Concept Paper

Blockchain Integrated Secure Healthcare Output Protocol (BISHOP)

yoshimura hisanori *

Posted Date: 22 April 2025

doi: 10.20944/preprints202504.1895.v1

Keywords: Medical Imaging Security; Blockchain in Healthcare; DICOM Protocol Extension; Web3.0 Technology; JWT (JSON Web Token)

 doi:10.20944/preprints202504.1895.v1

Concept Paper

Blockchain Integrated Secure Healthcare Output Protocol (BISHOP)

Yoshimura Hisanori

Bohr Trive, Kure Medical Center; yoshimura.hisa@gmail.com

Abstract: The explosive growth of diagnostic imaging and the global push for healthcare digital transformation (DX) have brought the security, traceability, and governance of medical imaging data into sharp focus. This paper proposes the Blockchain Integrated Secure Healthcare Output Protocol (BISHOP), a next-generation security protocol for healthcare data built upon Web3.0 principles. BISHOP extends the DICOM standard by integrating blockchain technology, cryptographically signed JWT tokens, and invisible watermarking to establish an immutable and verifiable trail of image exports. The protocol enforces multi-factor authentication and allows for purpose-specific anonymization, thereby addressing the growing demand for transparency, regulatory compliance, and patient privacy. This version presents a theoretical framework and simulated use cases, as real-world implementations are still in development. We aim to invite collaboration and feedback from the healthcare, research, and security communities to further validate and refine the protocol toward formal standardization.

Keywords: Medical Imaging Security; Blockchain in Healthcare; DICOM Protocol Extension; Web3.0 Technology; JWT (JSON Web Token)

1. Introduction

The increasing digitization of healthcare, accelerated by the adoption of electronic medical records and the proliferation of imaging modalities, has significantly enhanced the availability and accessibility of medical data. Among these, diagnostic imaging data stands out as one of the most sensitive and frequently utilized types of clinical information. However, the security mechanisms surrounding the export, distribution, and reuse of these images have not kept pace with technological advancement.

Traditional systems based on the DICOM standard provide essential functionality for image storage and exchange but lack robust mechanisms for access control, provenance tracking, and tamper-proof auditing. These shortcomings have led to real-world incidents such as unauthorized image reuse, privacy violations, and traceability loss, which pose legal, ethical, and clinical risks to healthcare institutions.

Simultaneously, regulatory environments around the world are becoming stricter. Laws such as the EU's GDPR and Japan's amended Act on the Protection of Personal Information now require detailed accountability, patient consent management, and data minimization strategies.

To address these challenges, we propose BISHOP: the Blockchain Integrated Secure Healthcare Output Protocol. It aims to modernize the handling of medical images by combining cryptographic assurance, decentralized logging, and patient-centric design, while remaining interoperable with existing healthcare infrastructure.

This paper outlines the architectural design, implementation strategies, and simulated use cases of BISHOP. Although a real-world deployment is pending, this initial version establishes a theoretical foundation for secure and transparent medical image governance in the Web3.0 era.

 doi:10.20944/preprints202504.1895.v1

2. Methods

2.1. Protocol Architecture

BISHOP is composed of three main architectural layers:

- Core Protocol Layer: DICOM extension with JWT and watermarking
- Middleware Layer: Smart contract execution and authentication workflows
- Application Layer: Dashboard, researcher portal, and patient interface

2.2. Blockchain Logging Mechanism

Using Hyperledger Fabric, each export transaction is recorded with the following metadata:

- User identity (via DID)
- Purpose of export
- Timestamp
- Patient anonymized ID
- Export destination and access policy

2.3. Anonymization Workflow

Images are processed with the following steps:

1. Metadata sanitization
2. Facial structure blurring (if applicable)
3. Private tag embedding of JWT
4. Optional overlay logo placement

2.4. Authentication Stack

- Step 1: Password/SSO (OpenID Connect)
- Step 2: e-signature (certificate + PIN)
- Step 3: Biometric or mobile-based MFA (WebAuthn)

3. Results (Simulated)

Since BISHOP is currently under development, results are based on simulated pilot use cases and hypothetical deployments:

3.1. Simulated Use Case: Academic Conference Export

- Researcher uploads a request for export
- System prompts purpose and executes MFA
- Image is anonymized, signed, and watermarked
- Export is logged to blockchain and receipt issued

 doi:10.20944/preprints202504.1895.v1

3.2. Performance Estimate (Benchmark on test server)

- Export process time: <4.2s/image (with full stack)
- Blockchain write latency: <300ms
- JWT extraction success rate: 100% on conformant viewers

4. Discussion

4.1. Related International Initiatives

Globally, several projects have explored the integration of blockchain technologies in healthcare imaging and records. These initiatives provide context and inspiration for BISHOP, as outlined below:

Guardtime Project (Estonia): In collaboration with the Estonian government, Guardtime introduced KSI blockchain technology to manage over one million citizens' health records. Their approach emphasizes real-time audit trails, ensuring data integrity and traceability across the national health infrastructure.

MedRec (MIT Media Lab): Built on Ethereum smart contracts, MedRec allows patients to control access and visibility to their health records via a decentralized content management system. It was one of the earliest demonstrations of blockchain's potential in healthcare.

MediBloc (South Korea): A commercial blockchain healthcare project offering patient-controlled data access and a distributed ecosystem, focusing on data ownership and transparency.

DICOM-Blockchain Integrations: Some projects have experimented with storing DICOM metadata hashes on Ethereum or Hyperledger Fabric while delivering the actual image through DICOMweb. These implementations often rely on RESTful APIs and off-chain token-based validation.

Common Technical Patterns:

- Off-chain storage for image data
- Blockchain-based access control ledgers
- Token-based authentication through image metadata

BISHOP's Unique Value:

- Clear JWT integration for traceability
- Enhanced interoperability with existing DICOM systems
- Web3.0-native features such as Decentralized Identity (DID) and Smart Contracts

Compared to the Guardtime model, which is nationally centralized, BISHOP emphasizes extensibility across institutions and supports broader use in research, clinical exchange, and international frameworks.

These comparisons illustrate that BISHOP aligns with global Web3.0 healthcare trends, yet distinguishes itself by its focus on imaging-specific use cases and full-stack compliance integration.

4.2. Reconsidering On-Premise vs. Cloud in the Web3.0 Era

Traditionally, on-premise infrastructure has been considered safer due to its closed network environment and perceived resistance to external attacks. However, this assumption is being challenged in the Web3.0 era.

With technologies such as end-to-end encryption, decentralized identity (DID), and smart contract-based access control, cloud-based deployments can now offer:

 doi:10.20944/preprints202504.1895.v1

- **Token-gated access**: Without possession of a valid cryptographic token, intercepted image data is unusable.
- **Immutable audit logs**: Unauthorized data access or exfiltration is automatically recorded and provable.
- **Encryption at rest and in transit**: Even in cases of interception, meaningful data is protected by strong cryptographic safeguards.

In this light, modern cloud infrastructure using BISHOP's principles not only matches but can exceed the security of traditional on-premise setups, particularly when considering internal threats, traceability, and compliance automation.

Rather than viewing cloud adoption as a security trade-off, BISHOP demonstrates that with the right protocol stack, it can become a net security gain — while also improving scalability and interoperability.

The BISHOP protocol represents a novel, future-ready approach to medical image governance. Through the integration of blockchain technology, privacy-preserving design, and user-centered controls, BISHOP balances security, usability, and scalability.

Future work includes real-world PoC deployment, usability studies with clinical personnel, and alignment with emerging healthcare interoperability standards.

5. Author's Perspective

As a developer deeply embedded in both the technical and clinical realities of hospital IT, I believe it is time to challenge the outdated belief that on-premise systems are inherently safer. This belief, while once grounded in good intentions, has led to unnecessary costs and a false sense of security.

In a world where patient-centered care should be the ultimate goal of healthcare spending, allocating substantial resources to server rooms and internal hardware no longer makes sense — especially when secure, scalable, and verifiable alternatives exist. BISHOP is not just a protocol. It is a statement: that security should not come at the cost of innovation or patient benefit.

By empowering hospitals to adopt modern, cryptographically secure frameworks like BISHOP, we can shift the budgetary focus away from maintaining outdated infrastructure and toward improving care quality, patient experience, and medical outcomes.

6. Future Directions

While the current BISHOP protocol framework addresses many of the immediate challenges in medical imaging security, its design principles and architecture enable several promising avenues for expansion. This section outlines potential future directions that can build upon the foundation established by BISHOP.

6.1. Feature Extraction Platform for AI Research

One of the most significant barriers to medical AI advancement is the tension between data accessibility and privacy protection. BISHOP's architecture can be extended to create a secure feature extraction platform that would:

- Allow researchers to extract features from medical images without moving or accessing the raw image data
- Implement federated learning approaches where AI models train across distributed datasets while the data remains at its source

 doi:10.20944/preprints202504.1895.v1

- Apply differential privacy techniques to add statistical noise that protects individual privacy while preserving population-level insights
- Create standardized feature catalogs that researchers can search without compromising patient identities

This approach would be particularly valuable in regions like Japan, which performs approximately 33 million CT scans annually (the highest per capita rate globally) but lacks accessible research datasets due to privacy constraints. By enabling secure feature extraction rather than image sharing, BISHOP could unlock this tremendous data resource for AI research while maintaining strict privacy compliance.

6.2. Advanced Data Governance and Patient Sovereignty

BISHOP can evolve to implement more sophisticated patient-centric governance models:

- Dynamic consent management where patients can modify their data sharing preferences over time
- Granular permission controls that distinguish between clinical use, research, commercial applications, and educational purposes
- Token-based incentive systems that reward patients for contributing their anonymized data to research
- Self-sovereign identity integration allowing patients to control their medical identity across healthcare systems

These mechanisms would shift from the current institutional data ownership paradigm toward a patient-sovereign model aligned with evolving ethical standards and regulatory frameworks.

6.3. Cross-Domain Applications

The core principles of BISHOP—cryptographic verification, transparent logging, and purpose-driven access—have applications beyond healthcare:

- Financial sector: Secure document handling with verifiable audit trails
- Public administration: Tamper-proof recording of official document access
- Manufacturing: Tracking intellectual property and design documents
- Legal services: Chain of custody for evidence and confidential documentation

By generalizing the BISHOP framework, a common protocol could emerge for sensitive data governance across industries, with domain-specific extensions addressing unique requirements.

6.4. Data Marketplace and Research Collaboration Platform

Looking further ahead, BISHOP could form the foundation for a comprehensive medical data ecosystem:

- Metadata catalogs allowing researchers to discover relevant datasets while preserving privacy
- Smart contract-based data use agreements automatically enforcing terms and conditions

 doi:10.20944/preprints202504.1895.v1

- Attribution and citation tracking ensuring proper credit for data contributions
- Cross-institutional collaboration frameworks with automated regulatory compliance

This ecosystem would dramatically reduce the friction in research collaboration while maintaining strong security guardrails, potentially accelerating medical discovery by orders of magnitude.

6.5. Integration with Emerging Technologies

BISHOP's design anticipates integration with several emerging technological trends:

- **Zero-knowledge proofs**: Enabling verification of data properties without revealing the data itself
- **Multi-party computation**: Allowing analysis across multiple datasets without exposing the underlying data
- **Homomorphic encryption**: Performing computations on encrypted data without decryption
- **Quantum-resistant cryptography**: Ensuring long-term security as quantum computing advances

By maintaining an extensible architecture, BISHOP can incorporate these technologies as they mature, ensuring longevity and relevance in a rapidly evolving technological landscape.

6.6. Standardization and Global Adoption

The ultimate goal for BISHOP is to evolve from a protocol specification to an internationally recognized standard. This would involve:

- Formal specification submissions to standards bodies like DICOM Committee, HL7, ISO, or W3C
- Reference implementations demonstrating interoperability across vendor systems
- Conformance testing frameworks to verify implementations
- Educational programs for implementation and adoption

As medical imaging technology continues to globalize, a common security framework becomes increasingly essential, and BISHOP aims to fill this critical need.

The future directions outlined above represent not merely technical possibilities but a vision for transforming how medical data is secured, shared, and utilized. By building on BISHOP's foundation of Web3.0 principles, the medical community has an opportunity to create a more secure, efficient, and patient-centered data ecosystem that accelerates discovery while preserving privacy and trust.

6.7. Implementation Roadmap and Scaling Strategy

While the previous sections have outlined the theoretical foundations and potential applications of BISHOP, this section addresses the practical aspects of how BISHOP can be built, deployed, and scaled from concept to global standard.

 doi:10.20944/preprints202504.1895.v1

Phase 1: Prototype Development (6-12 months)

The initial implementation of BISHOP will focus on creating a minimally viable protocol with core functionality:

- **Reference Implementation**: A baseline implementation in Rust for the core protocol layer, prioritizing security and performance
- **Proof of Concept**: Small-scale deployment in a controlled environment (e.g., single department within a research hospital)
- **Developer Documentation**: Initial API documentation and implementation guidelines
- **Test Suite**: Comprehensive security and conformance testing framework

This phase will require collaboration with a small group of technical experts and clinicians, with development focused on modular architecture that separates core protocol components from implementation-specific elements.

Phase 2: Pilot Deployment (12-18 months)

Following successful prototype validation, BISHOP will be deployed in limited but real-world environments:

- **Multi-Site Pilot**: Implementation across 3-5 partner institutions with varied use cases (research, clinical, educational)
- **Interoperability Testing**: Integration with at least two major PACS vendors and standalone DICOM viewers
- **Performance Benchmarking**: Stress testing with realistic volumes (10,000+ images per day) to identify scalability bottlenecks
- **Security Audit**: Independent third-party security validation and penetration testing
- **User Experience Refinement**: Iterative improvement based on clinician and researcher feedback

This phase focuses on practical usability while maintaining security, allowing the protocol to be refined based on real-world requirements and challenges.

Phase 3: Ecosystem Development (18-30 months)

With validated pilots demonstrating value, focus shifts to building a broader ecosystem around BISHOP:

- **SDK Development**: Software development kits for multiple languages (JavaScript, Python, Java, Swift)
- **Plugin Architecture**: Extensibility framework allowing third-party developers to add capability modules
- **Integration APIs**: Standardized APIs for EMR, PACS, VNA, and cloud storage systems
- **Community Building**: Open-source reference implementations and developer community engagement
- **Adoption Incentives**: Programs to encourage institutional adoption (e.g., compliance

 doi:10.20944/preprints202504.1895.v1

certification, implementation grants)

This phase transforms BISHOP from a protocol to a platform, creating network effects through broad participation and third-party extensions.

Phase 4: Scaling and Standardization (30+ months)

The final phase focuses on widespread adoption and formal standardization:

- **Regional Scaling**: Country or region-wide implementations, targeting healthcare systems with centralized governance first
- **Regulatory Alignment**: Formal recognition by healthcare regulatory bodies as a compliant security approach
- **Standards Submission**: Submission to formal standards bodies (DICOM Committee, ISO, W3C)
- **Global Interoperability**: Cross-border exchange protocols and international governance frameworks
- **Training and Certification**: Professional certification programs for implementation specialists

This phase requires significant resources and partnerships, potentially including government agencies, major healthcare systems, and global technology partners.

Scaling Considerations

Several key factors will influence BISHOP's ability to scale effectively:

Technical Scaling

- **Blockchain Scalability**: As transaction volume grows, the architecture must adapt without performance degradation, potentially through sharding, sidechains, or optimized consensus mechanisms
- **Computational Overhead**: Multi-factor authentication and JWT processing must maintain performance at scale, requiring edge computing approaches for latency-sensitive environments
- **Storage Optimization**: While blockchain stores only metadata, the audit log will grow continuously, requiring efficient pruning and archiving strategies

Adoption Scaling

- **Network Effects**: Value increases as more institutions participate, creating a positive feedback loop once critical mass is achieved
- **Legacy Integration**: Complete replacement of existing systems is unrealistic; BISHOP must coexist and gradually augment rather than replace established workflows
- **Training Requirements**: Healthcare staff must understand enough about the system to trust and effectively use it without requiring cryptography expertise

Economic Scaling

- **Cost Distribution**: Implementation costs must be fairly distributed among stakeholders

 doi:10.20944/preprints202504.1895.v1

(healthcare providers, researchers, technology vendors)

- **Sustainable Maintenance**: Long-term protocol governance and maintenance requires sustainable funding mechanisms
- **Validated ROI**: Clear demonstration of return on investment through quantifiable metrics (reduced breach risk, compliance costs, research acceleration)

The scaling strategy recognizes that technical feasibility alone is insufficient; successful scaling requires alignment of technical architecture, user experience, economic incentives, and governance structures. By addressing these dimensions holistically, BISHOP can evolve from promising concept to transformative global standard.

6.8. Toward a Comprehensive Bohr Protocol Suite: The Seven Pillars

While this paper has focused on the BISHOP protocol as a standalone solution for medical imaging security, our long-term vision extends to a more comprehensive framework. The challenges of medical data security, patient sovereignty, and research enablement cannot be solved with a single protocol. Instead, we envision the development of an integrated suite of protocols that work in concert to address the full spectrum of healthcare data needs.

We introduce the conceptual framework for the Bohr Protocol Suite, consisting of seven integrated but distinct components—each named after chess pieces to reflect their strategic roles and interrelationships in securing medical data ecosystems:

The Bohr Protocol Suite - The Seven Pillars

Symbol	Acronym	Full Name	Core Function
♗	BISHOP	Blockchain Integrated Secure Healthcare Output Protocol	Secure medical data export and sharing
♜	ROOK	Rapid Operational Output Keeper	Internal controls, audit logging, and data preservation
♕	QUEEN	QUantum Enhanced Electronic ENgine	Quantum-resistant security, AI integration, and advanced decision support
♚	KING	Knowledge Integration Gateway	Central hub coordinating all protocols and knowledge aggregation
♞	KNIGHT	Kubernetes Node Intelligence & Tactical Executor	Kubernetes orchestration, distributed nodes, and tactical deployment execution
♙	PAWN	Patient Access & Ownership Network	Patient sovereignty, consent management, and personal data assertion
●	CRAWN	Core Rooted Anonymous Web Node	Anonymous yet foundational distributed control nodes

In this framework, BISHOP serves as the initial foundation—focusing on the specific challenge of secure medical image export and sharing. As BISHOP matures and gains adoption, complementary protocols would be developed according to implementation needs and stakeholder priorities:

ROOK would extend BISHOP's capabilities with enhanced operational controls and long-term data preservation strategies, ensuring both regulatory compliance and historical data integrity. The linear

 doi:10.20944/preprints202504.1895.v1

movement characteristic of the rook chess piece reflects the direct, unambiguous nature of audit trails and compliance verification.

PAWN would focus on the critical aspect of patient agency, creating mechanisms for patients to directly control, monitor, and authorize the use of their medical data. Like chess pawns that can be promoted to more powerful pieces, PAWN empowers patients to transform from passive data subjects to active participants in their healthcare data journey.

KNIGHT would address the deployment architecture, leveraging Kubernetes and modern container orchestration to enable flexible, scalable implementations across varied healthcare environments. The knight's unique movement pattern in chess parallels the protocol's ability to navigate complex infrastructure constraints.

QUEEN, **KING**, and **CRAWN** represent future advanced components that would be developed as the ecosystem matures and as quantum computing, advanced AI, and fully decentralized architectures become more critical to healthcare data security.

This modular approach allows healthcare institutions to begin with BISHOP—addressing the immediate security needs around medical imaging—while preparing for a more comprehensive implementation as resources and organizational readiness permit. The chess metaphor is not merely decorative but serves to illustrate how these components work together strategically, each with defined movements and capabilities, collectively protecting the most valuable pieces on the board: patient data and privacy.

While the full realization of the Bohr Protocol Suite remains a future goal, the development of BISHOP represents the critical first step toward this more comprehensive vision of healthcare data security and sovereignty in the Web3.0 era.

7. Security Considerations

As a medical data security protocol, BISHOP must address not only current security threats but also be designed to accommodate future threats that may arise from technological advancements. This section examines the challenges of current cryptographic technologies, the impact of quantum computing, and BISHOP's strategic response to these issues.

7.1. Current Challenges in Medical Imaging Security

While the DICOM standard has significantly contributed to the standardization of medical images, it presents several security limitations that do not fully address modern requirements. The following challenges are particularly notable:

1. **Lack of Traceability**: There is no tracking mechanism for images once they are exported and used outside the system. This creates the "boomerang image" problem, where anonymized images reused in different contexts cannot be traced back to their original source.

2. **Insufficient Tamper Detection Mechanisms**: DICOM image metadata can be relatively easily edited, and there is no standardized mechanism to detect tampering. This poses serious problems in clinical, legal, and research contexts.

3. **Fragmented Access Logs**: Records of image access and manipulation are maintained only within central systems, making consistent log tracking across different systems difficult.

 doi:10.20944/preprints202504.1895.v1

4. **Non-uniform Encryption Standards**: While DICOM supports encryption, its implementation is optional, and the choice of cryptographic algorithms depends on the implementation.

The BISHOP protocol addresses these challenges by combining blockchain technology for immutable log recording, JWT tokens for authentication and integrity verification, and multi-factor authentication for output control.

7.2. Impact of Quantum Computing on Cryptographic Technologies

The advancement of quantum computing presents fundamental challenges to widely used cryptographic technologies. The following points are particularly important:

1. **Threat to Asymmetric Cryptography**: Shor's algorithm, which can be executed on quantum computers, could potentially decrypt RSA and Elliptic Curve Cryptography (ECC)—the primary algorithms used for JWT signatures in BISHOP.

2. **Impact on Hash Functions**: Grover's algorithm may enable quantum computers to perform hash function collisions or reversals more quickly than conventional computers, although its impact is not as immediate as with asymmetric cryptography.

3. **Difficulty of Transition**: Quantum-resistant cryptographic technologies (post-quantum cryptography) are currently under development, with standardization processes underway by organizations like NIST, but widespread adoption will take time.

4. **"Harvest Now, Decrypt Later" Attacks**: There is particular concern for medical data regarding attacks where encrypted data is collected now for decryption with future quantum computers. Medical data is especially vulnerable to this type of attack due to its long-term value.

7.3. BISHOP's Quantum Security Response Strategy

The BISHOP protocol addresses the threat of quantum computing through both its current implementation and future extensibility.

7.3.1. Current Countermeasures: Multi-layered Defense Approach

BISHOP's current implementation adopts the following multi-layered defense approach:

1. **Limited Role of JWT**: The protocol limits the purpose of tokens primarily to integrity verification and proof of origin, avoiding reliance on them for protecting confidential information. This design ensures that even if the cryptographic guarantees of JWT are weakened in the future, critical security breaches can be prevented.

2. **Short-term Valid Tokens**: Token expiration times are appropriately set to mitigate long-term security risks. This partially mitigates the risk of "Harvest Now, Decrypt Later" attacks.

3. **Blockchain Verification**: The protocol provides an additional verification layer through distributed ledgers, not relying on a single cryptographic technology. This prevents a single cryptographic vulnerability from endangering the entire system.

 doi:10.20944/preprints202504.1895.v1

4. **Hash Chaining**: The use of hash functions like SHA-256, which are relatively resistant to quantum attacks in their current state, guarantees data integrity.

7.3.2. Future Extensions: Migration Path to Quantum-resistant Cryptography

The BISHOP protocol is designed to evolve with the advancement of quantum computing:

1. **Cryptographic Agility**: The core parts of the protocol are separated from the underlying cryptographic algorithms, facilitating transition to new algorithms. This allows for smooth migration when NIST's post-quantum cryptography standards are established.
2. **Preparation for Adoption of Lattice-based Cryptography**: The protocol is preparing for the adoption of promising lattice-based cryptographic algorithms such as CRYSTALS-Kyber (for key encapsulation) and CRYSTALS-Dilithium (for digital signatures).
3. **Hash-based Signature Mechanisms**: The evaluation and adoption of hash-based signature schemes such as XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signature) are being considered.
4. **Ensuring Backward Compatibility**: Migration mechanisms are designed to allow the coexistence of existing tokens and new quantum-resistant tokens.

7.4. Specific Security Use Cases

The BISHOP protocol addresses several specific security scenarios:

7.4.1. Image Preservation as Forensic Evidence

In medical malpractice lawsuits, the question of whether images have been tampered with can be a critical point of contention. The BISHOP protocol provides the following functions:

- Recording the hash value of the original image on the blockchain
- Maintaining a complete history of image export, editing, and import
- Providing cryptographically verifiable proof of tampering or proof of non-tampering

7.4.2. Ensuring Research Data Integrity

In multi-center collaborative research, ensuring the consistency and provenance of image data is essential for research reliability:

- Embedding unique tokens in each image exported for research
- Including anonymization level and scope of research consent in the token
- Making it possible to track the source of images incorporated into research databases

7.4.3. Detection of Malicious Internal Threats

For threats such as unauthorized data extraction from within medical institutions:

- Requiring multi-factor authentication for all legitimate outputs
- Explicit recording of output purpose and subject
- Automatic detection of abnormal patterns (such as large volume outputs during late night

 doi:10.20944/preprints202504.1895.v1

hours)

7.5. Balance Between Security and Usability

In healthcare settings, when security measures impede clinical workflow, users tend to adopt workaround measures such as "shadow IT." The BISHOP protocol considers the following balance:

1. **Context-dependent Authentication**: Applying different security levels for outputs from in-hospital terminals versus external connections
2. **Emergency Override**: Enabling rapid access in emergency clinical scenarios while ensuring post-event auditing
3. **Batch Processing Options**: Optimization for smooth bulk image output for educational and research purposes
4. **Usability Testing**: Continuous evaluation and improvement to minimize workflow impact in actual medical environments

Through this multifaceted security approach, the BISHOP protocol responds to current needs while securing a migration path for the future quantum computing era. With the adoption of Web3.0 technology and consideration of quantum resistance, it aims to be a sustainable medical image security solution for the long term.

References

1. HL7 FHIR R5 Specification. Health Level Seven International. https://www.hl7.org/fhir/
2. DICOM Standards Committee. Digital Imaging and Communications in Medicine (DICOM). https://www.dicomstandard.org/
3. European Parliament. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.
4. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA).
5. Hyperledger Fabric Documentation. https://hyperledger-fabric.readthedocs.io
6. WebAuthn Level 2. W3C Recommendation. https://www.w3.org/TR/webauthn-2/
7. Guardtime. (2016). "Estonian eHealth Authority Partners with Guardtime to Accelerate Transparency and Auditability in Health Care." https://guardtime.com/blog/estonian-ehealth-partners-guardtime-blockchain-based-transparency
8. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). "MedRec: Using Blockchain for Medical Data Access and Permission Management." 2nd International Conference on Open and Big Data.
9. MediBloc. (2017). "Blockchain-based Healthcare Information Ecosystem." https://medibloc.org/en
10. Patel, V. (2019). "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus." Health Informatics Journal, 25(4), 1398-1411.
11. Tang, H., Tong, N., & Ouyang, J. (2018). "Medical images sharing system based on blockchain and smart contract of credit scores." In Proceedings of 2018 IEEE Hot Information-Centric Networking, pp. 240-241.
12. National Institute of Standards and Technology. (2022). "Post-Quantum Cryptography Standardization." https://csrc.nist.gov/Projects/post-quantum-cryptography
13. Bernstein, D. J., & Lange, T. (2017). "Post-quantum cryptography." Nature, 549(7671), 188-194.
14. Alagic, G., et al. (2020). "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process." NIST Interagency Report 8309.
15. Johnson, D., et al. (2021). "Quantum-Resistant Cryptography: Challenges and Solutions for the Digital Era." IEEE Security & Privacy, 19(3), 49-57.

 doi:10.20944/preprints202504.1895.v1

16. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). "Blockchain distributed ledger technologies for biomedical and health care applications." Journal of the American Medical Informatics Association, 24(6), 1211-1220.
17. Roehrs, A., da Costa, C. A., & da Rosa Righi, R. (2017). "OmniPHR: A distributed architecture model to integrate personal health records." Journal of Biomedical Informatics, 71, 70-81.
18. Liang, X., et al. (2018). "Integrating blockchain for data sharing and collaboration in mobile healthcare applications." IEEE 28th International Conference on Personal, Indoor, and Mobile Radio Communications.
19. McGhin, T., et al. (2019). "Blockchain in healthcare applications: Research challenges and opportunities." Journal of Network and Computer Applications, 135, 62-75.
20. Esposito, C., et al. (2021). "Blockchain-based authentication and authorization for smart city applications." Information Processing & Management, 58(2), 102468.
21. DICOM Standards Committee. (2022). "DICOM PS3.15: Security and System Management Profiles." https://dicom.nema.org/medical/dicom/current/output/html/part15.html
22. RFC 7519. (2015). "JSON Web Token (JWT)." Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc7519
23. Abbas, A., & Khan, S. U. (2014). "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds." IEEE Journal of Biomedical and Health Informatics, 18(4), 1431-1441.
24. Wong, D. R., Bhattacharya, S., & Butte, A. J. (2019). "Prototype of running clinical trials in an untrustworthy environment using blockchain." Nature Communications, 10(1), 917.
25. Dagher, G. G., et al. (2018). "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology." Sustainable Cities and Society, 39, 283-297.
26. Hasselgren, A., et al. (2020). "Blockchain in healthcare and health sciences—A scoping review." International Journal of Medical Informatics, 134, 104040.
27. Moll, J., Rexhepi, H., & Cajander, Å. (2020). "Patient Empowerment and Access to Health Records." In Proceedings of 2020 IEEE International Conference on Healthcare Informatics, pp. 1-6.
28. Kumar, R., et al. (2021). "BIoT: Blockchain for the Internet of Things." In Proceedings of 2021 IEEE International Conference on Blockchain, pp. 144-151.
29. Dhieb, N., et al. (2022). "Blockchain-based Schemes for Integration, Interoperability and Secure Sharing of Medical Imaging Data." In Proceedings of 2022 IEEE International Conference on Healthcare Informatics, pp. 342-348.
30. Al-Jaroodi, J., & Mohamed, N. (2019). "Blockchain in Industries: A Survey." IEEE Access, 7, 36500-36515.