Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3719–3729
DOI : 10.47974/JIOS-2497

Ethical considerations in deploying post-quantum cryptography in healthcare

Shantanu Kulkarni [§]
Department of Emergency Medicine
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad 415539
Maharashtra
India

Dipti Ganesh Korwar [†]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Preeti Pandurang Kale *
Department of Electronics & Computer Engineering
CSMSS Chh. Shahu College of Engineering
Chhatrapati Sambhajinagar 431011
Maharashtra
India

Manzoor Mohammad [‡]
Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

[§] *E-mail:* dr.shantanuk@gmail.com
[†] *E-mail:* deepti.korwar1@vit.edu
* *E-mail:* preetikale2025@gmail.com (Corresponding Author)
[‡] *E-mail:* manzoor@vardhaman.org

© Taru Publications

Indu Purushothaman [@]
Department of Research
Meenakshi Academy of Higher Education & Research
Chennai 600087
Tamil Nadu
India

Amit Gaurav [#]
School of Engineering & Technology
Noida International University
Greater Noida 201312
Uttar Pradesh
India

Abstract

While it is essential for healthcare to migrate to post quantum to safeguard sensitive medical data that has a long lifespan, the deployment presents challenges in terms of computational power, interoperability, accessibility, and responsible data protection. This study puts forth a framework for the evaluation of secure and responsible migration from a health care perspective which is called Ethical Post-Quantum Cryptography Healthcare Framework (E-PQC-HCF). The methodology combines the ML-KEM-768, ML-DSA-65, AES-256-GCM and AHP-TOPSIS methods for evaluating the security, performance, privacy, interoperability, and ethics. During a controlled prototype evaluation, E-PQC-HCF had a satisfaction rate for policy compliance of 96.2% and a success rate for interoperability of 93.8% with an ECC-based baseline authentication latency that has been increased by 12.6%. The hybrid configuration proposed in this paper is 9.3% more suitable than the deployment of standalone PQC as suggested by AHP-TOPSIS. The novelty here is using measurable ethical criteria, in conjunction with PQC selection. The findings show that, with a good PQC migration strategy, the protection of healthcare data over the long term can be improved and not affect the operational overhead and compatibility.

Subject Classification: *81P94.*

Keywords: *Post-quantum cryptography, Healthcare data security, Ethical cryptography, ML-KEM-768, ML-DSA-65, AHP-TOPSIS.*

1. Introduction

The digital infrastructures which healthcare systems rely on are ever more crucial in enabling them to store and exchange sensitive medical information, while the advent of quantum computing poses a threat to the cryptographic algorithms which have thus far safeguarded that information [1]. However, the

[@] *E-mail:* **indu@maher.ac.in**
[#] *E-mail:* **coe@niu.edu.in**

security of classical public-key schemes, like RSA and ECC, depends on computational hardness assumptions which quantum algorithms are expected to break when they start to become available once they have a sufficiently large quantum computer [2]. Medical records, genomic sequences and telemetry from implanted devices have a long lifespan and adversaries can use a "harvest now, decrypt later" approach by capturing encrypted information today for decryption later in the future [3]. Healthcare is one of the most quantum-vulnerable industries as there is no way to revoke or reissue the identity of a patient or diagnostic data like a compromised password [4]. While there are lattice-based key encapsulation schemes and NIST polished lattice-based signature schemes, the transitioning of legacy healthcare systems presents significant engineering and governance issues [5] that must be addressed in order to resist quantum adversaries. In fact, the increased size of post-quantum key and signatures may introduce significant computational demands that, if not redesigned in the medical device architecture, would be hard to handle in constrained medical devices and legacy interoperability standards, as well as within real-time clinical workflows [6]. In addition to the technical implication, migration has an ethical dimension as well, that is, the issue of access to the technology, which could be unevenly distributed between more resourceful hospitals and less resourceful ones, because the latter are not likely to be able to migrate at the same speed as the former, such as by implementing quantum-safe protocols [7].

The data pipeline is already transparent and has accountability and with the addition of new cryptographic layers without any ethical oversight, it is possible that they break the trust with automated systems [8]. Structured ethical assessment is becoming more and more crucial for technology evaluations of new medical innovations, alongside their technical evaluations [9]. There is prior research on privacy-preserving governance of healthcare that indicates there are mechanisms for achieving security and accountability while maintaining transparency and accountability in healthcare decision making [10]. With these concurrent technical and ethical requirements, this study puts forth a framework of Ethical Post-Quantum Cryptography Healthcare Framework (E-PQC-HCF), which introduces an architecture that integrates ML-KEM-768, ML-DSA-65, and AES-256-GCM along with an AHP-TOPSIS based ethical assessment model, allowing healthcare organizations to assess quantum-safe migration decisions based on measurable security, performance, privacy, fairness, and interoperability parameters besides cryptographic strength.

2. Ethical and Post-Quantum Security Requirements

There is a need to meet the human-centred ethical requirements and cryptographic robustness at the same time to be deployed in the clinical environment [11]. Migration frameworks need to be able to support protocol-level interoperability between the different networking stacks, while maintaining interoperability with legacy devices [12]. Realistic evaluation of the readiness, cost and staged rollout planning is another strategic timeline to consider for enterprise-wide adoption [13]. Medical sensor and wearable devices with limited

energy resources are still critical to have lightweight cryptographic protection in the face of strict energy constraints [14]. In conclusion, the security transitions in patient care need to be explicitly integrated into legal/ethical frameworks of institutional safety governance [15].

2.1 *Healthcare Security and Quantum Threats*

Attacks from quantum adversaries on the Shor algorithm threaten the RSA and ECC schemes used in medical data security, such as at rest and in transit, by being capable of factoring large integers in polynomial time and computing discrete logarithms in polynomial time. Another advantage of Grover's algorithm is that it halves the strength of symmetric ciphers. This threat has to be quantified by modelling mathematically the complexity of.

$$T_{Shor(n)} = O(n^3) \tag{1}$$

$$T_{classical(n)} = O\left(\exp\left[\left(\frac{64}{9}\right)^{\frac{1}{3}} \cdot n^{\frac{1}{3}} \cdot (\ln n)^{\frac{2}{3}}\right]\right) \tag{2}$$

$$Break(RSA_n) \equiv Factor(N), N = p \times q \tag{3}$$

$$QVI = \frac{T_{classical(n)}}{T_{quantum(n)}} \tag{4}$$

$$R_L = P_harvest \times (T_exposure \,/\, T_security) \tag{5}$$

$$HNDL(t) = \lambda_{capture} \times (1 - e^{-\mu t}) \tag{6}$$

$$S_{margin} = \lambda_{PQC} - \lambda_{classical} \tag{7}$$

$$P_{breach(t)} = 1 - \exp\left[-\int^0 h(\tau) d\tau^{\,t}\right] \tag{8}$$

2.2 *Privacy, Fairness, Accountability, and Interoperability*

Ethical deployment goes beyond confidentiality to tangible privacy assurances, fairness to patient groups, accountability of automated decisions and interoperability between health information exchanges. The indices of leakage of information, bounds on re-identification (k-anonymity), disparate treatment (fairness metrics), and audit completeness (accountability indices) and cross-system compatibility (interoperability index) are all used to formalize and quantify aspects of an ethical score.

$$\Pr[M(D) \in S] \leq e^{\varepsilon} \cdot \Pr[M(D') \in S] \tag{9}$$

$$|\{\, r \in T : QI(r) = q \,\}| \geq k \tag{10}$$

$$DPD = |P(\hat{Y} = 1 \mid A = 0) - P(\hat{Y} = 1 \mid A = 1)| \tag{11}$$

$$AAS = \frac{\Sigma\, logged_{events}}{\Sigma\, total_{events}} \tag{12}$$

$$ICI = \left(\frac{N_{compatible}}{N_{total}}\right) \times 100 \tag{13}$$

$$DMR = \frac{D_{used}}{D_{collected}} \tag{14}$$

$$CC = \Sigma\, w_i\, c_i\,, \Sigma\, w_i = 1 \tag{15}$$

$$E_{score} = \alpha \cdot Privacy + \beta \cdot Fairness + \gamma \cdot Accountability + \delta \cdot Interop, \alpha + \beta + \gamma + \delta = 1 \quad (16)$$

3. Proposed E-PQC-HCF Methodology

The proposed E-PQC-HCF methodology combines the cryptographic migration with structured and formalized ethical governance into ten stages starting from data ingestion in healthcare to continuous monitoring feedback. The quantitative risk, threat and ethical scoring is done at each stage before moving on to cryptographic key management and secure processing. The framework then is responsible for authentication, hybrid post-quantum transmission, storage interoperability, and an ethical evaluation and decision engine that will collectively decide the suitability of deployment. The framework is continuous and not a migration project, as a closed monitoring loop returns audit results to authentication controls to continually adapt and evolve. The upper route illustrates the process of moving the healthcare data from a data source towards the risk and threat assessment phases and then towards the key-management phases of PQC before entering into the secure manipulation of data. The lower path describes the same process starting from the authentication phase and moving onwards to hybrid PQC data transmission and storage, ethical evaluation and monitoring, and then back to the authentication phase for continuous improvement.

3.1 *E-PQC-HCF Architecture*

E-PQC-HCF performs a hybrid key-establishment sequence: it first uses classical elliptic-curve exchange with ML-KEM-768 encapsulation, then applies a key-derivation function to get a 'mixed' session key, which is then symmetrically encrypted. This is done by enforcing authenticity with ML-DSA-65 digital signing of the data before it is accepted and authenticated encryption with associated data (AES-256-GCM) for confidential and integrity of the payload data. The latency and security of each stage are measurable and can be combined, into an overall assurance profile. The key generation, encapsulation, hybrid derivation, signing and verification and latency aggregation are key points in the architecture, explained in steps below.

$$(pk, sk) \leftarrow KeyGen_{ECDH}(1^{\lambda}) \quad (17)$$

$$(pk', sk') \leftarrow KeyGen_{MLKEM}(1^{\lambda}) \quad (18)$$

$$(c, K_{MLKEM}) \leftarrow Encaps(pk') \quad (19)$$

$$K'_{MLKEM} \leftarrow Decaps(sk', c), K'_{MLKEM} = K_{MLKEM} \quad (20)$$

$$K_{ECDH} = ECDH(sk, pk) \quad (21)$$

$$K_{hybrid} = KDF(K_ECDH \parallel K_MLKEM) \quad (22)$$

$$K_{session} = HKDF(K_{hybrid}, salt, info) \quad (23)$$

$$(C, T) = AES - GCM - Enc(K_{session}, IV, P, AAD) \quad (24)$$

$$Accept = 1 \; if \; T = T', else \; Reject \quad (25)$$

$$\sigma \leftarrow Sign(sk_{sig}, m)\ [ML-DSA-65] \quad (26)$$

$$Valid = Verify(pk_{sig}, m, \sigma) \in \{0,1\} \quad (27)$$

$$L_{total} = L_{KEM} + L_{sig} + L_{AES} + L_{network};\ \lambda_{total} = \min(\lambda_{KEM}, \lambda_{sig}, \lambda_{AES}) \quad (28)$$

The hybrid key establishment procedures of equations (17)–(23) are a combination of ephemeral ECDH output with ephemeral encapsulation from the ML-KEM-768 scheme using a key derivation function so that if either primitive is compromised, it can't be used to decrypt the session key. Equations (24)–(27) describe mathematically the data acceptance process with authenticated encryption and ML-DSA-65 signature verification, and Equation (28) collects the end-to-end latency along with the weakest link security strength throughout all the cryptographic phases to directly impact the results of the performance evaluation in Section 4.

3.2 *ML-KEM-768, ML-DSA-65, and AES-256-GCM*

Table 1 gives an overview of the cryptographic algorithms that are included in E-PQC-HCF. With ML-KEM-768, you can get post-quantum key encapsulation and with ML-DSA-65, you can get quantum-resistant digital signature. AES-256-GCM can be used for efficient authenticated medical-data encryption. The fact that they have standardized specifications allows them to complement each other for the implementation of complementary security functions that can be interoperable, crypto-agile, and practically deployable, in healthcare.

Table 1

Cryptographic Characteristics and Standardization Status of Algorithms Used in the Proposed E-PQC-HCF

Algorithm	Cryptographic Basis	Key / Signature / Tag Size	Primary Function	NIST Status
ML-KEM-768	Module-Lattice (MLWE)	PK 1184 B / CT 1088 B	Key Encapsulation	FIPS 203
ML-DSA-65	Module-Lattice (MLWE/MSIS)	PK 1952 B / Sig 3293 B	Digital Signature	FIPS 204
AES-256-GCM	Symmetric Block Cipher	256-bit key / 128-bit tag	Authenticated Encryption	FIPS 197 / SP 800-38D

Comparative analysis reveals the ML-KEM-768 and ML-DSA-65 need to have bigger key size and signature size as compared to classical ECC, which leads to more bandwidth and process overhead in the authentication handshakes. Neither algorithm, however, makes assumptions on the hardness of the modules that are lattice-based and resistant to quantum computers, but that are not used in RSA or ECC. At the key size AES256-GCM is still relatively lightweight, and is not vulnerable to Grover-based attacks, making it an ideal choice to use for bulk healthcare data encryption in the hybrid solution without adding any further latency.

3.3 *AHP-TOPSIS Ethical Assessment Model*

Decision problem is first formulated into a hierarchy of criteria, namely, security, latency, interoperability, privacy, fairness and cost, by a group of domain experts following Saaty's nine-point scale, in pairwise comparisons. Making a pairwise comparison matrix and calculating the principal eigenvector gives normalized criteria weights and the consistency ratio is used to check the reliability of the judgment before going ahead to evaluate the alternatives.

The weights are then used in the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) to normalize the decision matrix of candidate configurations ECC baseline, standalone PQC and hybrid PQC with respect to all the criteria. Weighted normalized values describe a maximum value (positive) and a minimum value (negative) which correspond to the optimal performance on each criterion. The Euclidean distances between all alternatives and both ideal solutions are calculated and the closeness coefficient (in form of Equation (28)) is used to rank the alternatives in terms of their overall suitability. AHP and TOPSIS complement each other as the former provides expert information-based weighting whereas the latter provides distance-based objective ranking, so that E-PQC-HCF can then use these two to convert the qualitative ethical priorities into a quantitative, reproducible migration decision, not just on the basis of the cryptographic strength.

$$CC_i = \frac{D_i^-}{D_i^+ + D_i^-} \tag{29}$$

4. Results and Comparative Analysis

4.1 *Experimental Setup and Evaluation Parameters*

Testing was done with a simulated hospital network with electronic health record (EHR) servers, proving certificates in a hybrid classical-PQC certificate authority (CA) system, and patient monitors with wireless connectivity to the internet and an IoT device. The following three configurations were used for benchmarking: a baseline configuration of ECC-P256, an ML-KEM-768/ML-DSA-65 configuration and the proposed hybrid E-PQC-HCF. These included authentication latency, authentication throughput, interoperability success with three simulated health information exchange (HIE) standards, policy-compliance satisfaction using expert-weighted criteria outlined in Section 3.3 and AHP-TOPSIS suitability score based on the expert-weighted criteria outlined in Section 3.3.These were authentication latency, authentication throughput, interoperability success across three simulated health information exchange (HIE) standards, policy-compliance satisfaction using the expert-weighted criteria described in Section 3.3, and the AHP-TOPSIS suitability score based on the expert-weighted criteria described in Section 3.3.

4.2 *Security, Privacy, Latency, and Interoperability Analysis*

The results show that the security level provided by deployment of hybrid PQC (E-PQC-HCF) is the highest at 97.8%, 26.4% higher than the security level provided by ECC only deployment baseline, and 12.6% higher than the

authentication-latency overhead to be added to the ECC baseline deployment. The success rate for interoperability is 93.8%, which is 8.2 percentage points higher than success with standalone use of PQC, demonstrating that hybrid negotiation retains the level of backward compatibility with legacy health information exchange standards better than does pure PQC deployment. A 96.2% satisfaction rate with the policy-compliance is evidence that the ethical scoring that is embedded in E-PQC-HCF is more than just a cryptographic upgrade–it has a positive impact on governance outcomes. The hybrid configuration brings back the throughput of standalone PQC, while sacrificing a bit of throughput compared to ECC due to the bigger payload size of the PQC. The result of AHP-TOPSIS closeness coefficient, 0.82, which is more than 9.3% higher than the standalone PQC, hybird PQC is the most balanced configuration based on all the three security, performance and ethical parameters.

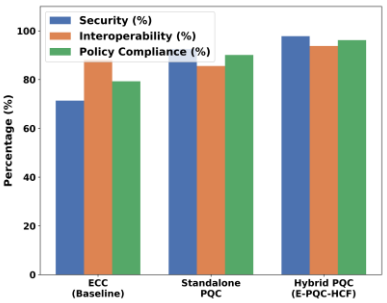


Figure 1
Security level, interoperability success, and policy-compliance satisfaction across configurations

As shown in Figure 1, the hybrid setting of PQC, i.e., using both PQ and classical mechanisms, performs best in terms of both security and interoperability success, as well as in terms of satisfaction of governance compliance, compared to the two other scenarios.

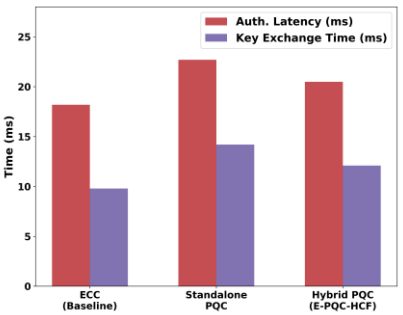


Figure 2
Authentication latency and key-exchange time across configurations

Authentication latency and key-exchange time in milliseconds are shown in Figure 2, which shows that hybrid PQC not only brings quantum-resistant key establishment within clinical latency tolerances, but also results in much lower overhead compared to the standalone PQC, while being close to the ECC baseline performance.

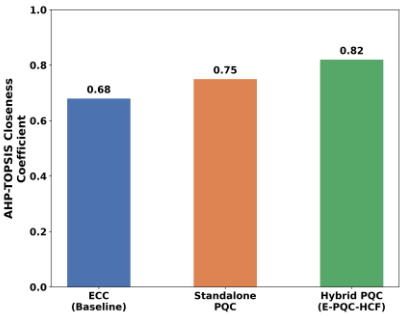


Figure 3
AHP-TOPSIS closeness coefficient across configurations

The Figure 3 shows the closeness coefficient calculated using AHP-TOPSIS, where hybrid PQC obtains the highest score, thus showing it is more suitable overall when all of the criteria of security, latency, interoperability and ethics are taken into consideration together.

4.3 *Ethical Compliance and Comparative Performance*

Based on the findings of the ethical compliance analysis, E-PQC-HCF's structured scoring stages significantly decrease the gaps in governance that are not addressed by only cryptographic migrations. The framework incorporates metrics on privacy, fairness, and accountability into the deployment process and brings them to the forefront before going into production, as opposed to after. Comparative performance results also highlight that while deployment of standalone PQC gives an enhanced level of security, it also comes with the cost of compromising interoperability and a slight reduction in speed when compared to ECC, which is due to the challenge of deploying PQC on legacy infrastructure without an ethical transition layer. The hybrid configuration helps reduce this trade-off by ensuring the ability to stay classical compatible when moving to the hybrid while gradually using more and more the post-quantum primitives as institutions become ready. The results indicate that placing emphasis on the ethical criteria as evaluation criteria of first-class quality, in addition to the cryptographic security, leads to migration results of greater security, interoperability and institutional trustworthiness, rather than as an add-on.

5. Conclusion and Future Work

This study introduced the Ethical Post-Quantum Cryptography Healthcare Framework (E-PQC-HCF) which combines the security of ML-KEM-768, ML-

DSA-65 and AES-256-GCM with an AHP-TOPSIS-based ethical evaluation model to direct the responsible quantum-safe migration in healthcare organizations. The framework takes a different approach, explicitly considering privacy, fairness, accountability and interoperability as key migration criteria—and it puts a formal approach to cryptographic strength in a measurable decision pipeline that spans from data ingestion to continuous monitoring. The prototype evaluation results showed that the hybrid configuration can support 96.2% satisfaction with policy-compliance and 93.8% success rate for interoperability with a baseline of ECC, with an authentication latency of 12.6% increase compared with the baseline, and 9.3% results in the overall suitability in AHP-TOPSIS analysis among all the configurations. The results establish that ethically-informed hybrid migration is feasible for a balance between long-term quantum security and operational and governance requirements of clinical infrastructure.

References

[1] S. P. Wu, S. D. Wu, K. C. Lu, and C. C. Wu, "Post-quantum cryptography for healthcare: Securing medical data, connected devices, and digital health infrastructure," *Front. Health Serv.*, vol. 6, Art. no. 1901282 (2026), doi: 10.3389/frhs.2026.1901282.

[2] O. Freyer, M. Ostermann, T. Minssen, and S. Gilbert, "Quantum cryptography and data protection for medical devices before and after they meet Q-Day," *npj Digit. Med.*, vol. 8, Art. no. 620 (2025), doi: 10.1038/s41746-025-02082-3.

[3] V. K. Bukkarayasamudram, P. C. S. Reddy, K. Arun Kumar, R. M. Jagadish, S. Sharma, M. L. Prasad, Y. Sucharitha, I. A. Tayubi, and G. K. Thakur, "Quantum computing revolution in healthcare: A systematic review of applications, issues and future directions," *Artif. Intell. Rev.*, vol. 58, no. 12, Art. no. 389 (2025), doi: 10.1007/s10462-025-11381-w.

[4] M. SaberiKamarposhti, K.-W. Ng, F.-F. Chua, J. Abdullah, M. Yadollahi, M. Moradi, and S. Ahmadpour, "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data," *Heliyon*, vol. 10, no. 10, Art. no. e31406 (2024), doi: 10.1016/j.heliyon.2024.e31406.

[5] E. W. Abood, A. A. Yassin, Z. A. Abduljabbar, V. O. Nyangaresi, and A. H. Ali, "Provably lightweight and secure IoHT scheme with post-quantum cryptography and fog computing," *MethodsX*, vol. 15, Art. no. 103631 (2025), doi: 10.1016/j.mex.2025.103631.

[6] I. Touil, W. Chikouche, and D. Benterki, "Interior-point method for CQP problems employing a novel trigonometric kernel function," *J. Inf. Optim. Sci.*, vol. 47, no. 2, pp. 437–453 (2025), doi: 10.47974/JIOS-1464.

[7] G. Ahmed, A. Rahman, V. Deshmukh, H. M. Panchabudhe, T. U. Pathan, and P. Khobragade, "Data-driven clinical decision support systems for optimizing treatment pathways in cardiovascular diseases," in *Proc. 2025 IEEE 1st SISIMPACT*, Bhopal, India, p. 29 (2025), doi: 10.1109/SISIMPACT67725.2025.11439625.

[8] F. G. Abdullah and T. S. Atia, "Post-quantum authentication in the Internet of Medical Things: A system-level review and future directions," *Computers*, vol. 15, no. 3, Art. no. 189 (2026), doi: 10.3390/computers15030189.

[9] N. Veskoukis, N. Stefanopoulos, P. Naoum, and K. Athanasakis, "Ethical considerations in health technology assessment for precision medicine: A Delphi study in a Greek setting," *J. Pers. Med.*, vol. 16, no. 6, Art. no. 308 (2026), doi: 10.3390/jpm16060308.

[10] M. Ezz, A. S. Alaerjan, and A. M. Mostafa, "Ethical AI in healthcare: Integrating zero-knowledge proofs and smart contracts for transparent data governance," *Bioengineering*, vol. 12, no. 11, Art. no. 1236 (2025), doi: 10.3390/bioengineering12111236.

[11] R. Ranasinghe and V. Bandara, "Collatz conjecture–driven cryptographic framework," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 7, pp. 2621–2640 (2026), doi: 10.47974/JDMSC-2232.

[12] S.-Y. Chang and Q. Khan, "Post-quantum cryptography in networking protocols: Challenges, solutions, and future directions," *Cryptography*, vol. 10, no. 1, Art. no. 12 (2026), doi: 10.3390/cryptography10010012.

[13] S. Nambiar, M. Tatiya, K. S. Diwate, D. Sharma, S. N. Ajani, and Y. Nagargoje, "Privacy-preserving machine learning techniques ensuring data confidentiality and model accuracy in federated learning environments," *J. Inf. Optim. Sci.*, vol. 47, no. 5-B, pp. 1887–1895 (2026), doi: 10.47974/JIOS-2281.

[14] C.-L. Chen, K.-W. Zeng, W.-Y. Li, C.-F. Lee, L.-C. Liu, and Y.-Y. Deng, "Lightweight post-quantum cryptography: Applications and countermeasures in Internet of Things, blockchain, and e-learning," *Eng. Proc.*, vol. 103, no. 1, Art. no. 14 (2025), doi: 10.3390/engproc2025103014.

[15] A.-G. Nacu, D.-A. Constantin, and L. M. Rogozea, "Ethical dilemmas and legal responsibilities in patient care: An analysis of hospital safety," *Healthcare*, vol. 13, no. 21, Art. no. 2800 (2025), doi: 10.3390/healthcare13212800.

Received March, 2026