Review MECAS V°22 / N° 1/ June 2026

PROTECTION OF MEDICAL DATA IN THE DIGITAL SPACE:A Field Study at the Public Community Health Institution of Bordj Menaïel

Diaf Nazim wail [1]
Laboratory for Evaluation and Forecasting of Economic Policies and Business Strategies (LEPPESE) / PhD student / University of Naama, Algeria
diaf.nazimwail@cuniv-naama.dz

Belaidi Abderrahim
Oran Graduate School of Economics, Algeria / Lecturer A
rah.belaidi@gmail.com

BELAIDI ZAKARIA
University of SIDI BEL-ABESS/ Lecturer B
belaidiadjim@gmail.com

Received date: 30.03.2026, Accepted date : 02.05.2026, Publication date: 02.06.2026

Abstract :
This study examines the protection of medical data in the context of digital transformation in healthcare. It highlights growing risks such as data breaches and unauthorized access due to increased reliance on digital systems. The research combines a theoretical review of key concepts, legal frameworks, and security challenges with a practical field study. The empirical part is based on a questionnaire conducted at the Public Community Health Institution of Bordj Menaïel to assess staff awareness and the effectiveness of data protection measures. The study aims to identify gaps between legislation and real-world practices. It ultimately proposes recommendations to strengthen data security, protect patient privacy, and improve institutional performance.

Keywords: Medical Data Protection; Digital Health; Data Security; Patient Privacy; Health Governance.
Jel Classification Codes: I11; I18; K24; O33

Introduction :

Digital transformation plays a pivotal role in optimizing the management of health institutions through innovative tools that facilitate the precise and efficient organization of medical data. Digital systems, such as Electronic Health Records (EHR), accelerate clinical decision-making and enhance inter-departmental coordination. Furthermore, they provide rapid access to patient medical histories,

[1] Corresponding Author.

thereby reducing medical errors and improving the quality of care. However, alongside these benefits, there is an urgent need to protect medical data from escalating cyber threats.

Medical data is considered among the most sensitive and critical types of information, as it pertains directly to individual health and reveals private life details. With the significant shift in the healthcare sector, medical records have transitioned from traditional paper archives to sophisticated digital systems, making them more accessible and shareable across various health institutions. While this transformation has streamlined diagnosis, treatment, and large-scale data management, it has also exposed this information to risks such as cyberattacks and unauthorized breaches. Consequently, it has become imperative to develop effective mechanisms and techniques to safeguard medical data, ensuring its confidentiality, integrity, and the protection of patient privacy.

Given the increasing reliance on digital systems within health institutions, medical data protection has become a central issue that cannot be overlooked. The electronic storage and networking of health information have increased vulnerability to hacking, tampering, or loss, making security a top priority. Protecting this data extends beyond technical aspects to encompass legal, ethical, and organizational dimensions. Concepts such as Health Information Security (HIS), encryption, and access control have emerged as essential tools to prevent illicit use. Thus, adopting strict policies and effective procedures is necessary to ensure data protection in a digital space where cyber threats are becoming increasingly sophisticated.

1.1 Research Problem :

The central research question guiding this study is as follows: What are the mechanisms for protecting medical data in the digital space, and what is the current state of their application within healthcare institutions?

This overarching question gives rise to the following secondary questions:

- What is meant by medical data, and how is this concept defined?
- What threats may affect medical data, and what procedures are adopted to protect them?
- What regulatory and legal procedures are nationally recognised to ensure the confidentiality and integrity of health information, and to what extent are they applied within the institution under study?
- To what degree do staff members at the institution possess the awareness and training necessary to handle medical data securely?

1.2 Study Hypotheses :

Main Hypothesis :

There exists a statistically significant effect of the level of knowledge held by employees at the Public Community Health Institution of Bordj Menaïel regarding the various dimensions of medical data protection (legal and legislative; technical and cybersecurity; institutional and structural; human and awareness-related; compliance and accountability) on their perceived assessment of the current reality and mechanisms of medical data protection applied within the institution.

Sub-Hypotheses :

- There exists a statistically significant positive correlation between employees' level of knowledge of the legal and legislative aspects of medical data

protection and their perceived level of application of the legal and regulatory mechanisms for data protection within the institution.

- There exists a statistically significant positive correlation between employees' level of knowledge of the technical aspects of medical data protection and their perceived level of application of technical data protection mechanisms within the institution.
- There exists a statistically significant positive correlation between employees' level of knowledge of the institutional aspects of medical data protection and their perceived existence of the institutional structures necessary for data protection within the institution.
- There exists a statistically significant positive correlation between employees' level of knowledge of the human aspects of medical data protection and their perceived level of application of awareness and sensitisation mechanisms related to data protection within the institution.
- There exists a statistically significant positive correlation between employees' level of knowledge regarding the compliance dimension of medical data protection and their perceived level of application of monitoring and audit mechanisms to ensure compliance within the institution.

1.3 Research Methodology :

The first part of this study adopts a descriptive approach in order to present and elucidate the foundational concepts pertaining to medical data protection. The second part employs an analytical approach, establishing a connection between the theoretical framework and the actual circumstances prevailing within the institution under study. Both a structured questionnaire and semi-structured interviews were utilised as primary data collection instruments, with the overarching aim of determining the level of awareness and knowledge held by employees of the Public Community Health Institution of Bordj Menaïel with respect to medical data protection, as well as their perception of the current application of protective mechanisms within the institution.

1.4 Literature Review

The protection of private medical data in the digital sphere is a contemporary topic in Algerian and Arab research, which has not yet received extensive academic attention from legal or technical perspectives, despite the increasing importance of digital policies mandated by the Ministry of Health.

- First Study: *"The Protection of Sensitive Medical Personal Data based on the Development of the Right to Health."* This study examines the evolution of the right to health in relation to sensitive data protection, reviewing international legislations such as the GDPR, and national laws in Egypt, France, the USA, and the UAE.
- Second Study: *"Cybersecurity Challenges and their Applications in the Algerian Health Sector."* This research highlights the challenges facing the sector amidst the absence of a clear strategic vision for data protection, concluding that while Algerian legislation addresses cybercrime, it lacks a comprehensive multidisciplinary approach (technical and institutional).

- Third Study: *"Organization of Electronic Medical Records and Data Protection within the Framework of Developing the Health Sector."* This study focuses on the accuracy and credibility of digital systems, identifying authorized access entities, and patient rights regarding the illicit use of data for administrative or commercial purposes.

1.5 Research Objectives :

This research aims to define medical data and understand its sensitive nature compared to other personal data. It seeks to examine how this data is protected during the transition from paper-based archives to advanced digital environments. Furthermore, the study analyzes the alignment between theoretical technical/legislative mechanisms and their practical application within health institutions to identify strengths and shortcomings.

1.6 Study Structure :

To achieve the aforementioned objectives, the study is organised around the following axes:

- Axis I: An examination of the mechanisms for protecting medical data in the digital environment.
- Axis II: Violations perpetrated against the automated processing of private medical data.
- Axis III: A field study of the reality of medical data protection amid digital transformation at the Public Community Health Institution of Bordj Menaïel.

2. MECHANISMS FOR PROTECTING MEDICAL DATA IN THE DIGITAL ENVIRONMENT

2.1 The Concept of Medical Data Protection

While Algerian legislation lacks a static, singular definition of "data security" owing to the concept's inherent flexibility and the rapid pace of technological change it establishes a comprehensive protective framework anchored in constitutional and statutory law.

- **Constitutional Foundations:** The 2020 Algerian Constitution provides the primary legal bedrock for data privacy. **Article 39** guarantees the inviolability of the human person, while **Article 47** explicitly enshrines the right to private life, honor, and the confidentiality of all forms of communication and correspondence.
- **Statutory Sanctions and Obligations:** To enforce these principles, the **Penal Code (Articles 303 bis et seq.)** criminalizes the unauthorized interception of private data or images. Furthermore, **Law 18-11 (The Health Law)** classifies medical information as a fundamental right, mandating strict professional confidentiality and requiring explicit consent for data processing, except where legally exempted.
- **Technological and Administrative Resilience:** Given the sensitivity of health records and the rising threat of cyber-attacks, the framework emphasizes a multidimensional approach. This necessitates the integration of robust technical protocols and administrative measures to preserve data integrity and prevent unauthorized access within a digital landscape.

2.2 Security of Medical Data Through the Protection of Electronic Systems :

In the context of the extensive flow of information and its widespread use particularly within critical infrastructure it has become imperative to strengthen information and network security in order to protect them against the varied cyberattacks that cause harm to individuals and disrupt essential services. This underscores the importance of protecting vital installations in particular healthcare institutions, which constitute an essential component of individuals' lives so as to ensure the continuity of their operations. These protective measures may be summarised as follows:

2.3 Security of Personal and Medical Data in Algerian Legislation :

Recognising the importance of keeping pace with the security challenges of the digital environment, the Algerian legislator introduced substantive legislative amendments to the Penal Code through Law No. 04-15, dated 10 November 2004, which added a specific section addressing crimes related to the automated processing of data. This legal framework was subsequently reinforced by Law No. 04-09 on the Prevention and Combating of Information and Communication Technology Crimes, which extended the scope of criminalisation to encompass new criminal behaviours in the digital space. Within the framework of the security of personal and medical data, the most significant piece of legislation governing the protection of such data was enacted: Law No. 07-18 on the Protection of Natural Persons in Connection with the Processing of Personal Data.

These legislative amendments aim to achieve three primary objectives: first, to broaden the scope of criminal protection to cover the diverse forms of attacks on information systems; second, to modernise the legal instruments available for combating emerging cybercrimes. Unauthorised entry into or unlawful presence within an information system in whole or in part using fraudulent means, the fraudulent introduction of data into an automated processing system, or the unlawful deletion or modification of data, are all classified as criminal acts under the law. The scope of criminalisation further encompasses the development, collection, distribution, sale, or dissemination of data stored, processed, or transmitted through information systems, as well as the unlawful possession, disclosure, publication, or exploitation of such data. Aggravated penalties apply in cases of data manipulation through deletion or alteration, or when a system's operational functionality is disrupted. [8]

3. VIOLATIONS AGAINST THE AUTOMATED PROCESSING OF PRIVATE MEDICAL DATA :

3.1 Recording Private Medical Data Without Compliance with Legal Conditions :

Any person or entity responsible for the creation or management of medical databases must comply with the following requirements: (i) information must be obtained by lawful means and within legal frameworks; (ii) only relevant and strictly necessary data, proportionate to the declared purposes, may be collected; (iii) the accuracy and reliability of the data must be verified to the greatest possible extent; and (iv) the content of files must be maintained as legally prescribed.

A person responsible for the registration of private medical data is considered to be acting unlawfully if he or she: obtains information by illegal or unfair means;

exploits a position of authority to collect medical data beyond the scope of authorisation; registers data without verifying its accuracy; or unlawfully alters medical records through falsification, forgery, deletion, or addition. In such cases, the offender is subject to the penalties prescribed in the national legislation governing the protection of medical data in the relevant jurisdiction.

3.2 Accessing Private Medical Data Without Legal Authorisation :

Unauthorised access to private medical data constitutes a criminal offence. The right of access is restricted to: (a) members of the medical and paramedical team, within the limits permitted by law and professional custom; and (b) where the exercise of any such professional's practice is suspended, his or her right of access, modification, or deletion is forfeit and may only be reinstated with the written consent of the data subject or the competent authority referred to in paragraph (F301), which determines the persons legally authorised to access the various types of medical databases.[9]

Should any of the aforementioned persons violate the law during a period of suspension of practice by accessing or processing private medical data without authorisation, they commit the crime of unlawful access to medical data, the penalties for which vary in accordance with the legislation and medical laws in force in each jurisdiction.

A person authorised to access private medical data pursuant to paragraph 501 is prohibited from using such data for purposes other than those specified within the scope of his or her professional duties; any departure therefrom constitutes a criminal offence punishable by law, unless one of the following exceptional circumstances applies: (i) use of the data has been authorised by the person concerned or by the authority referred to in paragraph (F301); (ii) the information has been rendered in a form that does not permit the identification of the person concerned; or (iii) the use, although contrary to the stipulated purpose, is accompanied by the additional obligation of obtaining the consent of the person concerned or, in the event of his or her death, the consent of his or her family or personal physician.

Disclosure of the content of a medical file or its data to any party outside the healthcare or public health sphere, or beyond the scope of scientific medical research, is legally prohibited without obtaining explicit written consent from the patient, accompanied by full disclosure of the content of the medical record intended for release in accordance with the principles of medical confidentiality and professional ethics. The law permits the interconnection of information stored in different medical databases for the purposes of medical care provision, public health promotion, and scientific research, provided full compliance with the applicable regulatory and legal controls governing such operations, along with the application of the highest standards of protection and confidentiality.

3.3 Violation of the Storage Duration and Integrity of Private Medical Data :

The time limit for the retention of personal data is determined in accordance with local legislation, which varies between jurisdictions and even between states within certain federal systems. The data controller is legally obliged to adhere strictly to the legally prescribed retention period; failure to do so renders the controller liable to legal accountability and the corresponding penalties, constituting a violation of the regulations governing data storage and a failure to honour the legal obligations incumbent thereupon. [10]

A cybercrime is committed when private medical data are retained without being used for the legitimate purposes of promoting public health, advancing medical

science, or conducting statistical research, in the absence of any legal justification or actual need for the retention of such data by the person concerned.
The processing of private medical data constitutes a cybercrime when the necessary technical measures are not adopted to ensure its protection. Those responsible for such data are obligated to implement rigorous security procedures encompassing advanced encryption systems, strict access controls, and secure backup mechanisms, along with mandatory documentation of all processing and access operations. Failure to comply with these requirements constitutes a violation of the regulations governing the protection of medical data particularly given the highly sensitive nature of such information as it relates to individuals' privacy and health thereby warranting the imposition of deterrent penalties on offenders.

4. FIELD STUDY: ANALYSIS OF MEDICAL DATA PROTECTION IN THE DIGITAL ENVIRONMENT AT THE PUBLIC COMMUNITY HEALTH INSTITUTION OF BORDJ MENAÏEL :

This section aims to identify and detail the methodological procedures and steps to be followed in order to achieve the objectives of the study, which consist in an empirical analysis of medical data protection in the context of digital transformation at the Public Community Health Institution of Bordj Menaïel. It presents the research design, the delineation of the study population and sample, the data collection instruments employed, and the procedures adopted for data collection and analysis.

4.1 Research Methodology :

4.1.1 Survey Instrument Construction :

Data were collected through a structured questionnaire, which constituted the most appropriate instrument for this study, informed by a thorough review of the relevant prior literature. Response scales were constructed in accordance with the Five-Point Likert Scale, as outlined in Table 1 below:

Table 1: Five-Point Likert Scale

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
5	**4**	**3**	**2**	**1**
4.20 – 5.00	3.40 – 4.19	2.60 – 3.39	1.80 – 2.59	1.00 – 1.79
Very High	High	Moderate	Low	Very Low

Source: Compiled by the authors based on SPSS output.

The questionnaire comprised an introductory section serving as a preamble and providing instructions for completion, followed by two substantive parts. Part One gathered personal and demographic data (gender, age, and educational level). Part Two consisted of 25 items designed to measure respondents' knowledge of medical data protection across its various dimensions, as well as their perception of the reality and mechanisms of medical data protection within healthcare institutions. The questionnaire was distributed to 48 employees of the health institution over successive periods spanning one week; 46 completed questionnaires were collected, and 2 were excluded due to invalidity.

4.1.2 Content Validity :

To assess the face validity of the questionnaire, it was submitted for review to two academic faculty members, the Director of the Public Community Health Institution under study, and a senior administrator within the health services, whose feedback was duly incorporated and the instrument revised accordingly before its final deployment to the study sample.

4.1.3 Internal Consistency and Reliability :

The internal consistency and reliability of the questionnaire were assessed using Cronbach's Alpha coefficient, which is widely employed to estimate the degree of homogeneity among a set of items or questions designed to measure the same construct. Cronbach's Alpha ranges between 0 and 1, with higher values indicating greater internal consistency and reliability. The internal consistency results for each axis are presented in Table 2:

Table 2: Cronbach's Alpha Internal Consistency Coefficients

Axis / Dimension	No. of Items	Cronbach's Alpha
Axis I: Knowledge of Medical Data Protection Across All Dimensions	15	–
Legal and Legislative Dimension	03	0.76
Technical and Cybersecurity Dimension	03	0.81
Institutional and Structural Dimension	03	0.73
Human and Awareness Dimension	03	0.70
Compliance and Accountability Dimension	03	0.78
Axis II: Reality and Mechanisms of Medical Data Protection	10	0.84

Source: Compiled by the authors based on SPSS output.

For Axis I (Knowledge of Medical Data Protection Across All Dimensions), Cronbach's Alpha values ranging between 0.70 and 0.81 for each dimension indicate that the items within each dimension are reasonably consistent with the axis they measure a value considered acceptable for research purposes. For Axis II (Reality and Mechanisms of Medical Data Protection in Health Institutions), a Cronbach's Alpha of 0.84 indicates strong inter-item correlations, confirming the internal consistency of the items with the axis they measure.

4.1.4 Statistical Analysis Methods :

Data were processed using a range of statistical methods derived from the SPSS (Statistical Package for the Social Sciences) software. The following analytical approaches were employed:

- Frequency distributions and percentage calculations to characterise the study sample;
- Arithmetic means and standard deviations as measures of central tendency, employed to describe selected study variables;
- Pearson's correlation coefficient to assess the internal consistency of the study axes;

- Cronbach's Alpha to measure the reliability of the questionnaire;
- The validity coefficient to assess construct validity; and
- Correlation coefficients to test the study hypotheses.

4.1.5 Study Sample :

The study sample comprised 46 participants, to whom the questionnaire was administered. The characteristics of the sample are presented in Table 3:

Table 3: Sample Characteristics

Variable	Category	Frequency	Percentage (%)
Gender	Female	28	60.9%
	Male	18	39.1%
Age	Under 30 years	15	32.6%
	31 – 40 years	18	39.1%
	41 – 50 years	10	21.7%
	Over 50 years	3	6.5%
Educational Level	Secondary or below	5	10.9%
	Technician / Senior Technician	12	26.1%
	Bachelor's (Licence)	15	32.6%
	Master's	10	21.7%
	Doctorate (PhD)	4	8.7%
Professional Category	Paramedical	20	43.5%
	Medical	12	26.1%
	Technical	5	10.9%
	Administrative	7	15.2%
	Other	2	4.3%
Professional Experience	Less than 3 years	10	21.7%
	4 – 10 years	16	34.8%
	11 – 15 years	12	26.1%
	More than 15 years	8	17.4%

Source: Compiled by the authors based on SPSS output.

The data presented in Table 3 yield the following observations regarding the characteristics of the 46 study participants:

- Gender: Females constitute the majority of the sample (60.9%) relative to males (39.1%), a distribution reflective of the general gender composition of the workforce at the Public Community Health Institution of Bordj Menaïel.
- Age: The age cohort of 31 to 40 years constitutes the largest proportion (39.1%), followed by those under 30 years (32.6%), indicating a strong representation of both young professionals and those with moderate experience within the sample.

- Educational Level: Holders of a Bachelor's degree (Licence) and Technicians or Senior Technicians constitute the largest proportions of the sample (32.6% and 26.1%, respectively), indicating that the majority of participants hold a post-secondary qualification.
- Professional Category: Paramedical staff predominate within the sample (43.5%), followed by medical staff (26.1%), reflecting the probable structural composition of the workforce within the community health institution.
- Professional Experience: Experience levels are well distributed, with those in the 4-to-10-year category constituting the largest proportion (34.8%), suggesting a healthy mix of relatively new and more experienced employees within the institution.

4.2 Data Analysis :

The results for each survey item are presented below in tabular form, displaying frequencies and percentages for each response option of the Likert scale.

4.2.1 Axis I: Knowledge of Medical Data Protection Across Its Various Dimensions

Legal and Legislative Dimension

Table 4: Arithmetic Mean Distribution – Legal and Legislative Dimension

No.	Item	Mean	Std. Dev.	Direction
01	I am familiar with the key laws and regulations pertaining to medical data protection.	3.78	1.15	Agree
02	I believe that patients' rights regarding their digital medical data are being respected.	3.89	1.01	Agree
03	The legal responsibilities of relevant staff members are clearly communicated.	3.28	1.09	Neutral
	Legal and Legislative Dimension (Overall)	**3.65**	**1.01**	**Agree**

Source: Compiled by the authors based on SPSS output.

The results indicate that the level of knowledge of the laws and regulations pertaining to medical data protection is moderate, with the majority of participants tending towards the "Agree" and "Neutral" response options. A non-negligible proportion of participants also expressed disagreement. With respect to respect for patients' rights, a similar trend is observed. Regarding the clarification of legal responsibilities, the relatively high proportions of "Neutral" and "Disagree" responses suggest a need to strengthen communication and awareness concerning these responsibilities. Standard deviations ranging between 1.01 and 1.15 indicate a moderate degree of dispersion in opinions concerning these legal aspects.

Technical and Cybersecurity Dimension

Table 5: Arithmetic Mean Distribution – Technical and Cybersecurity Dimension

No.	Item	Mean	Std. Dev.	Direction
04	The institution uses essential security technologies to protect digital data.	3.70	0.95	Agree
05	Systems and applications are regularly updated and maintained.	3.67	1.03	Agree

06	The institution relies on security monitoring systems to alert us in the event of suspicious activities.	2.87	1.02	Neutral
	Technical and Cybersecurity Dimension (Overall)	**3.41**	**0.93**	**Agree**

Source: Compiled by the authors based on SPSS output.

The data in Table 5 reveal that the majority of participants agree that the institution employs basic security technologies and performs regular system updates. Nevertheless, a higher proportion of "Neutral" responses is observed with respect to security monitoring systems, which may indicate that these systems lack visibility for some staff members or are not perceived as fully effective. Standard deviations ranging between 0.95 and 1.03 indicate an acceptable to moderate degree of dispersion in opinions.

Institutional and Structural Dimension

Table 6: Arithmetic Mean Distribution – Institutional and Structural Dimension

No.	Item	Mean	Std. Dev.	Direction
07	Clear policies exist governing the collection, storage, and sharing of data.	3.74	1.00	Agree
08	A specific department or unit is designated as responsible for implementing data protection policies.	3.86	0.97	Agree
09	Procedures exist for responding to data breach incidents.	3.00	1.01	Neutral
	Institutional and Structural Dimension (Overall)	**3.53**	**1.03**	**Agree**

Source: Compiled by the authors based on SPSS output.

A tendency toward agreement on the existence of policies and a designated unit responsible for data protection is evident; however, the proportion of "Neutral" responses remains elevated, suggesting that these policies and responsibilities may not be clearly communicated to all staff members. With respect to procedures for managing data breaches, the mean response tends toward "Neutral," underscoring the necessity of clarifying and disseminating these procedures more effectively. Standard deviations ranging between 0.97 and 1.01 indicate a moderate degree of dispersion in opinions.

Human and Awareness Dimension

Table 7: Arithmetic Mean Distribution – Human and Awareness Dimension

No.	Item	Mean	Std. Dev.	Direction
10	Staff receive adequate foundational training on the secure handling of data.	3.07	0.98	Neutral
11	I know to whom I can report any concerns related to data protection.	3.85	0.99	Agree
12	Staff are periodically reminded of the importance of data protection.	2.87	1.05	Neutral
	Human and Awareness Dimension (Overall)	**3.26**	**0.99**	**Neutral**

Source: Compiled by the authors based on SPSS output.

The results indicate that training in the secure handling of data may be insufficient or inadequate from the perspective of participants, with "Neutral" constituting the

predominant response. Knowledge of reporting channels for data protection concerns is relatively satisfactory; however, periodic reminders concerning the importance of data protection fall within the moderate range. Standard deviations ranging between 0.98 and 1.05 indicate a moderate degree of dispersion in opinions.

Compliance and Accountability Dimension

Table 8: Arithmetic Mean Distribution – Compliance and Accountability Dimension

No.	Item	Mean	Std. Dev.	Direction
13	There is monitoring of staff compliance with data protection policies.	2.83	0.96	Neutral
14	Accountability procedures exist in the event of data protection violations.	3.15	1.02	Neutral
15	I believe the institution generally seeks to comply with applicable laws and regulations.	3.69	0.92	Agree
	Compliance and Accountability Dimension (Overall)	**3.22**	**0.99**	**Neutral**

Source: Compiled by the authors based on SPSS output.

A moderate level of awareness concerning monitoring of compliance with policies is apparent; however, greater uncertainty is evident regarding the existence of clear accountability procedures in the event of violations with "Neutral" constituting the predominant response. The majority of participants agree that the institution generally seeks to comply with applicable laws and regulations. Standard deviations ranging between 0.92 and 1.02 indicate a moderate degree of dispersion in opinions.

4.2.2 Axis II: Reality and Mechanisms of Medical Data Protection in Health Institutions

Table 9: Arithmetic Mean Distribution – Reality and Mechanisms of Medical Data Protection

No.	Item	Mean	Std. Dev.	Direction
01	The institution effectively relies on mechanisms for the protection of digital data.	3.76	0.91	Agree
02	Access to medical data is restricted according to rank or functional authorisation.	3.85	0.88	Agree
03	Access to medical records is documented (access logs).	3.68	1.01	Agree
04	Bodies or designated officers are in place to oversee compliance with digital data protection.	3.82	0.96	Agree
05	Periodic audits of the security and protection of the information system are conducted.	2.76	0.98	Neutral
06	Clear procedures exist for reporting any security breach or data intrusion.	2.89	0.99	Neutral
07	Medical and administrative staff are included in workshops or meetings concerning data protection.	3.17	1.00	Neutral
08	Technical resources are adequate to guarantee the security of medical data.	3.76	0.95	Agree

09	There is coordination between the technical and administrative departments to ensure data protection.	3.69	0.97	Agree
10	I believe the institution effectively respects the national standards for the protection of medical data.	3.82	0.94	Agree
	Axis II: Reality and Mechanisms (Overall)	**3.52**	**0.95**	**Agree**

Source: Compiled by the authors based on SPSS output.

The results indicate that the majority of participants agree that the institution employs mechanisms for data protection, restricts access according to functional authorisation, and maintains documentation of access operations. Consensus also exists regarding the presence of designated oversight bodies and interdepartmental coordination. Nevertheless, greater uncertainty is expressed concerning the effectiveness of periodic audits, the clarity of breach-reporting procedures, the involvement of staff in awareness workshops, and the adequacy of technical resources. There appears to be a general perception that the institution respects national standards, though certain areas may require strengthening and clarification. Standard deviations ranging between 0.88 and 1.01 indicate an acceptable to moderate degree of dispersion in opinions.

4.3 Testing the Study Hypotheses：

Having completed the descriptive analysis of the data for each study dimension which provided an initial overview of participants' opinions and responses regarding their knowledge of medical data protection and their perception of the reality and mechanisms of its application within the institution the analysis now proceeds to the more rigorous stage of hypothesis testing. This section aims to statistically verify the hypothesised relationships between the variables identified in the theoretical framework of the study, drawing on the output of the SPSS software.

Inferential statistical methods (Inferential Statistics) were employed to test the sub-hypotheses derived from the main hypothesis of the study. This approach is grounded in the use of data collected from the study sample to draw inferences concerning the broader population from which the sample was drawn. Given the nature of the hypotheses which posit the existence of correlational relationships between the dimensions of medical data protection knowledge and the perceived level of application of medical data protection mechanisms correlation analysis was adopted as the primary statistical tool.

The correlation coefficient (Correlation Coefficient) ranges between -1 and +1, where values approaching +1 indicate a strong positive correlation, values approaching -1 indicate a strong negative correlation, and values approaching 0 indicate a weak or non-existent correlation. In light of the ordinal nature of Likert-scale data and the potential non-normality of their distribution, Spearman's rank correlation coefficient (ρ) was deemed the most appropriate statistical measure.

4.3.1 Correlation Matrix

Variable	LLD(K)	TCD(K)	ISD(K)	HAD(K)	CAD(K)	P.Legal	P.Tech	P.Instit	P.Aware	P.Control
LLD (K)	1	.352**	.489**	.287*	.415**	.521**	.318*	.456**	0.25	.389**
TCD (K)	.352**	1	.512**	.401**	.478**	.385**	.689**	.495**	.330*	.552**
ISD (K)	.489**	.512**	1	.455**	.530**	.610**	.501**	.723**	.392**	.638**
HAD (K)	.287*	.401**	.455**	1	.369**	.310*	.428**	.411**	.585**	.447**
CAD (K)	.415**	.478**	.530**	.369**	1	.450**	.525**	.518**	.305*	.691**
P. Legal	.521**	.385**	.610**	.310*	.450**	1	.402**	.655**	.280*	.510**
P. Tech	.318*	.689**	.501**	.428**	.525**	.402**	1	.532**	.355**	.605**
P. Instit	.456**	.495**	.723**	.411**	.518**	.655**	.532**	1	.370**	.680**
P. Aware	0.25	.330*	.392**	.585**	.305*	.280*	.355**	.370**	1	.362**
P. Control	.389**	.552**	.638**	.447**	.691**	.510**	.605**	.680**	.362**	1

Table 10: Correlation Matrix

Source: Compiled by the authors based on SPSS output.
Note: ** = significant at $p < 0.01$; * = significant at $p < 0.05$. LLD = Legal & Legislative Dimension; TCD = Technical & Cybersecurity Dimension; ISD = Institutional & Structural Dimension; HAD = Human & Awareness Dimension; CAD = Compliance & Accountability Dimension; P. = Perceived application of.

This section evaluates the correlation between employee knowledge across five distinct dimensions and their perceived efficacy of the corresponding medical data protection mechanisms. All five sub-hypotheses were validated at a high level of statistical significance ($p < 0.01$), leading to the acceptance of the main hypothesis.

- **Legal and Legislative Dimension (r = 0.521):** A moderate-to-strong positive correlation was observed, indicating that increased legal literacy significantly enhances an employee's perception of how effectively regulatory mechanisms are applied within the institution.
- **Technical and Cybersecurity Dimension (r = 0.689):** A very strong positive correlation confirms that technical knowledge is a critical driver of awareness regarding the effectiveness of digital security measures and cybersecurity protocols.
- **Institutional and Structural Dimension (r = 0.723):** Yielding the highest correlation coefficient in the study, this result suggests that a clear understanding of organizational hierarchy and responsibilities is intrinsically linked to a positive perception of institutional protective structures.
- **Human and Awareness Dimension (r = 0.585):** This moderate-to-strong correlation demonstrates that as employees become more aware of the "human factor" in data security, their appreciation for internal sensitization and awareness campaigns increases.
- **Compliance and Accountability Dimension (r = 0.691):** A very strong correlation indicates that a solid grasp of compliance requirements is strongly associated with the perceived presence of effective monitoring and auditing mechanisms.

Conclusion: Validation of the Main Hypothesis

The consistent statistical significance across all sub-hypotheses confirms the study's **Main Hypothesis**: there is a definitive, positive effect of employee knowledge on the perceived reality of medical data protection. These findings underscore that enhancing employee education is not merely a theoretical exercise; it fundamentally shapes the internal culture of security and the perceived legitimacy of the institution's protective safeguards.

CONCLUSION:

The theoretical framework of the study provided a comprehensive perspective on the importance of medical data protection in the digital age, shedding light on the legal and legislative, technical and cybersecurity, institutional and structural, human and awareness-related, and compliance and accountability dimensions that together constitute an integrated system for the protection of this sensitive data. The theoretical analysis confirmed that medical data protection is not merely a legal and ethical obligation, but an imperative necessity for the preservation of patients' rights, the guarantee of quality health services, and the reinforcement of public trust in the healthcare system. It further demonstrated that the effectiveness of medical data protection depends upon the integration and synergy of the efforts of all relevant parties from the formulation of clear policies and procedures, through the deployment of appropriate security technologies, to the awareness and training of personnel and the monitoring of compliance.

Notes

[1] Article 47, Constitution of the People's Democratic Republic of Algeria, Official Gazette No. 82, issued on 15 Jumada al-Ula 1442 AH, corresponding to 30 December 2020.
[2] Article 303 of Law No. 06-23, dated 29 Dhu al-Qi'da 1427 AH (20 December 2006), amending and supplementing Order No. 66-156 of 18 Safar 1386 AH (8 June 1966) containing the Penal Code, Official Gazette No. 84, dated 24 December 2006.
[3] Article 24 of Law 11-18 on Health.
[4] Ahmad Tariq Afif Mursid, cited in: Ahmad Sadiq, Electronic Crime, op. cit., p. 23.
[5] Nabila Harwal, Internet Crimes, op. cit., p. 56.
[6] Talal Yasir al-'Isa and 'Adi Muhammad 'Annab, "International Responsibility Arising from Cyberattacks in the Light of Contemporary International Law," Al-Zarqa Journal for Research and Humanities, Vol. 19, No. 1, Jordan, 2018, p. 16.
[7] Ibid., p. 28.
[8] Marouk Nasr al-Din, The Right to Privacy, op. cit., p. 67.
[9] Muhammad al-Asadi, The Effectiveness of Criminal Law Provisions in Combating Cybercrime, op. cit., p. 78.
[10] Kim Bartel Sheehan and Mariea Grubbs Hoy, "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns," The Journal of Advertising, Vol. 28, No. 3, Fall 1999, p. 39.

References:

Legal and Regulatory Texts :

Constitution of the People's Democratic Republic of Algeria. (2020). *Official Journal of the Algerian Republic*, No. 82, December 30, 2020.

Law No. 18-07 on the protection of natural persons in the processing of personal data. (2018).

Law No. 11-18 relating to health. (2018). *Official Journal of the Algerian Republic*.

Law No. 16-04 on the prevention and fight against ICT-related offenses. (2016). *Official Journal of the Algerian Republic*, No. 62.

Executive Decree No. 22-252 establishing the National Agency for Digital Health. (2022). *Official Journal of the Algerian Republic*, No. 44.

Books :
Basdevant, A., & Mignard, J.-P. (2017). *The empire of data: Essays on society, algorithms, and law*. Don Quichotte.
Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Academic Press.
Jabbour, M., & Jabbour, M. (2018). *Personal data and Arab legislation: Security concerns and individual rights*. Arab Center for Legal and Judicial Research.
Arab, Y. (2017). *Information security and privacy guide*. Dar Al-Masirah.
Peer-Reviewed Journal Articles
Mantelero, A., Vaciago, G., Esposito, M. S., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, 28.
Detsky, A. S., & Garber, A. M. (2016). Uber's message for health care. *The New England Journal of Medicine*.
Denis, F., Lethrosne, C., Pourel, N., et al. (2017). Randomized trial comparing a web-mediated follow-up with routine surveillance in lung cancer patients. *American Journal of Clinical Oncology*.
Ennis, L., Rose, D., Callard, F., Denis, M., & Wykes, T. (2011). Rapid progress or lengthy process? Electronic personal health records in mental health. *BMC Psychiatry*, 11, 117.
Reports and Institutional Publications :
Council of Europe. (2020). *Digital solutions to fight COVID-19: Data protection report*.
European Commission. (2017). *Health data: Saving lives and protecting patients' rights*.
Conference Proceedings :
Bougherra, K., & Mahfoudh, A. (2024). The role of smart technologies in improving healthcare service quality: Blockchain as a model. In *Proceedings of the International Conference on Digital Transformation in Public Healthcare Organizations*, Higher School of Social Security, Algeria.