CM ADVOCATES LLP



KENYA'S 2026 GUIDELINES ON ARTIFICIAL INTELLIGENCE, TELEMEDICINE AND DIGITAL HEALTHCARE

Regulatory Implications for Healthcare Providers, Technology Companies and International Investors

4th November 2026

An international legal and regulatory guide for healthcare institutions, pharmaceutical and medical device companies, artificial intelligence developers, digital health businesses and investors operating in or entering Kenya and East Africa

EXECUTIVE SUMMARY

The Kenya Medical Practitioners and Dentists Council (KMPDC) has issued a public notice on the Guidelines on the Use of Technology-Based Healthcare Services, pursuant to the Code of Professional Conduct and Ethics, 7th Edition (2026). The notice reinforces professional and regulatory obligations applicable to registered medical practitioners and healthcare institutions using telemedicine, electronic health (e-health), mobile health (m-health), robotic medicine, wearable medical devices and artificial intelligence (AI).

The Council's central position is clear,AI must remain a clinical support tool and must not replace human clinical decision-making or professional oversight. Healthcare practitioners remain professionally responsible for treatment decisions and recommendations, including those assisted by AI systems.

The Council's position reinforces an important principle, the adoption of technology in healthcare does not diminish the professional responsibility of medical practitioners or displace the regulatory obligations of healthcare institutions.

These developments are particularly relevant to hospitals, pharmaceutical and medical device manufacturers, telemedicine platforms, AI developers, healthcare technology suppliers and investors from Kenya, India, China, the United States, the United Kingdom, the European Union, the Middle East and other international markets seeking to establish or expand healthcare operations in Kenya and across Africa.

Foreign regulatory approvals, professional licenses and compliance with overseas data protection frameworks do not automatically satisfy Kenyan requirements. International businesses should therefore integrate healthcare regulation, intellectual property protection, cybersecurity, contractual risk allocation and regulatory due diligence into their market-entry and commercialization strategies.

1. KENYA'S LEGAL AND REGULATORY FRAMEWORK FOR DIGITAL HEALTHCARE

The regulation of technology-based healthcare services in Kenya is not confined to the professional regulation of medical practitioners. It involves an interconnected framework of legislation addressing healthcare delivery, professional conduct, digital health infrastructure, patient rights and the protection of personal data.

The principal instruments include:

a) **The Constitution of Kenya, 2010:** Articles 31, 43 and 46 protect privacy, access to healthcare and consumer rights.
b) **The Health Act, 2017 (Cap. 241):** Establishes the framework for healthcare delivery, patient rights, informed consent and confidentiality.
c) **The Medical Practitioners and Dentists Act (Cap. 253):** Regulates medical and dental practitioners, professional conduct and healthcare institutions within KMPDC's jurisdiction.
d) **The Digital Health Act, 2023:** Provides the statutory framework for digital health systems, health information governance and interoperability.
e) **The Data Protection Act, 2019 (Cap. 411C):** Regulates personal data processing, including sensitive health information, cybersecurity-related safeguards and data subject rights.
f) **The Pharmacy and Poisons Act (Cap. 244):** Governs relevant pharmaceutical activities, medicines and applicable health product requirements.
g) **The Standards Act (Cap. 496) and Consumer Protection Act, 2012:** Address applicable product standards, conformity assessment and consumer protection obligations.
h) **The Industrial Property Act, 2001, Trade Marks Act (Cap. 506), Copyright Act, 2001 and Anti-Counterfeit Act, 2008:** Provide the framework for protecting qualifying healthcare inventions, software, brands and other intellectual property against infringement and counterfeiting.
i) **The Code of Professional Conduct and Ethics, 7th Edition (2026):** Establishes the professional and ethical standards expressly referenced by KMPDC.
j) **The Kenya National Patients' Rights Charter, 2013:** Articulates patient rights concerning dignity, information, confidentiality and participation in treatment decisions.

These instruments operate alongside applicable subsidiary legislation, regulatory directions and sector-specific requirements. The KMPDC notice does not independently establish a universal licensing regime for all digital health technologies; applicable obligations depend on the service, product, intended use and relevant statutory framework.

2. ARTIFICIAL INTELLIGENCE IN HEALTHCARE: CLINICAL OVERSIGHT AND PROFESSIONAL ACCOUNTABILITY

The KMPDC notice expressly requires AI to remain a support tool rather than a substitute for professional clinical judgment.

This principle is particularly relevant to:

a) AI-assisted radiology, pathology and diagnostic imaging.
b) Clinical decision-support and automated diagnostic systems.
c) Virtual consultations, digital triage and symptom assessment.
d) Predictive analytics and patient risk assessment.
e) Robotic surgery and technology-assisted medical procedures.
f) Automated prescribing and medication management.
g) Wearable medical devices and remote patient monitoring.
h) Digital therapeutics, electronic medical records and generative AI applications used in clinical workflows.

Healthcare institutions should establish appropriate governance arrangements addressing clinical validation, human oversight, algorithmic accuracy, bias, cybersecurity, professional accountability and incident management.

Technology developers and healthcare providers should also define contractual responsibilities for software failures, defective outputs, maintenance, clinical use and associated liabilities.

Foreign AI certifications or regulatory clearances do not displace the professional responsibilities of healthcare practitioners operating in Kenya. The allocation of civil liability between practitioners, healthcare institutions and technology suppliers will depend on the applicable law, facts and contractual arrangements.

3. TELEMEDICINE, VIRTUAL CONSULTATIONS AND ELECTRONIC PRESCRIBING

The Council requires practitioners not to prescribe medication for patients whose medical conditions have not been properly ascertained.

Accordingly, telemedicine platforms, digital pharmacies and virtual healthcare providers should ensure that:

a) Consultations are conducted by appropriately authorised practitioners.
b) Patient identity and relevant medical history are adequately established.
c) Clinical assessments are appropriate to the patient's condition.
d) Patients are referred for physical examination or emergency treatment where necessary.
e) Electronic prescriptions comply with applicable professional and pharmaceutical requirements.
f) Clinical decisions, prescriptions and referrals are properly documented.
g) Patient consent, confidentiality and data protection obligations are observed.
h) AI systems do not independently assume functions reserved for qualified practitioners.

A professional licence issued in India, China, the United States, the United Kingdom or an EU member state does not automatically authorise clinical practice in Kenya. Foreign providers must assess applicable Kenyan licensing requirements, while Kenyan practitioners treating patients abroad should consider the laws of the relevant destination jurisdictions.

4. PROFESSIONAL LICENSING, HEALTHCARE FACILITIES AND CLINICAL GOVERNANCE

The KMPDC notice reinforces the obligation for practitioners to operate within their authorized scope of practice. Healthcare businesses should therefore distinguish regulated clinical activities from software development, technology licensing, administrative support and other non-clinical services.

Key compliance considerations include:

a) Practitioner registration, annual licensing and professional authorization.
b) Healthcare facility registration and licensing, where applicable.
c) Clinical governance, supervision and professional accountability.
d) Allocation of responsibilities between practitioners, institutions and technology providers.
e) Outsourcing, technology procurement and service agreements.

f) Professional indemnity and other appropriate insurance arrangements.
g) Clinical documentation, electronic signatures and audit trails.
h) Pharmaceutical and medical device regulatory requirements.
i) Employment, immigration and professional recognition requirements for foreign personnel.
j) Applicable healthcare advertising and consumer protection obligations.

Healthcare institutions should therefore maintain appropriate credential management and authentication procedures to prevent the unauthorized use of practitioners' professional identities.

The requirement also highlights the importance of clearly allocating responsibilities between practitioners, healthcare institutions and digital platform operators.

5. HEALTH DATA PROTECTION, CYBERSECURITY AND INTERNATIONAL DATA TRANSFERS

Although the notice primarily addresses the professional obligations of registered practitioners and health institutions, its implications extend to the wider digital healthcare ecosystem.

Healthcare institutions, technology developers, platform operators and other businesses supporting the delivery of digital healthcare services should consider whether their existing operational arrangements adequately address the applicable legal and regulatory requirements.

Under Kenya's Data Protection Act, health information constitutes sensitive personal data and attracts enhanced protection.

Healthcare businesses should implement appropriate measures addressing:

a) Lawful processing and applicable conditions for sensitive personal data.
b) Privacy notices, transparency and patient rights.
c) Data minimisation, accuracy and purpose limitation.
d) Encryption, authentication, access controls and cybersecurity.
e) Data protection impact assessments where required.
f) Cloud services and data processing agreements.
g) Cross-border data transfers and applicable safeguards.
h) Medical record retention, access, portability and lawful disposal.
i) Data breach prevention, response and notification obligations.

International businesses processing Kenyan patient information through infrastructure located in India, China, the United States, Europe or elsewhere must assess Kenyan requirements independently.

Compliance with GDPR, HIPAA, India's Digital Personal Data Protection framework or China's Personal Information Protection Law does not automatically establish compliance with Kenya's Data Protection Act.

6. MEDICAL DEVICES, WEARABLE TECHNOLOGIES AND ROBOTIC MEDICINE

The Council's notice expressly covers wearable devices and robotic medicine, reflecting the increasing integration of connected technologies into clinical practice.

Relevant products include AI-enabled diagnostic equipment, robotic surgical systems, connected monitoring devices, digital therapeutics, medical software, clinical wearables and automated medication management technologies.

Manufacturers, importers, distributors and healthcare institutions should assess applicable requirements concerning:

a) Medical device classification and regulatory approvals.
b) Product safety, clinical evidence and conformity assessment.
c) Importation, distribution and applicable technical standards.

d) Cybersecurity, maintenance and operator training.
e) Product warranties, liability and insurance.
f) Post-market surveillance, incident reporting and recalls.

Products approved, cleared or certified by foreign regulators, including the US FDA, European regulatory authorities, UK's MHRA, India's CDSCO and China's NMPA, may still require separate assessment under Kenyan law. Foreign approvals may provide useful technical evidence but should not be treated as automatically substituting for applicable Kenyan authorizations.

7. REGULATORY ENFORCEMENT, PROFESSIONAL DISCIPLINE AND LEGAL LIABILITY

The KMPDC notice warns that non-compliance may result in disciplinary action under the applicable professional framework.

Depending on the circumstances, healthcare providers, practitioners and technology companies may also face regulatory investigations, data protection enforcement, medical negligence claims, product liability disputes, contractual claims and other civil proceedings.

Criminal liability may arise where the relevant conduct independently satisfies the elements of an applicable statutory offence.

International healthcare businesses should therefore maintain appropriate compliance policies, professional indemnity and product liability insurance, contractual safeguards, incident-response procedures and mechanisms for engagement with competent regulators.

8. RECOMMENDED COMPLIANCE MEASURES FOR HEALTHCARE PROVIDERS AND INTERNATIONAL BUSINESSES

In light of the KMPDC notice and the broader regulatory framework, healthcare practitioners and institutions providing technology-based healthcare services should consider undertaking a structured compliance review.

The following measures provide a useful starting point:

Compliance area	Recommended action
Regulatory market entry	Assess corporate establishment, investment and applicable licensing requirements.
Professional licensing	Verify registration, authorisation and scope of practice.
Healthcare facilities	Confirm applicable institutional licensing requirements.
AI governance	Establish human oversight, clinical validation and accountability arrangements.
Telemedicine	Review remote consultations, clinical assessments and electronic prescribing procedures.
Medical devices	Determine product classification and applicable regulatory approvals.
Data protection	Assess lawful processing, cybersecurity and international data transfers.
Intellectual property	Protect patents, trademarks, software and confidential technologies.
Brand protection	Establish anti-counterfeiting and enforcement arrangements.

Commercial contracts	Allocate technology, clinical, regulatory and contractual responsibilities.
Insurance	Review professional indemnity, product liability and cyber insurance.
Regulatory enforcement	Establish incident-response and regulatory engagement procedures.
Train relevant personnel.	Ensure that practitioners, administrators, technology personnel and other employees involved in digital healthcare delivery understand their respective professional, contractual and regulatory responsibilities.
Regional expansion	Conduct separate compliance assessments for each target jurisdiction.

International businesses should integrate these measures into their market-entry, product commercialization and investment strategies rather than treating regulatory compliance as a post-launch exercise.

9. CONCLUSION

The KMPDC notice reinforces the need for healthcare delivery in Kenya to evolve alongside technological advancement without compromising professional accountability, patient safety and the protection of patient information.

The adoption of artificial intelligence, telemedicine and other digital healthcare solutions presents significant opportunities for improving access to healthcare and strengthening service delivery. However, those opportunities must be pursued within an appropriate legal and regulatory framework.

For healthcare institutions, compliance must therefore extend beyond obtaining the relevant licenses or procuring suitable technology. It must be reflected in the institution's governance arrangements, clinical oversight, data management practices, contractual relationships and day-to-day operations.

Similarly, technology providers and businesses operating within the healthcare ecosystem must appreciate that the deployment of technology in a regulated sector carries legal responsibilities that cannot be addressed solely through technical solutions.

As Kenya's digital healthcare ecosystem continues to develop, a proactive approach to regulatory compliance will be essential in protecting patients, supporting responsible innovation and maintaining confidence in technology-enabled healthcare services.

HOW WE CAN ASSIST

CM Advocates LLP advises healthcare institutions, medical practitioners, pharmaceutical companies, medical device manufacturers, digital health businesses, AI developers, technology suppliers, insurers and healthcare investors on legal, regulatory and commercial matters in Kenya and across Africa.

Our multidisciplinary approach brings together the firm's Healthcare, Life Sciences & Pharmaceuticals (HLSP) Practice, Intellectual Property, Brands & Commercialization (IPBC) Practice, and Brand Rights, Anti-Counterfeiting & New Developments (BRAND) Unit, alongside relevant corporate, investment, technology, data protection and dispute resolution expertise.

We support Kenyan businesses and international companies from India, China, the United States, the United Kingdom, the European Union, the Middle East and other markets seeking to establish, acquire, finance, supply technology to or expand healthcare operations in Kenya and across the region.

CM ADVOCATES LLP

Contact Us:

Healthcare, Life Sciences & Pharmaceuticals (HLSP) Practice
E: hlsppractice@cmadvocates.com

Intellectual Property, Brands & Commercialization (IPBC) Practice
E: ipbc@cmadvocates.com

Brand Rights, Anti-Counterfeiting & New Developments (BRAND) Unit
E: brandprotection@cmadvocates.com

Contributors:

Cyrus Maina
Managing Partner
cmaina@cmadvocates.com

Nelly Ng'ang'a
Associate Advocate
nnganga@cmadvocates.com

CM Advocates LLP – Contact Details

Head Office Nairobi
I&M Bank House, 7th Floor, 2nd Ngong Avenue
T: +254 20 2210978 or +254 716 209673
P.O. Box 22588 – 00505, Nairobi Kenya
E: law@cmadvocates.com

Mombasa Office
Links Plaza, 3rd Floor, Links Road, Nyali
T: +254 041 447 0758 / +254 41 447 0548
P.O. Box 90056 – 80100, Mombasa Kenya
E: mombasaoffice@cmadvocates.com

Regional Presence
Uganda | Tanzania | Rwanda | Zambia | Ethiopia | South Sudan

www.cmadvocates.com

Disclaimer: *This Regulatory Alert is intended for general information and does not constitute legal advice. The applicable requirements depend on the healthcare services, technologies, products, commercial arrangements and jurisdictions concerned.*

© 2026 CM Advocates LLP. All rights reserved.
Protecting Innovation. Preserving Value. Powering Commercial Growth.