

AI and Quantum Research Center (AIQRC), Asia University, Taiwan

Activities

Asia University and AIQRC, supported by the Ministry of Education's Taiwan Global Pathfinders Grant Program, provide Taiwan students with world-class experiential learning opportunities through programs in IBM quantum technologies, UCLA academic exchange, quantum finance, humanoid robotics, and astronaut mission training.



(A) IBM dream program



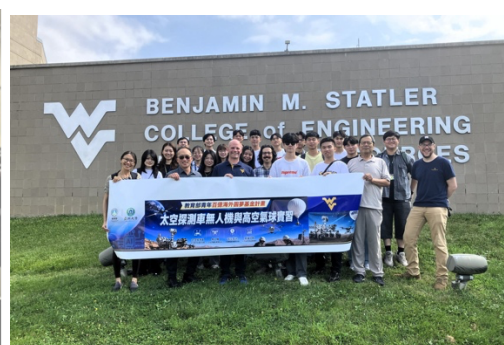
(B) UCLA elite program



(C) Quantum finance program



(D) Humanoid robot program



(E) Astronaut mission training program

Prepared and Edited by

Ka-Lok Ng ^{1,2}

Deputy Director ¹ & Distinguish Professor ²

¹ [AI and Quantum Research Center \(AIQRC\)](#),

² [Department of Bioinformatics and Medical Engineering](#), Asia University, Taiwan

Quantum-Native Channels for Multi-Institutional Federated Clinical AI: An Open Problem in Lifetime Confidentiality

Background

Multi-institution precision medicine is often framed as a governance problem, resolved once institutions agree on data-sharing terms. It is increasingly also a confidentiality-lifetime problem. Federated learning allows

institutions to train jointly without centralizing raw patient data, but the privacy-preserving mechanisms commonly layered on top of their secure aggregation, homomorphic encryption, multiparty computation, rely on classical cryptographic assumptions that are not designed to hold indefinitely.

NIST’s transition guidance identifies the practice of collecting encrypted data now for future decryption once quantum computing matures as a primary reason the shift to post-quantum cryptography (PQC) is urgent.¹ A healthcare-focused review reaches the same conclusion: because clinical and genomic data must remain confidential for many years, Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and National Institute of Standards and Technology (NIST) jointly urge healthcare organizations to complete cryptographic inventories and quantum-readiness plans well before quantum-capable adversaries emerge.² NIST addressed part of this problem in August 2024, finalizing FIPS 203 (ML-KEM, key encapsulation), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA, digital signatures) lattice- and hash-based algorithms designed to resist both classical and quantum cryptanalysis.³ The NSA's Commercial National Security Algorithm Suite 2.0 sets a comparable 2030 deadline for algorithm replacement in national-security systems, with comparable regulatory pressure emerging across regulated commercial sectors.⁴ These standards protect the message itself, but not what federated learning transmits beyond it: model gradients and intermediate representations that can carry statistical information about underlying patient data even over a properly encrypted channel. Closing that gap securing what a transmission reveals, not only the transmission itself is the problem three recent preprints address by moving privacy protection into the communication substrate.

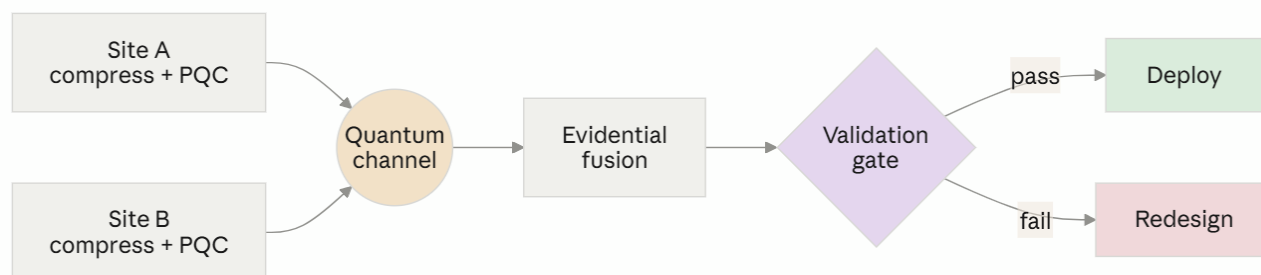


Figure 1 | Quantum-secured federated pipeline

Compression and MPC-secured aggregation occur locally at each site⁵; compressed states cross a quantum channel via teleportation;⁶ fusion occurs at the server through a non-parametric evidential circuit;⁷ and a four-endpoint gate comparative accuracy, communication cost, adversarial resistance, cryptographic readiness is proposed here as the standard to clear before deployment. The dashed PQC fallback layer in Figure 1 is this correspondence's own proposed addition, intended to let the architecture degrade gracefully to classical post-quantum security if a quantum channel is unavailable; it has not been implemented in any of the cited work.

Yamauchi et al. compress client-side medical image data through Matrix Product State and Tree Tensor Network representations before any quantum encoding, combined with MPC-secured aggregation and a post-aggregation quantum refinement step a design chosen because direct quantum encoding of raw, high-dimensional medical images is not feasible at current qubit counts⁵.

Kamei et al. motivate quantum federated learning for healthcare through its resistance to harvest-now-decrypt-later attacks, and separately introduce structured light-cone feature selection to reduce the communication overhead and channel noise that otherwise limit quantum federated learning's practicality⁶.

Luo et al. address vertical federation institutions holding different feature types (for example, clinical records at one site and molecular data at another) on overlapping patients mapping local features into quantum states, transmitting them by quantum teleportation, and fusing them at a central server with a non-parametric evidential circuit; this method achieved lower approximation error than classical alternatives under limited quantum resources across image-classification and other datasets⁷. An earlier framework combining quantum feature encoding with supervised contrastive learning, using classical communication channels, reported accuracy gains of up to 25% points over quantum cross-entropy baselines on medical imaging data⁸. A separate 5G-integrated quantum-assisted diagnosis algorithm demonstrated that quantum-assisted aggregation can synchronize model updates across distributed clinical devices without disrupting real-world device operation⁹.

Application

This architecture applies wherever separate institutions hold complementary, non-overlapping patient data that cannot be lawfully pooled but is jointly needed for a single prediction task for example, one site holding clinical or phenotypic records and another holding genomic, imaging, or laboratory data on an overlapping patient population. This vertical-federation structure is common in multi-site precision-medicine research, rare-disease consortia, and cross-institutional biomarker or diagnostic studies. The proposed PQC fallback layer would extend the architecture's relevance beyond quantum-capable settings, allowing an institution without quantum communication hardware to participate through a classical fallback once that layer is built and tested, while institutions with quantum access use the teleportation-based channel.

Broader adoption would benefit from evaluation on genuinely independent, multi-institutional clinical datasets and from direct comparison against classical, NIST-compliant post-quantum-encrypted federated learning under matched compute budgets. That comparison would clarify whether the quantum communication layer contributes a capability a well-implemented classical pipeline could not, or whether its main value lies elsewhere for example, in the physical rather than purely computational nature of its privacy guarantee.

Collaboration is sought from quantum communication engineering, applied cryptography, and clinical biostatistics to design and run that comparison: testing accuracy, communication rounds to convergence, and resistance to gradient-inversion and membership-inference attacks, evaluated against both the architecture in Figure 1 and its best available classical post-quantum-encrypted counterpart, on real multi-site clinical data held under existing institutional data-sharing agreements.

References

1. National Institute of Standards and Technology, NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards (Gaithersburg, MD: NIST, 2024).
2. "Post-Quantum Cryptography for Healthcare: Securing Medical Data, Connected Devices, and Digital Health Infrastructure," *Frontiers in Health Services* (2026).

3. National Institute of Standards and Technology, FIPS 203 (Module-Lattice-Based Key-Encapsulation Mechanism Standard), FIPS 204 (Module-Lattice-Based Digital Signature Standard), FIPS 205 (Stateless Hash-Based Digital Signature Standard) (Gaithersburg, MD: NIST, August 2024).
4. “Quantum-Safe: Bridging the Post-Quantum Production Gap with a Hybrid-by-Default Python Cryptography Library,” arXiv:2605.17061 (2026).
5. H. Yamauchi, A. P. K. Dalskov, H. Kawaguchi, and R. Van Meter, “Quantum-Enhanced Processing with Tensor-Network Frontends for Privacy-Aware Federated Medical Diagnosis,” arXiv:2604.01616 (2026).
6. S. Kamei, H. Kawaguchi, and T. Satoh, “Practical Quantum Federated Learning for Privacy-Sensitive Healthcare: Communication Efficiency and Noise Resilience,” arXiv:2603.03853 (2026).
7. H. Luo, Z. Zhai, Q. Zhou, J. Qi, Y. Deng, and X. Wang, “Evidential Quantum Vertical Federated Learning,” arXiv:2603.21102 (2026).
8. A. Kottahachchi Kankanamge Don and I. Khalil, “Q-VFL: Quantum-Enhanced Vertical Federated Learning with Contrastive Encoding for Privacy-Preserving Medical AI,” Quantum Machine Intelligence, vol. 8, article 44 (2026).
9. A. R. Camara Araujo, O. D. Okey, M. Saadi, P. Adasme, R. Lopes Rosa, and D. Zegarra Rodríguez, “Quantum-Assisted Federated Intelligent Diagnosis Algorithm with Variational Training Supported by 5G Networks,” Scientific Reports, vol. 14, article 26333 (2024).

Prepared by

Eskezeia Y. Dessie^{1, 2}, PhD

¹AI and Quantum Research Center (AIQRC), Asia University, Taichung, Taiwan

²Indiana University School of Medicine, Indianapolis, IN, USA

LINKEDIN: <https://www.linkedin.com/in/eskezeiadessie/>

RCID: <https://orcid.org/0000-0001-9194-5816>

GOOGLE SCHOLAR: <https://scholar.google.com/citations?user=NHxBY1EAAAAJ&hl=en>



AI and Quantum Research Center (AIQRC)

Room A110, Asia University, No. 500, LiuFeng Rd., WuFeng Dist., Taichung City 41354 Taiwan.

Email: qphys.qcomp@gmail.com Office: 04-23323456 ext. 6631

Web: <https://quantum.asia.edu.tw/>