Acta Universitatis Danubius

JURIDICA

The Impact of Digitalization on Conceptual Approaches to the Study of Medical Crimes

Constantin Pisarenco[1]

Abstract: Objectives: The paper analyses how the digital transformation of healthcare changes conceptual approaches to professional medical crimes. Prior Work: It builds on medical-law, criminological and patient-safety literature concerning medical error, malpractice, telemedicine, electronic health records and artificial intelligence. Approach: The study uses an interdisciplinary review based on comparative legal, criminological and systems analysis of scientific publications, reports and regulatory documents from Moldova, Ukraine, the European Union, the United Kingdom and the United States. Results: Digitalization creates new risk environments and new forms of misconduct, including manipulation of electronic data, telemedicine-related diagnostic failures and algorithm-assisted errors, while also strengthening traceability through audit trails, metadata and analytical monitoring. Implications: Legal, medical and information technology specialists should adapt investigative methods, professional standards and training. Value: The article offers an integrated conceptual framework for distinguishing criminal misconduct, civil malpractice and deontological violations in digital medicine.

Keywords: healthcare; professional misconduct; medical error; telemedicine; digital evidence

[1] Associate Professor, Doctor of Law, Free International University of Moldova (ULIM), Address: Str. Vlaicu Pârcălab 52, Chișinău, Republic of Moldova, ORCID: 0000-0003-0618-5360, Corresponding author: constantin.pisarenco@gmail.com.

1. Introduction

The empirical research indicates that diagnostic and treatment-related deficiencies remain a major patient-safety problem across jurisdictions, although estimates vary depending on data sources, case definitions and methodology. The scale of professional misconduct is additionally difficult to assess because of high latency: a substantial rate of incidents is not formally registered or reaches public oversight only in aggregated form.

The emergence of new digital technologies in medicine is compounding this complex situation. Electronic medical records (EMRs), telemedicine, mobile health apps, and artificial intelligence (AI)-based decision support systems are all designed to improve the quality and accessibility of care. The Republic of Moldova, like other countries, is actively implementing digital solutions: it has adopted strategies for the electronic transformation of healthcare and is implementing pilot telemedicine projects (an online consultation program for elderly patients was launched in 2022) (CIO.GOV.MD, 2025). The EU has adopted a set of regulations on patient data protection (GDPR) and is promoting the exchange of best e-health practices. The COVID-19 pandemic has catalyzed a massive shift to telemedicine and remote services, which, on the one hand, has allowed for the continuation of care, but on the other, it has exposed unsettled legal and ethical matters. The recent experience has revealed new types of risks and incidents: confidential information leaks, cyberattacks on hospitals, medical errors during remote consultations, algorithmic diagnostic failures, and more. Researchers and regulators face the following questions: how have the classic concepts of "medical error" and liability changed in the digital age? Are new approaches to defining and preventing medical malpractice required when decisions are made in collaboration with AI or when care is provided online? These questions underpin the relevance of this study.

The aim of this article is to comprehensively analyze the impact of digitalization on conceptual approaches to the study of professional medical crimes. This objective reflects the growing legal and criminological relevance of digital technologies in healthcare and the need to reassess traditional doctrinal categories in light of emerging forms of professional misconduct.

To achieve this aim, the analysis is conducted within an integrated conceptual framework that combines three complementary analytical models. First, a classification system for professional medical crimes in the digital age has been developed. This system organises criminal behaviour involving digital technologies,

such as telemedicine, electronic health records and artificial intelligence. These technologies can be used as tools, as environments or as objects in the commission of crimes. Second, a socio-technical model of medical criminal liability conceptualizes harmful outcomes as arising from the interaction between individual professional actions, organizational conditions such as workload, clinical protocols and supervision, and the design and operation of digital medical systems. Third, a digital-forensic medical criminality model emphasizes the evidentiary and investigative significance of electronic traces, including audit trails, device logs and metadata, as well as the necessity of interdisciplinary cooperation between legal, medical and IT specialists. Taken together, these models enable a clear differentiation between criminal offenses, civil malpractice and deontological violations, while providing a coherent analytical basis for assessing emerging digital risks in healthcare and identifying directions for the adaptation of legal and methodological approaches in the context of digital medicine.

2. Methodological Framework and Sources of Analysis

The study was conducted as an interdisciplinary review analysis using comparative legal, criminological, and systems approaches. The analyzed material included over 50 sources in Russian, English, and Romanian, published between 2000 and 2025, including scientific articles, dissertations, monographs, statistical reports, regulations, and international documents. Databases: DisserCat, CyberLeninka, IBN, PubMed, Scopus, Web of Science, HeinOnline, LexisNexis. Attention is paid to publications from Moldova, Ukraine, the EU countries, the UK, and the USA. Content analysis and a comparative legal method were applied. The following were considered: the typology of medical-legal offenses, the impact of digital technologies, and the adaptation of legislation. Data triangulation ensured reliability. The main limitation is the overview without original empirical data, which is offset by the breadth of sources and the geography of the analysis.

3. Digital Transformation of Medical Crime and Liability Concepts

3.1. Professional Crimes of Medical Workers: Definition and Types

Conceptually, professional crimes committed by medical professionals represent a special type of offense in which the perpetrator is a medical worker, and the act is committed in connection with their professional activities in providing medical care.

Classically, this category primarily includes cases of improper medical care resulting in harm to the patient. In legal literature, there are two large groups: crimes committed through negligence (due to carelessness, dishonesty or insufficient qualifications) and intentional crimes committed with the direct or indirect intent of a healthcare worker. The first group includes so-called medical errors and negligence - for example, an erroneous diagnosis or incorrect treatment resulting in serious harm to health or death of a patient, infection of a patient due to non-compliance with the rules or failure to provide assistance without good reason. These negligent acts constitute the main cause of medical malpractice cases; they are the most difficult to assess legally, as it is necessary to distinguish criminally punishable negligence from an unavoidable error in the course of bona fide treatment. The group of intentional acts includes rarer but extremely dangerous acts: direct intent – the use of medical knowledge to cause harm (e.g., murder of a patient for the purpose of organ removal, illegal abortion without medical indications, intentional infliction of grievous bodily harm under the guise of treatment, etc.); indirect intent – cases where a physician is aware of the possibility of harm but is indifferent to it (e.g., deliberate disregard for protocols, resulting in infection of a patient). Medical malfeasance, including bribery, forgery of medical documents, and commercial bribery, deserve special mention. These acts do not directly affect health, but rather the rights of patients and the rule of law within the healthcare system (for example, a doctor receiving a bribe for illegally issuing a certificate or for preferential treatment). According to research, such manifestations of corruption in medicine have increased and diversified in the last decade (Chervonnykh, 2009) – from theft of medications to collusion with pharmaceutical companies.

In legal doctrine, a medical error is often treated as a bona fide error of judgment that, by itself, does not constitute a criminal offense unless it is coupled with legally relevant culpable negligence (e.g., gross deviation from professional standards) and a proven causal link to harm.

It is important to note that in many cases, professional misconduct by doctors does not rise to the level of a crime, remaining at the level of civil liability (claims for damages) or disciplinary sanctions. In European countries and the United States, the institution of medical malpractice has traditionally prevailed, implying that an injured patient files a civil claim for the doctor's professional negligence (Payasan et al., 2022). Criminal cases against doctors are initiated there only in cases of gross negligence or clear intent (for example, a series of cases of causing harm, such as that of the British doctor H. Shipman, who intentionally killed over 200 patients). In

post-Soviet legal systems (Ukraine, Moldova), a number of medical errors are directly criminalized in the Criminal Code, although courts are quite cautious in convicting doctors for negligence. For example, in Ukraine, Article 139 of the Criminal Code provides for up to 3 years' imprisonment for a doctor's unjustified refusal to provide assistance to a patient, but this provision is rarely applied. In Moldova, issues of criminal liability for medical professionals are also on the agenda: the need to update legislation in line with international standards is being discussed in order to simultaneously protect the rights of patients and not discourage doctors with fear of punishment for honest mistakes (Pisarenco & Pisarenco, 2022).

Thus, the conceptual approach to defining this crime includes several aspects:

Industry-specific (medical-legal): a combination of criminal law, medical law, and ethical standards (the Nuremberg Code (The Nuremberg Code, 1996), the Declaration of Helsinki (World Medical Association, 2013), etc.) to define the boundaries of what is acceptable in the profession. For example, the distinction between the concepts of "medical error" (an unintentional misjudgment without gross negligence) and "criminal negligence" in legal doctrine.

Criminological: the study of the scale, structure, causes and conditions of the commission of these crimes. Here, high latency, the dependence of the crime rate on the training quality of doctors and the organization of the healthcare system, as well as the influence of socio-cultural factors (for example, the tradition of not airing dirty linen in public in the medical community).

Procedural and investigative: the specifics of investigating such crimes require specialized knowledge, forensic medical examinations, and the causal relationship between the physician's actions and the resulting harm is often complex. Concepts of iatrogenic crimes (criminal actions/inactions of a physician) are being developed with the aim of establishing investigative methods that take into account medical specifics (for example, methods for investigating crimes in obstetrics and others have been developed by a number of authors (Shepelev, 2022; Amirov, 2021; Ivanova, 2017).

Thus, modern researchers have the task of updating the concept of professional medical crimes, taking into account new realities: the commercialization of medicine and the emergence of high-tech procedures (transplants, robotic surgery, etc.), in which errors can have serious consequences. The classical typology of "intent versus negligence" is complemented by an analysis of systemic factors—work organization, physician workload, the presence of protocols, and safety culture.

These factors, as will be shown below, are becoming even more important in the age of digitalization, when the interaction between humans and technology comes to the fore.

3.2. Digitalization of Healthcare: New Opportunities and Crime Risks

Digitalization in healthcare encompasses the implementation of electronic information management systems, communication technologies, and automation in the medical care process. Key elements include electronic medical records (EMRs), telemedicine, mobile health apps, Big Data and analytics, artificial intelligence for diagnosis and treatment, robotic devices, and the general computerization of workflows (electronic prescriptions, online appointments, etc.) (Rowland et al., 2022; Katz et al., 2008). All these innovations are aimed at improving the efficiency and quality of medicine, but each carries specific risks in terms of medical errors and crimes. Below, we examine the main ways in which digitalization influences professional misconduct in medicine.

3.2.1. Telemedicine and Remote Treatment

The European regulatory perspective envisages telemedicine as best understood as a form of providing medical care rather than a separate medical profession; therefore, the core duties of care, documentation and informed consent remain applicable, adapted to the remote setting.

The dramatic growth of telemedicine services (especially during the pandemic) has opened up new opportunities for patients to access doctors, but has also revealed the limitations of the virtual environment, impacting the quality of diagnostics and, potentially, physician liability. The primary problem is the lack of an in-person examination: it is more difficult to collect a complete medical history, conduct a physical examination, and establish a trusting rapport via video link (Rowland et al., 2022; Finnegan, 2019). Statistics confirm that the rate of diagnostic errors in telemedicine consultations is higher: in the US, 66% of telemedicine-related claims from 2014–2018 were related to an incorrect diagnosis, compared to 47% for in-person visits (Bloomberg Law, 2020). In other words, the virtual format increases the likelihood of missing important symptoms or misinterpreting a patient's complaints. The consequences of these errors can be serious—in the aforementioned study, 44% of telemedicine cases with claims resulted in the patient's death.

The reasons for the higher risk are clear: technical connection failures, poor video quality, and the inability to conduct on-site testing. Furthermore, legal standards of "due care" have not yet been clearly defined for telemedicine. In traditional medicine, there are protocols regulating how a physician should act in person; in virtual medicine, there is no consensus on what is considered an appropriate standard. As researchers note, "what is generally accepted when collecting anamnesis and conducting an examination in telemedicine?" remains an open question (Rich, 2005). This creates uncertainty in assessing the physician's culpability: for example, if a diagnosis is missing due to the lack of an in-person examination, is this a systemic flaw or the physician's oversight? Courts in various countries are still cautious: as of 2019, there were virtually no precedents in the US for open litigation of claims solely for telemedicine malpractice – most disputed cases are settled out of court (Fogel & Kvedar, 2019), (Fogel, Lacktman & Kvedar, 2021) and through insurance payments. However, surveys show concern among physicians: ~69% of physicians asserted in one study that regulations preventing medical malpraxis in telemedicine were insufficient (Williams et al., 2020). In Moldova and several other post-Soviet countries, the regulatory framework for telemedicine is still in the process of formation. Romanian researchers point out that telemedicine raises new legal issues: for example, the question of jurisdiction - under which country's laws should a doctor be tried if the patient and doctor are in different countries? - and the issue of digital informed consent (Vida-Simiti, 2025). Thus, telemedicine expands access to care, but it requires the adaptation of diagnostic standards and protocols to prevent an increase in medical errors and to clearly classify possible violations.

3.2.2. Electronic Health Records (EHR) and Digital Systems

The transition from paper charts to electronic records has significantly changed the practice of documenting and accessing patient information. From an error prevention perspective, EHRs offer advantages: legibility of records (no risk of error due to illegible handwriting), accessibility of medical records for different specialists, and automatic alerts about potentially dangerous situations (allergies, drug interactions). The research notes that properly implemented systems can reduce the frequency of certain errors, such as medication errors, through built-in dose and interaction checks (Rosenbaum, Famularo & Segall, n.d.). However, in practice, the implementation of EHRs has also been accompanied by the emergence of new problems: physicians face "information overload" (large volumes of digital data are difficult to filter) (Rowland et al., 2022), input and template errors (copying old records, autofilling

fields that insert incorrect data) (Graber, Byrne & Johnston, 2017), as well as technical failures and interface complexity. Typical examples: duplication or conflicting records in the system when several electronic records are created for one patient – this can lead to some treatment information being lost or not being taken into account. In one study (Rosenbaum, Famularo & Segall, n.d.), the number of cases where EHRs were a factor in malpractice claims tripled between 2010 and 2018. The most common causes are diagnostic errors due to inconsistent or incorrect data entry, or a failure of reminders (for example, the system failing to issue an alarm for a critical lab result) (Leventhal, 2019). A practical example is a case study: at one clinic, automatic medication dosing in the EHR resulted in a 10-fold overdose and a patient's serious condition. The hospital was found liable for not properly setting up the dosage autofill system.

In terms of intentional crimes, digital records have also become a new target for abuse. First, there's the manipulation of medical documentation: whereas previously a doctor could retroactively rewrite a paper sheet, now any changes are recorded in the system's log. On the one hand, this serves as a deterrent—knowing that each record is time-stamped makes medical staff less likely to commit forgery. On the other hand, attempts at falsification do occur: in one case, a surgeon in New York, after making an error during a surgery, accessed a patient's electronic record and changed some entries in an attempt to cover up the mistake. However, the audit trail (the activity log) documented the unauthorized edits, and this data played a decisive role in the court case – the doctor was held accountable. Overall, the digital trail has become a crucial new source of evidence: the time of system login, the author of the entries, the sequence of actions—all of this can be analyzed by forensic cybernetic experts to establish the truth. Malpractice lawyers regularly request EHR metadata to check whether changes have been made post factum (which in itself can be classified as an attempt to conceal a crime). The possibility of exposure in this way certainly instills discipline: as experts note, falsifying electronic medical records is practically useless and fraught with criminal consequences, since lies are easily exposed through an audit (Rosenbaum, Famularo & Segall, n.d.). Secondly, digitalization has given rise to crimes against medical information: the theft of patients' personal data for the purpose of blackmail or sale – this makes medical institutions a target for hackers (CRB-Vedeno, 2024). However, there are also "internal" abuses: for example, a clinic employee may illegally copy patient databases and transfer them to insurance or pharmaceutical companies for a fee, which violates data protection laws (GDPR in the EU, HIPAA in the US). Such actions are treated as crimes (breach of confidentiality, illegal disclosure of medical

confidentiality), although they are difficult to detect without specialized cyber monitoring.

At the same time, digital systems have created a new front in the fight against crime: automated data analysis can identify suspicious patterns. For example, artificial intelligence algorithms are already being used in the US to detect fraud in medical billing – they recognize typical patterns of "redundant procedures" or repetitive write-offs, typical of insurance fraud by clinics (Martin, 2023). According to the FBI, healthcare fraud costs tens of billions of dollars annually, and the use of AI anomaly analyzers is becoming a key tool for preventing such crimes (Sharma, 2025). In the UK, following the famous Shipman case, national monitoring systems were introduced to analyze mortality rates for doctors and hospices; in the digital age, these systems have become even more effective, instantly identifying statistical anomalies that could indicate malicious activity or systemic failures.

3.2.3. Artificial Intelligence and Algorithms in Medicine

In the EU legal context, AI systems used in healthcare are generally treated as auxiliary tools or medical devices, not as independent subjects of criminal liability; accordingly, the physician's personal responsibility for clinical decisions remains central, while questions of producer liability may arise in parallel under civil and regulatory regimes (Wu et al., 2021).

The introduction of AI and machine learning is revolutionizing everything from X-ray interpretation to treatment recommendations. However, this also raises new conceptual questions: who is responsible for an error if a doctor relies on an AI recommendation? AI systems can outperform humans in accuracy in certain tasks (for example, algorithms are already outperforming ophthalmologists in detecting diabetic retinopathy in fundus images). But any model can fail—missing a tumor in an image or providing incorrect advice due to data corruption. Legal precedent is still limited, so researchers and lawyers are proposing theoretical models of liability. One proposal is that a doctor should be held liable if they entrust an AI with a decision that goes outside generally accepted professional standards, and conversely, if the AI recommended a standard solution and the doctor makes an incorrect one, the liability also falls on the doctor (Tobia, Nielsen & Stremitzer, 2021).

The situation becomes more complicated if the AI recommended a non-standard, but actually correct, solution (which may exceed an outdated standard), and the doctor chose not to implement it and harm occurred—who is then at fault? These scenarios remain largely hypothetical, and scholars consider them speculative until consistent

judicial practice emerges (Rowland et al., 2022). However, it is already clear that to minimize risks, algorithmic decision-making systems must be transparent: regulators in both the United States and the European Union increasingly require explainable AI, enabling physicians to understand the rationale behind algorithmic outputs and avoid blind reliance on erroneous recommendations (Wu et al., 2021).

Empirical evidence further suggests that legal assessments may depend on conformity with established standards. A simulation study conducted in the United States demonstrated that juries tend to assign lower culpability to physicians who followed AI recommendations consistent with accepted clinical protocols, and higher culpability when physicians deviated from such protocols without compelling justification (Tobia, Nielsen & Stremitzer, 2021). Currently, this creates an incentive structure in which adherence to standard decision-making—whether human or algorithm-assisted—appears legally safer. At the same time, physicians express concern that excessive fear of liability may inhibit the adoption of innovative AI solutions that depart from conventional standards, even when such solutions may be clinically superior (Rowland et al., 2022).

The opposite risk is excessive trust in AI systems. From a cognitive perspective, automation bias leads individuals to overestimate the reliability of algorithmic recommendations. There have already been documented cases in which clinicians disregarded their own professional judgment in favor of incorrect system outputs—for example, when a decision-support system recommended a medication and the physician failed to independently verify the dosage, resulting in patient harm. Consequently, current research emphasizes the importance of training physicians in digital literacy and responsible AI use, treating algorithmic tools as decision-support mechanisms rather than autonomous decision-makers. This problem is global in scope: a 2020 multi-country survey identified a lack of consensus and systematic training in telemedicine and medical IT competencies among physicians (Stovel et al., 2020). Many practitioners encounter digital technologies without adequate preparation, increasing the risk of error. In telemedicine in particular, deficiencies in virtual communication skills and remote examination techniques have been identified as significant sources of professional uncertainty and diagnostic risk (Venditti et al., 2022).

3.2.4. Cybersecurity and External Threats

While the main topic is professional crimes committed by healthcare workers themselves, one cannot ignore a related issue: digitalization has made medical institutions and their data targets for external cybercriminals. Ransomware attacks

on hospitals and the theft of patients' personal data are committed by hacker groups, not medical personnel, but the consequences affect the quality of care and can indirectly involve employees. For example, if a hospital's system is blocked by a virus, doctors lose access to historical patient data, increasing the risk of errors and fatalities (there have been cases where cyberattacks disrupted surgeries and resulted in patient deaths). From a legal perspective, healthcare institutions are obligated to ensure cybersecurity: in the EU, failure to comply with GDPR in the event of a data breach leads to large fines, while in the US, HIPAA requires the storage of electronic medical records. Recordings must be kept in compliance with security standards. If the investigation reveals that the leak occurred due to gross negligence on the part of the hospital's IT department, those responsible could theoretically face criminal liability (for example, for negligent handling of confidential information resulting in serious consequences). Furthermore, the digital environment poses the threat of medical device manipulation: for example, hacking a ventilator or insulin pump. Such cases are still isolated and are more related to cyberterrorism, but healthcare workers should be aware of these risks.

Thus, digitalization undoubtedly improves the capabilities of medicine, but it also creates a new risk landscape. Conceptual approaches to medical crimes must now take into account the influence of technological factors: some errors cease to be purely "human" and become a consequence of human interaction with technology (socio-technical errors). The literature increasingly advocates a systems approach to safety: viewing incidents not as isolated faults of the physician, but as the result of a flawed system (including software design, process organization, and staff training) (Lusk et al., 2022), (AACN, 2022), (American Nurses Association, 2022). This does not absolve individual responsibility, but requires differentiation: where is the line between a physician's oversight and the software developer's oversight? At the same time, digital technologies offer new tools for preventing and detecting crimes – from intelligent monitoring to transparency through logs. Next, we will tackle how approaches to investigation and legal regulation are changing in response to digital challenges.

Under conditions of digital transformation, harmful outcomes increasingly acquire a socio-technical character, arising from the interaction between individual professional actions, organizational factors and the functioning of digital medical systems; this calls for a comprehensive legal assessment that differentiates individual culpability from system-level failures.

3.3. Transformation of Approaches to Investigation and Evidence

The rise of digitalization is fundamentally changing the methodology for investigating and settling medical crimes. While medical malpractice investigations previously relied almost exclusively on expert testimony (forensic pathologists) and paper medical records, investigators and researchers now have access to digital data. Several important conceptual shifts can be identified:

3.3.1. Digital Evidence and Forensic Informatics

Electronic systems record a vast number of parameters that can serve as evidence. For example, the time of prescription and administration of each medication is recorded in the hospital information system. When investigating a case with a serious outcome, it is possible to determine precisely when the doctor received the test results, how long the response took, which staff member was at the patient's bedside and at what time – all of this leaves traces. EHR audit trails are now a standard object of study during the investigation of suspicious deaths in hospitals (Rosenbaum, Famularo & Segall, n.d.). Thus, subjective factors (the doctor's statement: "I did everything on time") are verified by objective data (the system log shows that the vital signs monitoring record has not been updated for six hours). Furthermore, digital devices store logs: anesthesia machine – anesthesia parameters over time, ventilator – ventilation history, cardiac monitor – EKG, etc. Forensic examination is adapting: now experts must be able to analyze not only the condition of organs and tissues, but also these data sets. And information technology opens up new horizons for the objective study of medical incidents, right up to data-based modeling of what a doctor could have done and what the outcome would have been.

On the other hand, situations arise where data contradicts one another—for example, a paper medical record (if partially maintained) differs from an electronic one. Such discrepancies are also considered a sign of possible falsification or protocol violation. The development of forensics in medicine has led to the emergence of a specialized field – medical IT experts capable of recovering deleted records and confirming the authenticity of electronic evidence. For example, if someone attempted to erase or alter digital data (for example, a database administrator retroactively edited a journal entry), specialists can detect this. A precedent: in the US, during an investigation into the suspicious death of a patient, forensic IT auditors found artifacts indicating that someone with administrative rights had accessed the electronic medical record and edited the entries the day after the incident. This served as a separate basis for accusing not only the doctor but also the administration of concealing evidence (Rosenbaum, Famularo & Segall, n.d.).

3.3.2. Analytical Methods and Forecasting

Big data in healthcare enables not only post-factum investigations but also proactive prediction and detection of suspicious situations. In some jurisdictions (the US, the UK), healthcare regulators have implemented quality and safety indicator systems that monitor, for example, mortality and complication rates by physician and hospital. This approach is essentially criminological monitoring: if an individual physician or department deviates from the statistics (with an excessively high mortality rate compared to the average for the patient type), an investigation is launched. Of course, high rates can be explained objectively (a critical patient population, a coincidence), but they can also indicate criminal activity or systematic gross errors. In one well-known case, an abnormal frequency of cardiac arrests during an anesthesiologist on-call in England led to an undercover investigation, which revealed that he was intentionally administering drugs to patients in order to later "heroically resuscitate" them – thus uncovering serial criminal behavior. This incident occurred before full digitalization, but today such anomalies are easier to track through electronic registers. Digitizing this activity will allow for a better picture and the identification of serial cases if the same doctor systematically makes critical errors across different institutions (previously, they could quit and find a job elsewhere, losing their negative history).

This also includes the use of artificial intelligence in investigations. AI algorithms can analyze thousands of cases to identify hidden correlations—for example, comparing forensic autopsy results with electronic medical records to detect missed signs of deterioration that should have led to a different medical decision. While such technologies are still in their infancy, it is possible to develop expert systems that will automatically evaluate the sequence of medical personnel's actions retrospectively and alert them to potential violations. Of course, the human factor will remain in the investigation: the legal assessment of whether a crime has occurred requires consideration of numerous aspects (context, motive, circumstances). However, analytical support accelerates the evidence collection process and makes it more objective.

3.3.3. Protecting the Rights of Medical Professionals during Investigations

Interestingly, digitalization can also serve to protect wrongfully accused doctors. Previously, it was not uncommon for doctors to be accused based on the principle that "the last person to touch the patient must be guilty". Now, with detailed patient and treatment data, expert analysis can prove that the doctor acted correctly and that the outcome was due to objective reasons. For example, a monitoring system shows

that the doctor responded promptly to a drop in blood pressure and administered the necessary medications, but the patient's body failed to respond – meaning there are no grounds for accusing them of negligence. Or an algorithm models that even with ideal treatment, the probability of a fatal outcome for a given patient was high – this argument favors the doctor. Moreover, digital innovations reduce the influence of the "human factor" in court: previously, the outcome of a case could depend on the persuasiveness of a particular expert; now judges see graphs and system reports – it is easier for them to understand the chronology and essence. Of course, proper interpretation is necessary to prevent judges and juries from drawing erroneous conclusions from dry numbers. In the US, after the case of nurse RaDonda in the case of Vought (who was convicted of manslaughter due to a medication error), many safety experts warned that criminal penalties for system errors would make it difficult to report problems (AACN, 2022). In that case, a digital system (an automated medication cabinet) allowed for (American Nurses Association, 2022) overriding – dispensing a medication without fully entering its name. A nurse typed a few letters and received the wrong medication (1st Healthcare Compliance, 2022). After the incident, the hospital made technical changes (removing the dangerous drug from the overriding list and adding a barcode system for verification), acknowledging that the system had been configured unsafely. However, the healthcare worker faced criminal penalties, while hospital management did not. This case became a turning point: the professional community was divided between the demand for justice for patients and the fear that "criminalization of medical errors" would undermine safety culture (after all, if every error leads to prison, doctors will hide them rather than investigate them). The digital evidence in the Vought case essentially showed that the cause of the tragedy was complex: a combination of human inattention and flaws in the software and hardware system for dispensing medications (Lusk et al., 2022). Conceptually, this strengthens the position of a systems approach to investigation: not only to determine who made the mistake, but also why the error was not prevented by the system. In countries where, based on the report To Err is Human (IOM, 2000) (Institute of Medicine, 2000). The concept of "learning from mistakes" is being actively implemented, with priority given to non-punitive analysis of errors and the creation of anonymous systems for reporting them (in order to accumulate data and prevent recurrence) (Pătru, Barbu & Pătru, 2023). However, the balance between the need to punish obvious negligence and learning from unintentional mistakes is a fine line, especially when judicial authorities intervene.

Thus, methods for investigating crimes committed by medical professionals are becoming increasingly technologically advanced and rely on interdisciplinary collaboration: investigator, medical examiner, and IT specialist. Conceptually, this shifts the emphasis from individual to organizational and technical responsibility. For the scientific study of this crime, digital data is a true treasure, allowing for the construction of models and the testing of hypotheses about causes. However, researchers warn that both investigators and doctors must be trained in working with digital evidence, otherwise, misinterpretations are possible (for example, if a doctor fails to record an action in the system, but actually performed it, the computer will assume they failed to do so). This leads to a recommendation: introduce standards for maintaining electronic records, mandatory for forensic analysis, and ensure data integrity (any "disappearance" of data should be considered in itself an incident).

3.4. Impact of Digitalization on Legal Regulation and Prevention

The adaptation of legislation and the development of new conceptual approaches in jurisprudence follow technological changes. Various countries are actively updating their healthcare regulations in response to digitalization:

3.4.1. Regulatory Acts and Standards

In Moldova, national legislation needs to be supplemented with specific acts that take into account the realities of digital medicine and harmonize with international law (Pisarenco & Pisarenco, 2022). An example of a positive step: Moldova developed and adopted a series of strategies for the digital transformation of healthcare in 2022–2025, which, among other things, stipulate information security and ethics (e.g., the Law on Electronic Communications, which simplifies the use of digital platforms in medicine, 2025) (Legea nr. 241, 2007). In 2020, Romania quickly legalized a wide range of telemedicine services, but researchers pointed out gaps, ranging from unclear professional liability to the problem of cross-border telemedicine (Vida-Simiti, 2025). The EU is issuing recommendations and directives: the General Data Protection Regulation (GDPR) indirectly affects medicine by establishing strict requirements for the handling of digital medical data (non-compliance with which can be classified as an offense) (European Union, 2016). Overall, a trend is emerging: laws are beginning to take into account the digital component. For example, the classic requirement to store medical records for N years is being expanded to electronic systems (and answers the question of whether records can be edited – this is not allowed; only additions with a time stamp

can be made). Or: in the US, regulations have been introduced regarding the adoption of "reasonable cyber measures" in healthcare, and if a hospital fails to do so and an incident occurs, this will be an aggravating circumstance in court.

3.4.2. Ethical and Deontological Codes

Professional societies are also responding. Medical ethics codes are being updated. International organizations (such as the World Medical Association) issued a statement on telehealth ethics in 2019, emphasizing that the quality of care should not be compromised by the use of remote technologies; physicians are obligated to ensure the reliability of the technologies, the confidentiality of communications, etc. It is specifically stated that patients must be informed of the limitations of telemedicine and consent specifically to the remote format (to prevent them from later claiming they didn't understand the risks). These ethical standards effectively form the basis for legal ones—for example, in France, violating informed consent rules in telemedicine has been equated with professional misconduct. As for AI, ethical guidelines are also being developed: the principle of algorithm transparency, the principle of maintaining the physician's role as the ultimate decision maker, and the physician's responsibility for the results of using an AI tool. Some jurisdictions are discussing introducing certification for AI systems and developer liability insurance – meaning if a doctor uses a certified AI and it makes a mistake, some of the liability would fall on the manufacturer. Such mechanisms are still in their infancy. However, one of the first to adopt this approach is Germany: it has adopted the concept that harm caused by AI (for example, diagnostic software) could result in civil liability for the manufacturer, similar to liability for defective medical devices. In terms of criminal law, the situation is more complex—a machine is not a subject, so only those who created or used it can be held liable.

3.4.3. Increasing Transparency and Prevention

The digital age requires new measures from the healthcare system to prevent crimes. Here we can highlight: (a) technological solutions that increase transparency (for example, the use of blockchain technologies for clinical records keeping – they exclude the possibility of unauthorized changes, each edit is permanently recorded; in some pilot projects, blockchain is being used for transaction logs or drug supply chains, preventing counterfeiting); (b) training and a reporting culture – medical personnel need to be trained in cyber hygiene (not leaving sessions open in the system, not disclosing passwords), and correct data entry. It is also important to implement a culture of fairness (Just Culture): when errors are reported without fear of punishment, unless there was obvious malicious intent (Lusk et al., 2022). Once

staff are comfortable admitting mistakes, it's easier to identify systemic flaws. Otherwise, the digital system will be full of false data, which will only complicate the detection of violations; (c) interagency cooperation – healthcare regulators, law enforcement agencies, and IT services must exchange information. In Moldova, for example, a Cybersecurity Center in Healthcare was created to improve the security of electronic services, collecting information on incidents, and the Ministry of Health has commissions to analyze cases of medical errors. Digital tools allow such commissions to obtain more data and draw more substantiated conclusions, which can then form the basis of recommendations (or materials for law enforcement agencies if there are signs of a crime).

Finally, an important aspect is international legal cooperation. Medical crimes (e.g., organ trafficking, online sales of prescribed drugs) are increasingly taking place across borders, using the internet. Therefore, the concepts for combating them are linked to cybercrime in general. Modern extradition treaties and joint cyberinvestigation teams all apply to medicine. Of particular importance in this area is the Convention on Human Rights and Biomedicine (Council of Europe, 1997), which establishes the framework for what is permissible in medicine. While not directly addressing digitalization, it obliges states to protect patients' rights, which includes protection from new digital threats. National legislation should be harmonized with such principles (Pisarenco & Pisarenco, 2022).

Thus, the legal system is adapting to digital healthcare, but requires accelerated development. Experts call for the concept of "anticipatory lawmaking" (Baranova, 2016) – legislators must anticipate the potential of technologies and build in protective mechanisms before negative consequences manifest themselves en masse. It is recommended to introduce special regulations for AI errors, detailed guidelines for telemedicine practice, and responsibilities for data management. Furthermore, standardization of terminology and approaches is needed: so that "medical negligence" encompasses situations involving the use of digital systems, and "appropriate provision of care" includes adherence to digital protocols (for example, timely maintenance of electronic medical records). Without this, investigative bodies and courts will have difficulty classifying new cases. Ultimately, digitalization dictates a revision of conceptual approaches in law and quality management in medicine – a shift in emphasis to systems, prevention, and training, while maintaining the inevitability of punishment in cases of truly criminal abuse of the profession, regardless of whether it is "digital" or "analog."

4. Conclusion

The digital transformation of healthcare has a complex impact on the nature, detection, and prevention of professional medical crimes, requiring an evolution of conceptual approaches in both science and practice. Based on the analysis, the following conclusions and recommendations can be drawn:

The expansion of the concept and typology of crimes in the digital age includes not only traditional forms of offenses by medical workers (negligence, intent, corruption), but also new manifestations, such as unauthorized access to electronic medical data. Data manipulation, falsification, manipulation of treatment algorithms, and promotion of commercial interests through IT systems significantly expand the scope of professional liability. The concept of medical crime should encompass actions using technology, and legislation should clarify the classification of such acts and provide for the corresponding legal consequences.

New methodological approaches to research and investigation reflect a shift from post-hoc analysis to proactive monitoring, as digitalization has provided unprecedented access to objective data and new analytical capabilities. Scientific approaches require a change in how we work with large amounts of data and risk modelling. For investigative bodies, this means creating teams made up of people with different skills, training in working with digital evidence, and putting in place ways to prevent problems based on data from medical information systems.

The balance of responsibility: systemic versus individual requires rethinking, as medical errors often arise from both individual actions and systemic factors – institutional culture, digital interfaces, and ineffective protocols. When analyzing incidents, it is important to consider the organizational context, develop the practice of educational debriefings, and distinguish cases requiring civil or disciplinary action from those that warrant criminal prosecution for gross negligence or intent.

Updating the regulatory framework and standards in the context of digitalization requires the inclusion of new legal concepts (e.g., telemedicine services, electronic medical information) and clarification of the definitions of crimes committed using digital technologies and official access. Legislation must be harmonized with international standards (GDPR, Oviedo Convention), as well as the development of national guidelines on telemedicine and AI, which will establish professional liability standards and mechanisms for legal assessment of physician actions.

Personnel training and education must take into account digital changes in medicine and law, integrating the training of future and current doctors, lawyers, and

administrators within a unified approach to the risks of the digital environment. It is necessary to introduce courses on the law and ethics of digital medicine, work with electronic medical records, telemedicine consultations, and cybersecurity, as well as develop joint formats such as interdisciplinary seminars and trainings that foster mutual understanding between specialists from different fields.

A culture of fairness and patient-centeredness remain key guidelines for the implementation of digital technologies, which should be assessed through the lens of their impact on patient safety and well-being. Transparency in data management, patient education about digital tools and the development of digital competence among physicians are all essential for minimizing risks, improving the quality of medical care and strengthening trust between patients and the healthcare system. They also ensure that technology is used responsibly in accordance with ethical and legal principles.

In summary, the digitalization of medicine represents a dual challenge: on the one hand, it strengthens control, traceability, and accountability; on the other, it gives rise to new forms of errors and violations that were previously unthinkable. This requires the evolution of scientific and practical approaches based on the integration of medicine, law, and digital technologies. For Moldova, it is important not only to consider international experience but also to actively participate in the development of global standards. A comprehensive approach will maximize the benefits of digitalization while minimizing the associated risks.

References

AACN. (2022, March 28). AACN's statement on the conviction of RaDonda Vaught. *American Association of Critical-Care Nurses*. https://www.aacn.org/newsroom/aacns-statement-on-the-conviction-of-radonda-vaught

American Nurses Association. (2022, March 25). Statement in response to the conviction of nurse RaDonda Vaught. *American Nurses Association*. https://www.nursingworld.org/news/news-releases/2022-news-releases/statement-in-response-to-the-conviction-of-nurse-radonda-vaught/

Amirov, R. G. (2021). *Metodika rassledovaniya prichineniya tyazhkogo vreda zdorov'yu vsledstvie nenadlezhashchego okazaniya meditsinskoy pomoshchi [Methodology for investigating the infliction of serious harm to health as a result of improper medical care]* (Doctoral dissertation). Rostov-on-Don, Russia.

Baranova, M. V. (2016). Operezhayushchee pravotvorchestvo v pravovoy sisteme sovremennosti [Anticipatory law-making in the modern legal system]. *Vestnik Saratovskoy Gosudarstvennoy Yuridicheskoy Akademii [Bulletin of the Saratov State Law Academy]*, *1*(108), 43-45.

Bloomberg Law. (2020, April 14). *Uptick in telehealth reveals medical malpractice concerns*. https://news.bloomberglaw.com/health-law-and-business/uptick-in-telehealth-reveals-medical-malpractice-concerns

Chervonnykh, E. V. (2009). *Prestupleniya, sovershaemye v sfere zdravookhraneniya, i ikh preduprezhdenie [Crimes committed in the field of healthcare and their prevention]* (Doctoral dissertation). Saratov, Russia.

Council of Europe. (1997, April 4). *Convention for the protection of human rights and dignity of the human being with regard to the application of biology and medicine (Convention on Human Rights and Biomedicine)* (ETS No. 164). Oviedo, Spain.

CRB-Vedeno. (2024, September 20). *IT-prestupleniya v zdravookhranenii [IT crimes in healthcare]*. https://crb-vedeno.ru/it-prestupleniya-v-zdravoohranenii/

European Union. (2016, April 27). *Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119*, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Finnegan, J. (2019, July 25). Diagnostic errors are top reason for liability claims against primary care doctors, report says. *Fierce Healthcare*. https://www.fiercehealthcare.com/practices/diagnostic-errors-are-top-reason-for-liability-claims-against-primary-care-doctors-report

Fogel, A. L., & Kvedar, J. C. (2019). Reported cases of medical malpractice in direct-to-consumer telemedicine. *JAMA, 321*(13), 1309-1310. https://doi.org/10.1001/jama.2019.0395

Fogel, A. L., Lacktman, N. M., & Kvedar, J. C. (2021). Skin cancer telemedicine medical malpractice risk. *JAMA Dermatology, 157*(7), 870-871. https://doi.org/10.1001/jamadermatol.2021.1475

Graber, M. L., Byrne, C., & Johnston, D. (2017). The impact of electronic health records on diagnosis. *Diagnosis, 4*(4), 211-223. https://doi.org/10.1515/dx-2017-0012

Institute of Medicine (US) Committee on Quality of Health Care in America. (2000). *To err is human: Building a safer health system* (L. T. Kohn et al., Eds.). National Academies Press. https://doi.org/10.17226/9728

Ivanova, Ya. I. (2017). *Metodika rassledovaniya yatrogennykh prestupleniy, sovershaemykh v sfere rodovspomozheniya [Methodology for investigating iatrogenic crimes committed in the field of obstetrics]* (Doctoral dissertation). Moscow, Russia.

Katz, H. P., Kaltsounis, D., Halloran, L., & Mondor, M. (2008). Patient safety and telephone medicine: Some lessons from closed claim case review. *Journal of General Internal Medicine, 23*(5), 517-522. https://doi.org/10.1007/s11606-007-0491-y

egea nr. 241 din 15-11-2007 privind comunicatiile electronice [Law No. 241 on electronic communications]. *Monitorul Oficial al Republicii Moldova*, 399-410, art. 679.

Leventhal, R. (2019, June 18). EHRs more frequently factor into medical malpractice claims, study finds. *Healthcare Innovation*. https://www.hcinnovationgroup.com/clinical-it/news/21095449/ehrs-more-frequently-factor-into-medical-malpractice-claims-study-finds

Lusk, C., DeForest, E., Segarra, G., Neyens, D. M., Abernathy, J. H. III, & Catchpole, K. (2022). Reconsidering the application of systems thinking in healthcare: The RaDonda Vaught case. *British Journal of Anaesthesia, 129*(3), e61-e62. https://doi.org/10.1016/j.bja.2022.05.023

Martin, D. (2023, October 9). Government agencies using AI to detect healthcare fraud. *Managed Healthcare Executive*. https://www.managedhealthcareexecutive.com/view/government-agencies-using-ai-to-detect-healthcare-fraud

Payasan, L. G., et al. (2022). Doctors say "Not only me": Medical malpractice as a professional crime in the internet medical era. *International Journal of Science and Healthcare Research, 7*(4), 326-333. https://doi.org/10.52403/ijshr.20221046

Pisarenco, C. S., & Pisarenco, S. V. (2022). Medico-legal aspects of digitalization of national healthcare on the example of phthisiopneumology. *Sanatate Publica, Economie si Management in Medicina*, 2(93-S), 273-277. ISSN 1729-8687.

Patru, L., Barbu, C. A., & Patru, C. L. (2023). Digitalization of medical services: A new ally for malpractice risk management. *"Ovidius" University Annals, Economic Sciences Series, 23*(1), 750-756. https://stec.univ-ovidius.ro/html/anale/RO/2023-i1/Section%204/27.pdf

Rich, B. A. (2005). Medical custom and medical ethics: Rethinking the standard of care. *Cambridge Quarterly of Healthcare Ethics, 14*(1), 27-39. https://doi.org/10.1017/S0963180105050048

Rosenbaum, Famularo & Segall, P.C. (n.d.). *The role of electronic health records in medical malpractice lawsuits*. Rosenbaum, Famularo & Segall LLP Blog.

Rowland, S. P., Fitzgerald, J. E., & Lungren, M. P. (2022). Digital health technology-specific risks for medical malpractice liability. *NPJ Digital Medicine, 5*(1), 157. https://doi.org/10.1038/s41746-022-00698-3

Sharma, A. (2025, May 9). *AI-driven health insurance: From complexity to clarity*. *Forbes Technology Council*. https://www.forbes.com/councils/forbestechcouncil/2025/05/09/ai-driven-health-insurance-from-complexity-to-clarity/

Shepelev, S. V. (2022). *Vzaimodeystvie sledovatelya so svedushchimi litsami v khode rassledovaniya prestupleniy, svyazannykh s nenadlezhashchim okazaniem meditsinskoy pomoshchi [Interaction of the investigator with experts in investigating crimes related to improper medical care]* (Doctoral dissertation). Moscow, Russia.

1st Healthcare Compliance. (2022, October 31). *Automatic dispensing cabinets & the case of RaDonda Vaught: Q&A. 1st Healthcare Compliance Blog*. https://1sthcc.com/automatic-dispensing-cabinets-the-case-of-radonda-vaught-qa/

Stovel, R. G., Gabarin, N., Cavalcanti, R. B., & Abrams, H. (2020). Curricular needs for training telemedicine physicians: A scoping review. *Medical Teacher, 42*(11), 1234-1242. https://doi.org/10.1080/0142159X.2020.1799959

Telemedicina - un nou concept digital va fi lansat in testare. (2025, July 9). *CIO.GOV.MD*. https://cio.gov.md/ro/node/39517

The Nuremberg Code. (1996). *JAMA, 276*(20), 1691. https://doi.org/10.1001/jama.1996.03540200075038

Tobia, K., Nielsen, A., & Stremitzer, A. (2021). When does physician use of AI increase liability? *Journal of Nuclear Medicine, 62*(1), 17-21. https://doi.org/10.2967/jnumed.120.256032

Venditti, S. A., Sazegar, P., Fuchs, L. C., & Snarskis, C. E. (2022). Family medicine resident and faculty perceptions about the strengths and limitations of telemedicine training. *PRiMER, 6*, 9. https://doi.org/10.22454/PRiMER.2022.665996

Vida-Simiti, I. (2025). The regulation of telemedicine in Romania: Issues of legal limitations in digital medical development. In A. L. Negrusa, M. M. Coros, & M. A. Camilleri (Eds.), *Sustainable and resilient businesses in the global economy* (pp. 309-321). Springer. https://doi.org/10.1007/978-3-031-75883-6_1

Williams, R., Jenkins, D. A., Ashcroft, D. M., Brown, B., Campbell, S., Carr, M. J., Cheraghi-Sohi, S., Kapur, N., Thomas, O., Webb, R. T., & Peek, N. (2020). Diagnosis of physical and mental health conditions in primary care during the COVID-19 pandemic: A retrospective cohort study. *The Lancet Public Health, 5*(10), e543-e550. https://doi.org/10.1016/S2468-2667(20)30201-2

World Medical Association. (2013, October). World Medical Association Declaration of Helsinki: Ethical principles for medical research involving human subjects. *JAMA, 310*(20), 2191-2194. https://doi.org/10.1001/jama.2013.281053

Wu, E., Wu, K., Daneshjou, R., Ouyang, D., Ho, D. E., & Zou, J. (2021). How medical AI devices are evaluated: Limitations and recommendations from an analysis of FDA approvals. *Nature Medicine, 27*(4), 582-584. https://doi.org/10.1038/s41591-021-01312-x