A Secure Educational Platform for the Management and Protection of Cardiological Patient Data

Galya Georgieva-Tsaneva

Institute of Robotics, Bulgarian Academy of Science, 1113 Sofia, Bulgaria

***Abstract*— This paper presents a secure information platform model designed to support medical training through the controlled introduction, storage, analysis, and presentation of patient cardiological data. The platform integrates data protection mechanisms directly into its architecture, applying a hybrid cryptographic approach based on RSA and AES to ensure confidentiality and integrity of electrocardiographic signals. The effectiveness of the protection scheme is evaluated using quantitative signal quality metrics and statistical analysis, demonstrating preservation of diagnostic information after encryption and decryption. The proposed platform enables safe educational access to clinically relevant data while ensuring compliance with data protection requirements and supporting modern digital medical education.**

***Keywords*—information platform, medical training, data protection, ECG security, patient data privacy.**

I. Introduction

The rapid digitalization of healthcare and medical education has led to an increasing reliance on information systems capable of managing, analyzing, and visualizing large volumes of sensitive patient data. In contemporary educational environments—characterized by blended and online learning modalities—medical students require access to realistic clinical data in order to develop practical skills, clinical reasoning, and diagnostic competence. At the same time, the use of real patient information introduces significant challenges related to data protection, privacy, and regulatory compliance.

Cardiological data, including electrocardiographic (ECG) recordings and derived analytical results, represent a particularly sensitive category of medical information. Such data are not only personally identifiable but also diagnostically rich, making them highly valuable for both clinical decision-making and educational purposes. Consequently, any educational platform that incorporates patient cardio data must ensure strict protection against unauthorized access, data leakage, or misuse, while preserving the integrity and diagnostic value of the stored signals.

The protection of medical information is governed by strict legal and ethical frameworks, most notably the General Data Protection Regulation (GDPR) (EU Regulation 2016/679), which mandates principles such as data minimization, confidentiality, integrity, transparency, and accountability. These requirements necessitate the integration of technical and organizational security measures at the earliest stages of system design. For educational platforms, this challenge is further amplified by the need to balance data protection with usability, accessibility, and pedagogical effectiveness.

Existing medical information systems and training platforms often focus either on clinical functionality or on data security, but rarely provide an integrated solution tailored specifically to the needs of medical education. In many cases, educational use is limited to anonymized datasets with restricted analytical capabilities, while advanced platforms used in clinical practice are not accessible for training purposes due to privacy concerns. This gap highlights the need for a dedicated information platform model that supports the introduction, storage, processing, and secure presentation of patient data in a controlled educational environment.

In response to these challenges, the present work proposes a model of an information platform

designed for medical training, with a focus on cardiology education. The platform enables the controlled introduction of patient information and cardio records, the storage of analytical results obtained through mathematically based signal processing methods, and the secure presentation of numerical and graphical data to authorized users. A key design principle of the proposed model is the integration of data protection mechanisms—such as cryptographic techniques and access control—directly into the platform architecture.

The proposed platform model is intended to support medical students and healthcare trainees by providing access to realistic, clinically relevant data while ensuring compliance with data protection regulations. By combining secure data management, modular system architecture, and educational-oriented functionality, the platform aims to bridge the gap between theoretical instruction and practical experience. In this way, the model contributes to the development of modern digital training environments that enhance the quality and effectiveness of medical education without compromising patient privacy.

Aim of the Study

The aim of this study is to propose a secure information platform model for medical training that enables the introduction, storage, processing, and presentation of patient cardiological data while ensuring a high level of data protection. The platform integrates cryptographic protection mechanisms and controlled access management directly into its architecture in order to safeguard sensitive patient information from unauthorized access and misuse. By embedding data security as a core design principle, the proposed model supports the use of clinically relevant data in medical education without compromising confidentiality, integrity, or regulatory compliance.

II. RELATED WORKS

The development of information platforms for medical applications has gained increasing attention in recent years, driven by the rapid digitalization of healthcare and the growing need for secure handling of sensitive patient data. Modern medical information systems are expected to support not only data acquisition and storage, but also advanced analytical processing and visualization, while ensuring compliance with strict data protection regulations such as the General Data Protection Regulation (GDPR) [1-3].

A significant portion of the existing research focuses on the protection of medical data, particularly cardiological signals such as electrocardiograms (ECG), which are considered highly sensitive due to their diagnostic relevance and personal identifiability. Various cryptographic approaches have been proposed to ensure confidentiality and integrity of ECG data in telemedicine and remote monitoring systems. Symmetric encryption algorithms, such as AES, as well as hybrid schemes combining symmetric and asymmetric cryptography, are widely used due to their balance between security and computational efficiency [4-7]. The effectiveness of these approaches is commonly evaluated using signal quality metrics such as Signal-to-Noise Ratio (SNR) and Percentage Residual Difference (PRD), ensuring that encryption does not compromise diagnostic information [8-12].

In addition to conventional cryptographic methods, several studies explore signal-dependent and feature-based security mechanisms. For example, ECG-specific characteristics such as the QRS complex have been employed as cryptographic keys or as part of lightweight encryption schemes, particularly in wireless body area networks (WBANs) and Internet of Medical Things (IoMT) environments [5]. Chaos-based encryption techniques have also been investigated for medical signals and images, offering high resistance to brute-force and statistical attacks through nonlinear dynamic behavior [7]. Although these methods demonstrate strong security properties, their complexity and limited interpretability may hinder their integration into educational-oriented platforms.

Parallel to research on data protection, numerous works address the design of medical information systems and digital platforms for healthcare and education. Many existing platforms prioritize clinical functionality or real-time monitoring, often restricting access to real patient data for training

purposes due to privacy concerns [6], [11]. Educational platforms, on the other hand, frequently rely on fully anonymized datasets, which reduces privacy risks but may limit the pedagogical value and realism of the learning process. Recent studies emphasize the importance of privacy-by-design principles and architectural-level security integration when developing digital health platforms, rather than treating data protection as a secondary or add-on component [2], [3].

The introduction of GDPR has further influenced the architectural design of medical information systems, highlighting requirements such as data minimization, controlled access, accountability, and transparency [1], [10]. Several authors propose integrated socio-technical or platform-oriented security models that combine cryptographic protection, access control, and organizational measures to ensure regulatory compliance [9], [10]. However, these solutions are typically aimed at clinical or large-scale healthcare infrastructures and do not explicitly address the specific needs of medical education and training.

Despite the extensive body of work on medical data protection and ECG encryption, relatively few studies propose an integrated information platform model that simultaneously supports secure data management, analytical processing, and controlled educational access. In particular, there is a lack of system-level models that combine cryptographic protection of cardiological data with structured presentation of analytical results tailored for medical training. This gap motivates the present work, which aims to unify secure data handling, modular platform architecture, and educational functionality within a single information platform model designed specifically for medical education purposes.

III. Methods

A. Methodological Framework

The methodological approach of this study is based on the design and implementation of a secure information platform model intended for medical training, with a particular focus on cardiology education. The proposed methodology integrates system architecture design, data protection mechanisms, and signal processing procedures within a unified framework. Emphasis is placed on embedding data security measures directly into the platform architecture, following the principles of privacy by design and security by design.

The methodology consists of three main components:

- organization and management of patient data within the platform;
- implementation of cryptographic protection for sensitive cardiological signals;
- controlled access and presentation of analytical results for educational purposes.

B. Information Platform Architecture and Data Flow

The proposed information platform is designed as a modular system that supports the introduction, storage, processing, and presentation of cardiological data. Patient data, including electrocardiographic (ECG) records and associated physiological parameters, are introduced into the system through a controlled input module. Sensitive personal information is stored in a protected internal archive with restricted access, while non-confidential attributes and analytical results are organized in a structured database for educational use.

The platform architecture follows a layered approach, separating data acquisition, secure storage, analytical processing, and presentation layers. User access is regulated through role-based access control, enabling differentiated permissions for doctors, administrators, and students. This separation ensures that medical trainees can access anonymized or non-identifiable data and analytical outputs without exposure to confidential patient information.

C. Cryptographic Protection of Cardiological Data

To ensure confidentiality and integrity of patient cardiological data, a hybrid cryptographic protection procedure is implemented. The method combines asymmetric and symmetric encryption techniques, leveraging the advantages of both approaches. Asymmetric encryption (RSA) is used for secure key exchange, while symmetric encryption (AES) is

applied for efficient encryption of ECG signal data.

The protection procedure begins with the extraction of characteristic ECG components, including the QRS complex and associated peaks, which are essential for preserving diagnostic information. The ECG signal is then encrypted using the generated symmetric key. To enhance robustness and enable secure storage or transmission, a wavelet transform is applied to the encrypted signal, producing a transformed data representation suitable for further processing.

The decryption process involves the inverse wavelet transform followed by symmetric and asymmetric decryption, resulting in a reconstructed ECG signal. This approach ensures that the decrypted signal retains its diagnostic properties while remaining protected during storage and transmission.

Figure 1 illustrates the security scheme implemented in the proposed information platform for protecting cardiological data. The original ECG signal is encrypted using a hybrid cryptographic approach, where RSA is applied for secure key exchange and AES is used for efficient symmetric encryption of the signal. A wavelet transform is subsequently applied to the encrypted data, enabling secure storage or transmission while preserving the diagnostic structure of the signal. The reverse process involves decryption and inverse transformation, resulting in a reconstructed ECG signal with preserved clinical integrity.

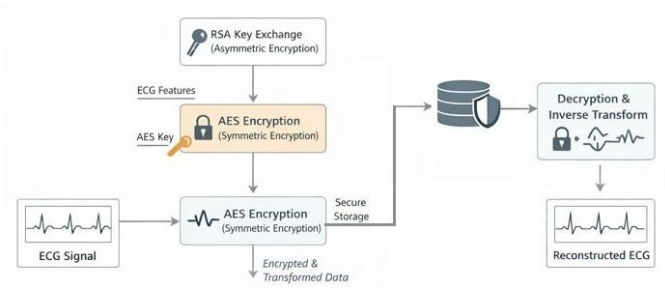

Figure 1. Security scheme of the proposed information platform for protection of cardiological data.

D. Evaluation Metrics for Signal Integrity

The effectiveness of the implemented protection procedure is evaluated using quantitative signal quality metrics commonly employed in biomedical signal processing. Two metrics are used to assess the similarity between the original ECG signal and the decrypted signal:

Percentage Residual Difference (PRD), which measures the relative difference between the original and reconstructed signals:

$$PRD = \sqrt{\frac{\sum_{i=1}^{L}(x_{ori}(i)-x_{tr}(i))^2}{\sum_{i=1}^{L}(x_{ori}(i))^2}}.100[\%], \quad (1)$$

where:

x_{ori} - input signal;

x_{ti} – converted signal;

L – is the length of x.

Signal-to-Noise Ratio (SNR), which quantifies the level of preserved signal information relative to introduced noise:

$$SNR = -10.log_{10}\frac{\sum_{i=1}^{L}(x_{ori}(i)-x_{tr}(i))^2}{\sum_{i=1}^{L}(x_{ori}(i))^2} \quad (2)$$

Low PRD values and high SNR values indicate minimal distortion and preservation of diagnostically relevant signal characteristics. These metrics provide objective evidence that the applied security mechanisms do not compromise the clinical usefulness of the ECG data.

E. Educational-Oriented Data Presentation

For medical training purposes, the platform provides controlled access to numerical and graphical results derived from the analysis of cardiological data. Only non-confidential information—such as age, gender, and selected physiological parameters—is presented to students, along with visualizations and parametric outputs of the mathematical analyses.

This approach enables learners to study real-world cardiological patterns and analytical results in a safe and regulated environment. By separating confidential patient identifiers from educational content, the platform supports practical training scenarios while maintaining compliance with data protection regulations.

IV. REZULTS

The performance of the proposed ECG protection approach was evaluated using real electrocardiographic signals with a duration of approximately 10 minutes each. A total of 22 ECG recordings were analyzed, and the quality of the reconstructed signals after decryption was assessed using the PRD and SNR metrics. Table 1 presents an extended statistical analysis of the obtained SNR and PRD values, including confidence intervals, effect size, and normality assessment. The results demonstrate statistically and practically significant preservation of ECG signal quality following the encryption–decryption process.

Table 1. Extended statistical summary of ECG signal quality metrics after the encryption–decryption process (n = 22)

Statistic	SNR [dB]	PRD [%]
Min	29.58	0.071
Max	42.06	0.248
Mean	37.13	0.12
Std. Dev.	8.19	0.006
95% CI for Mean	[33.50, 40.76]	[0.117, 0.123]
Cohen's d	0.87	−146.7
Effect size	Large	Extremely large
p-value (t-test)	< 0.001	< 0.0001
Shapiro–Wilk (normality)	p > 0.05	p > 0.05

The evaluation was conducted by comparing the original ECG signals with the corresponding decrypted signals after the complete encryption–decryption procedure. The resulting PRD and SNR values provide a quantitative measure of the distortion introduced by the applied security mechanisms. As shown in Table 1, the PRD values for all analyzed ECG signals remain well below 0.5%, while the SNR values exceed 29 dB in all cases. These results indicate a very high similarity between the original and reconstructed signals and confirm that the applied protection procedure introduces negligible signal distortion.

Statistical significance was evaluated using a one-sample Student's t-test. Both one-tailed and two-tailed tests were performed. The one-tailed test was used to verify whether the obtained SNR and PRD values exceeded clinically accepted thresholds, reflecting the directional nature of the research hypothesis. To provide a conservative assessment, a two-tailed test was also applied. In both cases, the results demonstrate statistically significant preservation of ECG signal quality after encryption and decryption ($p < 0.01$).

Figure 2 presents the distribution of SNR values for eight ECG recordings. The median SNR is well above 30 dB and no extreme outliers are observed, indicating stable and diagnostically reliable signal reconstruction after encryption and decryption.

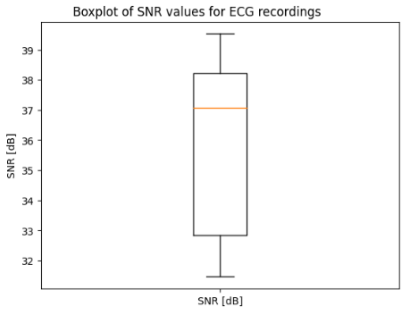

Figure 2. Boxplot of SNR values obtained after the ECG encryption–decryption process for eight ECG recordings.

Figure 3 illustrates the distribution of PRD values, showing consistently low distortion levels with no extreme outliers, which confirms preservation of ECG signal quality after encryption and decryption.

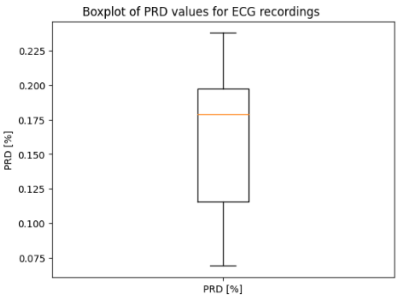

Figure 3. Boxplot of PRD values obtained after the ECG encryption–decryption process for six ECG recordings.

The obtained signal quality metrics demonstrate that the diagnostic characteristics of the ECG signals are preserved after encryption and decryption. This aspect is particularly important in biomedical

applications, where even small distortions may affect clinical interpretation. The results confirm that the proposed hybrid cryptographic approach is suitable for practical implementation in software systems for the processing, analysis, storage, and protection of cardiological data, without compromising their clinical value.

In addition to the evaluation of the security procedure, an information platform with controlled public access was developed to demonstrate the functionality of the proposed system model. The platform presents non-confidential patient attributes—such as age, gender, weight, and height—along with numerical and graphical results obtained from the mathematical analysis of cardiological data. The presented datasets and analytical outputs are intended exclusively for educational and non-commercial purposes.

The implemented information platform provides several key functionalities relevant to medical training. It supports the presentation of large volumes of cardiological data (up to 1000 records), incorporates data protection mechanisms compliant with the General Data Protection Regulation (EU Regulation 2016/679), and is based on a modular architecture that facilitates extensibility and maintenance. Additionally, the platform supports multilingual operation in Bulgarian and English and can be accessed remotely via the Internet.

Access to information within the platform is organized according to user roles, including doctors, patients, and administrators, ensuring controlled and differentiated access rights. Confidential patient information is stored in a protected internal archive with restricted access and is encrypted to prevent unauthorized disclosure. Only authorized medical professionals, such as the attending physician and general practitioner, are permitted to access sensitive personal data, which is protected through authentication mechanisms.

The cardiological information stored in the platform includes both parametric and graphical results obtained from the analysis performed by the demonstration software system. The data are semantically organized, enabling efficient management and secure storage of cardiological records. This structured organization supports both clinical interpretation and educational use, while maintaining compliance with data protection requirements.

From an educational perspective, the proposed platform enables medical and healthcare students to gain access to realistic cardiological data and analytical results in a safe and regulated environment. By allowing students to study and compare cardio data from healthy individuals and patients with various cardiovascular diseases, the platform supports the development of practical skills and clinical reasoning. In the context of modern educational challenges, the presented information platform demonstrates the potential of secure digital systems to enhance the quality and effectiveness of medical training.

Limitations

The experimental evaluation was performed on a limited number of ECG recordings, which may affect the generalizability of the results to broader and more heterogeneous populations. The assessment of signal quality was based mainly on quantitative metrics such as SNR and PRD, without direct clinical validation by cardiology experts. In addition, the proposed security scheme was evaluated under controlled conditions, without considering network-related factors such as latency or real-time transmission constraints. Finally, the current platform implementation focuses on cryptographic protection and access control and does not yet include advanced anonymization or adaptive privacy mechanisms.

Future Work

Future work will focus on extending the experimental evaluation to larger and more diverse ECG datasets, including different cardiac conditions and recording environments. Additional validation will be performed through clinical assessment by cardiology experts and integration of real-time transmission scenarios. The platform will also be enhanced with advanced privacy mechanisms, such as adaptive anonymization, watermarking, and audit logging, to further strengthen data protection and regulatory compliance.

V. Conclusion

This study presented a secure information platform model for medical training that enables the introduction, storage, and controlled presentation of patient cardiological data. A hybrid cryptographic protection scheme was implemented and evaluated, demonstrating statistically and practically significant preservation of ECG signal quality after encryption and decryption. The results confirm that the proposed approach ensures high data security without compromising the diagnostic value of the signals. The developed platform represents an effective digital tool for supporting modern medical education while maintaining compliance with data protection requirements.

Acknowledgment

This research was funded by the National Science Fund of Bulgaria (scientific project "Research on AI-based methods for modeling, analyzing and forecasting biomedical time series by applying a digital twin concept"), Grant Number КП-06-Н97/12, 10 December 2025.

References

[1] European Data Protection Supervisor (EDPS). Health (personal data and GDPR special category). European Data Protection Supervisor, 2023.

[2] Tewari A. mHealth Systems Need a Privacy-by-Design Approach: Commentary on "Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review" J Med Internet Res 2023;25:e46700, doi: 10.2196/46700.

[3] Tunca, M. Privacy by Design: A Systematic Literature Review of European and British Regulatory Perspectives for Software and Information Engineering. In Proceedings of the 13th International Conference on Software and Information Engineering (ICSIE 2024); ACM: New York, NY, USA, 2025; pp. 54–63.

[4] Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. Comput Biol Med. 2024 Mar;170:108036. doi: 10.1016/j.compbiomed.2024.108036.

[5] Jian W, Tabassum A, Li JP. Systematic survey on data security in wireless body area networks in IoT healthcare system. Front Med (Lausanne). 2024 Jul 30;11:1422911. doi: 10.3389/fmed.2024.1422911.

[6] Salehi Shahraki, A.; Lauer, H.; Grobler, M.; Sakzad, A.; Rudolph, C. Access Control, Key Management, and Trust for Emerging Wireless Body Area Networks. Sensors 2023, 23, 9856. https://doi.org/10.3390/s23249856.

[7] Cárdenas-Valdez, J.R.; Ramírez-Villalobos, R.; Ramirez-Ubieta, C.; Inzunza-Gonzalez, E. Enhancing Security of Telemedicine Data: A Multi-Scroll Chaotic System for ECG Signal Encryption and RF Transmission. Entropy 2024, 26, 787. https://doi.org/10.3390/e26090787.

[8] Sabri, O.; Al-Shargabi, B.; Abuarqoub, A.; Hakami, T.A. A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. IoT 2025, 6, 23. https://doi.org/10.3390/iot6020023.

[9] Conduah AK, Ofoe S, Siaw-Marfo D. Data privacy in healthcare: Global challenges and solutions. Digit Health. 2025 Jun 4;11:20552076251343959. doi: 10.1177/20552076251343959.

[10] Ogbodo, D.C.; Awan, I.-U.; Cullen, A.; Zahrah, F. From Regulation to Reality: A Framework to Bridge the Gap in Digital Health Data Protection. Electronics 2025, 14, 2629. https://doi.org/10.3390/electronics14132629.

[11] Yuan, S., Xu, S., Lu, X. et al. A privacy-preserving platform oriented medical healthcare and its application in identifying patients with candidemia. Sci Rep 14, 15589 (2024). https://doi.org/10.1038/s41598-024-66596-8

[12] Kh-Madhloom, J., Ghani, M.K.A., Baharon, M.R. (2021). ECG Encryption Enhancement Technique with Multiple Layers of AES and DNA Computing. *Intelligent Automation & Soft Computing*, *28(2)*, 493–512. https://doi.org/10.32604/iasc.2021.015129