International Journal of Law and Jurisprudence
Volume 15 · Issue 2 · 2026 · Pages 1963–1977
e-ISSN 2255-1824 (Online) · revistaidj.com/IJLJ

Towards A Legal Framework for Artificial Intelligence (AI) in the Health Sector: Data Protection and Improving Health Outcomes in Algerian Legislation

Dr. MERNIZ Fatima

Faculty of Law - Relizane University, Algeria, Email: mernizfatima@yahoo.com

Received: 26 March 2026 | **Accepted:** 27 July 2026 | **Published:** 18 October 2026

Abstract

The Rapid Integration of Artificial Intelligence (AI) into the Healthcare Sector has brought about a Qualitative Shift in the Delivery of Medical Services by Enhancing Diagnostic Accuracy, Supporting Clinical Decision-Making, Optimizing Resource Allocation, and Bolstering Healthcare Security. Conversely; The Expanding Usage of Artificial Intelligence (AI) Technologies has raised Growing Legal and Ethical Challenges, particularly regarding the Protection of Patients' Personal Health Data, the Preservation of Privacy, the Assurance of Transparency, and the Determination of Legal Liability. Accordingly; This Study Seeks to Address the Following Question: **To What Extent Does Artificial Intelligence (AI) Contribute to Enhancing Healthcare Security, Protecting Patient Data, and Improving Health Outcomes? Furthermore; How Adequate is Algerian Legislation in Regulating Its Use and Ensuring the Protection of Individuals' Fundamental Rights?**

The Study Employs an Analytical Approach to Examine the Relevant Algerian Legislative Framework—Specifically the Provisions of the Constitution, the Health Law, and the Law on the Protection of Natural Persons regarding the Processing of Personal Data. It Also Utilizes a Comparative Approach by Drawing Upon the Latest Regulatory Developments Introduced by International Organizations and the European Union Concerning Artificial Intelligence (AI) Governance in the Healthcare Sector.

The Study Concludes that Artificial Intelligence (AI) Serves as A Strategic Tool for Enhancing Healthcare Security. However; The Effective and Safe Implementation of these Technologies remains Contingent Upon a Comprehensive Legal Framework that Ensures the Security of Health Data, Enhances the Transparency and Explainability of Algorithms, Clearly Defines Legal Liability, and Provides Effective Safeguards for the Protection of Patients' Fundamental Rights.

Keywords: Artificial Intelligence (AI); Healthcare Security; Patient Data Protection; Health Outcomes; Algerian Legislation.

Introduction:

The Healthcare Sector is Undergoing a Transformative Shift Driven by Artificial Intelligence (AI) Technologies, which have Contributed to Advancements in Diagnosis and Treatment, Health Resource Management, and the Highly Efficient Analysis of Medical Data. This Evolution has reshaped the Concept of Health Security; It now Extends beyond merely Ensuring the Continuity of Medical Services to Encompass the Protection of Health Data, the Enhancement of Care Quality, the Mitigation of Health Risks, and the Strengthening of Health Systems' Crisis-Response Readiness. Consequently; Artificial Intelligence (AI) has Emerged as A Pivotal Tool for Supporting Health Security—Provided Its Use is Governed by A Legal and Ethical Framework that Safeguards Rights and Freedoms.

Against this Backdrop; Many Countries and International Organizations have Moved to Develop Specialized Regulatory Frameworks to Keep Pace with the Growing Use of Artificial Intelligence (AI) in the Healthcare.[1] Furthermore; The Governance of these Technologies—Grounded in Transparency, Accountability, and Human Oversight—has become A Fundamental Prerequisite for Fostering Trust and Supporting Health Security.

This; A Review of the Literature reveals A Clear Research Gap; Most Studies have Focused on Technical, Ethical, or General Regulatory Aspects, whereas the Relationship between Healthcare Security, Patient Data Protection, and the Improvement of Health Outcomes has not received A Comprehensive Legal Analysis Integrating these Dimensions into A Single Framework. Furthermore; There is A Scarcity of Studies addressing this Issue within the Context of Algerian Legislation or Evaluating the Readiness of the Algerian Legal System to Accommodate the Requirements of Artificial Intelligence (AI) Governance in the Health Sector, in Light of Recent International Legislative Developments.

Hence; This Study Seeks to Fill this Gap by Providing an Integrated Legal Analysis that Links these Three Dimensions, while Taking Advantage of the Latest International Regulatory Trends to Assess the Adequacy of Algerian Legislation, and Proposing

Mechanisms to Enhance the Safe and Responsible Use of Artificial Intelligence (AI) in the Field of Health Care.

In Light of the Foregoing; The Core Problem addressed by this Study Crystallizes around the Following Central Issue: **To What Extent Does Artificial Intelligence (AI) Contribute to Enhancing Healthcare Security by Protecting Patient Data and Improving Health Outcomes? Furthermore; How Adequate is Algerian Legislation in Regulating Its Use to Strike the Balance between Fostering Innovation and Ensuring the Protection of Individuals' Fundamental Rights?**

The Study Employs the Analytical Approach by Examining Relevant Algerian Legal Texts to Determine their Capacity to Address Emerging Legal Issues Associated with Artificial Intelligence (AI). It Also Utilizes the Comparative Approach to Explore Key International Legislative Trends—Particularly those Introduced by the European Union's Artificial Intelligence (AI) Act—with the Aim of Identifying Best Practices for Artificial Intelligence (AI) Governance in the Healthcare Sector.

The Scholarly Contribution of this Study Lies in Providing a Comprehensive Legal Analysis that Integrates Three Interconnected Pillars—Healthcare Security, Health Data Protection, and the Improvement of Health Outcomes—While Assessing the Readiness of Algerian Legislation to Keep Pace with the Digital Transformation of the Health Sector. Furthermore; The Study Proposes a Set of Legislative and Regulatory Recommendations Designed to Strengthen the Protection of Patients' Fundamental Rights and to Embed Principles of Transparency, Accountability, and Explainability within Artificial Intelligence (AI) Systems, thereby; Striking A Balance between Fostering Innovation and Ensuring Legal Certainty in the Healthcare Domain.

Accordingly; This Article is Organized into Two Main Chapters; The First Chapter addresses the Conceptual and Functional Framework of Artificial Intelligence (AI) in Enhancing Healthcare Security, while the Second Chapter Examines the Role of Artificial Intelligence (AI) in Protecting Patient Data and Improving Health Outcomes.

1st Chapter: The Conceptual Framework of Artificial Intelligence (AI)-Supported Health Security

Artificial Intelligence (AI) has Emerged as A Pivotal Technology Capable of Driving a Qualitative Transformation in the Health Sector by Supporting Medical Diagnosis, Analyzing Big Data, Predicting Diseases and Epidemics, and Enhancing the Efficiency of Health Resource Management. Numerous International Reports have affirmed that the Responsible Use of Artificial Intelligence (AI) Holds Significant Potential to Improve the Quality of Healthcare and Boost the Effectiveness of Health Systems, thereby Contributing to Higher Levels of Health Security for Individuals and Communities.[2]

Accordingly; This Chapter is addressed through Two Sections; The First Outlines the Concept of Health Security and Its Dimensions, while the Second Examines the Role of Artificial Intelligence (AI) in Strengthening Health Security and the Challenges Associated with Its Application in the Health Sector.

1st Section: The Concept of Health Security

Health Security is A Concept that has Gained Increasing Importance in Contemporary Legal Studies and Public Policy, driven by the Rise of Cross-Border Health Risks and the Challenges They Pose to Nations and Societies. Global Health Crises—Particularly Widespread Epidemics—have Highlighted the Pivotal Role of Health Security as A Component of Human Security and A Fundamental Pillar for Achieving Sustainable Development, Ensuring the Continuity of Health Facilities, and Protecting the Right to Health.[3]

The Concept of Health Security is No Longer Limited to Disease Prevention and Epidemic Control; It has Expanded to Encompass Strengthening Health Systems' Capacity to Anticipate and Respond to Risks, Ensuring the Availability of Essential Health Services, and Protecting Health Infrastructure and Medical Data Amidst the Rapid Digital Transformation of the Health Sector.[4] In this Context; Health Security has become Closely Linked to the Ability of Nations to Employ Modern Technology Safely and Effectively, thereby Ensuring the Sustainability of Health Services and the Protection of Patients' Rights.

Accordingly; A Comprehensive Understanding of the Concept of Health Security requires; First; Defining Its Meaning and Outlining Its Fundamental Characteristics, and Subsequently Examining Its Dimensions and Requirements, given that It Serves as An Integrated Framework for Protecting Public Health and Enhancing the Efficiency of Health Systems. Therefore; This Section will be addressed by Defining Health Security in the First Subsection and then Outlining Its Dimensions and Requirements in the Second Subsection.

1st Subsection: Definition of Health Security

To Begin with; Legal Scholarship has not Settled on A Unified Definition of Health Security, given Its Multifaceted Nature and Its Intersection with the Fields of Security, Development, and Public Health. At the International Level; The World Health Organization Defines Health Security As: "The Activities Required—whether Proactive or Reactive—to Minimize the Risk and Impact of Acute Public Health Events that Endanger People's Health across Geographical Regions and International Boundaries".[5] This Definition Highlights the Preventive and Proactive Nature of Health Security, as well as Its Link to International Cooperation in Addressing Transboundary Health Risks.

From A Legal and Scholarly Perspective; American Jurist Lawrence O. Gostin Defines It As: "The Capacity of States and Health Institutions to Prevent, Detect, and Respond to Health Threats in A Manner that Ensures the Protection of Public Health and the Continued Delivery of Essential Health Services to the Population".[6] This Definition Focuses on Institutional Preparedness and the Capacity of Health Systems to Confront Crises and Emergencies.

As David B. Fiedler Views It; Health Security Constitutes the Set of Legal and Institutional Measures aimed at Addressing Health Risks that Could affect the Security of States—as well as their Political, Economic, and Social Stability—thereby Reflecting the Growing Interconnection between Health and National Security in Contemporary International Relations.[7]

From A Legal Perspective; The International Health Regulations (2005 CE) did not Establish an Explicit Definition of Health Security, however; They Laid an International Legal Framework Aimed at Preventing, Detecting, Reporting, and Responding to Public Health Risks in A Manner that is Effective and Proportionate to the Magnitude of the Risk, thereby Limiting the International Spread of Diseases and Ensuring the Protection of Public Health.[8]

The Concept of Health Security has acquired A More Comprehensive Dimension Following the COVID-19 Pandemic; Beyond Disease Prevention and Epidemic Control; It Now Encompasses Strengthening Health System Resilience, Ensuring the Continuity of Medical Services, and Protecting Health Infrastructure and Medical Data Amidst the Sector's Rapid Digital Transformation. Furthermore; Artificial Intelligence (AI) Applications and Big Data Analytics Have Contributed to Reshaping the Concept of Health Security to Include Digital and Technological Dimensions that were not Previously addressed to the Same Extent.[9]

Based on An Analysis of the Aforementioned Definitions, Health Security—For the Purposes of this Study—Can be Defined As: “A State of Protection and Preparedness Ensured by the State through An Integrated Legal, Institutional, and Technical System aimed at Preventing Health Risks, Detecting them Early, and Responding to them Effectively, while Ensuring the Continuity of Health Services and the Protection of Medical Data and Information, thereby Safeguarding the Right to Health and Achieving Health Safety for Individuals and Society”.

This Definition is Characterized by Its Comprehensiveness, Integrating Preventive, Therapeutic, Regulatory, and Digital Dimensions—An Approach that aligns with the Study’s Focus on Artificial Intelligence (AI)-Supported Health Security and Its Role in Protecting Patient Data and Improving Health Outcomes.

2nd Subsection: Dimensions of Health Security

Health Security is no longer a One-Dimensional Concept Limited to Combating Diseases and Epidemics, rather; It has Evolved into An Integrated Framework Comprising a Set of Interconnected Dimensions. These aim to Protect Individual Health, Ensure the Sustainability of Health Systems, and Bolster their Capacity to Confront Both Traditional and Emerging Health Risks. The Importance of these Dimensions is Further Heightened by the Rapid Technological Advancements in the Health Sector and the Resulting New Requirements for Ensuring the Security of Health Services and Medical Data.

The First Dimension is **the Preventive Dimension**, which Focuses on Taking the Necessary Measures to Prevent the Spread of Diseases, Detect Health Risks Early, and Mitigate their Impact before They Escalate into Large-Scale Crises. This Encompasses Epidemiological Surveillance Programs, Early Warning Systems, Vaccination, Health Awareness Initiatives, and Other Mechanisms that Enhance the Preparedness of the Health System to Address Potential Threats.[10]

As for **the Therapeutic and Service-Oriented Dimension**; It Pertains to Ensuring the Provision of Effective and Equitable Health Services for—All Members of Society, Encompassing Diagnosis, Treatment, and Both Primary and Specialized Healthcare. This Dimension Serves as A Key Indicator of a State’s Capacity to Protect the Right to Health and Achieve Health Security for Its Citizens—Particularly During Crises and Health-Related Disasters.[11]

The Institutional and Organizational Dimension Also Stands Out, characterized by the Existence of a Legal and Institutional Framework Capable of Managing Health Risks and Coordinating the Efforts of Various Stakeholders in the Health Sector. This requires Formulating Clear Health Policies, Establishing Emergency Response Mechanisms, and Developing the Human and Technical Capacities of Health Institutions to Ensure Rapid and Effective Intervention During Crises.[12]

With the Digital Transformation Sweeping the Healthcare Sector; **The Digital and Cyber Dimensions** of Health Security have Emerged as Critical, Modern Aspects of the Field. The Reliance of Healthcare Institutions on Health Information Systems, Electronic Medical Records, and Artificial Intelligence (AI) Technologies has Created New Challenges regarding the Protection of Health Data against Breaches, Tampering, or illicit Use. Consequently; The Integrity of Digital Infrastructure has become An Integral Component of the Contemporary Concept of Health Security, given the Severe Consequences that Targeting Such Infrastructure Could have on Patient Lives and the Continuity of Health Services.[13]

Health Security Also Encompasses **a Rights-Based and Ethical Dimension**, which relates to the Protection of Individuals' Fundamental Rights—Foremost among them the Right to Health, the Right to Privacy, and the Confidentiality of Medical Information. This Dimension is Gaining Increasing Importance with the Expanding Usage of Artificial Intelligence (AI) Technologies in the Healthcare Sector, necessitating A Balance between Leveraging Technological Innovation and Ensuring that Patients' Rights are respected and that No Discrimination Occurs.[14]

Achieving these Dimensions requires Several Fundamental Prerequisites, most notably; An Effective Legislative Framework that regulates the Health Sector and Protects Health Data; Advanced Health and Digital Infrastructure; The Enhancement of Human and Technical Capabilities for Healthcare Professionals; And the Promotion of Scientific Research and Innovation in Modern Health Technologies. Furthermore; It Necessitates Strengthening International Cooperation to Address Cross-Border Health Threats, as well as the Exchange of Information and Expertise—All of which Contribute to Improving Preparedness and Response to Health Crises.[15]

Thus; It becomes Clear that Health Security is no longer Limited to Preventive or Curative Measures alone, rather; It has Evolved into An Integrated System Encompassing Health, Legal, Regulatory, and Digital Dimensions. This Explains the Growing Interest in Leveraging Artificial Intelligence (AI) Technologies to Enhance the Efficiency of this System and Achieve Higher Levels of Health Protection and Security.

It Should be noted that the Algerian Legislator has not yet Established a Specific Legal Framework for Health Security or for Artificial Intelligence (AI) in the Healthcare Sector—at least not in the Strict Sense of these Terms. Nevertheless; The Legislative Trend reveals A Growing Interest in Protecting the Digital Environment Upon Which Modern Healthcare Systems are Built. This is Primarily Evidenced by Law No. 18-07 of (June 10, 2018 CE), Concerning the Protection of Natural Persons with Regard to the Processing of Personal Data—As Amended and Supplemented by Law No. 25-11 of (2025 CE)—which has Established a Legal Framework for the Protection of Personal Data, including Health-Related Data, which is Considered Sensitive Information and thus requires A Higher Level of Legal Protection.

This Approach reflects the Legislator's Awareness of the Risks Posed by Digital Advancement and the Reliance of Healthcare Institutions on the Automated Processing of Data. Consequently; The Collection, Storage, and Processing of Personal Data have been Made Subject to A Set of Controls—Pertaining to Legality, Transparency, Security, and Confidentiality—Designed to Safeguard Individuals' Private Lives and Mitigate the Risks of illicit Exploitation of Health Data. Furthermore; The Establishment of a National Authority for the Protection of Personal Data represents A Significant Institutional Step toward Strengthening Oversight of Data Processing Operations and Fostering Trust within the Digital Environment.

On the Other Hand; The Algerian Legislator is Gradually Moving toward Strengthening Cybersecurity and the Governance of Digital Data—Both of which are Fundamental Requirements for Modern Health Security, especially given the Expanding Use of Electronic Medical Records and Digital Health Platforms. Although Algerian Legislation has yet to Regulate the Legal Liability Arising from Medical Decisions Based on Artificial Intelligence (AI) Systems; The General Rules Concerning the Protection of Personal Data and the Right to Privacy Provide a Legal Foundation Upon which a Future Legislative Framework for Artificial Intelligence (AI) in the Healthcare Sector Can be Built.

Accordingly; It Can be Said that the Current Approach of the Algerian Legislator is Focused on Protecting the Legal Framework for Health Data and Digital Privacy, as these Constitute Fundamental Pillars of Health Security. However; The Rapid Evolution of Artificial Intelligence (AI) Applications Necessitates a Transition from General Data Protection toward a Specialized Legal Regime—One that Defines the Conditions for Using Intelligent Systems in the Healthcare Sector, establishes Safeguards for their Operation, and Sets Out Mechanisms for Accountability regarding Any Harm They May Cause.

2nd Section: The Role of Artificial Intelligence (AI) in Strengthening Health Security and Its Challenges

Evaluating the Role of Artificial Intelligence (AI) in Strengthening Health Security requires More than Just Highlighting Its Practical Advantages and Benefits; It Also Necessitates an Examination of the Legal Challenges Posed by Its Applications in the Healthcare Sector. The Goal is to Strike a Balance between the Requirements of Technological Innovation and the Protection of Individuals' Fundamental Rights and Freedoms. Accordingly; This Section will First address the Contributions of Artificial Intelligence (AI) to Strengthening Health Security; Followed by An Analysis of the Legal and Ethical Challenges Associated with Its Use in the Healthcare Field.

1st Subsection: Contributions of Artificial Intelligence (AI) to Strengthening Health Security

Artificial Intelligence (AI) has Emerged as A key Modern Pillar for Enhancing Health Security, Offering Advanced Capabilities for Predicting Health Risks, Improving the Quality of Medical Services, Supporting Decision-Making, and Bolstering the Readiness of Health Systems to Confront Epidemics and Health-Related Disasters. In the Digital Era; Health Security is no longer Limited to the Provision of Curative Services; It has Expanded to Encompass the Capacity to Manage Health Risks—Leveraging Big Data and Intelligent Algorithms—Thereby Ensuring the Protection of the Health of Individuals and Society in A More Efficient and Sustainable Manner.[16]

In Algeria; Although the Use of Artificial Intelligence (AI) in the Healthcare Sector is A Recent Development, Legislative Trends and Public Policies reflect A Growing Interest in the Digitalization of the Healthcare System—Viewed as A Fundamental Pillar for Achieving National Health Security—As Evidenced by A Range of Legal Texts and National Strategies.[17]

Firstly: Enhancing Disease Prevention and Early Detection

One of the Most Significant Contributions of Artificial Intelligence (AI) Lies in Its Ability to Analyze Vast Amounts of Health Data in Record Time, Uncovering Hidden Patterns that May Signal the Onset or Spread of Diseases. Through Machine Learning and Deep Learning Technologies; It has become Possible to Analyze Medical Images, Electronic Health Records, and Epidemiological Data, Enabling the Early Detection of Chronic Diseases, Cancers, and Infectious Diseases before Clinical Symptoms Manifest.[18]

Artificial Intelligence (AI) Also Contributes to the Development of Early-Warning Systems Based on Epidemiological Data to Monitor the Potential Spread of Infectious Diseases. This Assists Health Authorities in Taking Preventive Action before Such Situations Escalate into Large-Scale Health Crises—A Fact Clearly Demonstrated During the COVID-19 Pandemic.[19]

In Algeria; **Law No. 18-11 on Health** Enshrines the Principle of Prevention as A Cornerstone of the National Health Policy, mandating that the State Implement the Necessary Measures for Disease Prevention and the Promotion of Public Health.[20]

Secondly: Improving the Quality of Diagnosis and Treatment

Artificial Intelligence (AI) has Brought about A Qualitative Shift in Medical Diagnostics; Algorithms are Now Capable of Analyzing X-Rays, Magnetic Resonance Imaging (MRI) Scans, and Computed Tomography (CT) Scans with High Precision, thereby Reducing Medical Errors and Accelerating the Diagnostic Process.[21]

Furthermore; Artificial Intelligence (AI) Supports Precision Medicine by Tailoring Treatment Plans to the Specific Genetic and Biological Characteristics of Each Patient, which Helps Improve Health Outcomes and Minimize Complications.[22]

Algerian Law No. 18-11 on Health;[23] Affirms the Right of Patients to Access High-Quality Healthcare Services. Healthcare Institutions are Also required to Provide Scientific and Technical Resources Capable of Improving Healthcare, which Paves the Way for Integrating Artificial Intelligence (AI) Applications into Diagnosis and Treatment.

Thirdly: Supporting the Management of Epidemics and Health Crises

The COVID-19 Pandemic Demonstrated that Artificial Intelligence (AI) has become An Essential Tool for Managing Health Crises. It was Utilized to Predict the Spread of Infections, Track Chains of Virus Transmission, Analyze Epidemiological Data, Manage Medical Resources, and Prioritize Treatment.[24]

Artificial Intelligence (AI) Also Contributes to Improving Hospital Management by Forecasting Patient Numbers, Managing Hospital Beds, and Efficiently Distributing Equipment and Medication—All of which Strengthen the Healthcare System's Capacity to Respond to Health Emergencies.[25]

In Algeria; The State—Under the Health Law—Bears the Responsibility for Preventing Health Risks and Combating Epidemics. Furthermore; The Experience of the COVID-19 Pandemic accelerated the Shift toward the Digitalization of the Health Sector, Creating A Suitable Foundation for the Future Deployment of Artificial Intelligence (AI) Technologies.[26]

Fourthly: Supporting Scientific Research and Health Policymaking

Artificial Intelligence (AI) Plays an Increasingly Significant Role in Supporting Medical Research. It Enables the Analysis of Massive Datasets, the Discovery of Relationships between Genetic and Environmental Factors, the Acceleration of Drug and Vaccine Development, and the Reduction of Costs Associated with Scientific Research.[27]

It Also Provides Predictive Analytical Tools that Assist Policymakers in Shaping Health Policies and Estimating Future Requirements for Human and Financial Resources, thereby Strengthening Strategic Planning for Health Security.[28]

This Approach aligns with **Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data**, which Classifies Health Data as Sensitive Information and Subjects Its Processing to Specific Legal Safeguards. This Provides A Legal Basis for Utilizing Medical Data in Artificial Intelligence (AI) Applications while Upholding the Right to Privacy.[29]

Fifthly: Enhancing Health Security through the Digitization of the Healthcare System

Digital Transformation is A Fundamental Prerequisite for Implementing Artificial Intelligence (AI) Applications in the Healthcare Sector; It relies on Electronic Medical Records, the Digital Interconnection of Healthcare Institutions, and the Secure, Rapid Exchange of Data.[30]

Algeria is Striving to Digitize Its Healthcare System by Developing Electronic Medical Records and Strengthening Digital Infrastructure. However; The Success of these Initiatives remains Contingent Upon the Enactment of Specialized Legislation that Regulates Artificial Intelligence (AI) Applications, Defines the Responsibilities of Various Stakeholders, and Ensures the Security of Health Data—Protecting It against Breaches or illicit Exploitation.[31]

2nd Subsection: Legal Challenges of Using Artificial Intelligence (AI) in the Healthcare Sector

Despite the Significant Potential that Artificial Intelligence (AI) Offers for Supporting Health Security, Its Deployment in the Healthcare Sector raises Numerous Legal Issues Concerning the Protection of Individuals' Fundamental Rights and Freedoms —most notably the Right to Privacy, the Integrity of Health Data, Liability for Medical Errors, Algorithmic Transparency, and Cybersecurity. These Challenges are Further Complicated by the Sensitive Nature of Health Data and the Direct Impact that Artificial Intelligence (AI)-Driven Medical Decisions Can have on Human Life and Safety.[32]

In Algeria; The Legal Framework Governing the Use of Artificial Intelligence (AI) in the Healthcare Sector is Still in Its Formative Stages. Current Applications rely on General Legal Provisions—Such as those Found in the Health Law, the Law on the Protection of Personal Data, and Various Regulations Concerning Cybersecurity—in the Absence of Specific Legislation Dedicated to Medical Artificial Intelligence (AI). This Absence gives rise to A Number of Legal Challenges.

Firstly: The Protection of Health Data and Privacy

Artificial Intelligence (AI) Applications rely on the Processing of Vast Quantities of Health Data, including Electronic Medical Records, Genetic Data, Diagnostic Imaging, and Biomarkers. Such Data are Considered among the Most Sensitive Types of Information, due to the Potential Consequences of their Disclosure or Misuse, such as the Violation of Privacy, Discrimination against Patients, or Exploitation for Commercial Purposes without their Consent.[33]

Consequently; Upholding the Principle of Data Protection has become One of the Primary Legal Requirements for the Application of Artificial Intelligence (AI) in the Healthcare Sector. This Necessitates that Data Collection and Processing

Operations Adhere to the Principle of Legality, Require the Consent of the Data Subject, and Ensure Data Security—Including the Prevention of Unauthorized Access.[34]

In Algeria; **Law No. 18-07—Concerning the Protection of Natural Persons with regard to the Processing of Personal Data** —Classifies Health-Related Information as “Sensitive Data”. It Subjects the Processing of Such Data to Specific Conditions and Safeguards, Including the Requirement to Adhere to the Stated Purpose of Processing, Ensure Data Confidentiality, and Implement the Necessary Technical and Organizational Measures for Its Protection.[35]

However; This Law does not Explicitly Address the Unique Characteristics of Artificial Intelligence (AI)—Such as the Reuse of Data for Training Algorithms or the Continuous, Autonomous Processing of Health Data—which Highlights the Need to Develop a More Specialized Legal Framework.

Secondly: The Issue of Legal Liability for Errors Involving Artificial Intelligence (AI) in Healthcare

One of the Most Complex Issues; Determining who is Liable for Harm Resulting from A Medical Decision Made Based on An Artificial Intelligence (AI) System—Particularly when the System Leads to A Misdiagnosis, the Prescription of Inappropriate Treatment, or the Failure to Detect Serious Clinical Indicators—is A Complex Issue.[36]

Several Scenarios may arise; Liability Could rest with the Physician, as the Final Decision-Maker; With the Healthcare Institution, for Failing to Provide Necessary Oversight; Or with the System’s Developer, due to Flaws in Programming or Training. Alternatively; Liability might be Distributed among—All these Parties, depending on the Extent to which Each Contributed to the Harm.[37]

In Algerian Legislation; There are No Specific Rules Governing Civil or Criminal Liability arising from the Use of Artificial Intelligence (AI) in the Healthcare Sector. Consequently; One must rely on the General Provisions of **the Civil Code** and the Health Law. This Can Create Practical Difficulties in Proving Fault and Establishing A Causal Link—Especially when An Algorithm Operates Autonomously or relies on Deep-Learning Techniques, the Outputs of which are Often Difficult to Interpret.[38]

Therefore; The Algerian Legislator Should adopt A Specific Legal Framework to Address Liability for Harm Caused by Artificial Intelligence (AI) in Medicine, ensuring that Such Liability is Distributed Equitably among the Various Stakeholders—Consistent with Approaches Proposed within European Legislation.

Thirdly: Lack of Transparency and Explainability of Automated Decisions

Some Artificial Intelligence (AI) Systems—Particularly those based on Deep Learning—rely on Complex Models where the Decision-Making Process is Difficult to Comprehend; This is Known as the “Black Box” Problem. This Makes It Difficult to Explain the Rationale behind A Diagnosis or Treatment Recommendation, Potentially Infringing Upon the Patient's Right to Know the Basis of a Medical Decision and Limiting the Ability of Physicians or Judges to Verify the Soundness of that Decision.[39]

Consequently; Modern Legislation has Moved toward Enshrining the Principles of Transparency and Algorithmic Explainability, especially for Systems Classified as High-Risk—Such as Artificial Intelligence (AI) Systems Used in Healthcare. For Instance; **The European Artificial Intelligence (AI) Act** mandates that Developers of Such Systems Ensure an Appropriate Level of Transparency, Risk Management, and Human Oversight.[40]

In Algeria, however; There is No Legal Provision Requiring Developers or Users of Medical Artificial Intelligence (AI) Systems to Disclose How their Algorithms Function or to Allow Patients to Challenge Automated Decisions; This Constitutes a Legislative Gap that requires Intervention.

Fourthly: Cybersecurity Risks and the Integrity of Health Systems

Artificial Intelligence (AI) is Intrinsically Linked to the Digital Infrastructure of the Healthcare System, rendering It Vulnerable to Cyberattacks—Such as the Breach of Health Databases, the Manipulation of Algorithms, or the Disruption of Smart Medical Systems—which Could threaten National Health Security and Endanger Patients' Lives.[41]

The Risk of Such Attacks is Compounded by An Increasing Reliance on Internet-Connected Medical Devices, Electronic Health Records, and Telemedicine Platforms—All of which Serve as Potential Targets for Cyberattacks.

In Algeria; **Law No. 09-04, which Concerns the Prevention and Combating of Crimes Related to Information and Communication Technologies**, provides Criminal Protection against Attacks on Information Systems. However; It does not address the Specific Risks Associated with Medical Artificial Intelligence (AI) Systems, necessitating the Supplementation of the Existing Legal Framework with More Specialized Regulations that Account for the Unique Nature of the Healthcare Sector.[42]

Fifthly: Legislative Gaps and the Need for Specialized Legal Regulation

The Absence of Legislation Specifically Addressing Artificial Intelligence (AI) in the Healthcare Sector Stands as the Most Significant Legal Challenge in Algeria. Currently; Relevant Provisions remain Scattered across the Health Law, the Personal Data Protection Law, and Legislation Concerning Cybercrime. There is No Unified Legislative Framework to Govern the Design, Adoption, and Oversight of Intelligent Systems, nor to Define the Responsibilities of the Various Stakeholders Involved.[43]

This Necessitates the Adoption of a Modern Legislative Policy Rooted in the Principles of Sound Artificial Intelligence (AI) Governance—A Policy Centered on Risk Management, Transparency, Human Oversight, Data Protection, and Respect for

Patients' Rights. Such An Approach Would Strike a Balance Between Fostering Innovation and Ensuring Health Security.

It is Advisable for the Algerian Legislator to Draw Inspiration from Comparative Experiences—most notably **the European Artificial Intelligence (AI) Act**, which Classifies Artificial Intelligence (AI) Applications in the Healthcare Sector as “High-Risk” Systems. This Classification Subjects them to Stringent Requirements regarding Risk Assessment, Data Quality, Human Supervision, and Legal Accountability—while Adapting these Principles to the Specificities of the Algerian Legal System.

Ultimately; The Success of Artificial Intelligence (AI) in Enhancing Health Security depends not only on Technical Advancement but Also on the Existence of a Comprehensive Legal Framework that Ensures the Safe and Responsible Use of this Technology. Although Algerian Legislation Has Established General Rules for the Protection of Health and Personal Data; It Lacks a Specific Framework for Artificial Intelligence (AI). There remains A Lack of Specific Regulation for Artificial Intelligence (AI) in the Medical Field, which Necessitates Legislative Intervention to Establish a Specialized Legal Framework. Such A Framework Should Define the Parameters for the Use of these Applications, uphold the Principles of Transparency and Accountability, and Protect Fundamental Rights—thereby Striking a Balance between Technological Innovation and the Requirements of Health Security.

2nd Chapter: Applications of Artificial Intelligence (AI) in Protecting Patient Data and Improving Health Outcomes

The Most Prominent Applications of Artificial Intelligence (AI) in the Healthcare Sector Manifest in Two Complementary Areas. The First Involves **Protecting Patient Data** by Developing Intelligent Mechanisms to Enhance the Security of Health Information, Detect Intrusion Attempts, and Ensure Data Confidentiality and Integrity, in Compliance with Privacy Protection Requirements. The Second Area Focuses on **Improving Health Outcomes** by Supporting Early Diagnosis, Advancing Precision Medicine, Refining Treatment Decisions, and Enhancing the Efficiency of Health Resource Management—All of which Contribute to Better Quality of Care and More Effective Health Security.

Accordingly; This Chapter Examines Key Applications of Artificial Intelligence (AI) in Strengthening Health Security; The First Section addresses **the Protection of Patient Data**, while the Second Section Explores the Role of these Technologies in **Improving Health Outcomes**.

1st Section: Artificial Intelligence Applications in Protecting Patient Data

Health Data is among the Most Sensitive Types of Information, as It Encompasses Details regarding An Individual’s Physical, Psychological, and Genetic Condition. Consequently; Protecting Such Data is Essential to Ensuring Trust in the Healthcare System and Maintaining Health Security.

Accordingly; This Section will Examine the Technical Mechanisms Provided by Artificial Intelligence (AI) for the Protection of Health Data, followed by An Overview of the Legal Safeguards Established to Protect Patient Data in the Context of Using these Technologies.

1st Subsection: Technical Mechanisms of Artificial Intelligence (AI) in Enhancing the Protection of Health Data

Artificial Intelligence (AI) has Emerged as A Vital Tool for Bolstering the Security of Health Information; By Analyzing Big Data; It Can Proactively Detect and Respond to Cyber Threats, thereby Contributing to Enhanced Health Security and the Protection of Patient Privacy.[44]

One Such Technical Mechanism Involves **Intelligent Intrusion Detection Systems**. These Systems Utilize Machine Learning Algorithms to Analyze Data Traffic within Healthcare Networks, distinguishing between Normal Patterns and Unusual Behaviors that May Indicate an Attempted Breach or Cyberattack. A Key Feature of these Systems is their Capacity for Continuous Learning from New Data. This Enables the Early Detection of Cyberattacks—Even those Previously Unknown—Unlike Traditional Security Software, which relies on Fixed, Pre-Established Rules.[45]

Artificial Intelligence (AI) Also Contributes to **Identity Management and the Control of Access Privileges to Health Data**; By Analyzing User Behavior and Continuously Verifying the Identities of those Authorized to Access Medical Databases—A Process Known as “Intelligent Authentication”—This Technology Helps Prevent Unauthorized Access to Electronic Medical Records. It Also Mitigates the Risk of Account Misuse, particularly in Hospitals that Utilize Interconnected Health Information Systems.[46]

Another Significant Application is **the Detection of Anomalous Activity**. Artificial Intelligence (AI) Algorithms Analyze Millions of Operations Performed on Health Data to Identify Patterns that Deviate from the Norm—Such as the Copying of Large Volumes of Medical Files, Access to Patient Data Outside the User’s Scope of Responsibility, or Attempts to Transfer Data to External Parties. This Analysis allows for Immediate Intervention to Contain Breaches before Significant Damage Occurs.[47]

Furthermore; Artificial Intelligence (AI) **Enhances Encryption and Anonymization Techniques;** By Developing Intelligent Methods for Processing Health Data. This allows Such Data to be Used for Scientific Research or the Training of Artificial Intelligence (AI) Models without Revealing the Identities of the Individuals to Whom the Data Belongs. This Technology Serves as A Crucial Safeguard for Balancing the Utilization of Medical Data with the Protection of Patient Privacy—A Balance that has become Increasingly Important given the Expanding Use of Big Data within the Healthcare Sector.[48]

Furthermore; Artificial Intelligence (AI) has Emerged as An Effective Tool for **Predicting Cyberattacks**. Predictive Models Analyze Historical Data and Patterns from Past Incidents to Anticipate Potential Attacks before They Occur, Enabling

Healthcare Organizations to Implement Proactive Preventive Measures and Strengthen the Resilience of their Digital Infrastructure against Cyber Threats. This Function is Particularly Significant in Light of the Rising Number of Cyberattacks Targeting Hospitals and Health Databases Globally.[49]

From A Legal Perspective; These Technical Mechanisms represent A Practical Embodiment of the Obligation to Protect Health Data, which is Classified as Sensitive Data. Law No. 18-07 of (June 10, 2018 CE), Concerning the Protection of Natural Persons with Regard to the Processing of Personal Data, stipulates that the Processing of Health Data Must be Subject to Specific Safeguards. It Mandates that the Data Controller Implement Technical and Organizational Measures to Ensure the Confidentiality and Integrity of the Data and to Prevent Unauthorized Access. Furthermore; It Prohibits the Processing of Sensitive Data Except in Cases Authorized by Law or Upon the Explicit Consent of the Data Subject, while Requiring Adherence to the Principle of Proportionality and the Existence of a Legitimate Purpose for Such Processing.[50]

This is Complemented by the Provisions of Law No. 18-11 on Health, which Enshrines a Patient's Right to Privacy and the Confidentiality of Information Regarding their Health Status. It Obligates Healthcare Professionals and Institutions to Maintain Professional Secrecy and Prohibits the Disclosure of Medical Information, except within the Limits Permitted by Law. This Legal Obligation Serves as A Foundation for the Integration of Artificial Intelligence (AI) Technologies into the Management of Health Data; Provided that this is Carried Out within A Framework that Ensures Respect for Patients' Privacy and does not Infringe Upon their Fundamental Rights.[51]

Furthermore; This Protection Acquires a Criminal-Law Dimension through Law No. 09-04 of (August 05, 2009 CE), which Establishes Specific Rules for the Prevention and Combating of Crimes Related to Information and Communication Technologies. This Law Provides Mechanisms to Counter Cybercrimes Targeting Systems and Databases, including those Used within Healthcare Institutions. However; Much Like Other National Legislation, this Law Lacks Specific Provisions Addressing Threats Associated with Artificial Intelligence (AI) Systems—Such as Attacks Directed at Algorithms or the Manipulation of Training Data. This reveals A Legislative Gap that Necessitates Intervention by the Algerian Legislator to Establish a Specialized Legal Framework Governing the Security of Artificial Intelligence (AI) Systems in the Healthcare Sector.[52]

It is Evident from the Above that Artificial Intelligence (AI) Serves as An Effective Tool for Enhancing the Security of Health Data through the Early Detection of Breaches, the Management of Access Privileges, the Analysis of Anomalous Behavior, Intelligent Encryption, and the Prediction of Cyberattacks. However; The Effectiveness of these Mechanisms remains Contingent Upon the Existence of a Comprehensive Legal Framework that Defines the Parameters for their Use and Ensures Adherence to the Principles of Legality, Transparency, and Accountability—thereby Striking a Balance between Leveraging Technological Innovation and Protecting the Fundamental Rights of Patients.

2nd Subsection: Legal Safeguards for the Protection of Patient Data in the Context of Artificial Intelligence (AI) Usage

The Algerian Legislator has moved to Establish a Legal Framework that Enshrines the Protection of Personal Data in General, while Granting Specific, Heightened Protection to Health Data—Given Its Sensitive Nature—And Mandating that Healthcare Institutions and Professionals Uphold Professional Secrecy and Ensure the Confidentiality of Medical Information.

Firstly: The Protection and Processing of Health Data Privacy Under Algerian Legislation

The Protection of Health Data is An Extension of the Constitutional Right to the Protection of Private Life; It Also Serves as A Foundational Principle for Modern Personal Data Protection Systems. This Principle has Gained Even Greater Significance with the Adoption of Artificial Intelligence (AI) Technologies, which rely on the Collection, Processing, and Analysis of Vast Quantities of Health Data to Improve Diagnostics, Predict Diseases, and Support Medical Decision-Making. Consequently; Such Operations Must be Subject to Rigorous Legal Controls to Prevent the Misuse of Data or Its Processing for Purposes Other than those for which It was Originally Collected.[53]

The Algerian Legislator has addressed this Matter through Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data. This Law Establishes a Set of Governing Principles for the Processing of Personal Data, most notably; The Principles of Legality, Purpose Specification, Proportionality, Data Accuracy, and the Assurance of Data Security and Confidentiality. It Follows that; Any Processing of Health Data by Artificial Intelligence (AI) Applications Must be Based on A Legitimate Legal Foundation, Be Linked to A Specific Medical Purpose, and the Data Processed Must Not Exceed What is Necessary to Achieve that Purpose.[54]

Furthermore; The Law Accords Special Attention to Health-Related Data, Classifying It as Sensitive Information that requires A Higher Level of Protection. Such Data May Only Be Processed within the Limits Permitted by Law or Upon the Explicit Consent of the Data Subject, while Ensuring that Measures are in Place to Maintain Confidentiality and Prevent Unauthorized Access.[55]

The Effectiveness of these Safeguards is reflected in the Requirement for the Data Controller to Implement Appropriate Technical and Organizational Measures to Protect Data against Destruction, Alteration, Disclosure, or Unauthorized Access. This Obligation becomes Even More Critical when Artificial Intelligence (AI) Systems are Used, given their Reliance on Extensive Databases that Necessitate High Levels of Digital Protection.[56]

The Legislator did not Limit Itself to Establishing the Obligations of the Data Controller; It Also Granted Data Subjects A Range of Rights, including; This Includes the Right to be Informed, the Right to Access, Correct, or Update One's Data, and the Right to Object to Its Processing in Cases Permitted by Law. Such Provisions Reinforce the Principle of Patient Control Over Personal

Data and Establish a Balance between Leveraging Artificial Intelligence (AI) Applications and Ensuring Respect for Individual Rights and Freedoms.[57]

However; An Analytical Reading of Law No. 18-07 reveals that It Establishes Only General Rules for Personal Data Protection, Failing to Address the Specificities of Artificial Intelligence (AI)-Driven Data Processing. It does not regulate Matters Such as Automated Decision-Making, Data Processing for the Purpose of Training Algorithms, Transparency Requirements, or the Explainability of Automated Decisions—Limitations that Hinder the Law's Ability to Keep Pace with the Technological Transformations Occurring in the Healthcare Sector.[58]

Secondly: Confidentiality of Medical Information and the Responsibility of Healthcare Institutions

Beyond the Protection of Personal Data, the Principle of Medical Confidentiality Serves as One of the Most Significant Legal Safeguards Governing the Practice of Healthcare Professions. The Patient-Physician Relationship is Rooted in Trust and the Assurance that Information Concerning A Patient's Health Status will be Used Exclusively for the Purposes of Treatment and Healthcare.

Law No. 18-11 on Health Enshrines this Principle, mandating Respect for A Patient's Private Life. It Obligates Healthcare Professionals to Maintain Professional Secrecy, prohibiting the Disclosure of Information Acquired During the Performance of their Duties—Except in Cases Permitted by Law or Required for the Protection of Public Health.[59]

With the Shift toward Digitalization and the Adoption of Artificial Intelligence (AI) Applications, the Obligation of Confidentiality is No Longer Confined to the Individual Physician; It Now Extends to the Healthcare Institution Itself, as the Entity Responsible for Managing Health Databases and Operating Digital Systems. Consequently; These Institutions are Required to Establish Internal Policies Governing Data Access, Define User Permissions, and Implement Technical Measures that Log Access to Medical Records, thereby Enabling the Monitoring of Any Unauthorized Use of Health Information.[60]

Furthermore; Healthcare Institutions bear the Responsibility of Selecting Intelligent Systems that Meet Established Standards for Security and Reliability, ensuring their Compliance with Personal Data Protection Requirements, and Providing Training to Staff on the Secure Use of these Systems. Failure to Fulfill these Obligations Constitutes a Form of Negligence that may give rise to Civil Liability; Provided that Such Failure Results in Harm to A Patient—whether through the Leakage or Misuse of their Data—in Accordance with the General Rules of Liability Stipulated in the Algerian Civil Code.[61]

It Should be noted that; Although Algerian Legislation Establishes Clear Obligations regarding Data Protection and Medical Confidentiality; It does not Precisely Define the Liability of the Various Parties Involved in the Use of Artificial Intelligence (AI) Applications—Such as the System Developer, the Cloud Service Provider, the Healthcare Institution, or the Physician Who relies on the Algorithm's Outputs. This Legislative Gap Creates Practical Difficulties in Determining Liability when Harm Occurs due to A Malfunction in An Artificial Intelligence (AI) System or A Breach of Health Data.[62]

In Light of this; It is Essential to Develop the Algerian Legislative Framework by Drawing Upon Comparative Approaches—most notably; the European Union's Artificial Intelligence Act (EU AI Act 2024 CE). This Regulation Subjects Artificial Intelligence (AI) Systems Used in the Healthcare Sector to Stringent Legal Requirements Concerning Risk Management, Data Quality, Human Oversight, Transparency, and Documentation. Such Measures Serve to Enhance Patient Protection and Foster Trust in the Use of these Technologies, all while Ensuring that the Fundamental Rights of Individuals remain Uncompromised.

Accordingly; It is Evident that the Algerian Legislator has Established an Important Legal Foundation for the Protection of Patient Data through Laws No. 18-07 and 18-11, which Enshrine the Principles of Privacy Protection and the Confidentiality of Medical Information. However; The Rapid Development of Artificial Intelligence (AI) Applications in the Healthcare Sector Necessitates a Transition from General Rules to A Specialized Legal Framework. Such a Framework Should Define the Parameters for Processing Health Data Via Intelligent Systems and Clarify the Responsibilities of Various Stakeholders, thereby Striking a Balance between Fostering Innovation, ensuring the Protection of Patients' Rights, and Strengthening Health Security.

2nd Section: The Contribution of Artificial Intelligence (AI) to Improving Health Outcomes

The Role of Artificial Intelligence (AI) in the Healthcare Sector is No Longer Limited to Protecting and Securing Health Data; It has Expanded to become A Key Driver for Improving Health Outcomes and Enhancing the Efficiency of the Healthcare System.

Accordingly; This Section will Examine the Role of Artificial Intelligence (AI) in Improving the Quality of Healthcare Services (1st Subsection) and Its Contribution to Managing Health Risks to Strengthen Health Security (2nd Subsection).

1st Subsection: Improving the Quality of Healthcare Services

The Assessment of Healthcare System Efficiency is No Longer Measured Solely by the Availability of Human and Material Resources. It is Now Also Linked to A System's Capacity to Employ Smart Technologies to Develop Therapeutic and Preventive Services and to Elevate the Quality of Healthcare—Ultimately Leading to Better Patient Outcomes and Greater Institutional Efficiency. This Shift is Rooted in Artificial Intelligence's Ability to Analyze Vast Amounts of Medical Data, Identifying Patterns and Relationships that would be Difficult for Humans to Detect with the Same Speed and Precision. Consequently; Artificial Intelligence (AI) has become A Cornerstone in Building a More Efficient and Sustainable Healthcare System.[63]

One of the Primary Ways in which Artificial Intelligence (AI) Improves the Quality of Healthcare Services is by **Enhancing the Accuracy of Medical Diagnoses and Enabling the Early Detection of Diseases**. Deep Learning Algorithms have brought

about A Paradigm Shift in the Analysis of Medical Imagery—Such as X-Rays, Magnetic Resonance Imaging (MRI), and Computed Tomography (CT) Scans. These Algorithms are Now Capable of Detecting Early Indicators of Various Conditions, including Cancerous Tumors, Heart Disease, and Retinal Disorders, with A Level of Accuracy that, in Some Instances, rivals that of Medical Specialists when Used as A Clinical Decision-Support Tool. The Role of these Systems Extends beyond Enhancing Diagnostic Accuracy; They Also reduce the Time required to Analyze Medical Examinations, which Facilitates Faster Therapeutic Intervention and Mitigates Complications arising from Diagnostic Delays.[64]

Early Diagnosis Carries Legal Significance alongside Its Medical Importance, as It Upholds a Patient's Right to Receive Appropriate and Timely Healthcare. This aligns with the Principles Enshrined in Algerian Health Legislation, which aims to Ensure the Quality of Healthcare Services and Improve Patient Care.

Artificial Intelligence (AI) Plays an Equally Vital Role in Supporting Clinical Decision-Making. Intelligent Systems Provide Physicians with Analytical Tools to Evaluate a Patient's Health Status by Synthesizing their Medical History, Laboratory Test Results, Medical Imagery, and the Latest Clinical Guidelines. Integrating this Data into A Unified Platform Enables the Generation of Evidence-Based Recommendations, Assisting in the Selection of the Most Suitable Treatment Plan for Each Individual Patient. This Type of Support does not Replace the Physician, rather; It Enhances their Ability to Make More Accurate and Informed Decisions—Particularly in Complex Cases that Require the Analysis of Numerous Medical Indicators within A Short Timeframe.[65]

Furthermore; Artificial Intelligence (AI) Contributes to the Effectiveness of Treatment Plans by Advancing the Concept of "Precision Medicine". This Approach Tailors Treatments to the Individual Characteristics of Each Patient, Drawing on Clinical, Genetic, and Environmental Data, as well as Lifestyle Factors. This Shift—Moving Away from Standardized Treatment Models toward Highly Personalized Plans—has Helped Increase Treatment Response Rates, Reduce Side Effects, and Improve Quality of Life, especially in the Management of Chronic Diseases and Cancer. Additionally; Artificial Intelligence (AI)-Driven Predictive Models Can Estimate the Likelihood of Treatment Success or the Emergence of Complications, allowing for Proactive Adjustments to Treatment Plans and More Efficient Health Outcomes.[66]

In the Algerian Context; The Integration of Artificial Intelligence (AI) Applications into Diagnosis and Treatment Presents a Significant Opportunity to Enhance the Quality of Healthcare Services. This is Particularly Relevant Given the State's Current Focus on Digitizing the Health Sector, Promoting the Use of Electronic Medical Records, and Developing Digital Health Services. However; Maximizing the Benefits of these Applications remains Contingent Upon Upgrading Digital Infrastructure, Establishing Accurate and Secure Health Databases, and Training Medical and Technical Professionals Capable of Operating Intelligent Systems and Evaluating their Outputs. This Ensures that Artificial Intelligence (AI) Serves as An Aid to Improve the Quality of Healthcare, rather than A Replacement for Human Medical Expertise.

Consequently; It Can be argued that Artificial Intelligence (AI) is Poised to become A Cornerstone of the Future Healthcare System—not as A Substitute for Physicians, but as A Supportive Tool that Enhances the Efficiency of Diagnosis and Treatment and Elevates the Quality of Health Services. Nevertheless; The Success of this Transformation Depends on the Ability of Policymakers to Keep Pace with Technological Advancements by Adopting Flexible, Specialized Legislation; Upholding the Principles of Digital Governance; Protecting Health Data; and Fostering Public Trust in Artificial Intelligence (AI) Applications. Such Measures will Contribute to Achieving Sustainable Health Security Rooted in Both Innovation and Responsibility.

2nd Subsection: The Contribution of Artificial Intelligence (AI) to Health Risk Management

Health Risk Management has become A Cornerstone of Modern Health Policy. Epidemic Crises—most notably the COVID-19 Pandemic—have Demonstrated that the Success of a Healthcare System is Measured not merely by Its Capacity to Treat Patients, but by Its Readiness to Anticipate Risks, Respond Rapidly, and Mitigate their Health, Economic, and Social Impacts.

In this Context; Artificial Intelligence (AI) has Emerged as A Vital Tool for Health Risk Management. Its Ability to Analyze Vast Quantities of Health, Environmental, and Demographic Data in Record Time allows for the Extraction of Indicators that Help Health Authorities Make Evidence-Based Decisions. This, in turn; Strengthens the Resilience of Healthcare Systems and Proactively Ensures Health Security.[67]

Among the Most Prominent Applications of Artificial Intelligence (AI) in this Field are **Early-Warning Systems for Epidemics and Infectious Diseases**. These Systems Utilize Machine Learning Algorithms to Analyze Data from Hospitals, Laboratories, and Epidemiological Surveillance Networks—as well as Information from Digital Platforms and Media—to Detect Early Signs of the Emergence and Spread of Diseases before They Escalate into Large-Scale Health Crises. Such Systems Help Shorten the Interval between the Emergence of Initial Cases and the Implementation of Preventive Measures, enabling Health Authorities to Mobilize Necessary Resources and Contain the Spread of Infection During Its Early Stages.[68]

The Value of Artificial Intelligence (AI) Extends beyond Early Detection; It Also Encompasses **Predicting the Trajectories of Disease Spread** by Developing Mathematical Models Based on the Analysis of Epidemiological Data, Population Density, Human Mobility, and Climatic or Environmental Factors. These Models Make It Possible to Estimate the Potential Scale of Infections, Identify High-Risk Areas, and Evaluate the Impact of Various Preventive Measures. This Provides a Scientific Basis for Decision-Making regarding Quarantine Protocols, Vaccine Distribution, and the Strengthening of Healthcare Capacity in Vulnerable Regions.[69]

Furthermore; Artificial Intelligence (AI) Plays A Vital Role in **Health Emergency and Crisis Management** by Supporting Planning Processes and Coordinating Responses among Various Stakeholders in the Healthcare Sector. Through Predictive Analytics, Intelligent Systems Can Estimate Future Requirements for Hospital Beds, Ventilators, Medications, and Medical Personnel. This Facilitates a More Efficient and Equitable Allocation of Resources, while Alleviating the Strain that Healthcare Institutions May Face During Major Health Crises. This Function is Particularly Significant for Countries that Contend with Challenges Such as the Unequal Distribution of Health Services or Limited Material and Human Resources.[70]

In addition to this, Artificial Intelligence (AI) Contributes to **Improving the Management of Healthcare Supply Chains** by Forecasting Future Needs for Medicines and Medical Supplies, and by Monitoring Any Disruptions in Procurement or Distribution Processes. This Helps Reduce the Likelihood of Shortages in Essential Equipment During Disasters and Pandemics. Furthermore; Intelligent Models Assist in Optimizing the Use of Healthcare Resources, directing them toward Actual Priorities; This Enhances the Efficiency of Healthcare Spending and Strengthens the Capacity of Healthcare Institutions to Respond to Exceptional Circumstances.[71]

The Algerian Legislator Has Sought to Establish a Legal Framework that Ensures the Protection of Public Health and the Regulation of the Healthcare Sector. This is Embodied in Law No. 18-11 on Health, which affirms the State's Responsibility for Disease Prevention, Health Promotion, the Organization of Health Surveillance Systems, and the Implementation of Necessary Measures to Address Risks and Epidemics—All with the Aim of Safeguarding Public Health. The Law Also Establishes Principles for Health Planning and the Coordination of Efforts among Various Healthcare Structures; These Principles Could Serve as A Legal Basis for Integrating Artificial Intelligence (AI) Technologies into Health Risk Management.[72]

Consequently; Strengthening Health Security in Algeria does not Depend Solely on the Development of Digital Infrastructure; It Also requires the Development of A Specialized Legal Framework that Regulates the Use of Artificial Intelligence (AI) in Health Risk Management, Defines the Responsibilities of Various Stakeholders, and Establishes Standards for Transparency, Oversight, and Risk Assessment—thereby Ensuring that the Benefits of these Technologies are Maximized while Safeguarding Individual Rights and the Integrity of Health-Related Decisions.

Conclusion:

In Conclusion; Building A Smart and Secure Healthcare System is No Longer Merely a Technical Option; It has become A Legal and Developmental Necessity, driven by Global Digital Transformations. The Success of this Transition Depends on the Algerian Legislator's Ability to Anticipate Technological Developments by Adopting a Flexible and Comprehensive Legislative Policy. Such A Policy Should Establish Sound Governance for Artificial Intelligence (AI) in the Healthcare Sector, Striking A Balance between Fostering Innovation, Safeguarding Rights and Freedoms, and Strengthening Health Security—A Fundamental Pillar of Sustainable Development.

The Study reached Several Key Findings; Most Notably:

1) Artificial Intelligence (AI) has become A Vital Component in Enhancing Health Security by Supporting Early Diagnosis, Improving Treatment, Managing Health Risks, and Increasing the Efficiency of the Healthcare System.
2) Maximizing the Benefits of Artificial Intelligence (AI) Applications in the Healthcare Sector requires A Delicate Balance between Encouraging Technological Innovation and Ensuring Respect for Individuals' Fundamental Rights.
3) Health Data Serves as the Foundation for Artificial Intelligence (AI) Applications, therefore; Its Legal and Technical Protection is An Essential Prerequisite for Ensuring the Safe and Responsible Usage of these Technologies.
4) Algerian Legislation Provides General Protection for Health Data through Law No. 18-07 and Law No. 18-11. However; It Lacks Specific Regulations Governing the Use of Artificial Intelligence (AI) in the Healthcare Sector, which Limits Its Ability to Keep Pace with Rapid Technological Advancements.
5) Digital Health Security Cannot be Achieved through Technical Solutions alone, rather; It requires An Integrated Ecosystem that Encompasses Legislation, Governance, Cybersecurity, Digital Infrastructure, and the Development of Human Resources.

In Light of the Findings; The Study makes the following recommendations:

1) Develop A Specific Algerian Legislative Framework to Regulate the Usage of Artificial Intelligence (AI) in the Healthcare Sector. This Framework Should Define the Standards for the Development and Deployment of Artificial Intelligence (AI)-Driven Systems and Clarify the Responsibilities of All Stakeholders, including Healthcare Institutions, Software Developers, and Digital Service Providers.
2) Revise Law No. 18-07 to Align with Recent Advancements in Artificial Intelligence (AI). This Should Include Provisions for Specific Safeguards regarding the Processing of Health Data by Artificial Intelligence (AI) Systems, while Enshrining Principles Such as Transparency, the Explainability of Automated Decisions, and Human Oversight of Medical Decision-Making.
3) Advance the Digitalization of the National Healthcare System by Developing Electronic Medical Records and Establishing Unified National Health Databases that Adhere to Cybersecurity and Privacy Protection Requirements.

4) Establish A Multidisciplinary National Body Dedicated to the Governance of Artificial Intelligence (AI) in the Healthcare Sector. Comprising Experts in Law, Medicine, Artificial Intelligence (AI), and Cybersecurity, this Body would be tasked with Evaluating Artificial Intelligence (AI) Systems Prior to their Adoption and Monitoring their Compliance with Legal and Ethical Standards.
5) Adopt National Criteria for Assessing the Safety and Reliability of Artificial Intelligence (AI) Applications Used within Healthcare Institutions. Such Applications Should be Subject to Periodic Audits to Ensure the Quality of their Performance and to Verify that They do not Pose Risks or Harbor Biases that Could Infringe Upon Patients' Rights.
6) Strengthening Training and Scientific Research Programs in the Fields of Health Law, Artificial Intelligence (AI), and Cybersecurity, while Fostering Collaboration between Universities, Research Centers, and the Healthcare Sector to Develop National Digital Solutions tailored to the Specificities of the Algerian Healthcare System.
7) Leveraging Leading International Experiences—most notably the European Regulation on Artificial Intelligence (AI)—when Drafting National Legislation, while Remaining Mindful of Algeria's Unique Constitutional, Legal, and Institutional Framework; This Ensures the Adoption of Best Practices without Overlooking the Requirements of the National Context.

List of Sources and References

Firstly: Legal Texts:

1. **Algerian Legal Texts:**
   - People's Democratic Republic of Algeria. (1975). Ordinance No. 75-58 of September 26, 1975, establishing the Civil Code, as amended and supplemented. Official Gazette of the People's Democratic Republic of Algeria. Official texts and subsequent amendments.
   - People's Democratic Republic of Algeria. (1989). Law No. 89-01 of February 7, 1989, supplementing Ordinance No. 75-58 of September 26, 1975, establishing the Civil Code. Official Gazette of the People's Democratic Republic of Algeria, Issue 6.
   - People's Democratic Republic of Algeria. (2009). Law No. 09-04 of August 5, 2009, establishing specific rules for the prevention and combating of crimes related to information and communication technologies. Official Gazette of the People's Democratic Republic of Algeria, Issue 47, August 16, 2009. Official archive of the Official Gazette for the year 2009.
   - People's Democratic Republic of Algeria. (2018a). Law No. 18-07 of June 10, 2018, regarding the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, Issue 34, June 10, 2018.
   - People's Democratic Republic of Algeria. (2018b). Law No. 18-11 of July 2, 2018, relating to health. Official Gazette of the People's Democratic Republic of Algeria, Issue 46, July 29, 2018.
   - People's Democratic Republic of Algeria. (2020). Presidential Decree No. 20-442 of December 30, 2020, regarding the promulgation of the constitutional amendment approved in the referendum of November 1, 2020. Official Gazette of the People's Democratic Republic of Algeria, Issue 82, December 30, 2020.
2. **International Legislation and Legal Documents:**
   - European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
   - European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689, 12 July 2024.
   - UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence. UNESCO.

Secondly: Books:

- Buzan, B. (1991). **People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era** (2nd ed.). Lynne Rienner Publishers.
- Gostin, L. O. (2021). **Global Health Security: A Blueprint for the Future**. Harvard University Press.
- Russell, S., & Norvig, P. (2021). **Artificial Intelligence: A Modern Approach** (4th ed.). Pearson.
- Topol, E. (2019). **Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again**. Basic Books.

Thirdly: Reports and Documents Issued by International Organizations:

- National Institute of Standards and Technology. (2023). **Artificial Intelligence Risk Management Framework** (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
- Organisation for Economic Co-operation and Development. (2023). **Health at a Glance 2023: OECD Indicators**. OECD Publishing. https://doi.org/10.1787/7a7afb35-en

- Organisation for Economic Co-operation and Development. (2026). **Scaling Artificial Intelligence in Health**. OECD Publishing. https://doi.org/10.1787/a436e12d-en.
- **OECD:** World Health Organization. (2019). **Health Emergency and Disaster Risk Management Framework**. World Health Organization.
- **OECD:** World Health Organization. (2021a). **Ethics and Governance of Artificial Intelligence for Health: WHO Guidance**. World Health Organization. https://www.who.int/publications/i/item/9789240029200.
- **World Health Organization:** World Health Organization. (2021b). **Global Strategy on Digital Health 2020–2025**. World Health Organization. https://www.who.int/publications/i/item/9789240020924.
- **World Health Organization:** World Health Organization. (2025). **Global Strategy on Digital Health 2020–2027**. World Health Organization. https://www.who.int/publications/i/item/9789240116870.
- **World Health Organization:** World Health Organization. (n.d.). **Health Security**. https://www.who.int/health-topics/health-security.
- **World Health Organization**: World Health Organization. (n.d.). **Universal Health Coverage**. https://www.who.int/health-topics/universal-health-coverage.

Fourthly: Scientific Articles:

- Fidler, D. P. (2005). **Health as foreign policy: Between principle and power. The Whitehead Journal of Diplomacy and International Relations**, 6(2), 179–194. https://scholarship.shu.edu/diplo_ir/vol6/iss2/15.

List of Margins/Endnotes:

Notes

[1] - **Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024** laying down harmonised rules on artificial intelligence **(Artificial Intelligence Act) [2024 CE]** OJ L 2024/1689, 12 July 2024 accessed 10 October 2026 CE.

[2] - OECD, **Scaling Artificial Intelligence in Health** (OECD Publishing 2026 CE) accessed 10 October 2026 CE.

[3] - Barry Buzan, **People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era** (2nd ed, Lynne Rienner Publishers 1991) 19 ff accessed 10 October 2026 CE.

[4] - **OECD** (n 2).

[5] - World Health Organization (WHO), '**Health Security**' accessed 10 October 2026 CE.

[6] - Lawrence O. Gostin, **Global Health Security: A Blueprint for the Future** (Harvard University Press 2021) 10.

[7] - **Gostin** (n 6) 10.

[8] - David P. Fidler, '**Health as Foreign Policy: Between Principle and Power**' (2005) 6(2) **Journal of Diplomacy and International Relations** 179 https://scholarship.shu.edu/diplo_ir/vol6/iss2/15 accessed 10 October 2026 CE.

[9] - OECD, **Scaling Artificial Intelligence in Health** (OECD Publishing 2026) 27 https://doi.org/10.1787/a436e12d-en.

[10] - World Health Organization, **Health Emergency and Disaster Risk Management Framework** (WHO 2019 CE).

[11] - World Health Organization, '**Universal Health Coverage**' https://www.who.int/health-topics/universal-health-coverage accessed 10 October 2026 CE.

[12] - World Bank, '**Pandemic Prevention, Preparedness, and Response Projects funded by the Pandemic Fund in the first Call for Proposals**' (12 September 2023) https://www.worldbank.org/en/brief/2023/09/12/the-pandemic-fund-project-descriptions accessed 10 October 2026 CE.

[13] - World Health Organization (WHO), **Global Strategy on Digital Health 2020–2025** (WHO 2021) https://www.who.int/publications/i/item/9789240020924 accessed 10 October 2026 CE.

[14] - WHO, **Ethics and Governance of Artificial Intelligence for Health: WHO Guidance** (WHO 2021) https://www.who.int/publications/i/item/9789240029200 accessed 10 October 2026 CE.

[15] - OECD, **Scaling Artificial Intelligence in Health** (n 2).

[16] - WHO, **Global Strategy on Digital Health 2020–2025** (n 13).

[17] - **Law No. 18-11 of July 2, 2018, on Health, Official Gazette of the People's Democratic Republic of Algeria**, No. 46, July 29, 2018 CE. **Loi n° 18-11 du 2 juillet 2018 relative à la santé, Journal officiel de la République algérienne démocratique et populaire**, no 46, 29 July 2018 CE.

[18] - Stuart Russell and Peter Norvig, **Artificial Intelligence: A Modern Approach** (4th ed, Pearson 2021) 1035–1048. [Verify page range against the edition consulted].

[19] - WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 14); **Law No. 18-11 of 2 July 2018 on Health** (n 17). WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 14); **Loi n° 18-11 du 2 juillet 2018 relative à la santé** (n 17).

[20] - **Law No. 18-11 of 2 July 2018 relating to health** (No. 17). [Insert the specific article number after checking the official text]. **Loi n° 18-11 du 2 juillet 2018 relative à la santé** (n 17). [Insert the specific article number after checking the official text].

[21] - Eric Topol, **Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again** (Basic Books 2019) 43–82. [Verify page range against the edition consulted].

[22] - OECD, **AI in Health: Huge Potential, Huge Risks** (OECD Publishing 2024) https://doi.org/10.1787/2f709270-en accessed 10 October 2026 CE.

[23] - **Law No. 18-11 of July 2, 2018 CE, relating to health** (No. 17). [Insert the specific provisions on patients' rights and quality of care after checking the official text].

[24] - WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 14).

[25] - OECD, **Health at a Glance 2023: OECD Indicators** (OECD Publishing 2023) https://doi.org/10.1787/7a7afb35-en accessed 10 October 2026 CE.

[26] - **Law No. 18-11 of 2 July 2018 relating to health** (No. 17). [Specify the relevant provisions on prevention and epidemic control].

[27] - Topol, **Deep Medicine** (n 21) 201–235. [Verify page range against the edition consulted].

[28] - OECD, **AI in Health: Huge Potential, Huge Risks** (n 22).

[29] - **Law No. 18-07 of June 10, 2018, on the protection of natural persons with regard to the processing of personal data, Official Gazette of the People's Democratic Republic of Algeria**, No. 34, June 10, 2018 CE.

[30] - WHO, **Global Strategy on Digital Health 2020–2025** (n 13).

[31] - **Law No. 09-04 of August 5, 2009, establishing specific rules for the prevention of and the fight against offenses related to information and communication technologies, Official Gazette of the People's Democratic Republic of Algeria**, No. 47, August 16, 2009 CE.

[32] - WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 14).

[33] - OECD, **AI in Health: Huge Potential, Huge Risks** (n 22).

[34] - **Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ** L119/1, arts 5, 6 and 9 https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed 10 October 2026 CE.

[35] - **Law No. 18-07 of June 10, 2018, on the protection of natural persons with regard to the processing of personal data** (No. 29), particularly the provisions governing sensitive personal data.

[36] - Topol, **Deep Medicine** (n 21) 175–210. [Verify page range against the edition consulted].

[37] - European Commission, **Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, COM (2020) 64 final (19 February 2020)** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0064 accessed 10 October 2026 CE.

[38] - **Ordinance No. 75-58 of September 26, 1975, establishing the Civil Code, as amended; Law No. 18-11 of July 2, 2018, relating to health** (No. 17).

[39] - UNESCO, **Recommendation on the Ethics of Artificial Intelligence** (adopted 23 November 2021) https://unesdoc.unesco.org/ark:/48223/pf0000381137 accessed 10 October 2026 CE.

[40] - Regulation (EU) 2024/1689 (**Artificial Intelligence Act**), particularly the provisions on high-risk AI systems https://eur-lex.europa.eu/eli/reg/2024/1689/oj accessed 10 October 2026 CE.

[41] - WHO, **Global Strategy on Digital Health 2020–2025** (n 13).

[42] - **Law No. 09-04 of August 5, 2009, relating to the prevention of and the fight against offenses linked to information and communication technologies** (No. 31). **Loi n° 09-04 du 5 août 2009 relative à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication** (n 31).

[43] - Regulation (EU) 2024/1689 (**Artificial Intelligence Act**) (n 40).

[44] - WHO, **Global Strategy on Digital Health 2020–2025** (n 13).

[45] - Russell and Norvig, **Artificial Intelligence: A Modern Approach** (n 18) 1056–1068.

[46] - National Institute of Standards and Technology (NIST), **Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (January 2023)** https://doi.org/10.6028/NIST.AI.100-1 accessed 10 October 2026 CE.

[47] - OECD, **AI in Health: Huge Potential, Huge Risks** (n 22).

[48] - WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 14).

[49] - European Union Agency for Cybersecurity (ENISA), **Cybersecurity and Privacy in AI – Medical Imaging Diagnosis (7 June 2023)** https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis accessed 10 October 2026 CE.

[50] - **Law No. 18-07 of June 10, 2018, on the protection of natural persons with regard to the processing of personal data** (No. 29), particularly the provisions governing sensitive data and the security of processing. **Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le domaine du traitement des données à caractère personnel** (n 29), particularly the provisions governing sensitive data and security of processing.

[51] - **Law No. 18-11 of July 2, 2018, relating to health** (No. 17). [Specify the articles governing medical confidentiality and patients' rights after checking the official source]. **Loi n° 18-11 du 2 juillet 2018 relative à la santé** (n 17). [Specify the articles governing medical confidentiality and patients' rights after checking the official.

[52] - **Law No. 09-04 of August 5, 2009, relating to the prevention of and the fight against offenses linked to information and communication technologies** (No. 31). **Loi n° 09-04 du 5 août 2009 relative à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication** (n 31).

[53] - **Constitution of the People's Democratic Republic of Algeria, as amended by Presidential Decree No. 20-442 of 30 December 2020, Official Gazette of the People's Democratic Republic of Algeria, No. 82, 30 December 2020; Law No. 18-07 of 10 June 2018 on the protection of natural persons with regard to the processing of personal data** (No. 29). **Constitution of the People's Democratic Republic of Algeria, as amended by Presidential Decree No 20-442 of 30 December 2020, Journal officiel de la République algérienne démocratique et populaire, no 82, 30 December 2020; Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le domaine du traitement des données à caractère personnel** (n 29).

[54] - **Law No. 18-07 of June 10, 2018, on the protection of natural persons with regard to the processing of personal data** (No. 29). **Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le domaine du traitement des données à caractère personnel** (n 29).

[55] - **Law No. 18-07 of June 10, 2018, on the protection of natural persons with regard to the processing of personal data** (No. 29). **Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le domaine du traitement des données à caractère personnel** (n 29).

[56] - World Health Organization (WHO), **Ethics and Governance of Artificial Intelligence for Health: WHO Guidance** (WHO 2021) accessed 10 October 2026 CE.

[57] - **Law No. 18-07 of 25 Ramadan 1439, corresponding to June 10, 2018, on the protection of natural persons with regard to the processing of personal data, Official Gazette of the People's Democratic Republic of Algeria**, No. 34, June 10, 2018, as amended and supplemented by Law No. 25-11 of 28 Muharram 1447, corresponding to July 24, 2025, **Official Gazette**, No. 48, July 24, 2025 CE. The two official texts: **Law 18-07; Law 25-11**. **Loi n° 18-07 du 25 ramadan 1439, correspondant au 10 juin 2018, relative à la protection des personnes physiques dans le traitement des données à caractère personnel, Journal officiel de la République algérienne démocratique et populaire**, n° 34 du 10 juin 2018, telle que modifiée et complétée par la loi n° 25-11 du 28 moharram 1447, correspondant au 24 juillet 2025, **Journal officiel**, n° 48 du 24 juillet 2025. Les deux textes officiels: **loi n° 18-07; loi n° 25-11**.

[58] - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence **(Artificial Intelligence Act), arts 13–14 and Annex III, where applicable, Official Journal of the European Union** accessed 10 October 2026 CE.

[59] - **Law No. 18-11 of July 2, 2018, relating to health, Official Gazette of the People's Democratic Republic of Algeria**, No. 46, July 29, 2018 CE. **Loi n° 18-11 du 2 juillet 2018 relative à la santé, Journal officiel de la République algérienne démocratique et populaire**, n° 46, 29 juillet 2018 CE.

[60] **Ibid.**

[61] - **Ordinance No. 75-58 of September 26, 1975, promulgating the Civil Code, as amended and supplemented**, Article 124. This article is invoked when discussing civil liability based on fault, damage, and a causal link. **Ordonnance n° 75-58 du 26 septembre 1975 portant Code civil, modifiée et complétée**, article 124. Cet article sert de fondement lors de l'examen de la responsabilité civile, laquelle repose sur la faute, le préjudice et le lien de causalité.

[62] - European Commission, **Ethics Guidelines for Trustworthy AI (High-Level Expert Group on Artificial Intelligence**, 8 April 2019 accessed 10 October 2026 CE.

[63] - WHO, **Global Strategy on Digital Health 2020–2025** (WHO 2021) accessed 10 October 2026 CE.

[64] - WHO, **Ethics and Governance of Artificial Intelligence for Health: WHO Guidance** (n 56); OECD, **Scaling Artificial Intelligence in Health** (OECD Publishing 2026) accessed 10 October 2026 CE.

[65] - UNESCO, **Recommendation on the Ethics of Artificial Intelligence** (adopted 23 November 2021 accessed 10 October 2026 CE.

[66] - OECD, **AI in Health: Huge Potential, Huge Risks** (OECD Publishing 2024); WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 56).

[67] - WHO, **Global Strategy on Digital Health 2020–2025** (n 63).

[68] - WHO, **Ethics and Governance of Artificial Intelligence for Health** (n 56).

[69] - OECD, **AI in Health: Huge Potential, Huge Risks** (n 66).

[70] - WHO, **Health Emergency and Disaster Risk Management Framework** (WHO 2019) accessed 10 October 2026 CE.

[71] - OECD, **AI in Health: Huge Potential, Huge Risks** (n 66).

[72] - **Law No. 18-11 of July 2, 2018, relating to health** (No. 59). **Loi n° 18-11 du 2 juillet 2018 relative à la santé** (n 59).