
# DATA PRIVACY AND SECURITY

**MARA ZHANET MICHELO**
CEO- JACARANDA HUB

HPCSA
Health Professions Council of South Africa

# ANNUAL CONFERENCE

## ASSOCIATION OF MEDICAL COUNCILS OF AFRICA

ANNUAL CONFERENCE
ASSOCIATION OF MEDICAL COUNCILS OF AFRICA
REGULATION IN THE ERA OF ARTIFICIAL INTELLIGENCE
Proudly Hosted By: HEALTH PROFESSIONS COUNCIL OF ZAMBIA

REGULATION IN THE ERA
OF ARTIFICIAL INTELLIGENCE

JACARANDA HUB
ENGAGE. INNOVATE. INSPIRE


DATA SENTINELS


# Mara Zhanet Michelo



Mara is a social entrepreneur, a communications, business development and project management professional with 16 years professional experience. She is the Founder & Country Director at Jacaranda Hub, an organization that aims at developing young people through the provision of collective services, infrastructure and specialized tools, finance and equipment for common use among the young and aspiring MSMEs with growth potential.
Mara is also a shareholder and CEO of Nkwasho Agro Processing a poultry processing facility situated in the heart of Northwestern Province.

Social Entrepreneur
Digital Transformation and Tech Enthusiast
Impact Communication Expert
Project Management Professional
Business Development Expert
Business and Life Coach & Mentor
Best of all Mother.

She serve as board member on the Smart Zambia Institute Tender Board, a board of trustee with Play It Forward, a UK Charity with social impact projects in Livingstone, she also serves on the board of the United Blockchain Association and sit on various committees with the African Union.

# Some Facts!



Link The Zambian health care system comprises more than 3,000 registered public and private health facilities in 116 districts across the 10 provinces of the country. These facilities include hospitals, general clinics, dental clinics, eye clinics, physiotherapy offices, health centers, health posts, and any other facilities where health care services are provided.

According to IBM's recently released "Cost of a Data Breach" statistics report, the average financial toll of a data breach has surged to an unprecedented $4.45 million globally. This reflects a 2.3% increase from the previous year and a substantial 15.3% surge from 2020.

The healthcare sector bears the heaviest burden, with an average cloud data breach cost of $10.10 million. Following (not so), pharmaceuticals ($5.01 million), technology ($4.97 million), and energy ($4.72 million). These sectors serve as the battlegrounds where the war for data security is most intense.

# The Role of AI in Healthcare

- The Role of AI in Healthcare: Opportunities and Risks
- AI offers immense opportunities for enhancing healthcare services, from personalized treatment plans to predictive analytics that can prevent diseases before they occur. However, these benefits come with significant risks.
- AI systems require vast amounts of data to function effectively, often involving sensitive patient information such as medical histories, genetic data, and real-time health monitoring. This dependency on data makes AI systems in healthcare particularly vulnerable to cyber threats.

# Types Of Sensitive Healthcare Data



- **Electronic Health Records (EHRs):** EHRs are designed to simplify medical processes and ensure fast real-time patient data access. However, EHRs are helpful when implemented with robust mechanisms of sensitive data protection.

- **Personal Identifiable Information (PII):** this type of data is used to identify an individual. PII consists of various identifiable elements, including name, date of birth, address, email address, phone number, medical identification number, and other personal data. PII is collected as a part of patients' medical records—

- **Protected Health Information (PHI):** created and stored by healthcare providers in rendering healthcare services. PHI includes patients' health status data, treatment, diagnosis, test results, and other health information. PII is one of the most crucial healthcare data since it enables physicians to treat patients accurately.
- **Research data:** collects data from two sources: clinical trials (includes raw data) and databases (such as EHRs). Research data often includes patients' identities, treatments, and other sensitive information.
- **Financial information:** includes various types of healthcare-related financial data, such as bills, payment records, and insurance coverage.

# Data Privacy in Healthcare Improving Exchange of Healthcare Information

ANNUAL CONFERENCE
ASSOCIATION OF MEDICAL COUNCILS OF AFRICA
REGULATION IN THE ERA OF ARTIFICIAL INTELLIGENCE
Proudly Hosted By: HEALTH PROFESSIONS COUNCIL OF ZAMBIA

REGULATION IN THE ERA
OF ARTIFICIAL INTELLIGENCE

JACARANDA HUB
ENGAGE. INNOVATE. INSPIRE

# Privacy And Data Protection In Ai-enabled Healthcare Systems,



- Privacy and data protection are of paramount importance in AI-enabled healthcare systems, where artificial intelligence (AI) technologies are increasingly being utilized to revolutionize the delivery of healthcare services
- **Data Minimization:** Collect and retain only the necessary data for the intended purpose. Minimize the collection of sensitive or personally identifiable information (PII) to reduce the risk of unauthorized access or misuse.
- **Data Encryption:** Employ encryption techniques to protect data both at rest and in transit. Encryption ensures that data is secure even if it is intercepted or accessed by unauthorized individuals.
- **Access Controls and User Permissions:** Implement robust access controls to restrict data access to authorized personnel only. Use role-based access control (RBAC) mechanisms to ensure that individuals can only access the data they need for their specific roles and responsibilities.
- **Data Sharing Agreements:** Establish clear data sharing agreements when sharing data with external entities. These agreements should outline the purpose of data sharing, specify security measures, and ensure compliance with privacy regulations.
- **Data Retention and Disposal:** Define retention periods for data and regularly review and securely dispose of data that is no longer necessary. Implement proper data disposal methods to prevent unauthorized access to discarded information.

# BEST PRACTICES

- **Secure Infrastructure and Network:** Implement robust security measures for the infrastructure and network supporting AI-enabled healthcare systems. This includes firewalls, intrusion detection systems, regular security updates, and monitoring mechanisms to detect and prevent unauthorized access or breaches.
- **Data Breach Response Plan:** Develop a comprehensive data breach response plan that outlines the steps to be taken in the event of a security incident. This plan should include procedures for notifying affected individuals, authorities, and relevant stakeholders, as well as strategies for mitigating the impact of the breach.
- **Compliance with Privacy Regulations:** Ensure compliance with relevant privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union or the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Understand the legal requirements and obligations related to data protection and privacy in the jurisdiction where the AI-enabled healthcare system is deployed.
- **Regular Security Audits and Assessments:** Conduct regular security audits and assessments to identify vulnerabilities, assess risks, and implement necessary security enhancements. Stay updated with emerging security threats and adopt best practices to address potential vulnerabilities.
- Data protection should be an ongoing priority throughout the lifecycle of AI-enabled healthcare systems. By implementing robust data protection measures, organizations can ensure the privacy and security of personal health information, build trust with patients, and comply with applicable privacy regulations.

## How Much Importance Does Privacy & Data Security Have in Healthcare?

# The Importance of Privacy And Data Protection



- **Patient Confidentiality:** Privacy safeguards in AI-enabled healthcare systems are essential to protect patient confidentiality. Maintaining patient confidentiality not only respects individuals' privacy rights but also fosters trust between patients and healthcare providers.
- **Data Security:** AI-enabled healthcare systems rely on the collection and storage of large volumes of patient data. Robust data security measures, including encryption, access controls, and secure storage and transmission protocols, are essential to protect against data breaches and ensure the integrity of patient information.
- **Regulatory Compliance:** Healthcare organizations must comply with data protection regulations, such as GDPR (in the European Union) and HIPAA (in the United States). Adhering to these regulations is not only a legal obligation but also helps ensure that patient data is handled securely, with appropriate consent, and in a manner that respects privacy rights
- **Preserving Public Trust:** Privacy breaches and data misuse can erode public trust in AI-enabled healthcare systems. Maintaining robust privacy and data protection measures is crucial to preserve public trust in the healthcare industry's adoption of AI technologies


# ANNUAL CONFERENCE

**ASSOCIATION OF MEDICAL COUNCILS OF AFRICA**

REGULATION IN THE ERA OF ARTIFICIAL INTELLIGENCE

Proudly Hosted By: HEALTH PROFESSIONS COUNCIL OF ZAMBIA

## REGULATION IN THE ERA OF ARTIFICIAL INTELLIGENCE

JACARANDA HUB

ENGAGE. INNOVATE. INSPIRE

# The Necessity of Regulatory Oversight

Given the heightened risks associated with AI in healthcare, regulatory oversight is more important than ever. Regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the

General Data Protection Regulation (GDPR) in Europe provide frameworks for protecting patient data.

However, these regulations must evolve to address the unique challenges posed by AI technologies across different regions

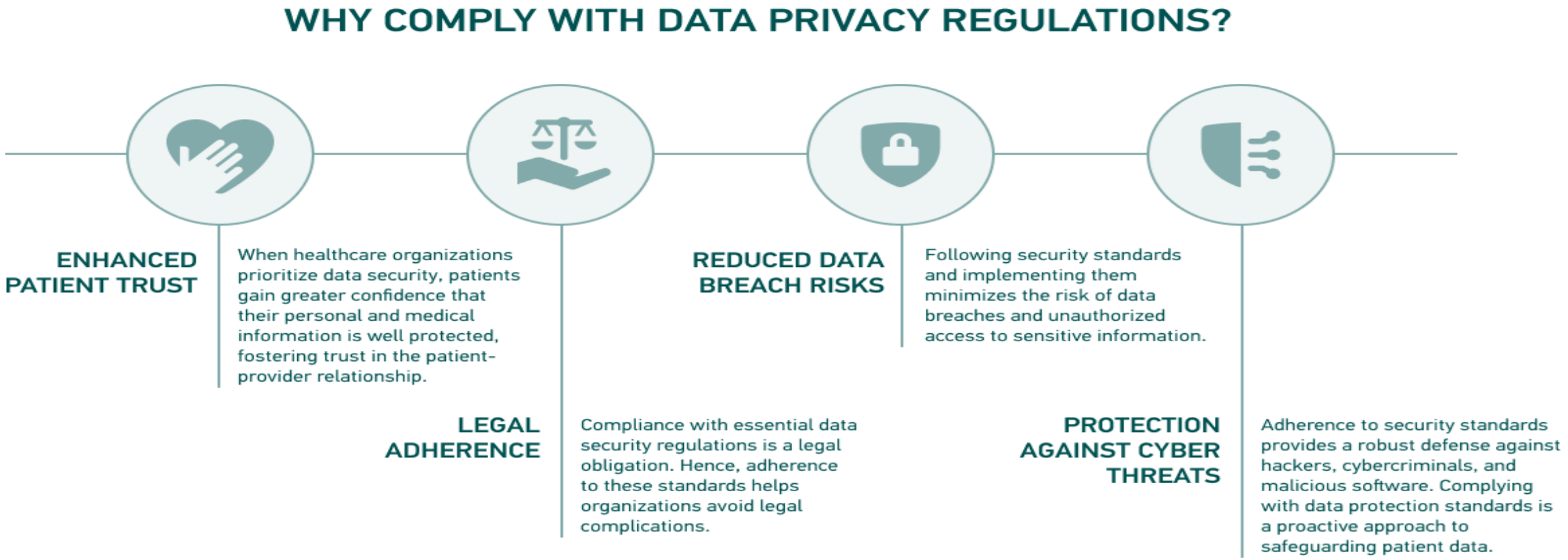
# Global Data Protection Standard



# Benefits of Adhering to Standards in Patient Data



Complying with health data privacy and protection standards offers numerous advantages for patients and healthcare providers. These standards are vital for ensuring the integrity, confidentiality, and accessibility of sensitive patient data. Here are the key benefits of such compliance:



## PRIVACY RULE

Entity should be responsible to keep the personal health records private

## SECURITY RULE

Must keep patient's file safe from any unauthorized access during transit and storage

## BREACH NOTIFICATION RULE

Have to inform affected individuals in case of a breach of unsecured patient information

## SAFETY RULE

Should protect identifiable PHI that can be used to analyze and improve the safety of patient

# Data Privacy and Security Challenges



# Challenges in attaining Data Privacy and Security



- One of the major challenges of healthcare data privacy is the protection of EHRs data.
- Wide use of EHRs cause the collection and transfer of a large amount of patient data. Unfortunately, not all systems are integrated with a supreme data protection mechanism. Moreover, poor access control via third-party applications also contributes to the list of data privacy issues in healthcare.
- Another concern of data privacy in healthcare is compliance with healthcare regulations, which require strict data protection measures, training personnel on the subject of data protection, and following robust security practices.
- Human error can also become a cause of healthcare data privacy violations. Accessing data via personal devices and sharing data with unauthorized individuals can cause much harm to both patients and healthcare providers. Hence, every healthcare organization requires basic data protection measures like a robust privacy and confidentiality protection plan, including measures like sensitive data encryption, regular backups, strict data access policies and monitoring, and regular data protection and privacy in healthcare training for personnel.
- Implementing a strict security plan and compliance with healthcare data privacy regulations are the best tools for overcoming data privacy challenges in the healthcare industry and protecting sensitive healthcare data.
- Sensitive data is personal information stored and used by healthcare providers. It includes medical histories, personal identification info (e.g., name, address, Social security number), laboratory test results, and other data that must remain confidential. Sensitive data disclosure can have severe consequences for healthcare actors.
- Unfortunately, the value of sensitive data makes it a tempting target for hackers and cybercriminals. In one of our previous articles on the importance of healthcare data security, we shared the concerning statistics of data breaches and theft of data from electronic health records. Along with other types of sensitive data, EHRs play a crucial role in healthcare.

# REGULATION IN THE ERA OF ARTIFICIAL INTELLIGENCE

ANNUAL CONFERENCE
ASSOCIATION OF MEDICAL COUNCILS OF AFRICA
REGULATION IN THE ERA OF ARTIFICIAL INTELLIGENCE
Proudly Hosted By: HEALTH PROFESSIONS COUNCIL OF ZAMBIA

JACARANDA HUB
ENGAGE. INNOVATE. INSPIRE

# Conclusion



- As AI continues to reshape the healthcare landscape, the importance of data privacy and security cannot be overstated.
- Regulators play a crucial role in enforcing the protocols necessary to protect patient data from misuse and unauthorized access. Healthcare organizations must also take proactive steps to secure their AI systems, ensuring that the benefits of AI are realized without compromising patient confidentiality.
- Implementing best practices for access controls, user permissions, regular audits, and monitoring is essential to safeguard sensitive data, ensure compliance with regulations, and maintain the trust of patients and stakeholders.
- It is crucial to establish a culture of security and privacy awareness, regularly assess and enhance security controls, and stay informed about emerging threats and regulatory changes.
- Continuous improvement and proactive measures will help organizations mitigate risks and protect the confidentiality, integrity, and availability of data in AI-enabled healthcare environments.
- Provide Change management capacitation to ensure adoption, adaption, adherence and end-user benefits
- In an era where data is one of the most valuable assets, safeguarding this data is paramount—not just for compliance, but for maintaining trust in the healthcare system and the technologies that are poised to transform it.

**Connect with Mara**:
Instagram: @MaraZhanet
LinkedIn: @MaraZhanet
Email: mara@jacarandahub.com
www.jacarandahub.org
www.nkwashoagro.com

# THANK YOU