9 December 2016)*, the rapid advancement and adoption of such technologies necessitate proactive engagement with the medical device industry, to promote patient safety, compliance, and responsible innovation. This is also in keeping with SAHPRA's 2025–2030 Strategic Plan, which explicitly highlights the need for clear guidelines and updated legislation (where necessary) to effectively regulate AI-based health technologies, and the institution's commitment to adapting regulatory frameworks so that AI can be safely and effectively integrated into South Africa's healthcare system.

This communication outlines SAHPRA's position and regulatory requirements of AI/ML-enabled medical devices. Critically, the guidance herein is designed to align with international best practices and ethical standards. The guidance included outlines key definitions, fundamental principles, and explicit regulatory requirements. It also draws on emerging frameworks from leading regulators and expert bodies, including: the International Medical Device Regulators Forum (IMDRF), the US Food and Drug Administration (FDA), the European Union (EU), the Singapore Health Sciences Authority (HSA), the UK Medicines and Healthcare products Regulatory Agency (MHRA), and the World Health Organization (WHO). SAHPRA intends to harmonise its approach with global trends while addressing South Africa's unique healthcare and data governance context. Importers, manufacturers, developers,

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

and other stakeholders are encouraged to familiarise themselves with these requirements to ensure the safe development, effective performance, and ethical oversight of AI/ML medical technologies available for use in South Africa.

Key Definitions

The definition of a medical device in South Africa is established by the Medicines and Related Substances Act 101 of 1965:

> A *"medical device" means any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, including Group III and IV Hazardous Substances contemplated in the Hazardous Substances Act, 1973 (Act No. 15 of 1973)—intended by the manufacturer to be used, alone or in combination, for humans or animals, for one or more of the following:*
>
> *(i) diagnosis, prevention, monitoring, treatment, or alleviation of disease;*
> *(ii) diagnosis, monitoring, treatment, alleviation of, or compensation for an injury;*
> *(iii) investigation, replacement, modification, or support of the anatomy or of a physiological process;*
> *(iv) supporting or sustaining life;*
> *(v) control of conception;*
> *(vi) disinfection of medical devices; or*
> *(vii) providing information for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body;*
>
> *and which does not achieve its primary intended action by pharmacological, immunological, or metabolic means, in or on the human or animal body, but which may be assisted in its intended function by such means.*

*Note that this definition of a medical device is aligned with the IMDRF harmonized definition [*IMDRF/AIMD WG/N67]*[2].*

Defining Artificial Intelligence (AI) and Machine Learning (ML)-Enabled Medical Devices

> *"Artificial Intelligence (AI) is a branch of computer science, statistics, and engineering that uses algorithms or models to perform tasks and exhibit behaviors such as learning, making decisions and making predictions.*
>
> *AI-based systems demonstrate various degrees of autonomy (the level of capacity to perform tasks in a complex environment without constant guidance/input from a user)*

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

and capacity for adaptability (extent of the ability to learn from experience and thereby change performance).

The subset of AI known as Machine Learning (ML) involves a computer implementing an ML training algorithm to learn patterns from data, including classification, inference, matching previous patterns, predicting future outputs, etc., which results in an ML model to be applied to new data." [2]

- IMDRF/AIMDWG/N67

An AI/ML-enabled medical device is therefore defined as a product that conforms to the definition of a medical device and utilises one or more AI or machine-learning algorithms to perform, in part or in whole, its intended medical purpose.

This includes but is not limited to AI/ML applications in:

- Medical imaging analysis (e.g., software using AI to detect tumours or fractures in radiological images);
- Predictive algorithms (e.g., an ML model that forecasts risk of patient deterioration);
- Clinical decision support systems (e.g., AI-driven diagnostic aids or treatment recommendation systems for healthcare professionals);
- Wearable health monitoring technologies (e.g., wearables that analyse biosignals and alert to abnormalities).

An AI/ML-enabled medical device can either be Software as a Medical Device (SaMD) or Software embedded in a Medical Device (SiMD). The former is distinguished by the fact that it performs its intended functions without being part of a hardware medical device.

Note: *Mobile apps that meet the definition above are considered SaMD* [2].

Essential Principles of Safety and Performance for Medical Devices

All AI/ML-enabled medical devices must comply with the same fundamental safety and performance requirements that apply to conventional medical devices. SAHPRA's existing Essential Principles of Safety and Performance (as outlined in Regulation 20) provide a regulatory framework to ensure that devices are safe and effective. These principles cover general requirements such as device design and manufacturing quality, risk management, clinical evaluation, usability, and labelling, as well as specific considerations like electrical safety and cybersecurity.

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

Manufacturers of AI/ML-enabled devices should ensure that they meet all applicable essential principles. In practice, this means:

- Implementing a robust Quality Management System (QMS) (e.g., ISO 13485) covering software development and maintenance lifecycle [2].
- Conducting thorough risk management (per ISO 14971 & IEC 62304) to identify and mitigate risks associated with the device's hardware and software, including risks unique to AI such as algorithm errors, data drift, etc. [2]
- Demonstrating clinical performance and benefit through appropriate validation studies. AI/ML devices should undergo clinical evaluation to confirm they fulfil their intended medical purpose and improve patient outcomes under real-world conditions [2].
- Ensuring usability and human factors are considered – interfaces should be designed so that healthcare professionals or users can understand and appropriately respond to the device outputs.
- Incorporating cybersecurity controls to protect data integrity and device function from unauthorised access or alterations [2].

The use of AI/ML does not exempt a device from any existing safety or performance obligation; rather, these technologies introduce additional considerations that manufacturers must address within the established framework of essential requirements. In essence, an AI/ML-enabled medical device should be as safe and effective as a traditional device intended for the same purpose, and the manufacturer must account for any new risks introduced by the AI/ML functionality.

Guiding Principles for the Safe and Responsible Use of AI/ML-enabled Medical Devices

While formal regulatory pathways for AI/ML-enabled medical devices are yet to be developed, SAHPRA expects developers and manufacturers to adhere to key guiding principles to ensure the responsible development and use of these products. These principles are informed by internationally recognised best practices (i.e., IMDRF's guiding principles for Machine Learning in medical devices [2] and various FDA, EU, and MHRA guidance documents), and are intended to supplement the essential safety and performance requirements:

a. Patient Safety and Risk Management: The protection of patients' well-being is paramount. AI/ML-enabled devices should be developed with rigorous software engineering, medical device design, quality assurance, and risk management practices from inception through post-market use. Potential failure modes (e.g., an incorrect prediction or misclassification by the algorithm) must be identified and mitigated. Manufacturers should establish appropriate safeguards, such as human oversight or fallback mechanisms, especially in high-risk clinical applications.

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

b. Transparency and Explainability: AI algorithms should be as transparent as possible to regulators, users, and patients. Developers need to document and disclose essential information about how the AI makes decisions, its intended use and limitations, and the level of uncertainty of its outputs. Clinicians and end-users should be provided with understandable explanations or rationale for the AI's recommendations to support informed decision-making. When full algorithmic transparency is not feasible (as with complex neural networks), emphasis should be placed on clear communication of performance (including metrics like sensitivity/specificity and error rates) and appropriate training for users.

c. Cybersecurity, Data Integrity and Privacy: Robust cybersecurity measures must be in place to protect AI/ML devices from unauthorised access or malicious tampering, which could lead to dangerous malfunctions. Data used by the device (whether patient data inputs or training datasets) must be handled with integrity – protected from corruption, loss, or alteration. Privacy is critical: any personal health data used by AI/ML devices must be collected, stored, and utilised in compliance with South Africa's data protection law (Protection of Personal Information Act, POPIA, Act No. 4 of 2013) and other relevant regulations. Ensuring privacy includes data anonymisation/pseudonymisation where appropriate and obtaining informed consent for data use when required.

d. Performance Monitoring and Adaptability: Manufacturers should build in mechanisms for ongoing performance monitoring of AI/ML devices in the field. Software is liable to "drift" in performance, especially if input data characteristics change over time or if the device is used in patient populations that differ from the training data. There should be processes to continuously monitor the algorithm's output quality and detect any degradation in accuracy or safety signals. If the AI model is designed to adapt or learn from new data (continuous learning), strict controls must govern how and when such adaptation occurs (see Change Management in Regulatory Requirements below). Adaptability must not come at the cost of unpredictable behaviour; any updates to the algorithm should maintain or improve safety and effectiveness and trigger regulatory reassessment when needed.

e. Clinical Evaluation and Performance: AI/ML medical devices must undergo thorough clinical validation, using independent test datasets, to ensure they deliver meaningful benefits to patients and healthcare providers. This includes evaluating the device with representative patient populations and clinical settings. Performance metrics (sensitivity, specificity, accuracy, etc.) should be established not just in ideal conditions but in real-world scenarios (i.e., capturing the complexity of human-AI interactions). Where applicable, developers should conduct subgroup analyses to confirm that the device performs reliably across different demographic groups (e.g., across sexes, ages, ethnicities). Any biases or limitations observed in performance should be transparently acknowledged and claims about the device's clinical benefits should be supported by robust evidence. Regulatory bodies

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

worldwide increasingly emphasise the importance of such evidence, and SAHPRA aligns with this principle.

By incorporating these guiding principles into the product life cycle, developers can bolster public and regulator confidence in AI/ML medical devices. SAHPRA encourages a "responsible innovation" mindset – one that proactively addresses potential risks and ethical questions rather than reacting to problems after the fact. This approach will help ensure that the benefits of AI/ML technologies in healthcare are realized in a manner that upholds safety, effectiveness, and the public interest.

Regulatory Requirements

Regulatory Authorisation and Licensing: Each AI/ML-enabled medical device (including those that are stand-alone software as well as those integrated in hardware devices) is subject to the South African medical device including IVDs regulation and shall require authorisation from SAHPRA before it can be made available for use in the South African population.

Albeit that SAHPRA has not yet called up medical devices (i.e., a single medical device and / *in-vitro* diagnostic, a medical device group, medical device family, medical device group family, or a medical device system) for product registration, any person or company intending to import, manufacture and market such a product in South Africa shall apply to the Authority for a medical device establishment licence issued under Section 22C of the Medicines and Related Substances Act 101 of 1965, as amended. This process includes a listing of the medical devices (including IVDs) that shall be imported into and manufactured in South Africa.

Product Risk Classification: An AI/ML-enabled device shall be classified according to the existing South African risk classification rules for medical devices, including IVDs. SAHPRA uses a four-tier risk class system (Class A – lowest risk, Class B – low/moderate risk, Class C – moderate/high risk, Class D – highest risk), in line with IMDRF principles[2]. While each importer or manufacturer must determine the class of the AI device by applying the classification rules provided in SAHPRA's Classification Guideline [SAHPGL-MD-04][4], the final determination of the risk class is the responsibility of SAHPRA.

In general, an AI software that is intended to drive or influence clinical decisions directly (and where such decisions could result in significant patient harm if incorrect) will likely fall into Class C or D (higher risk). Illustrative examples for SaMD are provided in the corresponding IMDRF guidance document[2]. The risk class dictates the level of regulatory scrutiny and evidence required. SAHPRA expects manufacturers to provide a rationale for the classification of their AI/ML device. If there is any uncertainty, it should be resolved in consultation with the Authority.

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

SAHPRA Head Office
Building A
Loftus Park
2nd Floor
Kirkness Str
Arcadia
0083

Quality Management System (QMS) Compliance: Each AI/ML medical device must be developed and manufactured under a quality management system that meets regulatory standards. SAHPRA requires evidence that the manufacturing facility (and software development process) complies with ISO 13485:2016 (Medical devices – Quality management systems – Requirements for regulatory purposes). This includes having design controls for software, validation processes, risk management, and a system for handling complaints and field actions. Given the complexity of AI algorithms, manufacturers should ensure their QMS encompasses software life cycle processes (as outlined in ISO 13485 and IEC 62304) and, if applicable, governance for data management and model training.

Evidence of Safety and Performance (Technical and Clinical): In an application to SAHPRA, the manufacturer must be prepared to submit documentation demonstrating the device's safety, performance, and effectiveness for its intended use. This typically includes:

- Technical File: A dossier with a detailed device description (including the AI algorithm's purpose, logic, and inputs/outputs), software documentation, risk analysis, verification and validation results (including software verification, algorithm training results, and performance metrics on validation datasets), and cybersecurity controls. If the device incorporates a Pre-Determined Change Control Plan (PCCP) (see below), documentation of that plan and its elements would also be part of the submission.
- Clinical Evidence: Results of clinical validation studies, usability studies, or literature that demonstrate the device's real-world performance. For AI/ML devices, clinical evidence should confirm that the algorithm performs as claimed in relevant patient populations and settings. Bias and generalisability should be addressed – for instance, if the device was trained on data from outside South Africa, does it perform equally well on local populations? Any known limitations (cases where the algorithm may not perform well) should be disclosed. SAHPRA will require that any gaps in the dataset are justified and risk-mitigated (e.g., through labelling or post-market obligations).
- Reference to Prior Approvals: For higher-risk devices (Classes C and D), SAHPRA requires evidence of prior approval from a trusted jurisdiction or body. Specifically, for any Class C or Class D AI/ML medical device (including IVD), the Applicant should provide evidence of pre-market approval or registration from at least one of the six reference regulatory jurisdictions recognised by SAHPRA, these are: Australia (TGA), Brazil (ANVISA), Canada (Health Canada), Europe (CE marking under EU MDR/IVDR), Japan (PMDA), or the United States (FDA), or proof of prequalification by the World Health Organization (WHO). Such prior approval will be taken into account in SAHPRA's evaluation. For example, if an AI diagnostic software has FDA clearance or CE Marking, that documentation and the basis for approval should be submitted. SAHPRA reserves the right to ask for additional information or impose further requirements even if a device is approved elsewhere, to ensure local suitability.

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

Post-Market Surveillance and Reporting: Once an AI/ML-enabled device is in use, robust post-market surveillance is essential. Manufacturers are expected to actively monitor the real-world performance of their AI devices and promptly address any safety or quality issues that arise. Post-market surveillance for AI devices should include:

- Continuous Performance Monitoring: Establish metrics and collect data to verify that the device's performance in the field matches the pre-market expectations. For AI, this could involve periodic sampling of cases to check the algorithm's output against ground truth, tracking outcome data from patients, and monitoring for instances where the device suggestions were not followed due to clinician concern. As noted, performance can drift if the input data characteristics shift; therefore, ongoing monitoring can detect early signs of reduced accuracy or emerging bias. If performance deviates significantly, the manufacturer should investigate the cause (e.g., a new type of input not well-handled by the algorithm) and take corrective action (which might include retraining the model or updating instructions for use - see subsequent guidance on 'Pre-determined Change Control Plans').
- Incident Reporting: Any adverse events or incidents involving medical devices must be reported to SAHPRA following the relevant guidance (Guideline SAHPGL-MD-03)[3]. This includes scenarios where use of the AI device contributed to harm or had the potential to cause harm (for example, a misdiagnosis by the software that led to a delay in treatment). Given the complexity of AI decisions, manufacturers should also encourage healthcare providers to report unexpected or erratic behaviour of the algorithm, even if no patient harm has occurred yet. SAHPRA will assess such reports to determine if regulatory action is needed (such as safety communications, recalls, or requiring design changes).

Manufacturers should note that SAHPRA's oversight of AI/ML devices does not end at market entry. The Authority may conduct post-market audits or inspections, requesting documentation of how the AI algorithm is performing and being maintained. If the device's performance in the field falls short of claims or regulatory standards, SAHPRA can require corrective actions, impose additional conditions, or in severe cases suspend or revoke the authorisation. It is in the industry's interest to institute a strong post-market surveillance program internally, as this will both improve patient outcomes and facilitate a positive, trust-based relationship with the Regulator.

Emerging Opportunities

Adaptive Algorithms and Change Control (Pre-Determined Change Control Plans): One of the unique regulatory challenges of AI/ML medical devices is how to manage software changes and algorithm updates. Traditional medical devices are generally "locked" – their design remains fixed unless a new approval is sought – but AI algorithms might improve or change over time (e.g., through model

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

updates or retraining on new data). Recognising this, leading regulators are introducing mechanisms to allow a degree of controlled innovation post-approval. In particular, the US FDA developed the concept of a Predetermined Change Control Plan (PCCP): a plan, submitted during the pre-market phase, that describes anticipated future modifications to the AI algorithm and the associated methodologies that will be used to implement and validate those changes[1]. If approved as part of the device's original authorisation, the PCCP then permits the manufacturer to make those specific changes later without submitting a brand-new pre-market application, so long as they adhere to the plan.

SAHPRA is closely monitoring these international developments and awaiting the release of the IMDRF harmonised guidance on this topic. Until specific guidance is formalised, any changes to an AI/ML medical device that may affect its performance or safety should be communicated to SAHPRA. When a device is on the market under a medical device establishment licence, significant changes (especially those that expand usage or alter the algorithm's core logic) should not be made without notifying the Authority. In the future, SAHPRA may implement a formal mechanism akin to the PCCP for pre-specified changes. In the interim, manufacturers should document all changes in the device's technical file and be prepared to provide that documentation upon request. It is advisable to "lock" the algorithm version at the time of initial approval/licensing and only update it following a controlled process. Minor software updates (e.g., bug fixes or cybersecurity patches that do not affect the AI logic) can be made under the company's certified QMS change control, but major updates likely require regulatory review. Internationally, other regulators like the TGA (Australia) and EU have generally required that adaptive algorithms be reviewed as new devices unless a prior change protocol is agreed. SAHPRA will take a similar cautious stance: patient safety takes precedence over rapid deployment of untested updates.

That said, manufacturers of AI/ML devices are strongly encouraged to take a proactive approach to preparing for innovations in change management control. This means: if an update to the algorithm is anticipated (for example, periodically retraining the model with new data to improve performance or expanding the device's indications), a change control plan must be prepared and discussed and approved by the Authority, in preparation for the release of an updated guidance. **A robust change control plan will typically include:**

- Scope of the anticipated changes: For e.g., "the model will be retrained on additional local patient data to improve accuracy for certain sub-groups," or "the algorithm's decision threshold may be adjusted over time".
- Data for change: Identification of the new data that will trigger an update (e.g., detection of drift beyond a threshold).
- Protocol for implementation: The procedures for retraining or modifying the software, including validation testing that will be conducted for the updated model (for example,

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

performance benchmarks the updated algorithm must meet, and testing on independent datasets).

- Limits/Boundaries: Defining what aspects of the device will not change (for instance, no new clinical indications will be added without a new submission, and the algorithm's output format to users will remain the same).

Generative Artificial Intelligence-enabled Medical Device: A generative AI-enabled medical device is defined as a medical device that satisfies the requirements to be SaMD/SiMD, and where the underlying AI algorithm is considered to be of a novel set of generative algorithms (e.g., large language models, generative adversarial networks). Generative AI-enabled medical devices are potentially useful tools for improving the quality and quantity of healthcare that can be provided. **Examples include:**

- Conversational chatbots for patients, e.g., a symptom-checker or "virtual doctor" chatbot using a Large Language Model (LLM).
- Automated clinical note summarisers and scribes, e.g., generative models that listen to doctor-patient conversations or read medical records and produce summary documentation. The UK MHRA recently released guidance on the regulation of these types of systems[7].
- Open-ended clinical decision support systems, e.g., tools where a clinician might ask any question (e.g., "What's the differential diagnosis for a set of symptoms?" or "How do I manage this complex condition?") and the AI provides answers.

However, there are significant challenges for this technology to meet current medical device regulatory requirements, including:

- Broad Intended Use and Functionality: General-purpose LLMs lack a narrowly defined medical purpose, making them hard to classify and regulate under medical device frameworks. Notably, when LLMs themselves are not specifically intended for a medical purpose, they are not a medical device, but once adapted to specific medical purposes (e.g., with a relevant instruction prompt) it does qualify as one. This means developers must pin down a specific intended use (e.g., "clinical decision support for X"), and 'hard code' limits to prevent the 'broad' capabilities of the LLM from being exploited to carry out tasks that go beyond the intended use. The South Korean regulator (MFDS) recently highlighted this distinction in their guidance on large language and multi-modal models, purposefully excluding generalist medical AI systems[6].
- Inconsistent and Unpredictable Outputs: Generative AI models do not guarantee consistent outputs across identical inputs. In other words, two different users might get two different answers from asking the same model the same question. This lack of reliability makes it hard

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

to demonstrate that the device will consistently perform as intended, which is a critical requirement for regulatory approval.

- Opaque Training Data and Decision-Making: Developers of prominent proprietary LLMs typically do not disclose training data sources or model architectures, treating them as trade secrets. This opacity means a medical device sponsor incorporating such a model cannot easily provide regulators with basic assurances about the training provenance, potential biases, or failure modes of the software. From a quality and safety standpoint, a third-party LLM integrated into a medical product becomes "Software of Unknown Provenance" (SOUP) – the documentation requirements for which are non-trivially complex to achieve, and there is not yet evidence of a supplier successfully navigating the requirements.
- Challenges in Validation and Testing of Open-Ended Outputs: Traditional medical software can be validated on a finite set of inputs and expected outputs, but generative AI defies that paradigm. An LLM's output is essentially unbounded – it can produce novel free-text responses rather than a predetermined result – so creating a complete test plan is extremely complex. Demonstrating a generative model's safety/effectiveness requires enormous evaluation efforts, and a clinical study powerful enough to cover "almost infinite" permutations of patient cases and queries is needed to truly vet a GenAI's performance. This inadequate testability is a major regulatory sticking point. A device must be shown to perform reliably and repeatably, but a GenAI system that can always say something new makes repeatability hard to guarantee. Consistent behaviour across all inputs cannot be rigorously proven, only probabilistically estimated with confidence intervals. Such statistical assurances may not satisfy regulators unless the risk of a dangerous output is demonstrably very low.

At present, Generative (Gen) AI-enabled medical devices will be classified according to the potential harm from their intended use, following South Africa's risk-based classification rules (aligned with IMDRF). The corresponding processes for any other AI/ML-enabled medical device, as described above, will then prevail for those seeking authorisation to market a GenAI-based medical device. Where an importer or manufacturer is unable to fulfil a standard submission requirement (due to the challenges described above, or another issue), he or she should seek guidance from the Authority on whether the best available information is sufficient.

Conclusion

SAHPRA acknowledges the significant potential of AI/ML to improve healthcare outcomes in South Africa. However, this potential must be balanced with safeguards to protect patient safety and uphold ethical standards.

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

SAHPRA Head Office
Building A
Loftus Park
2nd Floor
Kirkness Str
Arcadia
0083

It remains the importer or manufacturer's responsibility to determine if the product qualifies as a medical device (and at which risk class) under South African law. Device characterisation, i.e., clearly defining the device's intended purpose, indications, and functionality, is a critical early step that underpins qualification as a medical device (including SaMD) and the subsequent regulatory pathway. Consistency between the stated intended purpose, the device's training/validation data, and its real-world use is essential. Importers and manufacturers should refer to pre-existing guidance on crafting an intended use statement for SaMD to ensure the AI/ML product is accurately characterised and falls within the appropriate regulatory scope [9]. If there is any uncertainty, early consultation with SAHPRA is advised to confirm whether a given AI/ML-enabled product will be regulated as a medical device.

Moving forward, SAHPRA will continue to build internal capacity and, where necessary, update its guidelines to accommodate advances in AI/ML-enabled medical devices. Stakeholders can expect further communications and consultative documents as we refine our approach, potentially including guidance on predefined change control plans, GenAI-specific validation requirements, and harmonisation with the African Union or other regional initiatives. Throughout this process, the overarching goal remains to promote the health of those in South Africa. We believe that with careful oversight, AI/ML-enabled medical devices can be integrated into our healthcare system in a way that is safe, effective, and beneficial to patients. SAHPRA looks forward to collaborating with importers and manufacturers of medical devices (including IVDs), healthcare providers and establishments, and the public in achieving these outcomes.

Boitumelo Semete-Makokotlela

Boitumelo Semete-Makokotlela

SIGNIFLOW

Dr Boitumelo Semete-Makokotlela
Chief Executive Officer (CEO)
SAHPRA

05 August 2025

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela

SAHPRA Head Office
Building A
Loftus Park
2nd Floor
Kirkness Str
Arcadia
0083

REFERENCES

1. U.S. Food and Drug Administration (FDA): https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device
2. International Medical Device Regulators Forum (IMDRF)
   IMDRF/AIMD WG/N67 Machine Learning-enabled Medical Devices: Key Terms and Definitions
   https://www.imdrf.org/documents/machine-learning-enabled-medical-devices-key-terms-and-definitions
3. SAHPRA medical device adverse events reporting guideline SAHPGL-MD-03:
   https://www.sahpra.org.za/wp-content/uploads/2024/12/SAHPGL-MD-03_v4-Guideline-for-Medical-Device-Adverse-Event-Reporting.pdf
4. SAHPRA Classification guideline (SAHPGL-MD-04): https://www.sahpra.org.za/wp-content/uploads/2025/03/SAHPGL-MD-04_v5-Guideline-for-Classification-of-MD-and-IVDs.pdf
5. World Health Organization: Generating Evidence for Artificial Intelligence Based Medical Devices: A Framework for Training Validation and Evaluation
   https://www.who.int/publications/i/item/9789240038462
6. Ministry of Health Singapore: https://isomer-user-content.by.gov.sg/3/9c0db09d-104c-48af-87c9-17e01695c67c/1-0-artificial-in-healthcare-guidelines-(aihgle)_publishedoct21.pdf
7. TGA: Artificial Intelligence (AI) and medical device software: https://www.tga.gov.au/how-we-regulate/manufacturing/manufacture-medical-device/manufacture-specific-types-medical-devices/artificial-intelligence-ai-and-medical-device-software
8. Korean Ministry of Food and Drug Safety. Guidelines for approving generative artificial intelligence technologies as medical devices. Available at:
   https://www.mfds.go.kr/brd/m_1060/view.do?seq=15628
9. UK Medicines and Healthcare products Regulatory Agency
   :https://assets.publishing.service.gov.uk/media/6866572fadfe29730ea3a9d5/MHRA_guidance_on_DMHT_-_Device_characterisation_regulatory_qualification_and_classification.pdf

• Chairperson: Dr Thapelo Motshudi • Vice-Chairperson: Prof Glenda Gray
• Dr Alfred Kgasi • Dr Chevon Clark • Dr Johanna Gouws • Dr Tobeka Boltina
• Ms Mmatebogo Nkoenyane • Mr Anthony Ngcezula • Mr Rajesh Mahabeer
• Mr Nkosenhle Ngongoma • Mr Moses Moselekwa
CEO: Dr Boitumelo Semete-Makokotlela