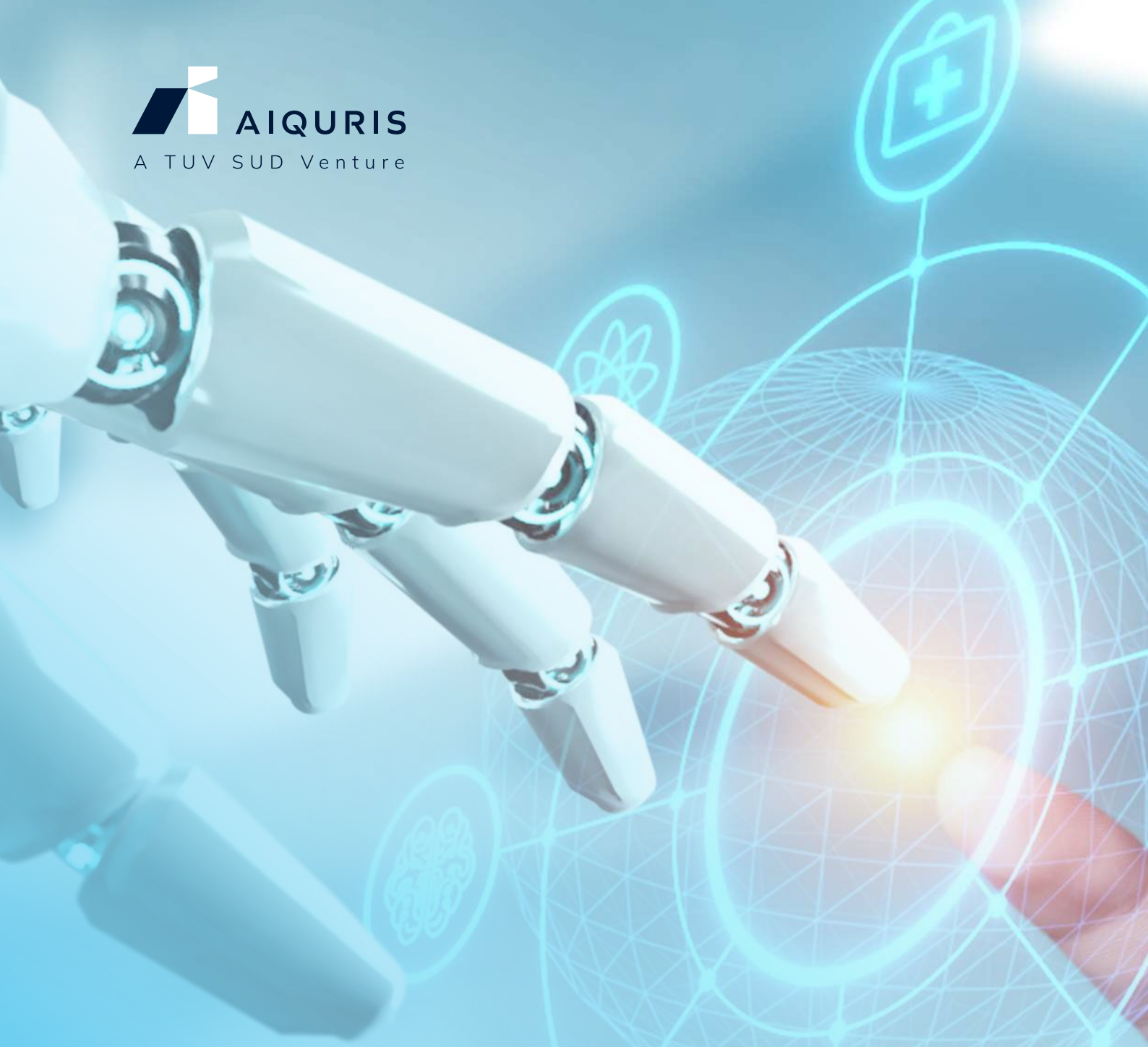
AIQURIS
A TUV SUD Venture



AIQURIS & DATA VACCINATOR

UNLOCKING THE POWER OF AI IN HEALTHCARE: Managing Data, Risk, and Compliance

WHITE PAPER DataVaccinator

CONTENTS

AUTHORS

KURT KAMMERER

CEO and Co-Founder of DataVaccinator

Kurt has developed health data sharing as a platform business. Leveraging the company's unique technology, he has been instrumental in creating offerings that combine local compliance with global reach. Kurt has worked in global markets throughout his career and drives the international expansion of DataVaccinator. He holds a Business and IT degree from the University of Karlsruhe.

DR. MARTIN SAERBECK

CTO and Co-Founder of AIQURIS

Dr. Saerbeck, with over 20 years of AI expertise, leads innovative solutions for the safe and efficient adoption of AI, including high-risk applications. He developed TÜV SÜD's AI Quality Framework and is a key figure in AI standardisation, holding roles with ISO/IEC, CEN/CENELEC, IEEE SA, and DIN. He holds a Master's and PhD in Computer Science.

DR. ANDREAS HAUSER

CEO and Co-Founder of AIQURIS

Dr. Hauser specialised in risk and quality management of AI systems. Previously, he headed Digital Service at TÜV SÜD, worked in research at Siemens and was a research associate at the University of Heidelberg. He began his career as a shipbuilding engineer. Dr Hauser holds degrees in Naval Architecture, Computer-Aided Engineering & a PhD in Applied Mathematics.

ABOUT

DataVaccinator

DataVaccinator "vaccinates data against abuse". We facilitate b2b health data exchange flows to help all stakeholders, from hospitals to pharma, benefit from healthcare ecosystems through better data that is ready for AI and smart automation. We hold 60 patents for secure data ecosystems as the foundation of our unique software. Based on our data exchange offerings, we strive to enable better healthcare and allow the stakeholders to monetise their data.

ABOUT

AIQURIS
A TUV SUD Venture

AIQURIS (AI·Quality·Risk) is a specialised platform that automates risk management and quality assurance for AI systems. Offering both one-time assessments and continuous monitoring, our solution ensures safety, compliance, and optimal performance while adapting to evolving regulations and AI use cases. Rooted in global standards and backed by TÜV SÜD's 150 years of excellence in testing, inspection, and certification (TIC), AIQURIS is the trusted partner for reliable AI adoption.

INTRODUCTION

Artificial intelligence (AI) has the potential to

REVOLUTIONISE HEALTHCARE BY IMPROVING DIAGNOSTICS, TREATMENT OPTIONS, AND OPERATIONAL EFFICIENCIES

However, for AI to reach its full potential in this sensitive industry, several critical challenges must be addressed. These challenges include ensuring the availability of high-quality data, adhering to complex regulatory frameworks, and managing the risks inherent in deploying AI systems.

Data is the lifeblood of AI, particularly in healthcare, where electronic health records and other sensitive information must be securely managed and used in compliance with strict privacy laws. Ensuring that this data is structured, accessible, and protected is essential for effective AI implementation. At the same time, robust risk management frameworks are needed to address potential threats such as bias, security vulnerabilities, and system performance failures.

This paper emphasises the role of Public-Private Partnerships (PPPs) in addressing these challenges. By combining governmental oversight with private sector innovation, PPPs provide a collaborative framework for managing health data ecosystems, ensuring regulatory compliance, and fostering safe AI adoption. Additionally, a structured approach to risk management, which includes the assessment, qualification, deployment, and monitoring of AI systems, is essential for minimising risks and ensuring the safe integration of AI into healthcare.

THE AI CHALLENGE IN HEALTHCARE

Healthcare manages the most sensitive category of data:

CITIZENS' ELECTRONIC HEALTH RECORDS

For AI to succeed in healthcare, several challenges must be overcome, including access to high-quality data and the complex web of regulations governing data use.

Governments must enforce data sovereignty with appropriate legislation while promoting practices that ensure the availability of high-quality health data. Without addressing these challenges, AI's full potential cannot be realised.

NO GOOD DATA, NO AI

It should go without saying that the quality of available data is a key factor for a successful AI. Still, this prerequisite must be emphasised as the current hype around AI silently assumes that good quality data is only waiting for AI algorithms to derive valuable insights. However, good quality data is a scarce resource, and for effective AI use, several conditions must be met:

WORKING WITH STRUCTURED AND UNSTRUCTURED DATA

While AI shall also overcome the hurdles that unstructured data brings about, AI will continue to be more effective the more structured the data is. As in traditional IT, it is beneficial for AI outcomes to work on a high portion of structured data.

WORKING WITH FEDERATED HEALTH DATA

Given the distributed nature of health data, healthcare AI will require processing data from different sources, such as healthcare organisations. While decentralised processing is a popular research topic that involves AI algorithms using various data sources and consolidating the outcomes, the more commonly used central model requires federated health data to be available in a central data lake or space for AI Processing.

ON DEMAND AVAILABILITY

AI in healthcare requires the availability of data on demand. As the sharing of (de-risked, i.e. anonymised, encrypted, etc) health data is growing, market mechanisms between data providers and data consumers will emerge.

WORKING WITH A COMMON DATA MODEL (E.G. OMOP)

The Observational Medical Outcomes Partnership (OMOP) is a common data model for organising healthcare data from various sources. The OMOP data model ensures that federated data is structured in a coherent way, thereby facilitating the application of AI. Other formats like HL7/ openEHR/ FHIR are also commonly used and help increase the structure in health data.

PROVIDING HIGH-QUALITY DATA THROUGH AFFORDABLE, REPLICABLE PROCESSES

Making high-quality data available on demand is essential for insights that shall be drawn from ever-changing real world data. Data that is up-to-date at any time requires a high degree of automation, both for reasons of quality and affordability.

USE OF DATA ACROSS THE AI SYSTEM LIFE CYCLE

Effective data management is crucial at every stage of the AI system life cycle—training, inference, and output. Each stage presents unique challenges and requires careful handling to ensure the system remains accurate, reliable, and compliant.

TRAINING DATA

The quality of training data directly affects AI performance. In healthcare, incomplete or biased data can lead to harmful predictions. Ensuring diverse, representative, and clean data is essential to avoid these risks. Proper versioning and tracking of training configurations support transparency and accountability.

INFERENCE DATA

AI systems rely on real-time data to make accurate decisions. To maximise effectiveness, data must be structured according to standardised models such as OMOP (Observational Medical Outcomes Partnership) or HL7/ openEHR/ FHIR, which ensure compatibility and interoperability between different healthcare systems. Federated health data, drawn from various sources like hospitals or research institutions, must be processed in a secure and structured way, either through centralised data lakes or decentralised processing systems. Strict access control is essential to protect against unauthorised use or adversarial attacks. Continuous monitoring and regular updates to the model ensure that the AI remains accurate and adaptable to new healthcare data.

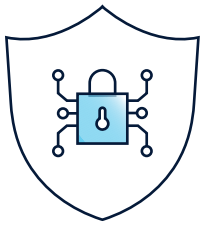
AI OUTPUT DATA

Human oversight is necessary to monitor AI outputs, especially in healthcare, where errors in decisions can have significant consequences. Compliance with regulations ensures that AI outputs are transparent and auditable. Ethical considerations, such as avoiding bias, are essential to safe AI deployment.

COMPLIANCE & AI REGULATION

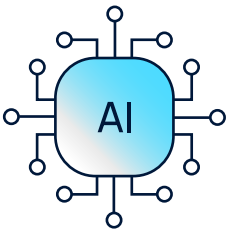
Governments are increasingly regulating AI to mitigate potential risks while unlocking opportunities for innovation.

In healthcare, AI must navigate the balance between access to personal health records and protecting privacy. While AI may have access to personal health data, de-identified records should be the primary focus for processing.



DATA REGULATION

AI systems must comply with stringent data privacy regulations, such as GDPR. This includes ensuring transparency, gaining user consent, and addressing challenges like the removal of incorrect PII from AI models. Compliance with standards like the EU Data Act ensures seamless data sharing while protecting privacy.



AI REGULATION

AI-specific regulations, including the EU AI Act, assess the risks of AI systems, especially in healthcare, a high-risk sector. These regulations address risks such as bias, discrimination, and performance failures. AI systems must be auditable and transparent, and their outputs must be explainable.

LEVERAGING PUBLIC-PRIVATE PARTNERSHIPS (PPP) STRUCTURES FOR AI

To prevent regulation from stifling AI innovation, governments and private organisations must collaborate through Public-Private Partnerships (PPPs). PPPs provide a promising model for managing health data ecosystems. Governments must enforce data sovereignty, while private organisations focus on enabling data sharing within regulatory constraints. This collaboration ensures both innovation and compliance, creating a balanced ecosystem for AI in healthcare.

PPP USE CASE: HEALTH DATA EXCHANGE

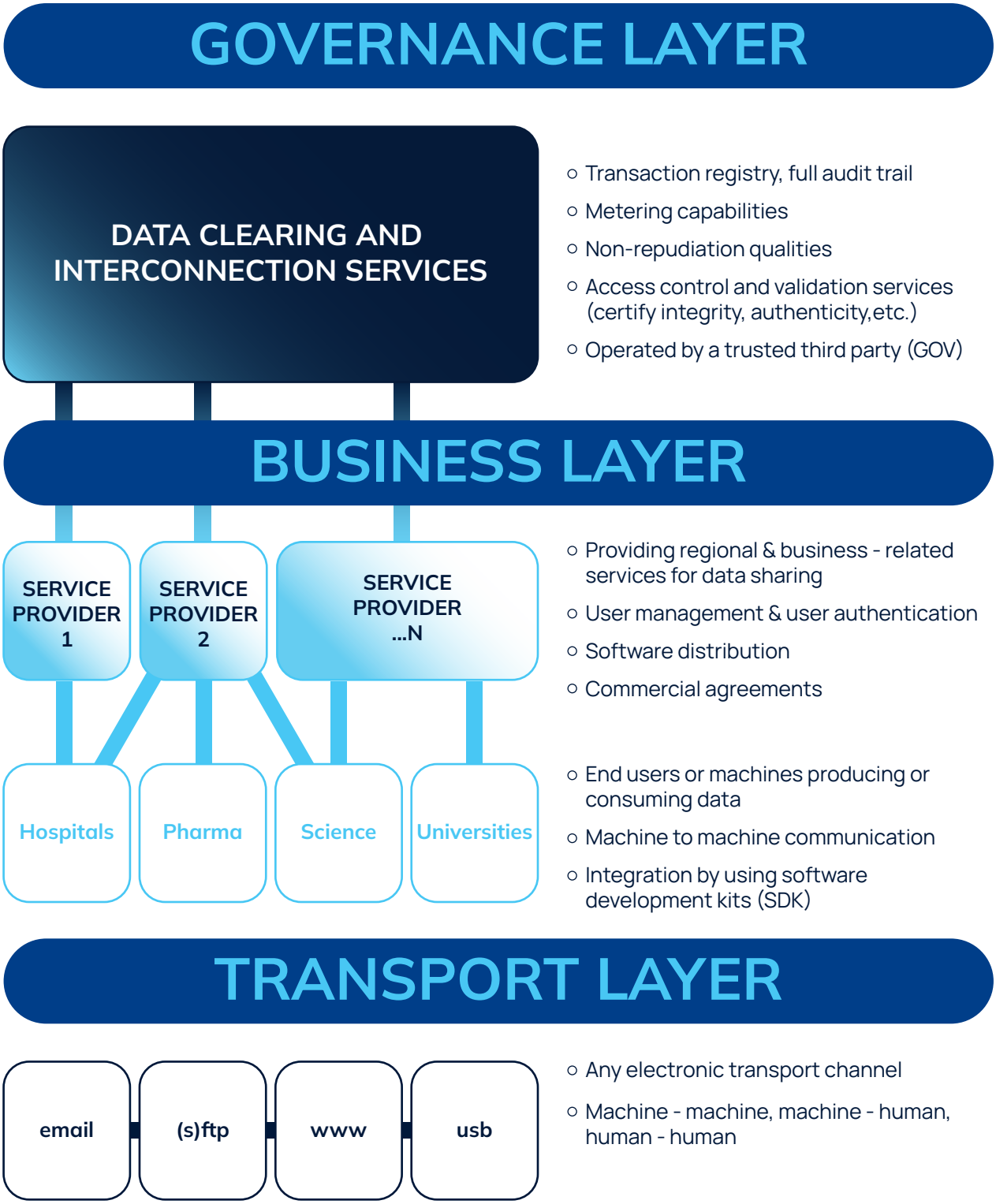
One of the most promising applications of Public-Private Partnerships (PPPs) in healthcare AI is the management of health data exchanges. In this model, governments take on the role of governing and facilitating the secure flow of data between healthcare organisations, research institutions, and private enterprises, ensuring that sensitive health data is managed in a compliant and transparent manner.

In a typical use case, a government entity (e.g., Ministry of Health or Department of Health) operates a data clearing and interconnection service. This service acts as a hub that grants access to eligible parties—such as hospitals, pharmaceutical companies, research laboratories, insurers, and even general practitioners—while also retaining the ability to revoke access when necessary. The clearing service manages only metadata, ensuring the protection of the sensitive health data itself, which flows securely between authorised parties.

This architecture ensures that data sovereignty is maintained, as the health data remains under the jurisdictional control of its origin, while facilitating secure end-to-end communication over any agreed-upon digital channels (e.g., encrypted email, secure FTP, or APIs). The system supports regional and business-related services for data sharing, allowing healthcare providers and other entities to share valuable health data within a framework that adheres to both national and international regulations.

The governance layer within the architecture ensures complete oversight and security, providing features such as a transaction registry for full audit trails, metering capabilities, non-repudiation qualities, and access control validation services that certify the integrity and authenticity of each transaction. The data clearing service is operated by a trusted third party, typically a government body, which guarantees that all data exchanges are compliant with regulatory standards and protect the privacy of the individuals involved.

Figure 1. - Illustrates the secure flow of health data within a Public-Private Partnership (PPP) structure. In this model, a data clearing and interconnection service governs the exchange of metadata between eligible parties (e.g., hospitals, pharmaceutical companies, research institutions). The actual health data flows end-to-end through secure, agreed-upon digital channels, ensuring that the data is handled according to both privacy regulations and jurisdictional requirements.



The governance layer ensures full audit trails, non-repudiation, and access control, all operated by a trusted third party, typically a government entity. This structure allows multiple service providers to interact in a secure environment while maintaining data sovereignty and safeguarding sensitive health information. By managing the data exchange through this layered architecture, the PPP ensures both compliance and operational flexibility in a complex health data ecosystem.

MANAGING THE RISK & QUALITY OF AI ADOPTION

AIQURIS provides automated, holistic risk identification and tailored quality requirements, ensuring AI use cases are safe, secure, compliant, ethical, and high-performing, along the AI life cycle.

PROFILE
Initiation

- Conduct comprehensive AI risk profiling of AI use case
- Determine risk consequences
- Specify quality requirements

Establish a solid foundation for integrating AI with minimised risk

ASSESS
Development/Procurement

- Assess provider capabilities and organisations' readiness
- Profile residual risks of AI solution and providers
- Select provider and set terms

Make confident, legally secure, procurement decisions

DEPLOY
Implementation

- Establish monitoring tools and metrics
- Facilitate a smooth transition to monitoring
- Confirm system readiness for continuous oversight

Ensure the AI system is ready for effective, continuous monitoring

MONITOR
Operation

- Monitor risk exposure and quality
- Track changes in regulation, AI solution and use case, and organisational readiness

Maintain compliance and performance with active oversight

CONCLUSION

Public-Private Partnerships (PPPs) are crucial for the

SAFE AND EFFECTIVE DEPLOYMENT OF AI IN HEALTHCARE

By combining governmental oversight with private sector innovation, these collaborations can ensure the availability of high-quality data while maintaining compliance with stringent privacy regulations. A structured approach to risk management, involving the assessment, qualification, deployment, and continuous monitoring of AI systems, is key to minimising potential risks and maximising the benefits of AI-driven healthcare solutions.

By fostering collaboration between government and private entities, the healthcare sector can navigate the complexities of AI adoption, promoting both innovation and safety. Through structured governance and risk management frameworks, AI can be responsibly integrated into healthcare, unlocking its transformative potential while safeguarding data security, patient safety, and regulatory compliance.

AIQURIS

A TUV SUD Venture

WHITE PAPER DataVaccinator

www.aiquris.com