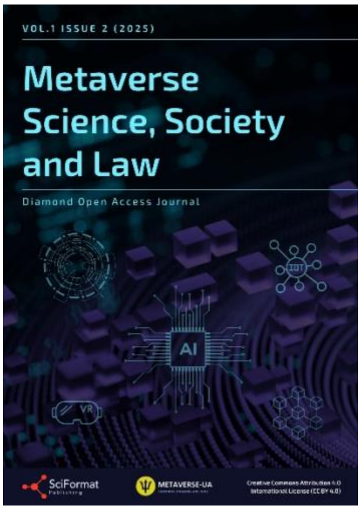


Metaverse Science, Society and Law

Vol. 1, Issue 2 (2025)

Publisher:
SciFormat Publishing Inc.

ISNI: 0000 0005 1449 8214
2734 17 Avenue Southwest, Calgary,
Alberta, Canada, T3E0A7

☎ +15878858911
✉ editorial-office@sciformat.ca

ARTICLE TITLE	SAFE USE OF DIGITAL MEDICAL DATA OF HIGH-TECH DIAGNOSTIC EXAMINATIONS IN EXPERT SIMULATION BASED ON VIRTUAL TWINS
DOI	https://doi.org/10.69635/mssl.2025.1.2.28
RECEIVED	10 October 2025
ACCEPTED	08 December 2025
PUBLISHED	15 December 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

SAFE USE OF DIGITAL MEDICAL DATA OF HIGH-TECH DIAGNOSTIC EXAMINATIONS IN EXPERT SIMULATION BASED ON VIRTUAL TWINS

Strelnykov Mykhailo
Candidate of Medical Sciences, Head of the Laboratory for the Study of Problems of Comprehensive Rehabilitation of the State Institution "Kundiev Institute of Occupational Medicine of the National Academy of Medical Sciences of Ukraine", Kyiv, Ukraine
ORCID ID: 0009-0006-1376-6664

Horobets Maria
Researcher of the Laboratory for the Study of Problems of Complex Rehabilitation, MDF of the Centre for Comprehensive Rehabilitation of the State Institution "Institute of Occupational Medicine named after Y.I. Kundiev of the National Academy of Medical Sciences of Ukraine", Kyiv, Ukraine
ORCID ID: 0009-0008-3756-1553

Kostenko Viktoria
Bachelor, Ministry of Justice of Ukraine
ORCID ID: 0009-0006-5939-6451

ABSTRACT

The article discusses the prerequisites for the safe use of digital medical data of high-tech diagnostic examinations, primarily magnetic resonance imaging (MRI), in expert medical modelling based on virtual patient twins (Digital Twin). Based on the analysis of modern research on privacy, security, and ethics of digital twins in medicine, cybersecurity, and the metaverse, the composition of the main threats has been clarified: falsification of images and metadata, personal data leaks, and non-transparent secondary use of information. A conceptual architecture of a medical digital twin for expert and forensic purposes is proposed, which integrates cryptographically secure storages, event logs, algorithms for detecting fake MRI data, and legal information processing policies. For quantitative assessment of risks, a probabilistic model has been built, as well as an optimization setting of the choice of technical and organizational protection measures. For automated data integrity control, a combination of convolutional and recurrent neural network (CNN+LSTM) for image analysis and an autoencoder with LSTM (AE+LSTM) for monitoring metadata sequences and access logs were used. It is shown how the proposed model is consistent with the requirements of the legislation of Ukraine on personal data protection, EU Regulation 2016/679 (GDPR) and the US HIPAA act and can be implemented within the framework of the Zero Trust architecture in medical information systems. The practical result of the work is the formation of a holistic methodology for the design of medical digital twins, focused on the expert use of MRI data, which minimizes legal risks and increases the reliability of conclusions.

KEYWORDS

Digital Twin, Magnetic Resonance Imaging, Medical Digital Data, MRI/CT Falsification, Privacy, Cybersecurity, Expert Medicine, Zero Trust, Multimodal Artificial Intelligence, GDPR, HIPAA

CITATION

Strelnykov Mykhailo, Horobets Maria, Kostenko Viktoria. (2025) Safe Use of Digital Medical Data of High-Tech Diagnostic Examinations in Expert Simulation Based on Virtual Twins. *Metaverse Science, Society and Law*. Vol. 1, Issue 2. doi: 10.69635/mssl.2025.1.2.28

COPYRIGHT

1. Introduction.

The purpose of this work is to analyse the vulnerability and threats of interference of third parties in digital databases of high-tech methods of diagnostic examinations for falsification of clinical diagnostic results (including through expert medical modelling) for the search and development of algorithms for safe ways to obtain, store, and distribute authentic data of modern digital medical imaging media.

Research materials and methods.

The methodological basis of the study is the analysis of the current regulatory and legal documentation, including acts of the Cabinet of Ministers of Ukraine on the digitalization of the healthcare sector, as well as scientific and analytical sources on medical informatics, digital medical diagnostics and the distribution of digital media. Methods of comparative analysis of the experience of using digital medical databases, content analysis of medical literature are applied.

Digital virtual twins (Digital Twin, Digital Twin, Digital Replica of Human) have become one of the key concepts of digital transformation, going far beyond industrial applications and actively penetrating medicine, public health, smart environments, and cybersecurity. In the medical plane, the patient's digital twin combines an electronic medical record (ID information, inclusive anatomical, physiological and functional data), 3-D scanning data of the body or individual organs, high-tech diagnostic examinations: (magnetic resonance imaging (MRI), spiral computed tomography (CT), positron emission tomography (PET), combined scanning (PET + CT), laboratory examinations, genetic, hereditary information and wearable sensor data for the construction of personalized models for health forecasting and decision support.

Digital Twins (DTs) have become a key tool for the digital transformation of medicine, enabling the creation of dynamic, personalized patient models for predicting, diagnosing, and optimizing treatment. They integrate multimodal data (clinical, genetic, imaging, sensor data) to support decision-making and personalized medicine.

Table 1. The main areas of application of digital twins in medicine

Application	Description	Source
Personalized treatment	Modelling the course of the disease, predicting response to therapy, selection of optimal drugs and dosage	[1,2,3,4]
Diagnostic support	Analysis of multi-level data (MRI, CT, genetics, laboratory) for early detection of diseases	[5,6,7]
Virtual clinical trials	Conducting in silico experiments to test new drugs and treatment strategies	[8,9,10]
Monitoring and prevention	Continuous data collection from wearable devices for dynamic risk prediction	[11,12,13]
Education and training	Virtual models for training doctors and planning complex procedures	[14,15,16]

At the same time, the use of digital twins in expert and forensic medical activities is developing modelling the development of pathological processes in the body and the course of diseases, reconstruction of injuries, checking the validity of diagnostic and therapeutic decisions, analysis of cause-and-effect relationships in clinical conflicts. The use of Digital Twins (DT) in forensic and expert practice opens new horizons for modelling pathological processes, reconstructing injuries, verifying the validity of clinical decisions and analysing cause-and-effect relationships in complex clinical situations. This direction is rapidly developing due to the integration of multimodal data, artificial intelligence and mathematical modelling

Modelling pathological processes and the course of diseases.

Digital twins allow you to create dynamic models of disease development, considering the individual characteristics of the patient, genetic, anatomical, physiological and behavioural data. Such models make it possible to predict the course of the disease, assess the impact of various factors (for example, injuries, medications, surgical interventions) and simulate alternative scenarios. This is especially valuable for expert assessment of complex cases, where it is necessary to reproduce the chronology of pathological changes or assess the influence of external factors.

Reconstruction of damage.

The use of 3D scanning, medical images (MRI, CT) and biomechanical modelling allows you to accurately reconstruct the mechanisms of injury, the nature and location of injuries. This increases the objectivity of forensic medical reports, allows you to virtually recreate events that led to injury or death, and assess their cause-and-effect relationship with diseases or external influences.

Verification of the validity of diagnostic and therapeutic decisions.

DTs allow you to simulate different diagnostic and treatment options, analyse their effectiveness and risks for a particular patient. This is important for expert assessment of the quality of medical care, verification of compliance of clinical decisions with modern standards and the validity of the choice of treatment tactics [17,18].

Analysis of cause-and-effect relationships in clinical conflicts.

Due to the ability to integrate large amounts of data and build complex cause-and-effect models, digital twins help to objectively analyse clinical conflicts, determine the role of various factors in the development of complications or deaths. This improves the quality of expert opinions and contributes to the fair resolution of medical and legal disputes [19].

The main advantages and limitations of digital twins in forensic science are given in Table 2.

Additional opportunities and prospects.

−Education and training: DTs are used to train experts, practice complex scenarios, improve the quality of expert opinions.

−Validation and ethics: Careful validation of models, compliance with ethical and legal norms, protection of personal data is necessary.

−Technological challenges: High demands on data quality, computing resources, standardization and interdisciplinary collaboration.

Table 2. Main Advantages and Limitations of Digital Twins in Forensic Science

Advantages	Restriction	Source
Objectivity and accuracy of reconstructions	High requirements for data quality and volume	[20,21,22,23]
Ability to simulate alternative scenarios	The need for standardization and validation	[24,25,26,27,28]
Improving the quality of expert opinions	Ethical and Legal Issues, Data Protection	[29,30,31]
Educational potential	Cost of implementation, need for specialists	[32,33]

Informed decision-making under the above scenarios depends on the reliability and integrity of the available digital data. Not only the predicted clinical outcome depends on the authenticity of MRI/CT, but also the legal consequences for patients, medical institutions and the state. Digital twins (CBs) accumulate large amounts of sensitive information, including biological, genetic, physiological, and behavioural data, which significantly increases the risk of privacy breaches due to unauthorized access, leaks, hacks, or improper use of data [34,35].

Digital twins (CBs) accumulate large amounts of sensitive information, including biological, genetic, physiological, and behavioural data, which significantly increases the risk of privacy breaches due to unauthorized access, leaks, hacks, or improper use of data [36,37].

Centralized storage and the ability to combine heterogeneous data sources, as well as the use of opaque machine learning algorithms, increase the risks of profiling, discriminatory decisions, and re-identification of individuals. These risks are particularly critical for children with rare diseases, where even anonymized data can be re-identified [38,39].

A separate dimension of risks is associated with the technical feasibility of falsifying medical images and metadata. Work on Generative Adversarial Networks (GAN) and diffusion models has shown that fake MRI images, with inserted or masked pathologies, can go unnoticed even by experienced radiologists [40,41,42,43]. In parallel, the vulnerability of medical image archives (PACS) and the lack of cryptographic signatures in the DICOM format create opportunities for metadata-level manipulation and network attacks [44,45,46].

The regulatory framework of the European Union (Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)), the USA (Health Insurance Portability and Accountability Act (HIPAA)) and Ukraine (the Law of Ukraine "On Personal Data Protection" No. 2297-VI) defines the general principles of medical data processing, but does not provide comprehensive answers regarding the specifics of digital twins and expert modelling based on them. Additional guidelines are set by the Council of Europe Convention 108+, industry guidance documents of data protection authorities on the processing of video and visual data, as well as recommendations for building a Zero Trust architecture, particularly NIST SP 800-207. For software medical devices based on artificial intelligence, regulatory recommendations on the life cycle of such solutions are important [47].

The relevance of the study is due to the need to combine technical means of protection and detection of falsification of MRI data with the legal requirements and organizational procedures of medical institutions, as well as to adapt these approaches to the Ukrainian legal context, considering the best practices of the EU and the USA. The purpose of the work is to develop methodological and mathematical foundations for the safe use of digital medical data of high-tech diagnostic examinations in expert medical modelling based on virtual twins, with an emphasis on identifying and reducing the risks of MRI/CT falsification and compliance with regulatory requirements.

To achieve the goal, the following tasks have been set:

1. to analyse modern approaches to building medical digital twins and protecting patient privacy;
2. to form a conceptual architecture of the digital twin for expert and forensic applications, focused on the use of MRI data;
3. to build a probabilistic model of the risks of falsification of images and MRI metadata and an optimization formulation of the choice of protection measures;
4. to offer algorithmic solutions for automated detection of falsifications based on convolutional and recurrent neural networks (CNN+LSTM, AE+LSTM);
5. to assess the compliance of the proposed architecture with the requirements of the legislation of Ukraine, the EU and the USA and to outline the organizational aspects of the implementation of Zero Trust in medical information systems.

2. Methods

2.1. Conceptual architecture of the medical digital twin (fig,1).

The proposed architecture of the medical digital twin for expert modelling consists of the following main subsystems:

1. a data collection subsystem that includes MRI/CT scanners, other diagnostic modalities, and wearable devices;
2. secure medical record storage that combines cloud resources with local nodes (edge computing);
3. digital twin generation module, which integrates multimodal data into a unified authentic model of the patient's condition;
4. MRI data falsification detection module based on CNN+LSTM and AE+LSTM hybrid models;
5. a legal policies and consent management module that implements the requirements of GDPR, HIPAA and national legislation;
6. event log and blockchain-like transaction ledger to ensure traceability of data changes;
7. an interface for interaction with experts and authorities, which considers the recommendations for software medical devices (SaMD).

Conclusion.

The study identifies the secure use of digital medical data from high-technology diagnostic examinations within the framework of medical digital twins as a complex technical-legal and organisational challenge that goes far beyond classical information security. It shows that MRI/CT data and their associated metadata have a dual nature: on the one hand, they constitute a critical resource for personalised medicine, while on the other, they are potentially important evidential material for expert and forensic medical practice. It is precisely this dual status that creates the need for specialised approaches to data integrity, authenticity and traceability throughout the entire life cycle of the digital twin.

The study defines the conceptual architecture of a medical digital twin as a central instrument for the minimisation of cyber risks and for counteracting the falsification of diagnostic images. The architecture integrates modules for cryptographic protection, secure storage, event logging and AI-based analysis, including models based on CNN+LSTM for detecting anomalies in images and AE+LSTM for analysing metadata and logs. In addition, a probabilistic model for assessing incident risks, formulated as an optimisation problem for selecting safeguards, has been constructed, making it possible to justify investment in security with due regard to probabilities, potential losses and the cost of controls.

The study treats the legal dimension as a necessary framework for technological implementation: a comparison of the proposed architecture with the requirements of national legislation, the GDPR, HIPAA and Convention 108+ demonstrates the possibility of embedding the principles of "privacy by design", data minimisation, protection of patients' rights and transparency of processing directly into the technical design of the system. In parallel, it outlines the organisational preconditions for effective implementation, including the formation of interdisciplinary teams, the introduction of internal regulations, staff training, regular compliance audits and a phased transition to a Zero Trust architecture in medical information systems.

The study also identifies further directions for development: the use of large volumes of real clinical data to validate the proposed models, the adaptation of the methodology to other types of diagnostic examination, and the extension of multimodal AI analysis (combining images, textual reports, time series and access logs). Taken together, these results from the methodological basis for a transition from isolated experiments with digital twins to integrated, legally protected and clinically significant systems capable of becoming a key instrument of safe medicine and forensic medical examination in the digital age.

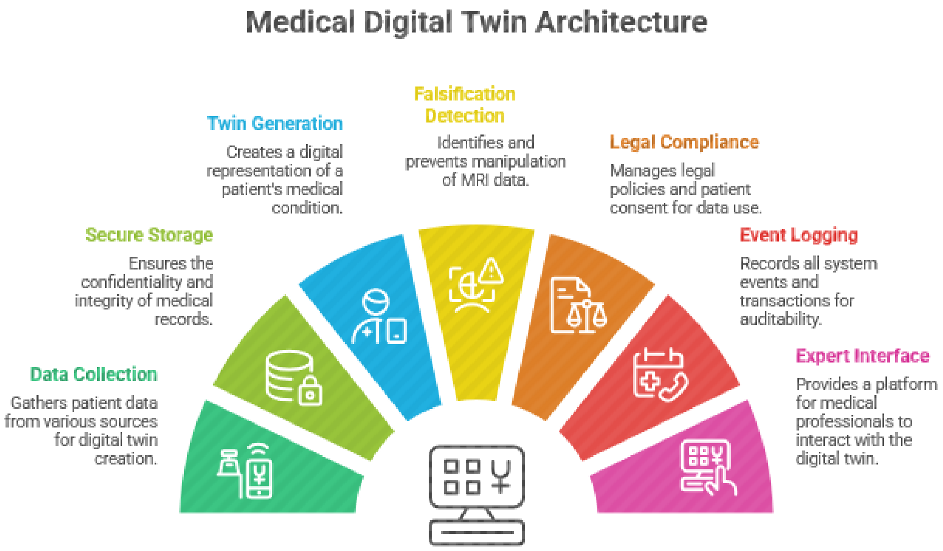

Medical Digital Twin Architecture
Twin Generation
Creates a digital representation of a patient's medical condition.
Falsification Detection
Identifies and prevents manipulation of MRI data.
Legal Compliance
Manages legal policies and patient consent for data use.
Secure Storage
Ensures the confidentiality and integrity of medical records.
Event Logging
Records all system events and transactions for auditability.
Data Collection
Gathers patient data from various sources for digital twin creation.
Expert Interface
Provides a platform for medical professionals to interact with the digital twin.

Fig. 1. *Conceptual architecture of the medical digital twin.*

For expert scenarios (medical and legal disputes, forensic medical examinations), the key requirements are: the impossibility of imperceptibly changing data, fixing all accesses, the possibility of independent verification of integrity and compliance of data processing procedures with the principles of legality, minimization and intended purpose.

2.2. Probabilistic model of falsification risks.

Let the set of potential incidents $\{E_1, ..., En\}$ describe events of falsification or data leakage (image editing, metadata substitution, man-in-the-middle attack, PACS compromise, etc. [9; 18]). For each event, the probability of its occurrence for a given period and the expected losses of Li are determined, which may include clinical, legal and reputational components.

Integral risk is written as the mathematical expectation of aggregate losses: (1) R=Σ (from i = 1 to n) pi · L_i.

Let's introduce the vector of protection measures $x=(x_1, ..., xm)$, where $xj \in \{0,1\}$ reflects the implementation or non-implementation of the j-th technical or organizational control (DICOM digital signatures, two-factor authentication, Zero Trust gateways, internal audit, federated training, etc.).

Let cj be the cost of implementing and maintaining the j-th control, and pi(x) be the modified probability of an incident Ei in the presence of the selected set of controls. Optimization problem for minimizing the amount of residual risk and defense costs: (2) minimize $F(x) = \Sigma$ (from $i = 1$ to n) $pi(x) \cdot L_i + \lambda \cdot \Sigma$ (from $j = 1$ to m) $cj\ xj$, where $\lambda > 0$ is the coefficient reflecting the acceptable trade-off between risk and cost. Restriction: (3) Σ ($j = 1$ to m) $cj\ xj \leq B$, where B is the available budget. In addition, regulatory requirements are taken into account, for example, the obligation to ensure certain rights of the data subject (right of access, rectification, erasure, restriction of processing) in accordance with the GDPR and Ukrainian legislation

2.3. CNN+LSTM model for detecting MRI image falsifications To detect pixel-level falsifications, we use a hybrid model that combines a convolutional neural network (CNN) to isolate spatial features from MRI volumes and Long Short-Term Memory (LSTM) to analyze sequences of slice or series of studies over time.

Let $Xt \in R^{\{H\times W\}}$ be a two-dimensional slice of the MRI at time t or in the sequence number of the series. CNN converts it to the feature vector $ft = CNN(Xt; \theta\_c)$, where θ_c are the parameters of the convolutional layers.

Next, the sequence $\{ft\}$ ($t = 1... T$) is applied to the input of the LSTM module: (4) $ht = LSTM(ft, ht_{-1}; \theta\_l)$, $yt = \sigma(W\_y\ ht + b\_y)$, where ht is the latent state, θ_l is the LSTM parameters, W_y, b_y is the output layer parameters, σ is the logistic activation function, and $yt \in (0; 1)$ is an assessment of the probability that the corresponding slice/series is falsified.

The model is trained on labeled data including both real and artificially modified images obtained using GAN and diffusion models [14–18; 12]. It is important to use a balanced dataset and regularization methods to avoid overtraining for specific "fingerprints" of individual generative models.

2.4. AE+LSTM Model for Metadata and Event Logs Analysis.

Falsification of MRI/CT data is often accompanied by irregularities in the sequence of DICOM metadata (change of StudyDate, PatientID, SeriesInstanceUID) or atypical user actions in PACS logs [7; 9; 10]. To detect such anomalies, it is proposed to use an autoencoder (Autoencoder, AE) in combination with LSTM, which simulates the "normal" dynamics of events and metadata.

Let $zt \in R^d$ be a feature vector describing the event in the log (operation type, user role, network host, time intervals) and aggregated DICOM metadata. AE+LSTM learns to reconstruct these sequences:(5) $\hat{z}_t = Dec(\ LSTM(\ Enc(z_t),\ h_{t-1}\ );\ \theta dec)$, where Enc and Dec are the encoding and decoding modules of the autoencoder with the parameters θenc, θdec, respectively, and LSTM simulates the time dependence. The loss function is given as the standard error of the reconstruction: (6) $J(\theta) = (1/T) \cdot \Sigma$ ($t = 1$ to T) $||z_t - \hat{z}_t||^2$, where $\theta = (\theta enc, \theta dec, \theta l)$. After training on "pure" data, anomalies are detected by exceeding the threshold value of the reconstruction error $Jt = ||z_t - \hat{z}_t||^2 > \tau$, while τ is chosen taking into account the desired sensitivity and specificity of the method.

2.5. Legal and organizational methods In parallel with the technical models, a legal analysis of the compliance of the digital twin architecture with the requirements was performed:

- GDPR regarding the rights of the data subject, the principles of "privacy by design" and "privacy by default";
- HIPAA in terms of health information protection, access logging and incident management;
- Law of Ukraine "On Personal Data Protection" No. 2297-VI and related acts in the field of health care;
- Council of Europe Convention 108+ on Automatic Processing of Personal Data;
- NIST recommendations for Zero Trust architecture [25];
- documents of data protection authorities on the processing of video and visual data;
- regulatory approaches to the life cycle of AI/ML-based software medical devices. The analysis is carried out by comparing the requirements for medical data processing with the functional modules of the digital twin architecture and determining the necessary organizational procedures (access policies, consent management, auditing, incident response).

3. Result.

3.1. Classification of risks and means of counteraction Based on the analysis of the literature and practices of cybersecurity, a classification of risks associated with the use of digital MRI data in digital twins and appropriate countermeasures has been formed (Table 3).

Table 3. Main risks of falsification of medical digital data and remedies

№	Type of riziku	Possible consequences	
1	Editing Image (pixel-level tampering)	Misdiagnosis, erroneous expert opinions, legal claims	countermeasures DICOM hashing files, digital signatures, PACS logs, CNN+LSTM falsification detectors,
2	Fraud DICOM metadata	Identity substitution, errors in dates and protocols, distortion of the medical history	Role-based access control, header integrity control, AE+LSTM analysis metadata sequences
3	Generation of artificial MRI (GAN-based fabrication)	Fraudulent Insured events, falsification of research data, manipulation in court	Cryptographic image signing, GAN fingerprint detectors, bill-level watermarks
4	Transmission Time Attacks (MITM) between the scanner and the PACS	Replacement or modification of research "on the way", unauthorized access to data	TLS/VPN countermeasures, Zero Trust gateways, rejection of unencrypted DICOM traffic, network monitoring
5	Compromise PACS/RIS/HIS and accounts	Mass modification or deletion of data, insider abuse	Multi-factor authentication, the principle of least privilege, regular log audits, backups

3.4. Integrating MATLAB Mobile into the Digital Twin Circuit

To illustrate the practical use, consider a simple scenario of applying MATLAB Mobile to send anonymized MRI data to secure cloud storage, where it is processed by a digital twin model. Below is an example of the code (Fig. 2).

4. Discussion

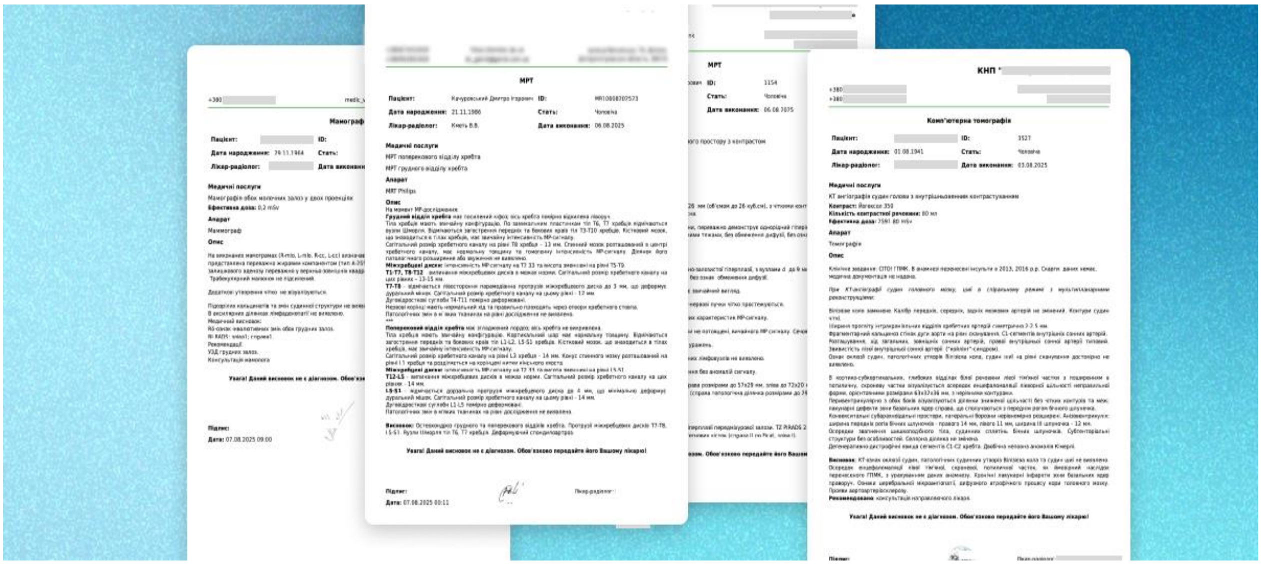
4.1 Comparison with other studies.

The results of the work logically continue and expand modern approaches to the analysis of privacy and security of digital twins. Proposes a model of legal co-governance, where responsibility for data security is shared between the platform operator, developers, and users. Our architecture supports this approach by adding technical mechanisms for integrity control and detection of MRI falsifications, which reduces information asymmetry between the parties.

Analyzes the legal and ethical aspects of digital twins of children with rare diseases, focusing on the challenges of re-identification and long-term data retention. The proposed model can be adapted to this context by supporting pseudonymization, consent management and access logging, which is especially important for the protection of vulnerable patient groups.

Unlike purely technical approaches to digital twin protection, the proposed solution integrates a probabilistic risk model, security cost optimization, deep learning methods, and legal analysis. This allows you to justify organizational decisions (choice of controls, policies, procedures) on a quantitative basis, and not only on intuitive assessments.

Organizational aspects of implementation in health care institutions.



МРТ

Пацієнт:	Качуровський Дмитро Ігорович	ID:	MR1080820?573
Дата народження:	21.11.1986	Стать:	Чоловіча
Лікар-радіолог:	Кметь В.В.	Дата виконання:	06.08.2025

Медичні послуги

МРТ поперекового відділу хребта

МРТ грудного відділу хребта

Апарат

МRТ Philips

Опис

Мамографія

Комп'ютерна томографія

Увага! Даний висновок не є діагнозом. Обов'язково передайте його Вашому лікарю!

Fig. 2. MATLAB Mobile to send anonymized MRI data to secure cloud storage, where it is processed by a digital twin model.

The procedure for undergoing MRI examination (standardized clinical protocol). The MRI process consists of several standardized steps that are used in most medical institutions in the world.

4.1.1. Referral and initial assessment. The doctor forms a clinical referral with a clear diagnostic task.

Indications and contraindications are checked: implanted metal structures, Pacemakers insulin pumps, claustrophobia, pregnancy (1st trimester).

4.1.2. Patient preparation. Removal of all metal objects. Clarification of medication intake (especially with MRI with contrast). Signature of informed consent. If necessary, an anxiety scale, sedation, screening for allergies to contrast.

4.1.3. Positioning in the tomograph. The patient is placed on the table of the device in a fixed position. Special coils are used in accordance with the area of study (main, spinal, abdominal). The patient receives a recommendation not to move.

4.1.4. Calibration and Adjustment. The technician conducts: Localizers (Scout/Localizer), selection of sequence parameters, signal-to-noise (SNR) check, checking motion artifacts.

4.1.5. Scanning. Sequence series are performed: T1, T2, FLAIR, DWI, SWI, GRE, MRA/MRV, proton density, depending on the readings. If necessary, intravenous administration of contrast (Gadolinium). Duration of the examination: 15–40 minutes.

4.1.6. Data processing. Saving the resulting slices in DICOM format. Quality Control (QA): evaluation of artifacts, completeness and correctness of series. Transfer data to the PACS or to the radiologist's workstation.

4.1.7. Description. The radiologist interprets the image. A structured protocol is formed (according to the BI-RADS, PI-RADS, LI-RADS, NI-RADS standard, depending on the body). Transferred: DICOM data, output, key frames.

As you can see, in no case is it a question of ensuring the authenticity of the examination, both by finding out the identity of the examinee, and by imposing the doctor's EDS on a digital medium after the examination is completed. And which is very discordant with the Procedure for Data Transfer between Hospitals.

Transfer of digital diagnostic data of patients between hospitals.

4.2. The Importance of Digital Medical Image Transmission. The transfer of diagnostic data between healthcare facilities is a key element of continuity of care. It allows: avoid repeated examinations (reduction of radiation exposure), speed up the diagnosis, provide council diagnostics, create a single digital patient profile. The growing number of MRI/CT scans makes standardized digital interoperability critical.

4.2.1 Standards and protocols for data transmission. International practice uses several technological protocols.

4.2.2. DICOM (Digital Imaging and Communications in Medicine). The main standard that determines: image format, metadata format, network transmission (DICOM C-STORE, C-MOVE, C-FIND), electronic

UIDs for series validation, encryption and authentication. Advantage: Hospitals can transmit images without changing the file structure.

4.2.3. PACS ↔ PACS Transmission. Hospitals use PACS servers to: storage (archive), Access (viewers), routing. The transfer is carried out through: DICOM network interface, VPN tunnels, HL7/FHIR integration.

4.2.4. International exchange systems: IHE XDS and XDS-I. XDS-I is an image exchange standard used in Europe (eHealth Digital Service Infrastructure). Functions: image indexing, centralized repository, inquiry/response between hospitals in different countries.

4.2.5. HL7 v2 / v3 and FHIR. It transmits not the image itself, but data about it: study number, patient's data, information about the provider, Series available. FHIR provides the transmission of: image links, metadata, clinical reports (Diagnostic Report).

4.3. Data Transfer Models Between Hospitals

4.3.1. Direct Transmission (P2P). Hospital A sends data directly to Hospital B through: DICOM C-STORE + VPN, encrypted PACS backend. Advantages: speed, simplicity. Disadvantages: dependence on network interoperability and IT compatibility.

4.3.2. Cloud Archives (Cloud-PACS, VNA – Vendor Neutral Archive). This is the model of the United States and Canada. The data is stored in a single cloud archive with access through authorization. Advantages: Easy access to another hospital, lack of physical media, impossibility of imperceptible substitution of files thanks to log entries.

4.3.3. Patient-centred model. The patient himself becomes the "owner" of the data. Used: electronic cabinets, QR code to download DICOM, mobile applications (Apple Health Records, EU Personal Health Viewer). Advantages: reduces administrative delays, The patient maintains access control.

4.4. Main risks during transmission between hospitals

4.4.1. Technical risks. Substitution of files during transfer (in the absence of encryption). Loss of metadata (name, ID, series UID). DICOM corruption due to incorrect export. Incompatibility of PACS systems.

4.4.2. Information risks. Incorrect identification of the patient. Leaks of personal data during transmission through flash drives, DVD, email.

4.4.3. Cybersecurity. Unauthorized access to PACS. Data theft in the transfer process. Injection of fake images (deepfake manipulations). Attacks on healthcare servers (observed worldwide).

5. Protection and safe transmission mechanisms.

5.1. Cryptographic means. TLS 1.3 encryption in PACS-PACS channels. Electronic digital signature for DICOM files. Series hashing (SHA-256) for integrity verification.

5.2. Audit and logging. Each operation: View, export, Transfer, Remove, must be written to the PACS logs with the impossibility of change.

5.3. Access Control. Two-factor authorization of the doctor. Role-based access. Access tokens with limited validity.

5.4. International requirements. Used: GDPR (EU) — protection of personal medical data, HIPAA (USA) — medical privacy, ISO/IEC 27799 — information security management in healthcare.

6. Perspectives: Digital Image Mobility.

New approaches that change the transmission of diagnostic data:

6.1. Blockchain archiving. impossibility of image forgery, version control, Evidence in court.

6.2. Central National Archives. It is used in: Sweden, Denmark, Estonia, Uk. All hospitals are connected to the same cloud registry.

6.3. AI Analysis Before Transmission. Quality control algorithms: detect damaged or suspicious series, check the compliance of protocol parameters.

7. Conclusions

The transfer of digital diagnostic data between hospitals is a critical element of modern digital medicine. Its effectiveness depends on: application of international standards (DICOM, HL7, FHIR, IHE XDS-I), secure communication channels, digital signatures and integrity control, integrated PACS/VNA archives.

Digital data mobility reduces the risks of repeat studies, improves the quality of treatment, and creates the basis for virtual twins and personalized medicine.

The implementation of medical digital twins for expert modelling requires not only technical modernization, but also changes in organizational culture. Based on the analysis of the privacy policies of large IT companies and the practices of medical institutions, several key areas can be distinguished:

- creation of interdisciplinary teams (clinicians, lawyers, IT specialists, information security specialists) to manage the life cycle of digital twins;
- development of internal regulations for the creation, use and deactivation of a digital twin, including expert access rules;
- implementation of training programs for medical personnel on the risks of digital data falsification, social engineering and basic principles of cyber hygiene;
- integration of audit procedures (internal and external) with the use of log analytics and AI methods for anomaly monitoring.

Organizational mechanisms should be formalized in policies and procedures that can be reviewed by regulators and used as evidence of due diligence by the institution in the event of litigation.

7.1. Limitations of the study

Main limitations of work:

- CNN+LSTM and AE+LSTM models are considered at the conceptual level;
- further research is needed using large, representative MRI datasets and event logs, considering different equipment manufacturers;
- the probabilistic risk model uses conditional estimates of probabilities and losses;
- for specific institutions, it is necessary to adapt parameters based on historical incident data;
- legal analysis focuses on three jurisdictions (Ukraine, EU, USA) and does not consider the specifics of other countries, which is important for international research;
- ethical aspects (fairness of algorithms, non-discrimination, informed consent in the context of complex AI systems) are partially covered and require separate research.

7.2. Prospects of Zero Trust and Multimodal Artificial Intelligence The further development of digital twin technologies in medicine is closely related to the implementation of the Zero Trust architecture and multimodal artificial intelligence models. Zero Trust involves the abandonment of the "secure perimeter" and the constant verification of each access to the resource, including the digital twin [25]. This corresponds to the fact that digital twins can be accessed from different locations (clinics, remote experts, mobile devices) and require context-sensitive access policies. Multimodal AI models capable of simultaneously processing text, images, time series, and structured data open new opportunities for complex analysis of digital twins [1; 12]. In the context of detecting falsifications, this allows:

- compare the content of MRI data with clinical documentation;
- identify inconsistencies between text descriptions and images;
- combine the analysis of images, metadata, and user behavioural patterns. At the same time, multimodal models strengthen the requirements for transparency and explainability, which should be reflected in the regulatory framework and organizational procedures of medical institutions.

Conclusions

The study identifies the secure use of digital medical data from high-technology diagnostic examinations within the framework of medical digital twins as a complex technical-legal and organisational challenge that goes far beyond classical information security. It shows that MRI/CT data and their associated metadata have a dual nature: on the one hand, they constitute a critical resource for personalised medicine, while on the other, they are potentially important evidential material for expert and forensic medical practice. It is precisely this dual status that creates the need for specialised approaches to data integrity, authenticity and traceability throughout the entire life cycle of the digital twin.

The study defines the conceptual architecture of a medical digital twin as a central instrument for the minimisation of cyber risks and for counteracting the falsification of diagnostic images. The architecture integrates modules for cryptographic protection, secure storage, event logging and AI-based analysis, including models based on CNN+LSTM for detecting anomalies in images and AE+LSTM for analysing metadata and logs. In addition, a probabilistic model for assessing incident risks, formulated as an optimisation problem for selecting safeguards, has been constructed, making it possible to justify investment in security with due regard to probabilities, potential losses and the cost of controls.

The study treats the legal dimension as a necessary framework for technological implementation: a comparison of the proposed architecture with the requirements of national legislation, the GDPR, HIPAA and Convention 108+ demonstrates the possibility of embedding the principles of “privacy by design”, data minimisation, protection of patients’ rights and transparency of processing directly into the technical design of the system. In parallel, it outlines the organisational preconditions for effective implementation, including the formation of interdisciplinary teams, the introduction of internal regulations, staff training, regular compliance audits and a phased transition to a Zero Trust architecture in medical information systems.

The study also identifies further directions for development: the use of large volumes of real clinical data to validate the proposed models, the adaptation of the methodology to other types of diagnostic examination, and the extension of multimodal AI analysis (combining images, textual reports, time series and access logs). Taken together, these results from the methodological basis for a transition from isolated experiments with digital twins to integrated, legally protected and clinically significant systems capable of becoming a key instrument of safe medicine and forensic medical examination in the digital age.

The paper proposes an integrated approach to the safe use of digital medical data of high-tech diagnostic examinations, primarily MRI, in expert medical modelling based on virtual patient twins. Main results:

1. Based on the analysis of modern research, a list of key risks associated with falsification of images and metadata, data leaks and vulnerabilities of digital twin infrastructure has been formed.

2. A conceptual architecture of a medical digital twin for expert and forensic applications is proposed, including modules for data collection, secure storage, AI analysis, and legal policies.

3. A probabilistic model for assessing the risk of incidents and an optimization setting of the choice of technical and organizational protection measures has been built, an example of quantitative justification of the feasibility of investments in security has been demonstrated.

4. An approach to detecting MRI data falsifications based on CNN+LSTM models for image analysis and AE+LSTM for metadata analysis and event logs has been developed.

5. The proposed architecture is compared with the requirements of the regulations of Ukraine, the EU and the USA, the possibility of its adaptation to the Zero Trust mode and multimodal AI analysis is shown.

Practical recommendations:

• implement digital signatures and hashing of DICOM files, mandatory logging and log analysis using AE+LSTM;

• form interdisciplinary teams to manage digital twins and conduct regular audits of compliance with GDPR, HIPAA and national legislation;

• to gradually implement the Zero Trust architecture in medical information systems, starting with modules that process MRI data in expert scenarios; • develop and maintain training programs for medical personnel on the risks of falsification and the basics of digital data security;

• conduct further research using large, real-world datasets to validate AI models and adapt the methodology to other types of diagnostic examinations.

REFERENCES

1 Vallée, A. (2025). Digital Twins for Personalized Medicine Require Epidemiological Data and Mathematical Modeling: Viewpoint.. *Journal of medical Internet research*, 27, e72411 . https://doi.org/10.2196/72411.

2 Li, X., Loscalzo, J., Mahmud, A., Aly, D., Rzhetsky, A., Zitnik, M., & Benson, M. (2025). Digital twins as global learning health and disease models for preventive and personalized medicine. *Genome Medicine*, 17. https://doi.org/10.1186/s13073-025-01435-7.

3 Fischer, R., Volpert, A., Antonino, P., & Ahrens, T. (2024). Digital patient twins for personalized therapeutics and pharmaceutical manufacturing. *Frontiers in Digital Health*, 5. https://doi.org/10.3389/fdgth.2023.1302338.

4 Roopa, M., & Venugopal, K. (2025). Digital Twins for Cyber-Physical Healthcare Systems: Architecture, Requirements, Systematic Analysis, and Future Prospects. *IEEE Access*, 13, 44963-44996. https://doi.org/10.1109/access.2025.3547991.

5 Padoan, A., & Plebani, M. (2024). Dynamic mirroring: unveiling the role of digital twins, artificial intelligence and synthetic data for personalized medicine in laboratory medicine. *Clinical Chemistry and Laboratory Medicine (CCLM)*, 62, 2156 - 2161. https://doi.org/10.1515/cclm-2024-0517.

6 Laubenbacher, R., Mehrad, B., Shmulevich, I., & Trayanova, N. (2024). Digital twins in medicine. *Nature computational science*, 4 3, 184-191 . https://doi.org/10.1038/s43588-024-00607-6.

7 Katsoulakis, E., Wang, Q., Wu, H., Shahriyari, L., Fletcher, R., Liu, J., Achenie, L., Liu, H., Jackson, P., Xiao, Y., Syeda-Mahmood, T., Tuli, R., & Deng, J. (2024). Digital twins for health: a scoping review. *NPJ Digital Medicine*, 7. https://doi.org/10.1038/s41746-024-01073-0.

8 Boulos, M., & Zhang, P. (2021). Digital Twins: From Personalised Medicine to Precision Public Health. *Journal of Personalized Medicine*, 11. https://doi.org/10.3390/jpm11080745.

9 Zhang, K., Zhou, H., Baptista-Hon, D., Gao, Y., Liu, X., Oermann, E., Xu, S., Jin, S., Zhang, J., Sun, Z., Yin, Y., Razmi, R., Loupy, A., Beck, S., Qu, J., & Wu, J. (2024). Концепції та застосування цифрових двійників в охороні здоров'я та медицині. *Patterns* , 5. https://doi.org/10.1016/j.patter.2024.101028 .

10 Björnsson, B., Borrebaeck, C., Elander, N., Gasslander, T., Gawel, D., Gustafsson, M., Jörnsten, R., Lee, E., Li, X., Lilja, S., Martínez-Enguita, D., Matussek, A., Sandström, P., Schäfer, S., Stenmarker, M., Sun, X., Sysoev, O., Zhang, H., & Benson, M. (2019). Digital twins to personalize medicine. *Genome Medicine*, 12. https://doi.org/10.1186/s13073-019-0701-3.

11 Roopa, M., & Venugopal, K. (2025). Digital Twins for Cyber-Physical Healthcare Systems: Architecture, Requirements, Systematic Analysis, and Future Prospects. *IEEE Access*, 13, 44963-44996. https://doi.org/10.1109/access.2025.3547991.

12 Sun, T., He, X., Song, X., Shu, L., & Li, Z. (2022). Цифровий двійник у медицині: ключ до майбутнього охорони здоров'я?. *Frontiers in Medicine* , 9. https://doi.org/10.3389/fmed.2022.907066 .

13 Diniz, P., Grimm, B., Garcia, F., Fayad, J., Ley, C., Mouton, C., Oeding, J., Hirschmann, M., Samuelsson, K., & Seil, R. (2025). Digital twin systems for musculoskeletal applications: A current concepts review.. *Knee surgery, sports traumatology, arthroscopy : official journal of the ESSKA*. https://doi.org/10.1002/ksa.12627.

14 Cellina, M., Ce', M., Alì, M., Irmici, G., Ibba, S., Caloro, E., Fazzini, D., Oliva, G., & Papa, S. (2023). Digital Twins: The New Frontier for Personalized Medicine?. *Applied Sciences*. https://doi.org/10.3390/app13137940.

15 Vallée, A. (2023). Digital twin for healthcare systems. *Frontiers in Digital Health*, 5. https://doi.org/10.3389/fdgth.2023.1253050.

16 Ganesan, K., & Ganesan, K. (2025). AI-Driven Digital Twins: Real-Time Multimodal Data Integration for Personalized Therapeutic Optimization in Healthcare. *International Journal of Innovative Science and Research Technology*. https://doi.org/10.38124/ijisrt/25may895.

17 Coorey, G., Figtree, G., Fletcher, D., Snelson, V., Vernon, S., Winlaw, D., Grieve, S., McEwan, A., Yang, J., Qian, P., O'Brien, K., Orchard, J., Kim, J., Patel, S., & Redfern, J. (2022). The health digital twin to tackle cardiovascular disease—a review of an emerging interdisciplinary field. NPJ Digital Medicine, 5. https://doi.org/10.1038/s41746-022-00640-7.

18 Shen, S., Qi, W., Liu, X., Zeng, J., Li, S., Zhu, X., Dong, C., Wang, B., Shi, Y., Yao, J., Wang, B., Jing, L., Cao, S., & Liang, G. (2025). From virtual to reality: innovative practices of digital twins in tumor therapy. Journal of Translational Medicine, 23. https://doi.org/10.1186/s12967-025-06371-z.

19 Giansanti, D., & Morelli, S. (2025). Exploring the Potential of Digital Twins in Cancer Treatment: A Narrative Review of Reviews. Journal of Clinical Medicine, 14. https://doi.org/10.3390/jcm14103574.

20 Wang, Y., Lu, Y., Xu, Y., , Z., Xu, H., Du, B., Gao, H., & Wu, J. (2024). TWIN-GPT: Digital Twins for Clinical Trials via Large Language Model. ACM Transactions on Multimedia Computing, Communications and Applications. https://doi.org/10.1145/3674838.

21 Vallée, A. (2025). Digital Twins for Personalized Medicine Require Epidemiological Data and Mathematical Modeling: Viewpoint.. Journal of medical Internet research, 27, e72411 . https://doi.org/10.2196/72411.

22 Vallée, A. (2023). Digital twin for healthcare systems. Frontiers in Digital Health, 5. https://doi.org/10.3389/fdgth.2023.1253050.

23 Huang, L., Pan, L., Wu, C., Tian, M., Li, Q., Peng, Y., Li, Q., & Li, Y. (2024). Application and development prospect of digital twin in the forensic identification of cardiovascular diseases. Digital Medicine. https://doi.org/10.1097/dm-2024-00013.

24 Gilbert, S., Drummond, D., Cotte, F., & Ziemssen, T. (2025). Editorial: Digital twins in medicine—transition from theoretical concept to tool used in everyday care. Frontiers in Digital Health, 7. https://doi.org/10.3389/fdgth.2025.1573727.

25 Allen, A., Siefkas, A., Pellegrini, E., Burdick, H., Barnes, G., Calvert, J., Mao, Q., & Das, R. (2021). A Digital Twins Machine Learning Model for Forecasting Disease Progression in Stroke Patients. Applied Sciences. https://doi.org/10.3390/app11125576.

26 Grieb, N., Schmierer, L., Kim, H., Strobel, S., Schulz, C., Meschke, T., Kubasch, A., Brioli, A., Platzbecker, U., Neumuth, T., Merz, M., & Oeser, A. (2023). A digital twin model for evidence-based clinical decision support in multiple myeloma treatment. Frontiers in Digital Health, 5. https://doi.org/10.3389/fdgth.2023.1324453.

27 Li, X., Loscalzo, J., Mahmud, A., Aly, D., Rzhetsky, A., Zitnik, M., & Benson, M. (2025). Digital twins as global learning health and disease models for preventive and personalized medicine. Genome Medicine, 17. https://doi.org/10.1186/s13073-025-01435-7.

28 Vallée, A. (2025). Digital Twins for Personalized Medicine Require Epidemiological Data and Mathematical Modeling: Viewpoint. Journal of medical Internet research, 27, e72411. https://doi.org/10.2196/72411.

29 Huang, L., Pan, L., Wu, C., Tian, M., Li, Q., Peng, Y., Li, Q., & Li, Y. (2024). Application and development prospect of digital twin in the forensic identification of cardiovascular diseases. Digital Medicine. https://doi.org/10.1097/dm-2024-00013.

30 Ren, Y., Pieper, A., & Cheng, F. (2025). Utilization of precision medicine digital twins for drug discovery in Alzheimer's disease. Neurotherapeutics, 22. https://doi.org/10.1016/j.neurot.2025.e00553.

31 Li, X., Loscalzo, J., Mahmud, A., Aly, D., Rzhetsky, A., Zitnik, M., & Benson, M. (2025). Digital twins as global learning health and disease models for preventive and personalized medicine. Genome Medicine, 17. https://doi.org/10.1186/s13073-025-01435-7.

32 Cellina, M., Ce', M., Alì, M., Irmici, G., Ibba, S., Caloro, E., Fazzini, D., Oliva, G., & Papa, S. (2023). Digital Twins: The New Frontier for Personalized Medicine? Applied Sciences. https://doi.org/10.3390/app13137940.

33 Huang, L., Pan, L., Wu, C., Tian, M., Li, Q., Peng, Y., Li, Q., & Li, Y. (2024). Application and development prospect of digital twin in the forensic identification of cardiovascular diseases. Digital Medicine. https://doi.org/10.1097/dm-2024-00013.

34 Guikema, S., & Flage, R. (2024). Digital twins as a security risk? *Risk Analysis*, 45, 269 - 273. https://doi.org/10.1111/risa.15749.

35 Sirigu, G., Carminati, B., & Ferrari, E. (2022). Privacy and Security Issues for Human Digital Twins. *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 1-9. https://doi.org/10.1109/tps-isa56441.2022.00011.

36 Yi, H. (2023). Improving cloud storage and privacy security for digital twin based medical records. *Journal of Cloud Computing*, 12, 1-16. https://doi.org/10.1186/s13677-023-00523-6.

37 Popa, E., Van Hilten, M., Oosterkamp, E., & Bogaardt, M. (2021). The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks. *Life Sciences, Society and Policy*, 17. https://doi.org/10.1186/s40504-021-00113-x.

38 Vallée, A. (2024). Envisioning the Future of Personalized Medicine: Role and Realities of Digital Twins. *Journal of Medical Internet Research*, 26. https://doi.org/10.2196/50204.

39 Marino, S., Cassidy, R., Nanni, J., Liu, Y., Tang, M., Chen, T., Pandian, B., Dinov, I., & Burns, M. (2025). Medical data sharing and synthetic clinical data generation – maximizing biomedical resource utilization and minimizing participant re-identification risks. *NPJ Digital Medicine*, 8. https://doi.org/10.1038/s41746-025-01935-1.

40 Alam, M., & Latifi, S. (2025). Early Detection of Alzheimer's Disease Using Generative Models: A Review of GANs and Diffusion Models in Medical Imaging. *Algorithms*. https://doi.org/10.3390/a18070434.

41 Müller-Franzes, G., Niehues, J., Khader, F., Arasteh, S., Haarburger, C., Kuhl, C., Wang, T., Han, T., Nebelung, S., Kather, J., & Truhn, D. (2022). A multimodal comparison of latent denoising diffusion probabilistic models and generative adversarial networks for medical image synthesis. *Scientific Reports*, 13. https://doi.org/10.1038/s41598-023-39278-0.

42 Eichelberg, M., Kleber, K., & Kämmerer, M. (2020). Cybersecurity Challenges for PACS and Medical Imaging. *Academic radiology*. https://doi.org/10.1016/j.acra.2020.03.026.

43 Ozbey, M., Dar, S., Bedel, H., Dalmaz, O., Ozturk, c., Gungor, A., & cCukur, T. (2022). Unsupervised Medical Image Translation With Adversarial Diffusion Models. *IEEE Transactions on Medical Imaging*, 42, 3524-3539. https://doi.org/10.1109/tmi.2023.3290149.

44 Sorin, V., Barash, Y., Konen, E., & Klang, E. (2020). Creating Artificial Images for Radiology Applications Using Generative Adversarial Networks (GANs) - A Systematic Review.. *Academic radiology*. https://doi.org/10.1016/j.acra.2019.12.024.

45 Raj, S., Mathew, J., & Mondal, A. (2024). Generalized and robust model for GAN-generated image detection. *Pattern Recognit. Lett.*, 182, 104-110. https://doi.org/10.1016/j.patrec.2024.04.018.

46 Cordero, D., & Barría, C. (2021). Cybersecurity Analysis in Nodes that Work on the DICOM Protocol, a Case Study. , 69-76. https://doi.org/10.1007/978-3-030-70416-2_9.

47 Kostenko O.V. Directions of development of law in the field of Internet of Things (IoT) and artificial intelligence. Actual problems of domestic jurisprudence. 2021. № 3. C. 130-136. DOI: https://doi.org/10.15421/392161