IETI Transactions on Ergonomics and Safety

https://www.ieti.net/tes/about.html

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

QUANTUM KEY DISTRIBUTION IN HEALTHCARE: A REVIEW WITH IMPLICATIONS FOR ERGONOMICS SYSTEMS SECURITY

Maria Laura Clemente[1, a], Giuliana Siddi Moreau[1,b] and Lidia Leoni[1,c]

[1]CRS4, Center for Advanced Studies, Research and Development in Sardinia, Loc. Piscina Manna Bld. 1, 09050 Pula, Italy

[a]marialaura.clemente@crs4.it, [b]giuliana.siddi@crs4.it, [c]lidia.leoni@crs4.it

Abstract The rapid digitalisation of healthcare systems through electronic health records, telemedicine, cloud infrastructures and connected medical devices has significantly increased the volume and sensitivity of transmitted medical data. However, emerging quantum computing capabilities pose a potential threat to traditional cryptographic systems, raising concerns about the long-term security of healthcare communications and data storage. Quantum Key Distribution (QKD) is a promising solution that leverages fundamental principles of quantum mechanics, such as the no-cloning theorem and the disturbance of non-orthogonal quantum states during measurement, to achieve information-theoretic security. This article reviews the main QKD protocols and explores their potential for securing data flows in healthcare and ergonomics-related applications. After presenting the main protocols, including BB84, B92, E91/E92, Measurement Device Independent QKD (MDI-QKD) and Continuous Variable QKD (CV-QKD), the paper examines current efforts towards network standardisation and integration with existing telecommunications infrastructures. Particular attention is given to the role of secure communication in human-centred systems, where data protection directly influences user trust, safety and system usability. The review discusses potential QKD applications in ergonomic contexts, such as remote health monitoring, Internet of Medical Things (IoMT) architectures, the secure transmission of wearable sensor data, privacy-aware ergonomic analysis and the protection of medical images and genomic data. Hybrid approaches combining QKD with post-quantum cryptography, blockchain systems and conventional encryption protocols are also considered as practical pathways towards deployment. Finally, the article presents selected real-world pilot projects and experimental implementations that demonstrate the feasibility of quantum-secure healthcare networks. Although technical, infrastructural and economic challenges remain, particularly with regard to deployment costs, distance limitations and hardware complexity, QKD is a promising, future-proof technology for safeguarding sensitive healthcare communications. Integrating it into medical and ergonomic information systems could help create resilient, privacy-preserving and trustworthy digital healthcare environments in the emerging quantum era.

Keywords: Quantum Key Distribution; healthcare cybersecurity; telemedicine security; Internet of Medical Things; human factors; ergonomics.

1. INTRODUCTION

The progressive integration of digital technologies into medical care services has led to a pervasive digital transformation in healthcare systems, from Electronic Health Records (EHRs) for the digitalization of patient records [1, 2], to telemedicine for video consultations and remote monitoring [3, 4]. This digital revolution has simultaneously brought new challenges in terms of the protection of sensitive data against current and future cyber attacks. The anticipated “Q-Day”—the point at which quantum computers become capable of breaking current encryption standards—poses a

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

significant threat to the cryptographic systems currently used to secure healthcare data and medical devices [5, 6, 7]. Traditional cybersecurity systems do not guarantee security against future quantum attacks. The vulnerability of sensitive data requires protection not only at the data storage level, but above all during transmission, when data is most exposed. Secure communication remains a fundamental challenge in information security, as cryptographic defences must continuously evolve to counter increasingly sophisticated attacks. In this context, quantum communication appears to be a promising paradigm for achieving information-theoretic security, in particular through the application of Quantum Key Distribution (QKD), which leverages the principles of quantum mechanics for the secure exchange of cryptographic keys [8, 9]. While traditional secure digital communication technologies are based on computationally hard mathematical algorithms, Quantum Key Distribution is based on the fundamental properties of quantum mechanics: the no-cloning theorem and the impossibility of distinguishing non-orthogonal quantum states without disturbing them [10]. For this reason, Quantum Key Distribution (QKD) can be considered revolutionary in the security of digital communication technologies. And on this basis QKD allows the transmission of encryption keys also over insecure channels. [10].

QKD complies well with the stringent regulatory requirements in force worldwide regarding data protection. This is the case of the Health Insurance Portability and Accountability Act [11] in the USA and the General Data Protection Regulation (GDPR) in Europe [12].

Dedicated standards from organisations such as the European Telecommunications Standards Institute (ETSI) [13] and the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [14] target security, interoperability and network architecture in QKD.

Ergonomics (or human factors) is the scientific discipline concerned with the understanding of the interactions among humans and other elements of a system, applying theory, principles, data, and methods to optimize both human well-being and overall system performance [15]. Wilson characterizes ergonomics as fundamentally about the study of humans as components of complex socio-technical systems, and the application of this understanding to design work, tools, and environments that fit human capabilities and limitations. The discipline is multidisciplinary, drawing on engineering, psychology, physiology, medicine, and organizational sciences, and is commonly categorized into physical, cognitive, and organizational ergonomics.

Modern ergonomic practice increasingly relies on networked, safety-critical, human-centred systems—including medical devices, industrial human-machine interfaces (HMIs), collaborative robots, construction safety platforms, and privacy-sensitive ergonomic monitoring—where communication must be both usable and secure. In this context, the security of data transmission channels is not merely an IT concern but a core ergonomic requirement: a breach in the communication infrastructure of an ergonomic monitoring system can compromise both worker safety and trust in the system itself.

This review therefore examines QKD as a technology relevant to ergonomics insofar as it can secure the data flows that underpin human-centred healthcare and occupational monitoring systems.

IETI Transactions on Ergonomics and Safety

https://www.ieti.net/tes/about.html

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

Specifically, the review considers the main applications of QKD in healthcare with a special focus on possible ergonomic-related applications relevant to occupational health monitoring and human-system interactions, such as remote monitoring and security of communications at various levels, from wearable devices to healthcare networks (intra-hospital communications, connections between hospitals, healthcare cloud).

The rest of the article is structured as follows: Section 2 describes the main protocols for QKD along with some notes on standardization; then Section 3 proposes areas of application for QKD in ergonomics; this is followed by Section 4 with a description of some significant examples of applications around the world; finally, the conclusions are presented.

2. MAIN QKD PROTOCOLS AND NETWORK STANDARDIZATION

This section is dedicated to a short summary of the most important QKD protocols (a scheme is provided in Table 1): the foundational BB84 [16], using a quantum channel to send qubits oriented according to two different bases of orthogonal quantum states (4 quantum states in all); the two-state B92 [17], showing that two non‑orthogonal quantum states suffice for secure key distribution; the entanglement-based E91 [18] and E92, introducing the use of pairs of entangled qubits instead of single qubits; the MDI-QKD (Measurement Device Independent) [19] which adds an untrusted central relay node to the architecture; the Continuous Variable QKD (CV-QKD) [20] which is based on encoding information in the continuous variables of light, such as amplitude and phase. Hybrid approaches have been developed as well, such as the BB84-E91 protocol [21].

Table 1. Main QKD protocols.

Protocol	Year	Type	Key Feature	Main Limitation
BB84	1984	Prepare & Measure	4 states, 2 bases; decoy-state enhancement	Distance limited by photon loss
B92	1992	Prepare & Measure	2 non-orthogonal states suffice	Lower key rate than BB84
E91	1991	Entanglement-based	Bell inequality violation detects eavesdropping	Requires entangled photon sources
MDI-QKD	2012	Measurement-device-independent	Eliminates detector side-channel attacks	Complex setup, lower key rate
CV-QKD	2002	Continuous variable	Standard telecom components, WDM compatible	Shorter secure distance than DV-QKD
BB84-E91	2015	Hybrid	Combines Prepare & Measure with entanglement	Theoretical, limited practical validation

As anticipated, all these protocols are based on important principles of quantum mechanics, such as the no-cloning theorem, quantum superposition, and (in some cases) entanglement, in order to detect if a message from a sender to a receiver was intercepted by a third party [10]. These protocols are described in the following subsections.

IETI Transactions on Ergonomics and Safety

https://www.ieti.net/tes/about.html

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

2.1. The BB84 Protocol

The BB84 QKD protocol can be considered the most researched and applied in commercial systems, above all in the enhanced version with decoy-states. The protocol is based on the encoding of a key in terms of qubits (from single photon pulse), transmitted through a quantum channel, through polarizers allowing only photons with particular orientation to pass, according to two different bases:

- orthogonal states |0> and |1> form a Standard Basis, also known as *Rectilinear* (horizontal and vertical), which is *Z basis*;
- orthogonal states |+> and |-> form a Hadamard Basis, also called *Diagonal* (diagonal and anti-diagonal), which is *X basis* (obtained by applying H gate).

The sender chooses one of these states randomly for each qubit, encoding it accordingly by means of proper Gates.

Parallel to the Quantum Channel, there is an authenticated Classical Channel to share the information. After the receiver has measured all the qubits, choosing a random state, not all the qubits will be the same as the ones sent by the sender. The sender and the receiver then use the Classical Channel to compare the basis they used for each qubit, but without revealing the qubit themselves. The subset of bits corresponding to the same basis, compound the final shared key, and statistically they are 50% of the total number of qubits exchanged. The error rate is used to understand if the channel was violated or not.

The vulnerability of this protocol is in the fact that a clever interception of only a few qubits exchanged through the quantum channel may not be noticed.

In [22] a technique for improving security of protocol BB84 through *decoy-states* was first proposed. Later contributions over the years led to more secure versions [23, 24] of the protocol. This technique adds some fake qubits sent through the quantum channel, used specifically to determine whether there had been some eavesdropping. For instance, the decoy states could be in a basis previously agreed between the sender and the receiver. When the bases are compared through the classical channel, the error rate of the decoy states will result higher than expected.

An interesting work about the protocol BB84 is [25] providing a detailed explanation of the fact that any eavesdropping of the generated key would be detectable because it would create errors.

Another important publication is [26] with a clear flow‐chart‐based specification of the practical decoy‐state BB84 quantum key distribution protocol.

The BB84 Protocol was used as the basis for more recent protocols, above all for the scheme made of a sequence of *"prepare-and-measure"*.

A limitation of this protocol is the achievable distance between sender and receiver, constrained by photon loss in optical fibers, which limits its applicability to metropolitan-area networks. Therefore, it is not suitable for security in long-distance communication.

IETI Transactions on Ergonomics and Safety

https://www.ieti.net/tes/about.html

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

2.2. The B92 Protocol

The B92 protocol [17] is a simplification of BB84 that uses only two non-orthogonal quantum states, one for each bit value (e.g., $|0\rangle$ for bit 0 and $|+\rangle$ for bit 1). Like BB84, it is a prepare-and-measure protocol: the sender prepares single qubits and the receiver measures them. The security of B92 relies on the quantum-mechanical impossibility of perfectly distinguishing two non-orthogonal states. After transmission, the receiver reports which qubits produced conclusive measurement outcomes (without revealing the results), and these form the raw key. Because B92 uses fewer states and a simpler setup than BB84, it offers reduced implementation complexity, but at the cost of a lower key generation rate.

2.3. The E91 and E92 Protocols

In the E91 variant, the qubits sent through the quantum channel are in maximally entangled Bell states and this makes this protocol fundamentally different in its security approach. The receiver measures the entangled state in one of the two possible bases, but since the states are entangled, there is a further layer of security against eavesdropping because any attempt to measure entangled qubits is detectable. The E92 variant, from the same author, differs from this in the way the measurement outcomes are used to generate the key, rather than in the qubits exchanged through the quantum channel.

2.4. The MDI-QKD Protocol

MDI-QKD provides an improved level of security by introducing an intermediate node (also called the *central station*) which collects the quantum states from both parties and performs a Bell-state measurement. The key advantage is that the measurement device can be completely untrusted, thereby eliminating all detector side-channel attacks. The research activity which demonstrated for the first time the validity of this protocol in real-world conditions is described in [27] which is an important step toward practical deployment.

2.5. The CV-QKD Protocol

The protocols so far described use a discrete number of quantum states, such as the polarization or phase of single photons, and are generally known as Discrete Variable QKD (DV-QKD). A more recent protocol is based on Continuous Variable QKD (CV-QKD), using continuously varying properties of light, with information encoded in the quadrature of its electromagnetic fields, and using coherent detectors, instead of single photon detectors (the overall architecture is depicted in Figure 1). This protocol allows a higher secret key rate generation. Another advantage is that it requires telecommunication optical components which can be used in conjunction with classical communication, in the same fiber, via wavelength-division multiplexing; this facilitates integration into existing networks [20, 28]. On the other hand, since DV-QKD is more tolerant to channel losses, it is suitable for metropolitan-area fiber networks [29].

IETI Transactions on Ergonomics and Safety

https://www.ieti.net/tes/about.html

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

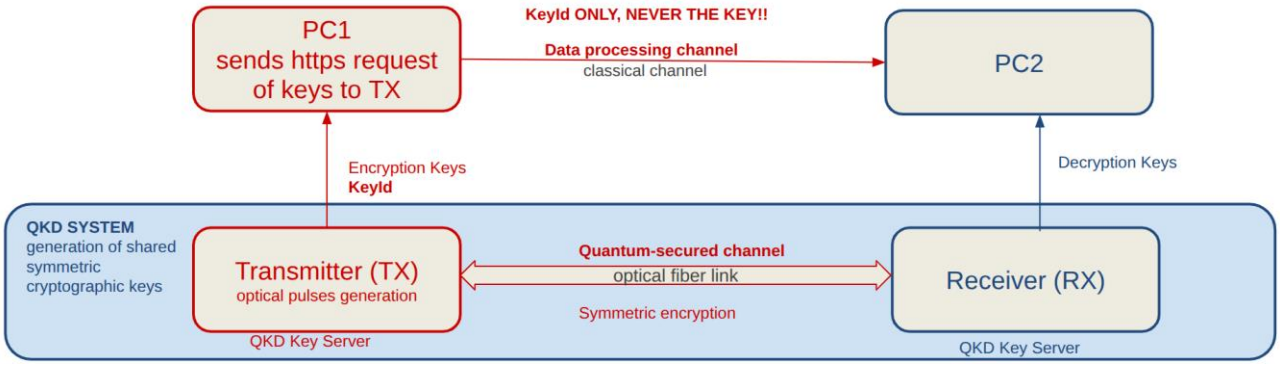

Figure 1. CV-QKD overall architecture.

2.6. QKD Networks Standardization

As mentioned in the introduction, standardising QKD networks is crucial for overcoming practical limitations and ensuring interoperability in various deployment scenarios. ETSI standard [13] focus particularly on QKD module specification, implementation security and protocol definitions, whereas ITU-T standard [14] concentrates on network architecture (QKDN), security and service integration. These standards have established foundational rules to enable multi-vendor QKD devices to operate within broader telecommunication networks. A comprehensive survey about standardization in QKD Networks is presented in [30], which explains how quantum key distribution (QKD) systems are moving from simple point‑to‑point links to scalable, network-wide deployment, thereby contributing to the realisation of a quantum internet (Qinternet). The multi‑node networks for QKD are based on two types of connections: classical channel and quantum channel. As the name suggests, the classical channel can use the same medium as classical data. Quantum signals are particularly vulnerable and their amplification would require measurements with an instantaneous, irreversible, and stochastic collapse of the wave function. Quantum signals need a quantum medium which at present can be of two types: *fiber-based* or *free space* optical links. The main differences between the two are described here after. Optical fiber have low loss and high stability, but are not suitable to easily traverse difficult natural barriers (rivers or mountains); in addition, the maximum point-to-point distance for quantum signals is still restricted to a few hundred kilometers, due to absorption and noise. Free-space optical links offer the benefits of broad coverage and high adaptability, as they can be easily redirected when needed; recently, significant experimental advancements have been made in implementing QKD over these links, also in *air-to-ground* and a feasibility experimentation in *satellite-to-ground;* although it is still an immature technology, it offers features that make it promising for the future (further details can be read in [30]).

3. IMPLICATIONS FOR ERGONOMICS

The relevance of QKD to ergonomics can be understood through the lens of several active research areas where secure data exchange is integral to human-centred system design:

Enterprise information systems. Ergonomic research on enterprise systems emphasizes the need to balance usability, security, and system resilience. User trust, emotional responses, and task efficiency

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

are all affected by the perceived and actual security of the services they use [31]. QKD can contribute to strengthening the security layer of such systems without adding cognitive burden on the end user.

Construction safety management. Human-computer interaction in construction safety relies on sensing, IoT, and AI technologies to monitor workers and site conditions. Secure data exchange between body-worn sensors, on-site devices, and back-end systems is essential for reliable safety monitoring [32]. The quantum-secure protection of these data channels represents a natural extension of ergonomic safety design.

Medical device design. Effective communication between manufacturers, clinical users, and internal teams is central to the design of safe medical device interfaces. When patient-critical or safety-critical information is exchanged during device development and deployment, secure communication channels are required [33]. QKD offers a pathway to physically unbreakable security for such exchanges.

Privacy-aware ergonomic analysis. Recent work on AI-based ergonomic analysis has highlighted the acute privacy challenges inherent in processing human posture, movement, and biometric data in industrial settings. De Coninck et al. [34] specifically addressed the problem of camera-based ergonomic assessment in factory environments, where continuous video or pose data must be transmitted from shop-floor cameras to processing servers. Their proposed framework uses visual obfuscation techniques and server-side AI inference to enable ergonomic risk assessment while preserving worker privacy and data confidentiality during transmission and processing. This work underscores a concrete scenario where quantum-secure key distribution could provide an additional layer of protection: the encrypted transmission of sensitive worker posture and movement data from factory sensors to cloud or edge servers for AI-driven ergonomic analysis.

It is important to clarify that at present the adoption of this technology is not suitable for direct integration into instruments for monitoring physical parameters. Wearable devices in general are characterized by very limited power, tiny hardware footprint, wireless protocols such as Bluetooth or Wi-Fi, in other words a lightweight structure that cannot accommodate an optical quantum transmitter/receiver.

Instead of this, QKD would be applied to making a more secure communication between a hospital or a cloud server and a device belonging to the patient being monitored. Although traditional encryption techniques can be considered effective at present, they could be vulnerable in the future, while long-term confidentiality and data integrity must be guaranteed.

The data flow to be secured would go from the wearable or implantable sensors to a mobile phone, a tablet, or PC and from there QKD would provide unbreakable, physically secure encryption to exchange sensitive data with future-proof security to a hospital or a cloud server. In fact, most healthcare applications are coupled to providers that store sensitive medical data in the cloud. Ergonomists use data related to digital human modeling in their research activity and QKD could be applied also to secure data exchange from cloud to research centers.

QKD can be used to protect data integrity and health records against future attacks of type “harvest now and decrypt later”.

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

Recent work has extended QKD concepts to the Internet of Medical Things (IoMT) domain. Chen [35] proposed a Grover search-based quantum key agreement (QKA) protocol specifically designed for IoMT, enabling patient devices and healthcare providers to collaboratively establish cryptographic keys without relying on a trusted third-party authority. The protocol employs decoy photons to ensure secure quantum transmission over the lossy and noisy channels typical of medical networks.

Complementing key distribution, Prajapat et al. [37] introduced a blockchain-enabled QKD-based signature scheme for IoMT systems. Their approach combines QKD-derived keys with a private blockchain and verifier-specific quantum signatures to authenticate medical sensor data, providing resistance against replay, forgery, and quantum-computing attacks.

At the body-sensor level, Prajapat et al. [37] proposed a privacy-preserving quantum authentication scheme for wireless body area networks (WBANs). The protocol uses QKD-derived keys for authentication and encryption of continuous biomedical data streams, with low computational, communication, and energy overhead suitable for resource-constrained body-worn sensors. This work directly addresses the gap between QKD backbone security and edge-device protection discussed above.

Realistic future applications may involve hybrid systems that combine QKD for backbone networks and post-quantum cryptography (PQC), which are software-based cryptographic algorithms resistant to quantum attacks, for edge devices.

The integration of QKD with established cryptographic protocols has also been explored for medical cyber-physical systems (MCPS). Gawali et al. [38] proposed a hybrid architecture combining a seven-step QKD key exchange process with RSA-AES encryption, demonstrating resistance to man-in-the-middle, brute-force, and other attacks in simulated medical environments.

Looking further ahead, Rana [39] investigated quantum-enabled secure and energy-efficient data transmission for bio-cyber interfaces (BCIs) within a Quantum Internet of Everything (QIoE) framework. The proposed architecture leverages QKD for neural data confidentiality alongside quantum-enhanced energy optimization, pointing toward future integration of quantum security into next-generation brain-computer healthcare systems.

4. REAL-WORLD HEALTHCARE PILOTS

Current limitations to real-world application of QKD are related above all to high costs. In fact, to apply a QKD technology, specific hardware and infrastructure are required along with dedicated fiber links, resulting neither easy nor economical to implement.

It should be noted that QKD has been subject to critical scrutiny within the cryptography community. The UK National Cyber Security Centre (NCSC) has advised against relying on QKD for most use cases, citing practical limitations including the need for dedicated fiber infrastructure, the challenge of authentication of the classical channel, and the existence of viable post-quantum cryptographic alternatives. Furthermore, extending QKD over long distances requires trusted intermediate nodes, which reintroduce classical security assumptions. A balanced assessment must acknowledge that

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

QKD provides information-theoretic security only for key distribution, while the overall system security depends on all components of the communication chain.

Moreover a widespread adoption of such innovative technology is held back by the delicate nature of quantum hardware, the need for error correction and to operate at limited distances. Despite these challenges, recent applications demonstrate the potential of quantum key distribution (QKD) for securing medical communications.

4.1. Examples of Applications in Europe

In Austria, Toshiba Europe Limited [40] recently deployed QKD to a secure medical back-up use case, alongside partners in Graz (Austria) as part of the European OpenQKD project, led by the Austrian Institute of Technology (AIT), aimed at testing real-world applications of quantum-secure communications and put the basis for a future European quantum-safe digital infrastructure [41]. The demonstration connected medical facilities, including the Medical University of Graz and the University Hospital Graz and large datasets, which needed to be securely stored in a remote place. In this application the Toshiba QKD system was used to generate encrypted keys, frequently refreshed, to send 10-Gbps encrypted data streams over fiber links of up to about 20 km away [42].

In 2025, in Madrid, two hospitals of the Vithas Healthcare Group were connected through a quantum-secure communication link using a fiber network operated by Telefónica. A dedicated quantum fiber link was used to distribute encryption keys using quantum key distribution (QKD). The QKD equipment was provided by LuxQuanta, the Spanish company, using the CV-QKD protocol to enable the secure exchange of cryptographic keys over the optical fiber network, ensuring extremely high security for sensitive healthcare data such as medical records, teleconsultation information, and remote patient monitoring data. A key-management technology from QoolNet was used to coordinate the quantum keys across the network [43].

4.2. Examples of Applications in the World

An interesting article published in 2025 in the journal Blockchain in Healthcare Today describes ways to improve the security of telehealth systems by combining quantum key distribution (QKD) with post-quantum cryptography (PQC) within a blockchain-based infrastructure. The PQC algorithms, such as CRYSTALS-Dilithium, were used to provide quantum-resistant digital signatures. The architecture was tested with a simulated telehealth network involving hospitals, clinics and patient devices. The results from the demonstration proved the proposed system to be effective against classical and quantum cyberattacks [44].

The work described in [45], published in 2025, presents a collaboration involving Toshiba and Tohoku University in the development and evaluation of a proof-of-concept (PoC) system combining Quantum Key Distribution (QKD) networks with quantum-secure cloud technology to protect highly sensitive genomic data. The system enabled the transmission of over 500 GB of data via an optical fiber approximately 7 km long in under 2 minutes, significantly faster than conventional physical media transport.

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

The data processing throughput obtained was of 22 Mbps, which is comparable to the raw data output of the Next-Generation Sequencing (NGS) system. This proved it to be suitable for practical, real-time clinical use.

4.3. Secure Image Medical Transmission

Mallick et al. [46] presented a multi-channel, multi-protocol QKD system for secure medical image transmission, integrating BB84, CASCADE, and DPS protocols over both fiber-optic and free-space optical links. Their architecture combines QKD-generated keys with chaotic image encryption and quantum bit-plane representation to protect electronic medical records and real-time diagnostic images. The system achieved a QBER of approximately 0.0028 and an entropy of 7.9896, demonstrating strong robustness for healthcare applications.

Prajapat et al. [47] proposed a chaos-assisted quantum image encryption protocol that combines entanglement-based E91 QKD with logistic chaotic maps for medical image protection. The E91 protocol is used for key generation, while chaos-based operations perform image encryption. The system includes CHSH-based eavesdropping detection and was validated through extensive entropy, histogram, and differential-attack analysis, explicitly targeting healthcare network applications.

Aljaedi et al. [48] introduced a hybrid 'fusion cryptography' approach combining quantum operations (quantum walks, quantum XOR, quantum key images) with classical hyperchaotic scrambling for medical image encryption. The method achieved near-ideal entropy (7.9999), low pixel correlation, and strong robustness against noise and clipping attacks, making it suitable for the secure transmission and storage of diagnostic imaging data

5. CONCLUSION

This review examines the current landscape of quantum key distribution (QKD) protocols and their emerging applications in healthcare data security, paying particular attention to their relevance for ergonomic systems where secure, human-centred communication is essential. Through a review of foundational protocols (BB84, B92, E91, MDI-QKD and CV-QKD), recent Internet of Medical Things (IoMT) and Wireless Body Area Network (WBAN)-oriented schemes, and real-world pilot deployments, this review provides a comprehensive overview of the potential and limitations of QKD in healthcare.

The evidence gathered suggests that QKD is maturing, but is not yet ready for widespread clinical deployment. On the one hand, QKD offers a guarantee that no other cryptographic technology, classical or quantum, can match: the key exchange process is information-theoretically secure, grounded in the laws of physics rather than computational assumptions. Real-world pilot projects, ranging from the OpenQKD medical backup use case in Graz to the quantum-secured hospital link in Madrid and the genomic data transmission system in Japan, demonstrate that QKD can already safeguard sensitive healthcare data over metropolitan fibre networks at practical data rates. The growing body of work on QKD for IoMT, WBANs, medical cyber-physical systems and secure medical image transmission further illustrates the range of healthcare scenarios in which quantum-secure key distribution could be valuable.

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

However, significant challenges remain. Current QKD systems require dedicated fibre-optic infrastructure and specialised hardware, and can only operate within distance limits that, for DV-QKD, rarely exceed a few hundred kilometres, even with trusted intermediate nodes. Costs remain prohibitive for most healthcare institutions. Furthermore, QKD only secures the key distribution step; the overall security of the communication chain also depends on classical encryption, authentication and network management. It should also be noted that the cryptographic community is not unanimous on the necessity of QKD. The UK's National Cyber Security Centre (NCSC), for example, has argued that post-quantum cryptography (PQC) may offer a more practical path to quantum resistance for many use cases without the infrastructure burden that QKD entails. A balanced assessment must acknowledge that QKD and PQC are complementary rather than mutually exclusive, and that the most realistic near-term healthcare architectures will likely be hybrid, combining QKD for high-security backbone links with PQC algorithms for edge devices and resource-constrained endpoints.

Several avenues for future research and deployment emerge. Firstly, integrating CV-QKD into existing telecommunications fibre networks via wavelength-division multiplexing, as demonstrated by recent European pilot schemes, reduces the infrastructure barrier and merits further investigation in the context of healthcare networks. Secondly, initiatives such as the European Quantum Communication Infrastructure (EuroQCI) could provide the shared backbone on which healthcare-specific QKD applications could be developed, thereby reducing costs through economies of scale. Thirdly, the secure transmission of medical images, an area in which recent work has yielded promising results in terms of entropy, error rates and robustness, represents a concrete and growing use case that warrants dedicated attention. Fourthly, as privacy-aware, AI-based ergonomic analysis becomes more prevalent in occupational health settings, the need to protect worker posture, movement and biometric data during transmission and processing will increase, creating new opportunities for QKD-secured data pipelines.

As ergonomics increasingly relies on networked sensors, wearable monitoring, and AI-based analysis, ensuring the secure protection of worker and patient data across the entire monitoring process—from body sensors to cloud servers—will become essential. This is necessary in order to design trustworthy, human-centred systems. Despite its current limitations, QKD offers a physically grounded pathway towards this goal.

Acknowledgements

This work was carried out with the financial contribution of the Sardinia Regional Authorities.

References

[1] Buntin M. B., Burke M. F., Hoaglin M. C., and Blumenthal D., 2011, The benefits of health information technology: a review of the recent literature, *Health Affairs*, 30(3), pp. 464–471.

[2] Evans R. S., 2016, Electronic Health Records: Then, Now, and in the Future, *Yearbook of Medical Informatics*, (Suppl. 1), pp. S48–S61.

[3] Kichloo A., Albosta M., Dettloff K., and Chowdhury M. J. M., 2020, Telemedicine, the current COVID-19 pandemic and the future: a narrative review and perspectives moving forward in the USA, *Family Medicine and Community Health*, 8, e000530.

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

[4] Tuckson R. V., Edmunds M., and Hodgkins M. L., 2017, Telehealth, *New England Journal of Medicine*, 377, pp. 1585–1592.

[5] Kop M., Slijpen J., Liu H., Lee J., Albrecht J., and Cohen I., 2024, How Quantum Technologies May Be Integrated Into Healthcare, What Regulators Should Consider, Stanford Law School, Stanford.

[6] Jeyaraman N., Jeyaraman M., Yadav S., and others, 2024, Revolutionizing healthcare: the emerging role of quantum computing in enhancing medical technology and treatment, *Cureus*, 16(8), e67486.

[7] Freyer O., Ostermann M., Minssen T., and Gilbert S., 2025, Quantum cryptography and data protection for medical devices before and after they meet Q-Day, *npj Digital Medicine*, 8, 620.

[8] Alif A., Hasan K. F., Laeuchli J., and Morshed Chowdhury M. J., 2024, *Quantum Threat in Healthcare IoT: Challenges and Mitigation Strategies*, arXiv, https://arxiv.org.

[9] Bishwas A., and Sen M., 2024, *Strategic Roadmap for Quantum-Resistant Security: A Framework for Preparing Industries for the Quantum Threat*, arXiv, https://arxiv.org.

[10] Nielsen M. A., and Chuang I. L., 2010, Quantum Computation and Quantum Information (10th Anniversary ed.), Cambridge University Press, Cambridge.

[11] U.S. Department of Health & Human Services, 2013, Standards for the Privacy of Individually Identifiable Health Information (HIPAA), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/standards-privacy-individually-identifiable-health-information/index.html.

[12] European Parliament and Council, 2016, General Data Protection Regulation (EU) 2016/679, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[13] European Telecommunications Standards Institute, 2026, Quantum Key Distribution (QKD), https://www.etsi.org/technologies/quantum-key-distribution.

[14] International Telecommunication Union, 2020, QKD Tutorial: Quantum Key Distribution – Principles and Practice, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2020-1-PDF-E.pdf

[15] Wilson, J. (2000). Fundamentals of ergonomics in theory and practice, *Applied Ergonomics*, 31(6), pp. 557–567.

[16] Bennett C. H., and Brassard G., 1984, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, IEEE, Bangalore.

[17] Bennett C. H., 1992, Quantum cryptography using any two nonorthogonal states, *Physical Review Letters*, 68(21), pp. 3121–3124.

[18] Ekert A. K., 1991, Quantum cryptography based on Bell's theorem, *Physical Review Letters*, 67(6), pp. 661–663.

[19] Lo H.-K., Curty M., and Qi B., 2012, Measurement-device-independent quantum key distribution, *Physical Review Letters*, 108(13), pp. 130503.

[20] Grosshans F., and Grangier P., 2002, Continuous variable quantum cryptography using coherent states, *Physical Review Letters*, 88(5), 057902.

[21] Thakur G., Chouksey P., Chopra M., and others, 2025, A comprehensive review on the hybrid BB84 E91 QKD protocol for enhanced security efficiency and practical hardware implementation in quantum cryptography, *Discover Computing*, 28(1), 343.

[22] Hwang W.-Y., 2003, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Physical Review Letters*, 91(5), pp. 057901.

[23] Lo H.-K., Ma X., and Chen K., 2005, Decoy state quantum key distribution, *Physical Review Letters*, 94(23), 230504.

[24] Liu B., Xia S., Xiao D., and others, 2022, Decoy-state method for quantum-key-distribution-based quantum private query, *Science China Physics, Mechanics & Astronomy*, 65, 240312.

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

[25] Shor P. W., and Preskill J., 2000, Simple proof of security of the BB84 quantum key distribution protocol, *Physical Review Letters*, 85(2), pp. 441–444.

[26] Mizutani A., Sasaki T., and Kato G., 2025, *Protocol-level description and self-contained security proof of decoy-state BB84 QKD protocol*, arXiv, https://arxiv.org/abs/2504.20417.

[27] Liu Y., Chen T.-Y., Wang L.-J., Liang H., Shentu G.-L., Wang J., and Pan J.-W., 2013, Experimental measurement-device-independent quantum key distribution, *Physical Review Letters*, 111, 130502.

[28] Leverrier A., 2015, *Composable security proof for continuous-variable quantum key distribution*, arXiv, https://arxiv.org/abs/1408.5689.

[29] Wang X., Guo S., Wang P., Liu W., and Li Y., 2019, Realistic rate–distance limit of continuous-variable quantum key distribution, *Optics Express*, 27, pp. 13372–13386.

[30] Cao Y., Zhao Y., Wang Q., Zhang J., Ng S., and Hanzo L., 2022, The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet, *IEEE Communications Surveys & Tutorials*, 24, pp. 839–894.

[31] Sarah, C., and Ashbrook, A., 2020, Human computer interaction on enterprise information systems, *International Journal of Advanced Information and Communication Technology*, 7(11), pp. 170–177.

[32] Peng, H., Wang, X., Wu, H., & Huang, B., 2025, Human-Computer Interaction Empowers Construction Safety Management: Breaking Through Difficulties to Achieving Innovative Leap, *Buildings*, 15(5), 771.

[33] Vincent, C., Li, Y., & Blandford, A., 2014, Integration of human factors and ergonomics during medical device design and development: it's all about communication, *Applied Ergonomics*, 45(3), pp. 413–419.

[34] De Coninck, S., Gamba, E., Van Doninck, B., Bey-Temsamani, A., Leroux, S., & Simoens, P., 2025, *Enabling Privacy-Aware AI-Based Ergonomic Analysis*, ArXiv, abs/2505.07306. https://doi.org/10.48550/arxiv.2505.07306

[35] Chen, T., 2025, A Grover Search-Based Quantum Key Agreement Protocol for Secure Internet of Medical Things Communication, *Future Internet*, 17, 263.

[36] Prajapat, S., Gautam, D., Kumar, P., Das, A., Pal, S., & Dong, C., 2025, Blockchain-Enabled Secure Signature Scheme with Quantum Key Distribution for IoMT-Based Healthcare Systems, *IEEE JBHI*, https://doi.org/10.1109/jbhi.2025.3614874

[37] Prajapat, S., Kumar, P., & Kumar, S., 2024, A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks, *Cluster Computing*, 27, pp. 9013–9029.

[38] Gawali, P., Sakhare, S., Mahalle, P., & More, P., 2025, Development of Quantum Key Exchange Mechanisms for Securing Medical Cyber-Physical Systems, *Int. J. Applied Mathematics*, 38(1s), pp. 454–477.

[39] Rana, D., 2025, Quantum-enabled energy efficient secure data transmission for bio-cyber interfaces with QIoE and QKD for future healthcare systems, *Proceedings of the 2025 IEEE Conference on Technologies for Sustainability (SusTech)*, pp. 1–6, IEEE.

[40] Toshiba, 2026, Toshiba Europe – Official Website, https://www.toshiba.eu/

[41] OpenQKD Project, 2024, OpenQKD project information, https://cordis.europa.eu/project/id/857156.

[42] Zatoukal, B., Kutschera, F., Poppe, A., Strasser, W., et al., 2021, OpenQKD use-case for securing sensitive medical data at rest and in transit. *Proceedings of the 2021 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)*, p. 1, IEEE, Munich.

[43] LuxQuanta, 2024, Continuous and discrete quantum key distribution (QKD), https://www.luxquanta.com/continuous-and-discrete-quantum-key-distribution-qkd-r-10-en.

[44] Roosan D., Khan R., Nirzhor S., and Hai F., 2025, Post-quantum cryptography resilience in telehealth using quantum key distribution, Blockchain in Healthcare Today, 8(1).

2026, Volume 10, Issue 1, 13-26, DOI: 10.6722/TES.202603_10(1).0002

[45] Tanizawa Y., Takesue H., Fujiwara M., Honjo T., Sasaki M., and Tokura T., 2025, Quantum key distribution network and quantum secure cloud technologies for genome medicine use cases, *IEEE Transactions on Quantum Engineering*, 6, pp. 1–15.

[46] Mallick, B., et al. (2025). Multi-Channel Multi-Protocol Quantum Key Distribution System for Secure Image Transmission in Healthcare, *IEEE Access*, 13, pp. 62476–62505.

[47] Prajapat, S., Kumar, D., & Kumar, P., 2024, Quantum image encryption protocol for secure communication in healthcare networks, *Cluster Computing*, 28(1), 3.

[48] Aljaedi, A., Jamal, S., Aljuhni, A., Alharbi, A., & Shah, T., 2025, Fusion cryptography for secure medical data transmission using mathematical quantum computing operations, *Scientific Reports*, 15, 33993.