E-mail: tony@cpcqualicare.co.za
Website: www.docweb.co.za

Medicolegal Implications of Artificial Intelligence

The integration of Artificial Intelligence (AI) into healthcare, has profound medicolegal implications. ;

AI's ability to process large datasets, learn patterns, and make decisions, introduces both opportunities and challenges that need to be addressed from a legal and ethical standpoint particularly issues related to liability, privacy, informed consent, and regulatory frameworks. Artificial Intelligence in healthcare encompasses a broad range of applications including diagnostic algorithms, treatment recommendation systems, and robotic surgery.

AI systems can enhance diagnostic accuracy, personalize treatment plans, and improve operational efficiencies.

However, the deployment of AI technologies also raises critical medicolegal issues that must be carefully navigated to ensure patient safety, uphold ethical standards, and maintain public trust.

Liability Issues

Determining Responsibility

A primary medicolegal challenge of AI in healthcare is determining liability when AI systems are involved in clinical decision-making. Traditional liability frameworks, which typically assign responsibility to human actors, become complex when decisions are influenced or made by AI. The key questions revolve around who is accountable when an AI system errs – the developers, the healthcare providers, or the institutions deploying the AI?

Product Liability vs. Professional Liability

In cases where AI is considered a product, product liability laws may apply. This would involve holding the manufacturers or developers responsible for defects in the AI system. Conversely, if the AI is viewed as a tool used by healthcare professionals, traditional professional liability might be applied, holding the user accountable for how the AI is used. The distinction between these liability types can significantly impact legal outcomes and the distribution of responsibility.

Legal Precedents and Case Law

There is currently a paucity of legal precedents directly addressing AI in healthcare, which creates uncertainty. As courts begin to encounter cases involving AI, the development of case law will be critical in shaping the medicolegal landscape. Future rulings will likely address issues such as the standard of care when using AI, the adequacy of AI training, and the disclosure of AI involvement to patients.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Privacy and Data Protection: Data Collection and Usage

AI systems often require large volumes of data to function effectively. This necessitates the collection, storage, and analysis of personal health information (PHI). Ensuring the privacy and security of this data is paramount, as breaches can lead to significant harm and legal repercussions.

Compliance with Regulations

Healthcare AI systems must comply with existing data protection regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, the General Data Protection Regulation (GDPR) in the European Union, and in RSA relevant local laws such as POPIA and PAIA.

Regulations strive to set strict guidelines on how PHI can be collected, used, and shared, and non-compliance can result in substantial fines and legal action.

Anonymization and De-identification

To mitigate privacy risks, data used by AI systems is often anonymized or de-identified. However, the effectiveness of these techniques can vary, and there is always a risk of re-identification, especially when datasets are combined. Legal standards for anonymization and de-identification must evolve to keep pace with advances in AI and data analytics.

Informed Consent: Transparency in AI Use

Patients must be informed when AI systems are involved in their care. This includes explaining how the AI functions, the role it plays in diagnosis or treatment, and the potential risks and benefits. Transparent communication is essential to obtain valid informed consent and maintain patient autonomy.

Complexity of AI Systems

The complexity and opacity of many AI systems, particularly those using deep learning techniques, can make it challenging for patients and even healthcare providers to understand how decisions are made. This opacity, often referred to as the "black box" problem, complicates the process of obtaining informed consent and necessitates new strategies for communicating AI's role in patient care.

Legal Requirements for Informed Consent

Legal standards for informed consent vary by jurisdiction but generally require that patients are provided with sufficient information to make an educated decision about their care. As AI

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

becomes more prevalent, these standards may need to be revised to address the unique aspects of AI-driven decision-making and ensure patients are adequately informed.

Regulatory Frameworks: Existing Regulatory Bodies

Regulatory bodies such as the Food and Drug Administration (FDA) in the United States and the European Medicines Agency (EMA) in the European Union are responsible for ensuring the safety and efficacy of medical devices, including AI systems. These agencies have begun to develop guidelines and frameworks specifically for AI in healthcare.
South Africa lags behind the international trends and has POPIA as the chief cornerstone of legislation when it comes to PHI. This is supported by the HPCSA booklets on the topics.

Challenges in Regulation

Regulating AI presents several challenges, including keeping pace with rapid technological advancements, ensuring transparency and accountability, and balancing innovation with patient safety. Regulatory frameworks must be flexible enough to accommodate new developments while providing clear guidelines for developers and users of AI systems.

International Coordination

Given the global nature of AI development and deployment, international coordination is crucial. Harmonizing regulations across different jurisdictions can help ensure that AI systems meet consistent safety and efficacy standards worldwide, facilitating cross-border collaborations and market access.

Ethical Considerations: Bias and Fairness

AI systems can inadvertently perpetuate or exacerbate existing biases in healthcare if they are trained on biased datasets. Ensuring fairness and equity in AI-driven healthcare requires diligent efforts to identify and mitigate biases in data and algorithms.

Autonomy and Control

AI's role in decision-making raises ethical questions about the autonomy of healthcare providers and patients. It is essential to balance the benefits of AI-assisted decisions with the need to maintain human oversight and control, ensuring that AI serves as a tool to augment rather than replace human judgment.

Trust and Public Perception

Building and maintaining trust in AI systems is critical for their acceptance and effective use in healthcare. Transparency, accountability, and clear communication about the capabilities and limitations of AI are key to fostering public trust and ensuring ethical deployment.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Future Direction: Evolving Legal and Ethical Standards

As AI technologies continue to evolve, so too must the legal and ethical standards governing their use. Ongoing dialogue between technologists, healthcare professionals, ethicists, and legal experts is necessary to develop frameworks that are responsive to new challenges and opportunities.

Education and Training

Healthcare providers must be educated and trained in the use of AI systems to ensure they can effectively and safely integrate these technologies into their practice. This includes understanding the technical aspects of AI, its ethical implications, and the legal responsibilities associated with its use.

Research and Development

Continued research is needed to address the medicolegal implications of AI in healthcare. This includes studying the impact of AI on clinical outcomes, exploring new methods for ensuring transparency and accountability, and developing best practices for integrating AI into healthcare systems.

The medicolegal implications of AI in healthcare are complex and multifaceted, encompassing issues of liability, privacy, informed consent, and regulation. As AI continues to transform healthcare, it is imperative to address these challenges through thoughtful and adaptive legal and ethical frameworks. Ensuring that AI is used responsibly and ethically will help maximize its benefits while minimizing risks, ultimately leading to improved patient care and outcomes. Artificial intelligence (AI) depends on data. Unlike traditional software, AI systems improve their performance by analysing large volumes of information. In healthcare, this information includes electronic health records (EHRs), laboratory results, radiological images, pathology slides, genomic data, prescriptions, wearable device data, and even patient-generated information from mobile health applications. While these data enable AI systems to produce accurate predictions and personalised recommendations, they also raise important medicolegal concerns regarding privacy, confidentiality, informed consent, cybersecurity, and governance.

Patients entrust healthcare professionals with highly sensitive personal information. The legal and ethical obligation to protect that information remains one of the cornerstones of medical practice. AI systems introduce additional risks because they often require data sharing across institutions, cloud computing environments, and third-party software providers. If not carefully managed, these processes may expose patients to privacy breaches, identity theft, discrimination, or misuse of personal information.

Privacy and Confidentiality

Privacy refers to an individual's right to control access to their personal information. Confidentiality is the professional duty of healthcare providers to protect information shared during the therapeutic relationship.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

These concepts are fundamental to healthcare because patients may withhold important information if they fear that their data will not remain confidential. Such reluctance can compromise diagnosis, treatment, and patient safety.
AI challenges confidentiality in several ways:

- Large datasets are required to train AI algorithms.
- Data are frequently shared between hospitals, universities, and technology companies.
- Cloud computing allows information to be processed on remote servers.
- AI developers may require access to patient records for algorithm improvement.
- Data may be transferred across international borders where legal protections differ.

Healthcare organisations therefore remain legally responsible for ensuring that patient information is adequately protected throughout the AI lifecycle.

Sources of Healthcare Data Used by AI

AI systems rely on numerous forms of health information, including:

- Electronic health records (EHRs)
- Laboratory results
- Radiological images
- Pathology slides
- Genomic and genetic information
- Pharmacy records
- Intensive care monitoring data
- Wearable fitness devices
- Smart watches
- Mobile health applications
- Patient questionnaires
- Insurance claims
- Public health databases

Combining multiple datasets enables AI systems to identify complex patterns that would otherwise remain undetected. However, combining datasets also increases the possibility that supposedly anonymous individuals may be re-identified.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Data Protection Legislation

South Africa: POPIA IN MORE DETAIL wrt AI.

The **Protection of Personal Information Act (POPIA)** governs how organisations collect, process, store, and share personal information.
Health information is classified as **"special personal information"** and receives additional legal protection.

POPIA requires healthcare institutions to:

- Process information lawfully and fairly.
- Collect only information that is necessary.
- Obtain appropriate consent where required.
- Protect information against loss or unauthorised access.
- Maintain data accuracy.
- Notify individuals of data breaches when legally required.
- Ensure third-party processors comply with the Act.

Hospitals and doctors implementing AI systems must therefore ensure that vendors also comply with POPIA requirements.

GDPR (European Union)

The General Data Protection Regulation (GDPR) is one of the world's most comprehensive privacy laws.

Important principles include:

- Lawfulness
- Fairness
- Transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity
- Confidentiality
- Accountability

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

GDPR also grants individuals several important rights, including the right to access their information, request corrections, object to processing, and in certain circumstances request deletion of their personal data.

One particularly relevant provision concerns automated decision-making. Individuals generally have the right not to be subjected solely to decisions made by automated systems that significantly affect them unless specific safeguards are in place.

HIPAA (United States)

The Health Insurance Portability and Accountability Act establishes standards for protecting protected health information (PHI).

HIPAA regulates:

- Disclosure of medical information
- Data security
- Patient access rights
- Administrative safeguards
- Physical safeguards
- Technical safeguards

Although HIPAA applies only within the United States, many multinational healthcare organisations follow similar standards globally.

De-identification and Anonymisation

AI developers frequently use anonymised or de-identified data to protect patient privacy.
De-identification removes identifiers such as:

- Names
- Identity numbers
- Addresses
- Telephone numbers
- Medical record numbers

However, complete anonymity is increasingly difficult.
Researchers have demonstrated that re-combining different datasets may allow individuals to be re-identified, particularly when genetic information or rare diseases are involved.

Consequently, healthcare organisations should recognise that de-identification reduces—but does not eliminate—privacy risks.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

A deeper dive into Informed Consent and AI

Informed consent is a legal and ethical process through which patients voluntarily agree to medical treatment after receiving adequate information.

Traditionally, informed consent includes explanations regarding:

- Diagnosis
- Proposed treatment
- Risks
- Benefits
- Alternatives
- Possible complications

AI introduces additional information that may need to be disclosed.

Patients may reasonably wish to know:

- Whether AI contributed to diagnosis.
- Whether AI recommended treatment.
- Whether humans reviewed the AI's conclusions.
- The limitations of the technology.
- Whether their information will be used to improve AI systems.

Healthcare providers should therefore explain the role of AI in understandable language, allowing patients to ask questions and participate meaningfully in decisions affecting their care.

The "Black Box" Problem

Many advanced AI systems—particularly deep learning models—cannot easily explain how they reached a particular conclusion.

This lack of transparency is commonly known as the **black box problem**.
For example, an AI system may identify cancer with very high accuracy but be unable to provide a clear explanation of which features influenced its decision.

This creates medicolegal concerns because:

- Clinicians may struggle to justify decisions based on AI.
- Patients may question recommendations they do not understand.
- Courts may find it difficult to establish negligence.
- Professional accountability becomes more complex.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

The development of **Explainable AI (XAI)** seeks to address this issue by creating systems capable of providing understandable reasons for their recommendations.
Explainable Artificial Intelligence (XAI)

Traditional AI systems, particularly deep learning models, often operate as "black boxes." They produce highly accurate predictions without explaining how those conclusions were reached.

Explainable Artificial Intelligence (XAI) seeks to overcome this limitation by providing understandable explanations for AI-generated decisions.
Explainability improves:

- Clinical confidence.
- Patient trust.
- Legal accountability.
- Ethical transparency.
- Professional oversight.

For example, an explainable AI system detecting pneumonia on a chest X-ray may highlight the abnormal region that influenced its diagnosis, allowing the radiologist to verify the findings.

Importance of Explainability in Litigation

Explainability has significant medicolegal implications.
Courts frequently require healthcare professionals to justify their clinical decisions.
If an AI recommendation cannot be explained, several legal questions arise:

- How can clinicians justify relying on it?
- How can expert witnesses evaluate its accuracy?
- How can patients challenge incorrect decisions?
- How can regulators assess safety?

Future legal standards may increasingly require AI systems used in healthcare to provide interpretable reasoning rather than merely accurate predictions.

Electronic Health Records and AI

Electronic Health Records (EHRs) have become the primary source of healthcare data for AI systems.

AI can analyse EHRs to:

- Predict hospital admissions.
- Identify high-risk patients.
- Recommend investigations.
- Detect medication errors.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Improve discharge planning.
- Reduce hospital readmissions.

While these applications improve efficiency, EHRs also create legal challenges.
Potential risks include:

- Inaccurate documentation
- Copy-and-paste errors
- Incomplete records
- Algorithm-generated misinformation
- Incorrect coding
- Over-reliance on automated documentation

Healthcare professionals remain legally responsible for verifying the accuracy of AI-generated documentation before it becomes part of the patient's permanent medical record.

Documentation and Record Keeping

Good documentation remains essential in the AI era.
Medical records should clearly indicate:

- Whether AI assisted decision-making.
- Which AI system was used.
- Whether clinicians accepted or overrode AI recommendations.
- Reasons for overriding recommendations.
- Information provided during informed consent.
- Patient questions and responses.

Accurate documentation provides evidence of appropriate clinical judgement and may be invaluable if litigation occurs.

Cybersecurity and AI

Healthcare organisations have become major targets for cybercriminals because medical records contain valuable personal and financial information.
AI introduces new cybersecurity risks.
These include:

- Ransomware attacks
- Data theft
- Malware
- Model manipulation
- Data poisoning
- Adversarial attacks

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Identity theft

Data poisoning occurs when attackers deliberately introduce false information into training datasets, causing AI systems to make incorrect predictions.

Adversarial attacks involve subtle modifications to medical images that may cause AI algorithms to misclassify diseases while remaining undetectable to human observers.

Strong cybersecurity measures should therefore include:

- Encryption
- Multi-factor authentication
- Network monitoring
- Regular software updates
- Access controls
- Incident response plans
- Staff training
- Penetration testing

Failure to implement appropriate safeguards may expose healthcare institutions to legal liability following data breaches.

AI Governance

AI governance refers to the policies, structures, and oversight mechanisms used to ensure that AI systems operate safely, ethically, and legally.

Effective governance includes:

- Clinical oversight committees
- Risk assessments
- Ethical review processes
- Continuous monitoring
- Performance auditing
- Bias assessment
- Incident reporting
- Regulatory compliance
- Staff education
- Patient engagement

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Hospitals should establish multidisciplinary AI governance committees comprising clinicians, lawyers, ethicists, data scientists, cybersecurity experts, and patient representatives.
These committees evaluate proposed AI systems before implementation and monitor their ongoing performance to ensure continued safety and effectiveness.

Ethical Principles in AI

The rapid adoption of artificial intelligence (AI) in healthcare has brought not only technological advances but also complex ethical and legal challenges. Healthcare has traditionally been guided by ethical principles that protect patients and promote professional integrity. These have traditionally been based on four fundamental principles described by Beauchamp and Childress:

- Autonomy
- Beneficence
- Non-maleficence
- Justice

These principles remain applicable in the era of AI but require reinterpretation to address the unique characteristics of intelligent systems. These principles must also include respect for confidentiality, honesty, and accountability. AI systems must operate within these ethical boundaries while also complying with legal requirements.

Unlike conventional medical technologies, AI systems often learn from experience, adapt to new information, and make recommendations that may not be fully understood even by their developers. This creates uncertainty regarding fairness, transparency, responsibility, and trust.

Ethical failures can quickly become medicolegal problems, particularly if they result in patient harm, discrimination, or violations of legal rights.

Respect for Autonomy

Autonomy recognises the patient's right to make informed decisions regarding their healthcare. AI should support, rather than replace, patient decision-making.

Patients should be informed:

- When AI has contributed to diagnosis or treatment planning.
- About the benefits and limitations of AI.
- Whether a clinician has reviewed the AI's recommendations.
- If their health information is being used to improve AI systems.

Patients should also retain the right to ask questions, seek a second opinion, or decline AI-assisted care where appropriate.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Beneficence

Beneficence requires healthcare professionals to act in the patient's best interests.
AI can enhance beneficence by:

- Improving diagnostic accuracy.
- Detecting diseases earlier.
- Personalising treatment.
- Reducing medical errors.
- Increasing access to healthcare.
- Supporting evidence-based practice.

However, AI recommendations should always be evaluated in the context of the individual patient's clinical condition rather than applied mechanically.

Non-maleficence

The principle of non-maleficence requires healthcare providers to avoid causing harm.
Potential harms associated with AI include:

- Incorrect diagnoses.
- Delayed treatment.
- Medication errors.
- Biased recommendations.
- Privacy breaches.
- Cybersecurity attacks.
- Over-reliance on technology.

Healthcare professionals therefore remain responsible for identifying situations where AI recommendations appear inconsistent with clinical findings.

Justice

Justice requires fair and equitable healthcare.

AI should not discriminate against patients based on:

- Race
- Sex
- Age
- Disability
- Socioeconomic status

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Geographic location
- Ethnicity

Developers must therefore ensure that AI algorithms are trained using representative datasets that reflect diverse populations.

Algorithmic Bias

One of the greatest medicolegal concerns surrounding AI is algorithmic bias.

Bias occurs when an AI system systematically disadvantages particular groups because of flaws in its training data or design.

Common causes include:

- Unrepresentative datasets.
- Historical inequalities.
- Poor-quality data.
- Sampling bias.
- Measurement bias.
- Human bias during algorithm development.

For example, an AI system trained primarily on images of lighter skin tones may perform poorly when diagnosing skin diseases in individuals with darker skin. Similarly, cardiovascular risk prediction tools developed using data from one population may be less accurate when applied to another.

Algorithmic bias may result in:

- Misdiagnosis.
- Delayed diagnosis.
- Inappropriate treatment.
- Unequal access to healthcare.
- Worsening health disparities.

From a legal perspective, biased AI systems may expose healthcare institutions and developers to claims of negligence, discrimination, or breaches of human rights legislation.

Prevention of Algorithmic Bias

Several strategies can reduce bias:

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Use diverse training datasets.
- Conduct independent validation studies.
- Continuously monitor algorithm performance.
- Audit outcomes across different demographic groups.
- Include multidisciplinary development teams.
- Regularly update algorithms using current data.
- Ensure transparency regarding limitations.

Healthcare organisations should also establish procedures for reporting suspected algorithmic bias.

Human Oversight

Current international guidance consistently emphasises that AI should augment—not replace—human judgement.

Meaningful human oversight includes:

- Reviewing AI recommendations.
- Considering patient preferences.
- Applying clinical experience.
- Identifying obvious errors.
- Making the final clinical decision.
- Documenting the reasoning behind decisions.

Human oversight remains central to professional accountability.

Intellectual Property

AI raises several intellectual property (IP) issues.

Questions include:

- Who owns AI-generated clinical reports?
- Who owns algorithms trained using patient data?
- Can AI-generated inventions receive patents?
- Who owns AI-created educational materials?

Most jurisdictions currently recognise human creators rather than AI systems as the legal owners of intellectual property.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

However, legal frameworks continue to evolve as generative AI becomes increasingly sophisticated.

Copyright Issues

Generative AI systems may produce:

- Clinical summaries.
- Research papers.
- Patient education materials.
- Medical illustrations.
- Educational presentations.

These outputs may unintentionally resemble copyrighted material used during training.

Healthcare professionals should therefore:

- Verify AI-generated information.
- Cite original sources appropriately.
- Avoid plagiarism.
- Ensure compliance with copyright legislation.

Academic institutions increasingly require students to disclose AI assistance when preparing assignments.

Regulatory Frameworks

AI regulation continues to develop rapidly worldwide.

Major regulatory bodies seek to balance innovation with patient safety.

World Health Organization (WHO)

The WHO has published guidance emphasising:

- Transparency.
- Accountability.
- Inclusiveness.
- Patient safety.
- Equity.
- Human rights.
- Continuous evaluation.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

WHO stresses that AI should strengthen—not replace—the clinician-patient relationship.

United States Food and Drug Administration (FDA)

The FDA regulates many AI-based medical devices as **Software as a Medical Device (SaMD).**

Manufacturers must demonstrate:

- Safety.
- Clinical effectiveness.
- Quality assurance.
- Risk management.
- Post-market monitoring.

The FDA also recognises that continuously learning AI systems require ongoing regulatory oversight because performance may change after deployment.

European Union AI Act

The European Union AI Act represents one of the world's first comprehensive AI laws.

Healthcare AI is generally classified as **high-risk** because incorrect decisions may directly affect patient safety.

The Act requires:

- Risk management systems.
- High-quality datasets.
- Human oversight.
- Technical documentation.
- Transparency.
- Cybersecurity.
- Post-market monitoring.

Failure to comply may result in substantial financial penalties.

Professional Regulation

Medical councils worldwide increasingly publish guidance regarding AI.

Healthcare professionals should:

- Maintain competence in AI-assisted practice.
- Understand AI limitations.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Protect patient confidentiality.
- Exercise independent judgement.
- Document AI involvement.
- Report adverse events.

Professional standards continue to evolve as AI becomes integrated into routine clinical care.

Medical Malpractice Insurance/Indemnity

AI also affects medical indemnity.

Insurers increasingly consider:

- Whether AI contributed to adverse events.
- Whether clinicians appropriately supervised AI.
- Whether hospitals implemented governance policies.
- Whether AI systems were approved by regulators.

Future insurance policies may specifically address AI-related risks.

International Legal Harmonisation

Healthcare increasingly operates across international borders.

Cloud computing allows AI systems to process data from multiple countries simultaneously. Consequently, international cooperation is becoming essential.

Areas requiring harmonisation include:

- Privacy legislation.
- Medical device regulation.
- AI safety standards.
- Cross-border data sharing.
- Professional accountability.
- Cybersecurity standards.

Organisations such as WHO, the Organisation for Economic Co-operation and Development (OECD), and the International Medical Device Regulators Forum (IMDRF) continue working toward globally consistent AI governance principles.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Emerging Legal Questions

Several important questions remain unresolved:

- Can AI ever be considered legally responsible?
- Should autonomous AI possess legal status?
- What constitutes the appropriate standard of care when AI outperforms clinicians?
- Should patients have a legal right to refuse AI-assisted care?
- How should courts evaluate AI-generated evidence?
- Should AI systems be required to explain every clinical recommendation?

Future Medicolegal Challenges, South African Perspective, Recommendations.

Future Medicolegal Challenges

Artificial intelligence is evolving at an extraordinary pace, and the law often struggles to keep up with technological innovation. While current legal principles can be adapted to many AI-related issues, future developments will present new medicolegal challenges that require updated legislation, professional guidance, and judicial interpretation. Healthcare systems must remain proactive rather than reactive in addressing these concerns.

Autonomous Clinical Decision-Making

Most AI systems currently function as clinical decision-support tools, meaning that healthcare professionals retain responsibility for final decisions. However, future AI systems are likely to become increasingly autonomous.

Potential future applications include:

- Fully automated interpretation of radiological images
- Autonomous robotic surgery
- AI-controlled intensive care monitoring
- Automated prescribing systems
- AI-assisted emergency triage
- Personalised treatment recommendations generated without direct clinician involvement

As autonomy increases, questions arise regarding legal responsibility. If an autonomous AI system makes a clinical decision that results in patient harm, should liability rest with the clinician, healthcare institution, software developer, or manufacturer? Existing negligence laws may not adequately address these scenarios, and new legal frameworks may be required.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

Continuous Learning Algorithms

Unlike traditional medical devices, some AI systems continue to learn after deployment by incorporating new clinical data into their algorithms. While this may improve performance over time, it also creates uncertainty because the system may evolve beyond its original regulatory approval.

Regulators and healthcare organisations will need to determine:

- How often should AI systems be revalidated?
- Who is responsible for monitoring changes in performance?
- When should updated algorithms require regulatory approval?
- How should clinicians be informed about software updates?

Continuous monitoring, post-market surveillance, and robust quality assurance processes will become increasingly important.

Cross-Border Healthcare and Data Sharing

AI frequently relies on cloud-based infrastructure, allowing patient information to be processed across international borders. While this facilitates collaboration and innovation, it also raises concerns regarding:

- Differences in privacy legislation
- Data sovereignty
- Jurisdictional disputes
- International liability
- Cybersecurity risks

International agreements and harmonised regulatory standards will be essential to ensure that patient information remains protected regardless of where data are processed.

Artificial General Intelligence (AGI)

Although current AI systems are designed for specific tasks, researchers are exploring Artificial General Intelligence (AGI)—systems capable of performing a wide range of intellectual tasks at or above human level. While AGI remains theoretical, its development could profoundly affect healthcare by enabling comprehensive clinical reasoning, diagnosis, and treatment planning. The introduction of AGI would raise unprecedented legal and ethical questions, including the extent to which clinicians should rely on its recommendations and whether existing liability frameworks remain adequate.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

AI and Medical Education

Medical schools are increasingly incorporating AI into their curricula. Future healthcare professionals must understand not only the capabilities of AI but also its limitations and medicolegal implications.

Training should include:

- Principles of AI and machine learning
- Ethical use of AI
- Interpretation of AI-generated outputs
- Data governance and privacy
- Clinical validation of AI recommendations
- Cybersecurity awareness
- Legal responsibilities when using AI

Continuing professional development programmes should also provide practising clinicians with ongoing education as AI technologies evolve.

The South African Perspective

South Africa has begun integrating AI into various aspects of healthcare, including diagnostic imaging, pathology, telemedicine, disease surveillance, and public health planning. AI offers significant opportunities to improve healthcare delivery, particularly in underserved rural areas where shortages of healthcare professionals remain a challenge.

Benefits in South Africa

Potential advantages include:

- Earlier diagnosis of tuberculosis through automated chest X-ray interpretation
- Improved screening for diabetic retinopathy
- Enhanced cervical cancer screening
- Better management of HIV and tuberculosis programmes
- Telemedicine support for remote communities
- Predictive analytics for disease outbreaks
- More efficient allocation of healthcare resources

Medicolegal Considerations

Despite these benefits, South Africa faces several challenges:

- Unequal access to digital technologies

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Variable internet connectivity
- Limited technical infrastructure in rural areas
- Shortage of trained AI specialists
- Data privacy concerns under POPIA
- Limited AI-specific legislation
- Ethical concerns regarding algorithmic bias in diverse populations

Healthcare institutions implementing AI must ensure compliance with the **National Health Act**, **Health Professions Council of South Africa (HPCSA) ethical guidelines**, and **POPIA**. Human oversight remains essential, and clinicians retain responsibility for decisions affecting patient care.

Recommendations

For Healthcare Professionals

Healthcare professionals should:

- Maintain clinical judgment and avoid over-reliance on AI.
- Understand the strengths and limitations of AI systems.
- Obtain appropriate informed consent when AI is involved in patient care.
- Verify AI-generated recommendations before implementation.
- Document AI use in the patient's medical record.
- Participate in continuing education on AI.
- Report AI-related adverse events or system failures.

For Healthcare Institutions

Healthcare organisations should:

- Establish AI governance committees.
- Conduct regular risk assessments.
- Ensure compliance with privacy legislation.
- Implement strong cybersecurity measures.
- Audit AI performance regularly.
- Develop policies governing AI use.

CPC DOCTOR'S FUND (PTY) LTD T/A QUALICARE
Directors: Dr A D Behrman, Dr Ph de Villiers, Dr E Meintjes, Dr A Zeeman , Dr D Augustyn, Dr P Galo, Dr T WentleyReg No 95/03533/07 (Vat No 470175882)

- Train healthcare workers in AI literacy.
- Monitor for algorithmic bias and discrimination.

For AI Developers

Developers should:

- Design transparent and explainable AI systems.
- Use representative and diverse datasets.
- Validate algorithms clinically before deployment.
- Continuously monitor system performance.
- Address cybersecurity vulnerabilities promptly.
- Clearly communicate system limitations to users.
- Collaborate with clinicians, ethicists, and legal experts throughout development.

For Policymakers

Governments and regulators should:

- Develop AI-specific healthcare legislation.
- Update medical negligence frameworks to address AI-assisted care.
- Promote international cooperation on AI governance.
- Support research into AI safety and effectiveness.
- Encourage equitable access to AI technologies.
- Establish standards for transparency and accountability.
- Foster public trust through education and stakeholder engagement.

References:

- The principles of biomedical ethics 8th edition Oxford press: Beauchamp and Childress
- The Health Professions Council of South Africa: General ethical guidelines for healthcare professionals and guidelines for AI.
- The World Health Organization 2021 Ethics and Governance of AI in health
- The European Commission 2024: Regulation laying down harmonized rules on AI - the AI Act
- The Protection of Personal Information Act 4 of 2013 South Africa

Article Compiled by Tony Behrman for CPC Qualicare June 2026