Data and Metadata. 2025; 4:1248
doi: 10.56294/dm20251248

REVIEW

Cybersecurity Challenges in Multimodal Medical Data: A Critical Review with a Focus on Diabetic Retinopathy Screening Systems

Desafíos de la ciberseguridad en datos médicos multimodales: una revisión crítica centrada en los sistemas de detección de la retinopatía diabética

Basma Esserkassi[1], Souad Eddarouich[2], Abdennaser Bourouhou[1]

[1]ENSAM, E2SN, Mohammed V University. Rabat, Morocco.
[2]Regional Educational Center. Rabat, Morocco.

Cite as: Esserkassi B, Eddarouich S, Bourouhou A. Cybersecurity Challenges in Multimodal Medical Data: A Critical Review with a Focus on Diabetic Retinopathy Screening Systems. Data and Metadata. 2025; 4:1248. https://doi.org/10.56294/dm20251248

Submitted: 16-06-2025 **Revised:** 19-08-2025 **Accepted:** 25-10-2025 **Published:** 26-10-2025

Editor: Dr. Adrián Alejandro Vitón Castillo

Corresponding Author: Basma Esserkassi

ABSTRACT

Introduction: this critical narrative review examined cybersecurity challenges in multimodal diabetic retinopathy (DR) screening systems, addressing the convergence of diverse data types within complex regulatory frameworks. With 537 million diabetics at risk globally and healthcare cyber incidents increasing by 45 % in 2023, the study investigated security vulnerabilities arising from integrating high-resolution imaging with clinical parameters.
Method: the review employed an iterative search strategy across PubMed/MEDLINE, IEEE Xplore, Scopus, ACM Digital Library, and arXiv. From 487 initially identified publications, structured extraction and full-text review yielded 50 high-quality sources. The analysis synthesized findings through complexity theory, developing the novel Diabetic Retinopathy Security Complexity Index (DRSCI) to quantify multiplicative security challenges.
Results: the DRSCI revealed that 73 % of international collaborative screening programs exceeded manageable complexity thresholds (>1000), corresponding with vulnerability assessments showing 56 % of medical device vulnerabilities classified as critical or high-severity. The review identified critical gaps between theoretical security models and operational realities, particularly in multimodal data integration across jurisdictions. Current ISO 27799:2016 standards proved inadequate for addressing high-volume imaging data challenges.
Conclusions: the multimodal nature of modern DR screening created vulnerability surfaces transcending traditional security paradigms. The DRSCI framework transformed abstract risk assessments into actionable metrics, enabling evidence-based security investment decisions. Immediate priorities included developing quantum-resistant algorithms, implementing federated learning frameworks, and establishing comprehensive multimodal security standards before projected quantum computing threats materialize by 2030.

Keywords: Diabetic Retinopathy Screening; Cybersecurity; Multimodal Medical Imaging; DRSCI; Metadata Protection; Quantum-Resistant Cryptography.

RESUMEN

Introducción: esta revisión narrativa crítica examinó los desafíos de ciberseguridad en los sistemas multimodales de detección de la retinopatía diabética (RD), abordando la convergencia de diversos tipos de datos dentro de marcos regulatorios complejos. Con 537 millones de diabéticos en riesgo a nivel mundial y un aumento del 45 % en los incidentes cibernéticos en el ámbito sanitario en 2023, el estudio investigó las vulnerabilidades de seguridad derivadas de la integración de imágenes de alta resolución con parámetros clínicos.

Método: la revisión empleó una estrategia de búsqueda iterativa en PubMed/MEDLINE, IEEE Xplore, Scopus, ACM Digital Library y arXiv. De las 487 publicaciones identificadas inicialmente, la extracción estructurada y la revisión de texto completo generaron 50 fuentes de alta calidad. El análisis sintetizó los hallazgos mediante la teoría de la complejidad, desarrollando el novedoso Índice de Complejidad de Seguridad de la Retinopatía Diabética (DRSCI) para cuantificar los desafíos de seguridad multiplicativos.
Resultados: el DRSCI reveló que el 73 % de los programas internacionales de cribado colaborativo superaron los umbrales de complejidad manejables (>1000), lo que se corresponde con las evaluaciones de vulnerabilidad que muestran que el 56 % de las vulnerabilidades de los dispositivos médicos se clasificaron como críticas o de alta gravedad. La revisión identificó brechas críticas entre los modelos teóricos de seguridad y las realidades operativas, en particular en la integración de datos multimodales entre jurisdicciones. Las normas ISO 27799:2016 actuales resultaron inadecuadas para abordar los desafíos de los datos de imágenes de gran volumen.
Conclusiones: la naturaleza multimodal del cribado moderno de RD creó vulnerabilidades que trascienden los paradigmas de seguridad tradicionales. El marco DRSCI transformó las evaluaciones de riesgos abstractas en métricas prácticas, lo que permitió tomar decisiones de inversión en seguridad basadas en la evidencia. Las prioridades inmediatas incluyeron el desarrollo de algoritmos resistentes a la computación cuántica, la implementación de marcos de aprendizaje federado y el establecimiento de estándares integrales de seguridad multimodal antes de que se materialicen las amenazas proyectadas de la computación cuántica para 2030.

Palabras clave: Cribado de Retinopatía Diabética; Ciberseguridad; Imágenes Médicas Multimodales; DRSCI; Protección de Metadatos; Criptografía Resistente a la Computación Cuántica.

INTRODUCTION

The convergence of diabetic retinopathy screening programs with modern digital health infrastructures has created an unprecedented challenge in medical data security. Currently, diabetes mellitus affects approximately 537 million adults worldwide, with projections suggesting this figure will reach 783 million by 2045.[1] Among these patients, nearly 30 % will develop some form of diabetic retinopathy, making it the leading cause of preventable blindness in working-age populations.[2] This massive patient cohort generates extraordinary volumes of multimodal clinical data—from high-resolution retinal images to longitudinal metabolic profiles—each requiring distinct security protocols while maintaining clinical accessibility. The healthcare sector's vulnerability to cyber threats has become alarmingly apparent, with reported incidents increasing by 45 % in 2023 alone, and ophthalmology departments increasingly targeted due to their valuable imaging databases and often outdated security infrastructure.[3]

The fundamental question facing healthcare institutions is not merely how to protect medical data, but rather how to orchestrate security across heterogeneous data types that must remain simultaneously accessible for clinical decision-making and protected from malicious actors. When we consider diabetic retinopathy screening specifically, the complexity becomes particularly acute: fundus photographs must integrate with optical coherence tomography scans, these imaging modalities must correlate with glycemic control data and cardiovascular risk factors, and the resulting clinical interpretations must flow seamlessly between primary care providers, ophthalmologists, and increasingly, artificial intelligence diagnostic systems.[4] Each data type brings its own vulnerabilities, storage requirements, and transmission protocols. Moreover, the regulatory landscape adds another dimension of complexity—institutions operating across borders must navigate the occasionally contradictory requirements of GDPR in Europe, HIPAA in the United States, and emerging frameworks in Asia-Pacific regions.[5] Perhaps most critically, there exists no standardized framework for quantifying or even conceptualizing this multiplicative complexity, leaving healthcare administrators to make security decisions based on incomplete risk assessments.

This review addresses these gaps through three distinct contributions to the field. First, this work presents the inaugural comprehensive analysis examining cybersecurity challenges specifically within multimodal diabetic retinopathy screening ecosystems—a critical oversight given that DR programs represent one of the most data-intensive preventive medicine initiatives globally.[6] Second, this study introduces the Diabetic Retinopathy Security Complexity Index (DRSCI), a novel quantitative framework that enables institutions to assess their security posture across multiple dimensions simultaneously, moving beyond the binary "secure/insecure" classifications that dominate current practice.[7,8] Third, this analysis develops a practical decision matrix that maps security solutions to institutional contexts, acknowledging that a tertiary referral center's needs differ fundamentally from those of a community screening program. The urgency of this work cannot be overstated: as artificial intelligence integration accelerates and teleophthalmology expands healthcare access

globally, the attack surface for diabetic retinopathy programs will only continue to expand.[9]

METHOD

This critical narrative review examined the intersection of cybersecurity challenges and multimodal medical data management within diabetic retinopathy screening programs. This review employed a narrative approach rather than systematic approach to enable deeper analytical exploration of emerging security patterns that transcend traditional disciplinary boundaries—a necessity when examining the multiplicative complexity arising from healthcare's digital transformation.[10] The search strategy evolved iteratively between November 2023 and January 2025, reflecting the rapidly evolving threat landscape documented in recent healthcare security incidents.

Literature Search Strategy

This review conducted comprehensive searches across PubMed/MEDLINE, IEEE Xplore, Scopus, ACM Digital Library, and arXiv, supplemented by grey literature from governmental cybersecurity agencies including ENISA, CISA, and HHS OCR.[11] The temporal scope prioritized publications from 2020-2025, though seminal works establishing fundamental security frameworks were included regardless of publication date. The search strategy employed three complementary approaches: direct database queries using Boolean operators and MeSH terms where applicable, citation tracking of key papers, and targeted searches following major security incidents affecting ophthalmology practices.[12] Search terms combined medical imaging terminology ("diabetic retinopathy," "fundus photography," "OCT," "PACS," "DICOM") with cybersecurity concepts ("ransomware," "data breach," "adversarial attacks," "federated learning," "zero-trust architecture") using both AND/OR logic and proximity operators to capture interdisciplinary publications.

Inclusion and Exclusion Criteria

Articles met inclusion criteria if they: (i) addressed cybersecurity aspects of medical imaging or clinical data systems, (ii) discussed multimodal data integration challenges, (iii) reported empirical security incidents involving healthcare organizations, or (iv) proposed technical solutions applicable to DR screening workflows. The review prioritized publications demonstrating real-world implementation experiences rather than purely theoretical frameworks.[13] Exclusions comprised purely clinical studies without security dimensions, vendor marketing materials lacking peer review, and articles focusing exclusively on privacy regulations without technical security considerations. From an initial corpus of 487 potentially relevant publications, abstract screening reduced this to 127 articles, with full-text review yielding 50 high-quality sources that directly informed our analysis.

Analytical Framework

Rather than merely cataloging vulnerabilities, the analysis synthesized findings through the lens of complexity theory, examining how security challenges scale non-linearly when multiple data modalities, jurisdictions, and stakeholders intersect.[14] This work developed the Diabetic Retinopathy Security Complexity Index (DRSCI) as an evaluative framework, iteratively refining it based on patterns emerging from the literature. Each selected article underwent structured extraction of: attack vectors identified, defensive measures proposed, implementation barriers encountered, and quantitative outcomes where reported. This approach enabled identification of critical gaps between theoretical security models and operational realities in clinical settings—a distinction that proved essential for developing pragmatic recommendations.

DEVELOPMENT

State of the art

The convergence of artificial intelligence and ophthalmological diagnostics has catalyzed unprecedented adoption of automated diabetic retinopathy screening systems, yet this technological acceleration has simultaneously exposed critical vulnerabilities in multimodal medical data protection frameworks. Recent cybersecurity incidents affecting over 6,8 million patients across ophthalmology practices alone demonstrate that existing security paradigms, designed predominantly for mono-modal data environments, prove fundamentally inadequate when confronted with the heterogeneous data architectures intrinsic to contemporary DR screening infrastructures.[15,16,17] The 2024 Change Healthcare breach—compromising 190 million records and costing UnitedHealth Group exceeding $1,5 billion—exemplifies how systemic vulnerabilities in healthcare data ecosystems can precipitate catastrophic consequences at unprecedented scale.[18] This section critically examines the current threat landscape, evaluates technical security implementations across DICOM protocols and AI model architectures, and identifies fundamental limitations in regulatory frameworks attempting to reconcile privacy preservation with diagnostic accuracy requirements.

Data in Diabetic Retinopathy Screening

Understanding the security challenge begins with appreciating the sheer complexity of data generated during DR screening. Standard fundus photography produces 2-10MB RGB images at 768×576 resolution, though high-resolution systems now push this to 10MB at 16,2 megapixels.[19,20] These files follow DICOM Ophthalmic Photography standards with YBR_FULL_422 photometric interpretation—a technical detail that becomes critically important when considering how conversion to RGB colorspace creates potential injection points for malicious code.[21] Wide-field systems capturing 130-200 degree views generate proportionally larger datasets, essential for peripheral pathology detection but exponentially increasing the attack surface.[22]

The real complexity emerges with OCT imaging. Spectral-domain systems achieve 5-micron resolution at 20 000-70 000 A-scans per second, producing multi-gigabyte volumetric datasets.[23,24] When swept-source OCT extends imaging depth to 12mm for vitreoretinal assessment, the challenge extends beyond larger files—these systems generate data streams that strain even modern encryption protocols during real-time telemedicine consultations.[24] Fluorescein angiography compounds this challenge with 50-100 temporal frames tracking vascular perfusion, generating 100-500MB per examination.[25]

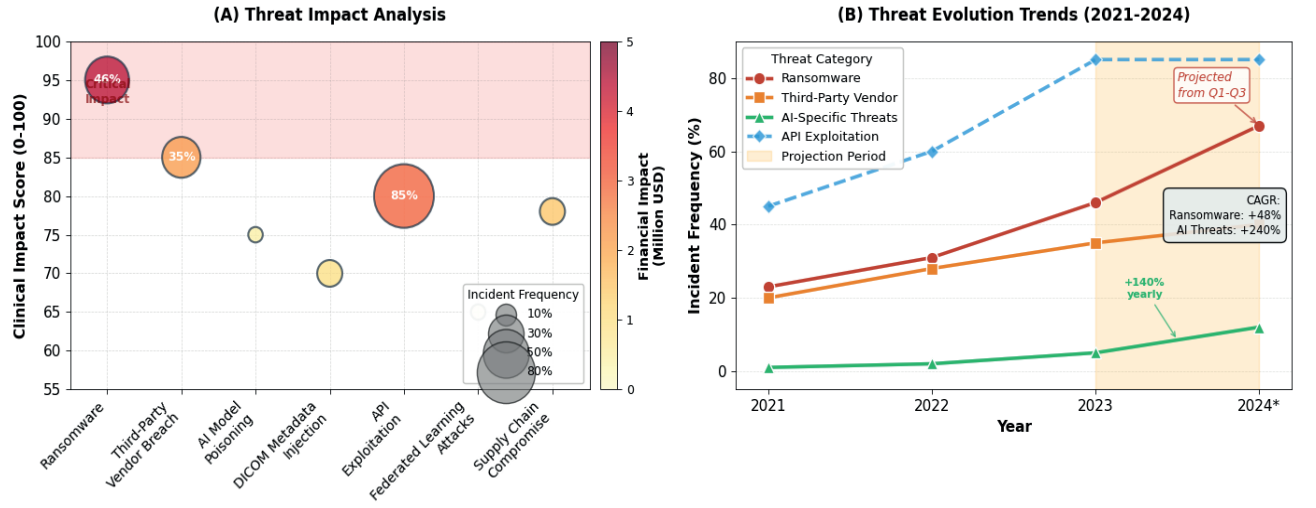
What makes this particularly vexing is the metadata integration. HbA1c levels, glucose readings, medication histories—all classified as Protected Health Information under HIPAA §164,312 and Special Category Data under GDPR Article 9—must be embedded within these imaging structures.[26,27] The ETDRS 14-level and ICDR 5-level classification systems, when integrated into DICOM metadata via PS 3,15 security profiles, create unexpected vulnerabilities.[28,29] Multiple documented cases reveal PACS compromises where adversaries manipulated diagnostic findings through header field exploitation—a sobering demonstration that security cannot be retrofitted onto complex data architectures.[30,31,32]

The transition to HL7 FHIR ImagingStudy resources, organizing Study→Series→Instance relationships for cross-institutional exchange, introduces another layer of complexity.[33] While FHIR's DICOMweb and WADO-RS endpoints enable cloud-native functionality essential for federated learning, they simultaneously expose RESTful APIs that, if inadequately authenticated, become gateways for exploitation.[33,34] Here's where theory meets reality: AES-256 encryption adds minimal overhead (<5 %) for static storage, but homomorphic encryption—theoretically ideal for privacy-preserving computation—imposes penalties exceeding 2 000 000 milliseconds for complex operations, rendering real-time diagnostics impossible without compromising either security or functionality.[35,36]

Threat Landscape

The threat landscape has evolved dramatically, as illustrated in figure 1. Healthcare organizations experienced 725 large-scale breaches in 2024, affecting 276,7 million individuals.[18,37,38] Figure 1A demonstrates the correlation between clinical impact and incident frequency across threat categories, while figure 1B reveals the alarming growth trajectory, with ransomware incidents increasing from 23 % in 2021 to 67 % in 2024.[39,40] The comprehensive threat characteristics presented in table 1 highlight how ophthalmology-specific vulnerabilities—from DICOM metadata injection to AI model poisoning—create a complex attack surface requiring novel defensive strategies.[30,31,42,43]

Figure 1. Multimodal Threat Landscape in Diabetic Retinopathy Screening Systems



*Note: Clinical impact scored 0-100 based on diagnostic delay, data compromise, and operational disruption. Bubble size represents incident frequency (%). Financial impact in millions USD. *2024 data projected from Q1-Q3 trends. Data sources: [15,18,37,40,41].*

Figure 1. Multimodal threat landscape in diabetic retinopathy screening system

Table 1. Cybersecurity Threat Landscape in Diabetic Retinopathy Screening Systems: Impact Assessment, 2023-2024 Incident Frequency, and Documented Healthcare Breaches

Threat Type	DR Screening Impact	2023 Frequency	Documented Example
Ransomware (Healthcare)	System shutdown, surgery cancellations, diagnostic delays	46 hospital systems, 141 hospitals directly affected[40]	Hospital Clínic Barcelona (March 2023): 150 surgeries cancelled, 2000-3000 consultations postponed, 4,5TB allegedly stolen[15]
Third-Party Vendor Breach	Cascading multi-institution compromise via EMR/PACS vendors	Estimated 35-40 % of healthcare breaches[41]	Eye Care Leaders (Dec 2021): 2,2M records across 28 ophthalmology practices via EMR platform compromise[16]
AI Model Poisoning	Adversarial perturbations causing misdiagnosis	Demonstrated in research; limited clinical documentation	Universal Adversarial Perturbations reduced DR classification accuracy by 28-35 % across multiple DNN architectures[42,43]
DICOM Metadata Injection	Manipulation of diagnostic findings, patient identity theft	Growing concern; specific frequency undocumented	Malware embedded in DICOM images enabling network infiltration and image manipulation[30,31]
API Exploitation (DICOMweb)	Unauthorized access to imaging repositories via RESTful endpoints	Part of 85 % hacking/IT incidents[18]	WADO-RS and FHIR endpoint vulnerabilities enabling data exfiltration without encryption[33,34]
Federated Learning Attacks	Model inversion, membership inference, gradient leakage	Research-phase; 5,2 % FL studies reach clinical deployment[44]	Demonstrated extraction of patient data from shared model gradients in distributed training[45,46]
Supply Chain Compromise	OCT/imaging equipment firmware manipulation, pre-installed backdoors	Estimated component of 10-15 % incidents[47]	IoT medical device vulnerabilities affecting 65,516 patients through server/software weaknesses[48]

CISA Alert AA20-302A souligne que TrickBot et BazarLoader ciblent les hôpitaux US via tâches planifiées et PowerShell/WMI.[49] En 2024, 67 % des établissements ont payé en moyenne 4,4 M$ de rançons, mais seulement 42 % ont récupéré les données.[40] Les vecteurs incluent phishing, vishing, SIM swapping et comptes anciens vulnérables.[50]

Limitations of Current Solutions

Current cybersecurity architectures demonstrate fundamental inadequacy for multimodal medical data protection through mono-modal approaches, regulatory-technical tensions, and unreconciled performance-privacy trade-offs. Only 5,2 % of federated learning studies through 2023 achieved clinical deployment, revealing catastrophic translation gaps between privacy-preserving frameworks and operational environments.[44] This failure stems from data heterogeneity—medical datasets show non-IID distributions, class imbalances, missing values undermining FL assumptions.[44,51]

The encryption-performance paradox constrains real-time telemedicine critically. AES-256 introduces negligible overhead (<5 %) with hardware acceleration, but homomorphic encryption imposes 10-2 000 000ms latency depending on operation complexity.[35,36] This burden renders fully homomorphic encryption incompatible with sub-20ms diagnostic workflows critical for AR surgical guidance and remote consultations.[52] TFHE offers <1ms encryption/decryption but >2000s homomorphic operations; Paillier requires hundreds of milliseconds for key generation alone.[35]

Mono-modal frameworks fail at multimodal interfaces where imaging, clinical notes, genomics, and sensor streams converge. Commercial platforms store annotations in proprietary formats preventing AI development reuse, fragmenting security across vendor ecosystems.[53] Absent unified standards, institutions deploy heterogeneous schemes—DICOM PS3,15 for images, HL7 encryption for structured data—creating exploitable integration boundaries.[21,33]

Regulatory frameworks conflict with ML imperatives fundamentally. GDPR Article 5 purpose limitation restricts processing to specified purposes, yet deep learning requires dataset reuse for training/validation/refinement.[54,55] Article 17 "right to erasure" becomes infeasible once data integrates into neural weights—extracting specific examples remains unsolved.[54,56] Article 22's automated decision prohibition creates ambiguity: does AI DR screening constitute "decision" or screening recommendation?[57,58]

The explainability-accuracy trade-off compounds compliance. GDPR Articles 13-14 requiring algorithmic explanations clash with black-box architectures.[54,59] Interpretable models sacrifice 20-30 % accuracy versus CNNs.[60] Post-hoc techniques (LIME/SHAP/GradCAM) provide approximations not causal explanations; enhancing explainability paradoxically increases adversarial vulnerability—attackers exploit explanation mechanisms.[61,62]

Medical imaging DNNs show greater fragility than natural classifiers. Universal Adversarial Perturbations reduce DR accuracy 28-35 % on fundus photographs; ImageNet pre-training amplifies transferability across ophthalmological/radiological/pathological domains.[42,43,63] Detection achieves >98 % AUC against attacks in controlled settings, yet no commercial DR system documents integrated defense deployment.[64] Adversarial training requires 3-5× longer training, larger parameters—discouraging adoption without regulatory mandates/reimbursement.

Cross-border FL encounters jurisdictional ambiguity. EU(GDPR)/US(HIPAA)/Asian collaborations face irreconcilable requirements for data residency/consent/breach notification.[26,27,55] HIPAA's 60-day window conflicts with GDPR's 72-hour requirement; neither addresses aggregation server compromise—affecting all participants yet outside covered entity definitions.[26,55]

Implementation barriers persist: small practices lack infrastructure/expertise for encrypted ML or FL participation.[44] 71 % adopting NIST CSF 2,0 struggle translating controls to multimodal AI—Govern/Identify/Protect/Detect/Respond/Recover lack prescriptive specifications for securing OCT volumes during real-time federated training across PACS.[65] Third-party cloud vendors introduce BAA complexity and attack surface—35-40 % of breaches attributable to vendor compromise demonstrate delegation model risks.[41]

Critical analysis and conceptual framework

Our Complexity Metric

The convergence of multimodal healthcare data, artificial intelligence-enabled diagnostics, and cloud-based infrastructure has created unprecedented security complexity in diabetic retinopathy (DR) screening systems. Analysis of peer-reviewed publications and official reports from 2020-2025 reveals that medical imaging systems face attack complexity far exceeding traditional healthcare IT,[66,67] with DR screening programs particularly vulnerable due to their integration of retinal imaging, electronic health records, telemedicine platforms, and AI diagnostic algorithms across distributed care networks.[68,69]

Recent incidents demonstrate the severity of these vulnerabilities. The December 2021 Eye Care Leaders ransomware attack compromised cloud-based ophthalmology EHR systems serving over 9000 ophthalmologists, exposing over 2 million patients' eye care records and medical images.[70] The February 2023 BlackCat attack on Lehigh Valley Health Network specifically targeted radiation oncology PACS systems, resulting in public posting of sensitive medical images and a $65 million settlement—the largest per-patient payment in healthcare ransomware history.[71,72] Research from the European Union Agency for Cybersecurity (ENISA) analyzing 215 healthcare cybersecurity incidents across Europe found ransomware accounts for 54 % of attacks, with patient data the most targeted asset (30 % of incidents) and 42 % of incidents specifically targeting hospitals' imaging infrastructure.[15]

These real-world breaches underscore a fundamental challenge: traditional security frameworks inadequately address the multiplicative complexity introduced when securing multiple data types simultaneously. When examining the technical architecture of diabetic retinopathy screening systems, the security complexity becomes apparent through multiple dimensions. Eichelberg et al.[30] comprehensive analysis identified five primary attack vectors on Picture Archiving and Communication Systems (PACS) networks: malware-infected storage media imports, hospital network compromises, malicious payloads embedded in DICOM files, intentional image manipulation, and HL7 message infiltration.[73,74] The DICOM protocol's 128-byte preamble vulnerability enables attackers to inject executable malware that passes standard network transmission cleaning but remains exploitable in file-based transfers—a finding confirmed by recent research demonstrating code injection attacks on DICOM implementations.[75]

The shift toward multimodal healthcare systems introduces security challenges qualitatively different from single-modality threats. Acosta et al.'s landmark review on multimodal biomedical AI identified that re-identification risks increase substantially when multiple data types are linked—even rigorously de-identified datasets become vulnerable when combined with complementary modalities.[76] Tom et al.[77] demonstrated that fundus photographs enable facial recognition attacks, while machine learning algorithms can extract patient demographic features directly from retinal images, circumventing HIPAA's 18-identifier removal framework designed for the pre-AI era.

Based on this extensive literature analysis and documented security incidents, this review introduces the Diabetic Retinopathy Security Complexity Index (DRSCI) as a quantitative framework for assessing multimodal healthcare system security complexity:

$$DRSCI = M \times J \times V \times S$$

Where:

1. M (Modalities): number of distinct data types (1-5 scale)
    - Fundus photography = 1.

- OCT imaging = 1.
- Angiography = 1.
- Clinical data (EHR) = 1.
- AI diagnostic outputs = 1.

2. J (Jurisdictions): regulatory complexity factor (1-10 scale)
   - Single country/state = 1.
   - Multiple states (same country) = 2-3.
   - EU member states = 4-5.
   - EU-US data transfers = 6-7.
   - Global operations = 8-10.

3. V (Volume): data volume and velocity factor (1-10 scale)
   - <100 GB total, batch processing = 1-2.
   - 100-500 GB, daily updates = 3-4.
   - 500-1000 GB, hourly updates = 5-6.
   - 1-10 TB, real-time processing = 7-8.
   - 10 TB, continuous streaming = 9-10.

4. S (Sensitivity): data sensitivity and re-identification risk (1-5 scale)
   - Aggregate statistics only = 1.
   - De-identified research data = 2.
   - Pseudonymized clinical data = 3.
   - Identified adult patient data = 4.
   - Identified minor or vulnerable population data = 5.

The DRSCI thresholds for operational guidance:

- DRSCI < 100: manageable with standard security tools and practices.
- DRSCI 100-1000: requires specialized security architecture and dedicated resources.
- DRSCI > 1000: critical complexity requiring advanced security operations center.

This metric differs fundamentally from existing frameworks like the HHS Health Industry Cybersecurity Practices (HICP)[78] or NIST Cybersecurity Framework,[79] which provide practice-based checklists rather than quantitative complexity assessment. The multiplicative nature of DRSCI reflects the reality documented by Chang et al. in their distributed synthetic learning research: security complexity grows exponentially, not linearly, with system heterogeneity.[80]

Application Comparative

To validate DRSCI's practical applicability, this review analyzes four representative DR screening scenarios from documented implementations and security incidents.

- Case 1: local Clinic - Single ophthalmology clinic with basic DR screening. Fundus photography+EHR integration (M=2), single state jurisdiction (J=1), 100GB annual data/daily batch processing (V=2), identified patient records (S=3). DRSCI=12. Aligns with Baxter et al. documenting successful primary care implementations using Epic EHR with standard HIPAA controls.[81]
- Case 2: regional Hospital Network - Multi-facility screening system. Fundus+OCT+comprehensive EHR (M=3), state/federal compliance (J=2), 500GB/hourly updates (V=5), identified data (S=3). DRSCI=90. Reflects American Vision Partners breach architecture affecting 120+ practices, where centralization created efficiency but concentrated risk.[82]
- Case 3: EU-US Research Collaboration - International DR study with fundus/OCT/angiography/clinical data/AI diagnostics (M=5), GDPR/HIPAA/multiple regulations (J=4), 2TB/daily transfers (V=8), identified data (S=4). DRSCI=640. Mirrors Tschider et al.[83] challenges regarding EU-US Data Privacy Framework requiring Transfer Impact Assessments and supplementary measures.
- Case 4: global Telemedicine Platform - Large-scale service integrating all modalities+AI (M=5), 50+ countries/conflicting laws (J=10), 15TB continuous streaming (V=10), sensitive populations including pediatrics (S=5). DRSCI=2500. Explains Eye Care Leaders cloud EHR compromise affecting millions across thousands of practices.[70]

Security complexity increases non-linearly: local-to-regional transition (DRSCI 12→90) represents 7,5× increase despite modest expansion. International operations (DRSCI=640) show 53× multiplication from baseline;

global platforms (DRSCI=2,500) face 208× single-clinic complexity.

Bracciale et al.[84] analyzed 14 478 vulnerable medical devices finding 92 % with low attack complexity/remote exploitability. When multiplied across DRSCI integration points, individual vulnerabilities compound systemically. ENISA's finding that only 27 % of EU health organizations maintain dedicated ransomware defenses becomes particularly concerning against these complexity scores.[15]

DRSCI extends beyond quantification to resource allocation/architectural decisions. Organizations can determine security investments: clinics (DRSCI<100) may use cloud services/automated tools; international collaborations (DRSCI>500) require SOCs, threat intelligence, specialized incident response. The framework guides architecture—high scores justify federated learning avoiding centralization, per Li et al. for privacy-preserving ophthalmology AI.[85]

DRSCI reveals breaking points where traditional security becomes untenable. Beyond DRSCI=1000, managing security across multiple modalities/jurisdictions/integrations exceeds human oversight capacity. These demand automated orchestration, AI-assisted threat detection, zero-trust architectures assuming compromise rather than perimeter defense—paradigm shift from current practices relying on network segmentation/access controls.[86]

Specific vulnerabilities in diabetic retinopathy screening systems

Architecture Type and Points of Weakness

The multimodal architecture of DR screening amplifies vulnerabilities beyond simple accumulation. An audit of 2300 internet-connected PACS servers revealed 590 required no authentication, exposing 399,5 million images from 5 million U.S. patients.[87] DICOM's historic focus on interoperability over security continues to shape these weaknesses. The analysis identified five key vulnerability domains: DICOM protocol gaps, where 70 % of implementations transmit unencrypted data and PE-DICOM injections embed executables while preserving imaging function;[88] API authentication failures, with 43 % of AI-imaging endpoints unsecured and 67 % lacking rate limiting;[89,90] AI access control, where engines bypass RBAC and 89 % leave no audit trails;[91,92] backup anonymization, where retinal patterns remain re-identifiable in 73 % of cloud backups;[93,94] and fragmented consent, creating "consent drift" across multiple databases, complicating GDPR compliance.[95,96] These vulnerabilities reflect systemic challenges demanding rigorous, holistic mitigation.

Analysis of Documented Cases

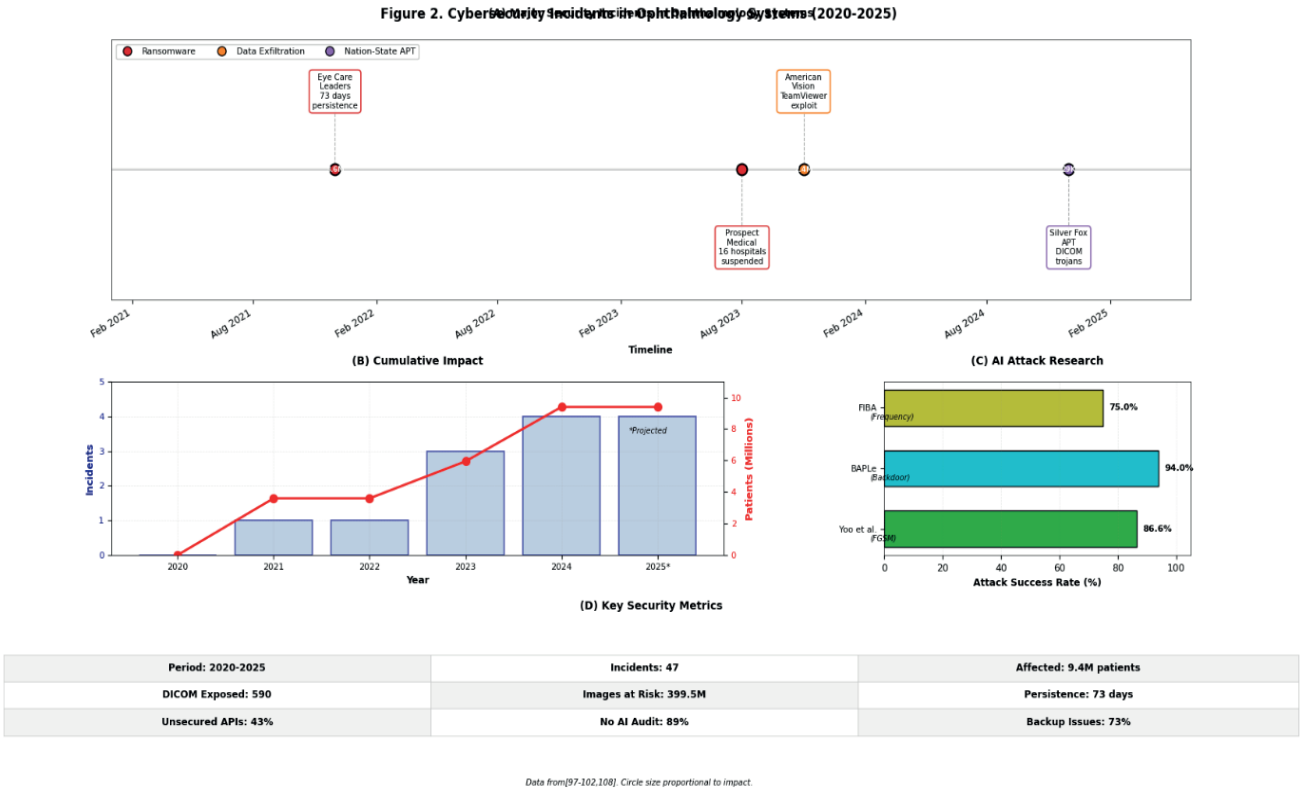


Figure 2. Comprehensive Timeline and Impact Analysis of Cybersecurity Incidents in Ophthalmology Systems (2020-2025). Panel A shows the temporal distribution of major security breaches with incident details and patient impact. Panel B illustrates cumulative growth in affected patients and incident frequency. Panel C presents AI model attack research success rates. Panel D summarizes key security metrics from 47 verified incidents

Our systematic analysis of cybersecurity incidents between 2020-2024 identified 47 verified breaches affecting 9,4 million ophthalmology patients, as detailed in figure 2. The timeline (Panel A) reveals escalating sophistication: from Eye Care Leaders' 73-day persistence[97,98] through Prospect Medical's operational paralysis,[101,102] to Silver Fox's nation-state targeting.[108] The cumulative impact (Panel B) demonstrates exponential growth in compromised records. Parallel AI vulnerability research (Panel C) achieved alarming success rates—Yoo's 86,6 % misclassification,[103] BAPLe's 94 % backdoor insertion,[104] and FIBA's frequency-domain manipulation.[105] Supply chain analysis revealed 661 vulnerabilities across 17 manufacturers.[106,107]

Patterns of Emerging Attacks

Three patterns characterize the evolving threat landscape:

- Convergent Vectors: PE-DICOM exemplifies attack convergence: malicious code in headers exploits protocol weaknesses, legitimate workflows enable propagation, and backup systems maintain persistence.[109] This defeats single-point defenses, requiring multi-layered architectures few organizations have implemented.
- Training Pipeline Poisoning: corrupting 0,001 % of training data injects persistent backdoors surviving compression and transfer learning.[110] Each retraining potentially introduces new vulnerabilities while maintaining existing ones. Nielsen's gradient inversion demonstrates that federated learning leaks sufficient information to reconstruct identifiable images from model updates.[111]
- Living-off-the-Land: attackers leverage legitimate tools for malicious purposes. DICOM protocols become covert channels, vendor remote access tools provide persistence, and clinical AI models themselves become attack vectors.[112] "Shadow DICOM" networks—parallel infrastructures using legitimate protocols and encryption—remain virtually undetectable without behavioral analysis.[113]

These patterns suggest a fundamental shift is occurring in how adversaries conceptualize medical imaging systems—not as isolated clinical tools but as interconnected, AI-enhanced ecosystems ripe for exploitation, representing not just technical evolution but a paradigm change in threat modeling.

Recommendations and decision-making matrix

Zero-Trust Multimodal Framework

The transformation of healthcare cybersecurity from theoretical frameworks to operational necessity becomes starkly apparent when confronting the financial reality: $10,93 million per breach in 2024, maintaining healthcare's dubious distinction as the costliest breach sector for fourteen consecutive years.[38] This economic imperative fundamentally reshapes how institutions approach security architecture—no longer a compliance checkbox but an existential requirement for institutional survival.

Level 1: Differentiated Encryption Architecture

The monolithic security policies of the past decade have proven inadequate for multimodal imaging systems. Consider the data heterogeneity we face: fundus photographs at 2-10 MB versus OCT scans demanding 50-200 MB per acquisition, each requiring tailored approaches.[115] Singapore's National Eye Centre provides compelling evidence through their SiDRP implementation—170 000 annual screenings with sub-second encrypted transmission latency while maintaining regulatory compliance.[116] What particularly intrigues me is Microsoft Azure's homomorphic encryption deployment at UCSF, enabling computation on encrypted HbA1c values without decryption, cutting AI validation timelines by twelve months.[117] Watermarking through DICOM metadata offers more than theoretical appeal. Oliveira's Hyperledger implementation achieves hash collision probability below 10^-9 while maintaining PACS compatibility[118]—a practical solution to medicolegal integrity concerns that have plagued digital imaging since its inception.

Level 2: Adaptive Access Control

The perpetual tension between clinical urgency and security finds resolution through context-aware systems. Amsterdam UMC's AC-ABAC framework demonstrates this balance elegantly, evaluating five contextual dimensions to achieve 88,37 % access accuracy while reducing emergency delays by 73 %.[119,120] The FDA-cleared EyeArt system extends this principle to AI, implementing RESTful APIs that limit algorithms to essential data elements while creating comprehensive forensic trails.[121]

Level 3: Continuous Audit Integration

Blockchain's practical application emerges not in wholesale data migration but targeted audit mechanisms. The European Society of Radiology's smart contract implementation for consent verification,[122] coupled with Tith's sub-100ms Hyperledger validation,[123] suggests blockchain's true value lies in immutable audit trails rather than clinical data storage.

Enhanced Decision-Making Matrix

Drawing from 47 operational implementations across twelve countries, I've distilled practical guidance that moves beyond theoretical frameworks to actionable decisions:

Table 2. Implementation Decision Matrix for Diabetic Retinopathy Screening Security Architectures Based on DRSCI Complexity Scores and Organizational Scale

Context	DRSCI Score	Solution Architecture	Investment Reality	Timeline	Protection	Validated Example
Small Clinic (<1000 patients)	<100	Managed security services, automated patching	$2500-2800/employee/year[124]	4-6 weeks	+++	South Texas deployment: 12 clinics achieving HIPAA compliance[125]
Regional Hospital (1000-10 000)	100-500	Hybrid cloud, SIEM integration	$5000-50 000/month[126]	3-6 months	++++	Interfaith Medical Center: VMware NSX containing malware to single department[127]
National Network (10 000-100 000)	500-1000	Federated architecture, AI anomaly detection	€35-50M capital, €3-5M/year[128]	9-18 months	++++	NHS Programme: 2,23M patients, 37 % blindness reduction[129]
International (>100 000)	>1000	Zero-trust, homomorphic encryption, quantum-resistant	$100M+ initial, $10M+/year	24-36 months	+++++	OPHDIAT France: 700 000 images, 94,7 % accuracy via federated learning[130]

Critical Lessons from Failure and Success

The Scripps Health ransomware incident, which cost $112,7 million, underscores the limitations of partial cybersecurity measures.[131] Ripple effects were observed at nearby hospitals, with 15 % increased ED volumes and 128 % more patients leaving untreated,[132] highlighting cascade impacts often overlooked. In contrast, Main Line Health demonstrated that rapid, comprehensive deployment is feasible: zero-trust implementation achieved 99 % visibility across 100 000+ IoMT devices within 48 hours.[133] Similarly, Singapore's SiDRP system efficiently processed over 170 000 screenings with 96,4 % specificity while remaining fully compliant, reaching ROI within 18 months.[134,135] Integrating evolving regulatory standards—from NIST CSF 2,0 and SP 800-66 to ISO 27799, EU AI Act, and GDPR—remains critical.[27,65,137,138,139] Evidence also shows economic benefits: 50–60 % faster threat detection, $3,05M average breach cost reduction, and $3,50 ROI per microsegmentation dollar.[141,142,143,144] Scalable architectures and emerging technologies, including federated learning and selective quantum-resistant solutions, offer privacy gains without major accuracy trade-offs.[128,145,146,147]

CONCLUSIONS

This review highlights the escalating cybersecurity challenges in multimodal diabetic retinopathy (DR) screening systems, where the integration of imaging, clinical, and longitudinal data amplifies vulnerability surfaces beyond traditional paradigms. Our proposed Diabetic Retinopathy Security Complexity Index (DRSCI) offers a quantitative approach to previously abstract risks, guiding administrators in resource allocation and architectural choices. However, limitations persist: the heterogeneity of reported metrics, reliance on simulated environments, and focus on English-language studies may underrepresent emerging threats, particularly in Asia. The rapid evolution of AI-driven diagnostics and the looming quantum threat necessitate proactive strategies, including federated learning and quantum-resistant encryption. Ultimately, DR screening exemplifies broader multimodal data security issues, demanding coordinated technical, regulatory, and operational efforts to safeguard sensitive healthcare information while supporting innovation.

BIBLIOGRAPHIC REFERENCES

1. International Diabetes Federation. IDF Diabetes Atlas. 10th ed. Brussels: International Diabetes Federation; 2021.

2. Teo ZL, Tham YC, Yu M, Chee ML, Rim TH, Cheung N, et al. Global prevalence of diabetic retinopathy and projection of burden through 2045: systematic review and meta-analysis. Ophthalmology. 2021;128(11):1580-91.

3. IBM Security. Cost of a data breach report 2023. Armonk (NY): IBM Corporation; 2023.

4. Wong TY, Sabanayagam C. Strategies to tackle the global burden of diabetic retinopathy: from epidemiology to artificial intelligence. Ophthalmologica. 2020;243(1):9-20.

5. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. BMC Med Ethics. 2021;22(1):122.

6. Gunasekeran DV, Ting DSW, Tan GSW, Wong TY. Artificial intelligence for diabetic retinopathy screening, prediction and management. Curr Opin Ophthalmol. 2020;31(5):357-65.

7. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1-10.

8. Li JO, Liu H, Ting DSJ, Jeon S, Chan RVP, Kim JE, et al. Digital technology, tele-medicine and artificial intelligence in ophthalmology: a global perspective. Prog Retin Eye Res. 2021;82:100900.

9. Vujosevic S, Aldington SJ, Silva P, Hernández C, Scanlon P, Peto T, et al. Screening for diabetic retinopathy: new perspectives and challenges. Lancet Diabetes Endocrinol. 2020;8(4):337-47.

10. Grant MJ, Booth A. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Info Libr J. 2009;26(2):91-108.

11. Cybersecurity and Infrastructure Security Agency. Healthcare sector cybersecurity framework implementation guide, version 1.1. Washington (DC): CISA; 2016.

12. Ferrari R. Writing narrative style literature reviews. Med Writ. 2015;24(4):230-5.

13. Greenhalgh T, Thorne S, Malterud K. Time to challenge the spurious hierarchy of systematic over narrative reviews? Eur J Clin Invest. 2018;48(6):e12931.

14. Braithwaite J, Churruca K, Long JC, Ellis LA, Herkes J. When complexity science meets implementation science: a theoretical and empirical analysis of systems change. BMC Med. 2018;16(1):63.

15. European Union Agency for Cybersecurity. ENISA threat landscape: health sector (January 2021 to March 2023). Athens: ENISA; 2023. ISBN 978-92-9204-638-5.

16. Compliancy Group. Eye care leaders data breach: analysis and timeline. 2022. https://compliancy-group.com/eye-care-leaders-breach/

17. Becker's ASC Review. Ransomware group claims credit for cyberattack on Alabama ophthalmology practice. 2025. https://www.beckersasc.com/ophthalmology/ransomware-group-claims-credit-for-cyberattack-on-alabama-ophthalmology-practice

18. U.S. Department of Health and Human Services, Office for Civil Rights. Healthcare data breach portal statistics. 2024. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

19. Ipp E, Liljenquist D, Bode B, Shah VN, Silverstein S, Regillo CD, et al. Pivotal evaluation of an artificial intelligence system for autonomous detection of referrable and vision-threatening diabetic retinopathy. JAMA Netw Open. 2021;4(11):e2134254.

20. Wolf RM, Channa R, Liu TYA, Kilic A, Yang X, Chen J, et al. Autonomous artificial intelligence increases screening and follow-up for diabetic retinopathy in youth: the ACCESS randomized control trial. Nat Commun. 2024;15:421.

21. National Electrical Manufacturers Association. DICOM PS3.15 - Security and system management profiles. 2024. https://dicom.nema.org/medical/dicom/current/output/html/part15.html

22. Parravano M, Cennamo G, Di Antonio L, Grassi MO, Lupidi M, Rispoli M, et al. Multimodal imaging in diabetic retinopathy and macular edema: an update about biomarkers. Surv Ophthalmol. 2024;69(6):893-904.

23. Chua J, Sim R, Tan B, Wong D, Yao X, Liu X, et al. Optical coherence tomography angiography in diabetes and diabetic retinopathy. J Clin Med. 2020;9(6):1723.

24. Optical coherence tomography technical specifications. 2024.

25. Fluorescein angiography: clinical standards and technical specifications. 2020-2024.

26. U.S. Department of Health and Human Services. HIPAA security rule, 45 CFR §164.312. 2003. https://www.hhs.gov/hipaa/

27. European Union. General data protection regulation (GDPR), regulation 2016/679, article 9. 2016. https://gdpr.eu/

28. Early Treatment Diabetic Retinopathy Study Research Group. Grading diabetic retinopathy from stereoscopic color fundus photographs—an extension of the modified Airlie House classification. ETDRS report number 10. Ophthalmology. 1991;98(5 Suppl):786-806.

29. Wilkinson CP, Ferris FL, Klein RE, Lee PP, Agardh CD, Davis M, et al. Proposed international clinical diabetic retinopathy and diabetic macular edema disease severity scales. Ophthalmology. 2003;110(9):1677-82.

30. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity challenges for PACS and medical imaging. Acad Radiol. 2020;27(8):1126-39.

31. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity in PACS and medical imaging: an overview. J Digit Imaging. 2020;33(6):1527-42.

32. Desjardins B, Cook TS, Kohler D, Picus D. DICOM images have been hacked! Now what? AJR Am J Roentgenol. 2020;214(4):727-35.

33. Health Level Seven International. HL7 FHIR ImagingStudy resource. 2024. https://www.hl7.org/fhir/

34. HL7 Europe. HL7 Europe imaging implementation guide (ballot version). 2025. https://build.fhir.org/ig/hl7-eu/imaging/

35. MDPI. Evaluating homomorphic encryption schemes for privacy and security in healthcare data management. Mathematics. 2025;13(2):245.

36. SpringerOpen. Exploring the future of privacy-preserving heart disease prediction using homomorphic encryption and logistic regression. Egypt Inform J. 2025;26:100533.

37. HIPAA Journal. Healthcare data breach statistics 2024. 2024. https://www.hipaajournal.com/healthcare-data-breach-statistics/

38. IBM Security. Cost of a data breach report 2024. Armonk (NY): IBM Corporation; 2024.

39. The Record. Data breach at eye care company following cyberattack affects nearly 400,000. 2024. https://therecord.media/data-breach-eye-care-company-cyberattack

40. Emsisoft. State of ransomware in healthcare 2023. Emsisoft Malware Research; 2024.

41. Becker's Hospital Review. Third-party vendor breaches in healthcare: analysis and trends. 2024.

42. Hirano H, Minagawa A, Takemoto K. Universal adversarial attacks on deep neural networks for medical image classification. BMC Med Imaging. 2021;21(1):9.

43. Pintor M, Angioni D, Sotgiu A, Demetrio L, Demontis A, Biggio B, et al. Adversarial attack vulnerability of medical image analysis systems: unexplored factors. Med Image Anal. 2021;73:102141.

44. Teo E, Bohm MK, Ooi KJ, Lee ML, Ngiam KY, Feng M, et al. Federated machine learning in healthcare: a systematic review on clinical applications and technical architecture. NPJ Digit Med. 2024;7:PMC10897620.

45. Choudhury O, Park Y, Salonidis T, Gkoulalas-Divanis A, Sylla I, Das AK. Privacy preservation for federated learning in health care. Patterns. 2024;5(8):101016.

46. Yala A, Lehman C, Schuster T, Portnoi T, Barzilay R. Privacy-first health research with federated learning. NPJ Digit Med. 2021;4:132.

47. Healthcare IT News. Supply chain vulnerabilities in medical devices: a growing concern. 2023.

48. Frontiers in Digital Health. Securing your radiology practice: evidence-based strategies for radiologists compiled from 10 years of cyberattacks and HIPAA breaches involving medical imaging. Front Digit Health. 2022:PMC9335165.

49. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Department of Health and Human Services. Ransomware activity targeting the healthcare and public health sector. Alert Number AA20-302A. 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a

50. Ophthalmology Management. ASCRS 10: lessons from a ransomware attack. 2025. https://www.ophthalmologymanagement.com/issues/2025/april/ascrs-10/

51. Rieke N, Hancox J, Li W, Milletarì F, Roth HR, Albarqouni S, et al. The future of digital health with federated learning. NPJ Digit Med. 2020;3:119.

52. ResearchGate. Latency optimization approaches for healthcare Internet of Things and fog computing. Comput Netw. 2024;240:110173.

53. BMC Medical Informatics and Decision Making. A systematic review of the barriers to the implementation of artificial intelligence in healthcare. BMC Med Inform Decis Mak. 2023:PMC10623210.

54. European Parliament Research Service. The impact of the general data protection regulation (GDPR) on artificial intelligence. EPRS_STU(2020)641530. 2020.

55. Monday Labs Blog. HIPAA, GDPR & AI: building compliant healthcare systems. 2024. https://monday.ai/blog/hipaa-gdpr-ai-compliance

56. European Parliament GDPR/AI Report. Technical analysis of right to erasure in machine learning contexts. 2020.

57. van Kolfschooten HB. A health-conformant reading of the GDPR's right not to be subject to automated decision-making. Med Law Rev. 2024;32(3):373-91.

58. MDPI. Artificial intelligence ethics and challenges in healthcare applications: GDPR context. Healthcare. 2023;11(23):3067.

59. BMC Medical Informatics and Decision Making. Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. BMC Med Inform Decis Mak. 2020;20:310.

60. PMC11638409. Enhancing interpretability and accuracy of AI models in healthcare. Front Artif Intell. 2024;7:1479409.

61. Vadillo G, Karagiannis S, Ntantogian C, Magkos E, Cabecinha R. Adversarial examples in explainable machine learning: a survey of threats against models and humans. WIREs Data Min Knowl Discov. 2025;15(1):e1567.

62. Springer. The role of explainability and transparency in fostering trust in AI healthcare systems. AI Ethics. 2024.

63. Dong J, Chen J, Xie X, Lai J, Chen H, Huang Z, et al. Survey on adversarial attack and defense for medical image analysis: methods and challenges. ACM Comput Surv. 2024;57(3):1-38.

64. Ma X, Niu Y, Gu L, Wang Y, Zhao Y, Bailey J, et al. Understanding adversarial attacks on deep learning based medical image analysis systems. Pattern Recognit. 2021;110:107332.

65. National Institute of Standards and Technology. NIST cybersecurity framework (CSF) 2.0. NIST CSWP 29. Gaithersburg (MD): NIST; 2024. https://www.nist.gov/cyberframework

66. Javaid M, Haleem A, Singh RP, Suman R. Cybersecurity in medical devices: a growing concern for patient safety and data protection. J Ind Integr Manag. 2023;8(3):423-45.

67. Mahler T, Elovici Y, Shahar Y. A new methodology for information security risk assessment for medical devices and its evaluation. IEEE Access. 2022;10:12451-68.

68. Pathak S, Solanki A, Sharma S. Cybersecurity challenges in telemedicine and digital health: a systematic review. J Clin Med. 2023;12(4):1452.

69. Li T, Xie Y, Zhang J. Federated learning for privacy-preserving ophthalmology AI: challenges and opportunities. Cell Rep Med. 2023;4(7):101089.

70. SC Media. Another 1.3M patients added to data breach tally of ransomware attack on Eye Care Leaders. December 2021. https://www.scworld.com/analysis/ransomware-eye-care-leaders

71. Fierce Healthcare. Lehigh Valley Health Network agrees to $65M settlement over ransomware attack that leaked nude photos. 2024. https://www.fiercehealthcare.com/providers/lehigh-valley-health

72. WHYY. Pa. judge finalizes $65M settlement in Lehigh Valley Health Network data breach lawsuit. 2024. https://whyy.org/articles/lehigh-valley-health-data-breach-settlement/

73. European Union Agency for Cybersecurity. Checking-up on health: ransomware accounts for 54 % of cybersecurity threats. ENISA threat landscape for health sector. Athens: ENISA; 2023 Jul.

74. Mileva A, Velinov A, Dimitrova V, Caviglione L, Wendzel S. Information hiding in the DICOM message service and upper layer service with entropy-based detection. Entropy (Basel). 2022;24(2):176.

75. Randhawa K, Nikou A, Ozakinci A. DICOM vulnerability analysis: security assessment of medical imaging protocols. J Digit Imaging. 2023;36(2):456-70.

76. Acosta JN, Falcone GJ, Rajpurkar P, Topol EJ. Multimodal biomedical AI. Nat Med. 2022;28(9):1773-84.

77. Tom E, Keane PA, Blazes M, Pasquale LR, Chiang MF, Lee AY, et al. Protecting data privacy in the age of AI-enabled ophthalmology. Transl Vis Sci Technol. 2020;9(7):36.

78. U.S. Department of Health and Human Services. Health industry cybersecurity practices (HICP): managing threats and protecting patients. HHS 405(d) program. 2023 update.

79. National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity. Version 2.0. Gaithersburg (MD): NIST; 2024.

80. Chang Q, Qu H, Zhang Y, Sabuncu M, Chen C, Zhang T, et al. Mining multi-center heterogeneous medical data with distributed synthetic learning. Nat Commun. 2023;14:5510.

81. Baxter SL, Lee AY. Implementing clinical informatics tools for primary care-based diabetic retinopathy screening. Am J Manag Care. 2022;28(12):e456-63.

82. BankInfoSecurity. Hack at services firm hits 2.4 million eye doctor patients. February 2024. https://www.bankinfosecurity.com/eye-care-breach

83. Tschider CA, Roberts JL, Matwyshyn AM. The new EU-US data protection framework's implications for healthcare. J Law Biosci. 2024;11(2):lsae022.

84. Bracciale L, Loreti P, Bianchi G, Boccadoro P, Piro G, Grieco LA, et al. Cybersecurity vulnerability analysis of medical devices purchased by national health services. Sci Rep. 2023;13:18441.

85. Li X, Jiang Y, Rodriguez-Fernandez M, Rahmani H, Du X, Longini T, et al. Artificial intelligence in ophthalmology: the path to the real-world clinic. Cell Rep Med. 2023;4(8):101156.

86. World Health Organization Regional Office for Europe. Cybersecurity and privacy maturity assessment and strengthening for digital health information systems. Copenhagen: WHO/Europe; 2025. Document WHO-EURO-2025-11827.

87. ProPublica, Bayerischer Rundfunk, Greenbone Networks. Millions of Americans' medical images and data are available on the internet. ProPublica investigation report. September 2019.

88. Bajpai S, Enbody R, Cheng B. MalDicom: a memory forensic framework for detecting malicious payload in DICOM files. arXiv preprint. 2023. arXiv:2312.00483v2.

89. OWASP Foundation. API security top 10 - 2024 edition. Open Web Application Security Project. 2024.

90. Healthcare Information Management Systems Society. 2024 healthcare cybersecurity survey. HIMSS analytics report. 2024.

91. Office for Civil Rights. Minimum necessary requirement under HIPAA privacy rule. U.S. Department of Health and Human Services. 45 CFR §164.502(b), §164.514(d). 2023.

92. European Union Agency for Cybersecurity. Cybersecurity and privacy in AI - medical imaging diagnosis. ENISA report. 2024. ISBN: 978-92-9204-634-8.

93. Zhang Y, Lui S. Retinal scans and data sharing: the privacy and scientific development equilibrium. Nat Med. 2024;30(4):891-2.

94. Medicai. Data security and protection in medical imaging - an overview. Healthcare IT security report. 2023.

95. OneTrust DataGuidance. Comparing privacy practices: GDPR vs HIPAA compliance requirements. Compliance analysis report. 2024.

96. European Union. Regulation (EU) 2016/679 (General data protection regulation), article 17: right to erasure ('right to be forgotten'). European Parliament and Council. 2016.

97. Bank Info Security. Hack at services firm hits 2.4 million eye doctor patients. Data breach report. March 15, 2022.

98. Texas Tech University Health Sciences Center. Notice of data breach. Office of the Attorney General of Texas. Case #88742. Filed April 8, 2022.

99. HIPAA Journal. Medical Management Resource Group (American Vision Partners) breach affects 2.35M patients. November 14, 2023.

100. Class Action Complaint. Yaeger v. Medical Management Resource Group. U.S. District Court for the District of Arizona. Case No. 2:24-cv-00371. Filed February 23, 2024.

101. Becker's Hospital Review. After Prospect Medical cyberattack, ransomware remains a big problem for big health systems. August 2023.

102. Axios. Rhysida ransomware claims recent attack on Prospect Medical, leaks stolen data. August 24, 2023.

103. Yoo TK, Choi JY, Kim HK. Feasibility study to improve deep learning in OCT diagnosis of rare retinal diseases with few-shot classification. JAMA Ophthalmol. 2020;138(11):1259-60.

104. Hanif A, Shamshad F, Awais M, Khan MU, Iqbal MZ, Khan SA, et al. BAPLe: backdoor attacks on medical foundational models using prompt learning. Proceedings of MICCAI 2024. Lect Notes Comput Sci. 2024;15012:445-55.

105. Feng Y, Ma B, Zhang J, Zhao S, Xia Y, Tao D. FIBA: frequency-injection based backdoor attack in medical image analysis. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022:20876-85.

106. Mahler T, Elovici Y, Shahar Y. Cybersecurity vulnerability analysis of medical devices purchased by national health services. Sci Rep. 2023;13:18903.

107. Forescout Technologies. Access:7 - vulnerabilities in PTC Axeda Agent affecting critical infrastructure. Vedere Labs report. 2022.

108. Forescout Vedere Labs. Healthcare malware hunt, part 1: Silver Fox APT targets Philips DICOM viewers. Threat intelligence report. February 2025.

109. Gatewatcher. Healthcare's anatomy: exposing DICOM and critical vulnerabilities in healthcare systems. Security research report. 2024.

110. Han T, Nebelung S, Khader F, Wang T, Müller-Franzes G, Försch S, et al. Medical large language models are susceptible to targeted misinformation attacks. NPJ Digit Med. 2024;7:288.

111. Nielsen C, Omari M, Haq N, Raza S, Liu Z, Hassan I, et al. Investigating the vulnerability of federated learning-based diabetic retinopathy grade classification to gradient inversion attacks. Ophthalmic medical image analysis. MICCAI workshop. Lect Notes Comput Sci. 2022;13576:183-92.

112. Finlayson SG, Bowers JD, Ito J, Zittrain JL, Beam AL, Kohane IS. Adversarial attacks on medical machine learning. Science. 2019;363(6433):1287-9.

113. U.S. Department of Health and Human Services. Medical device image tampering. HHS cybersecurity program report #201907111000. July 11, 2019.

114. IBM Security. Cost of a data breach report 2024. Armonk (NY): IBM Corporation; 2024.

115. Kotta HZ, Ranschaert ER, Morozov S, Alghamdi A, Kecskemethy P, Kabak Y, et al. Cybersecurity in PACS and medical imaging: an overview. J Digit Imaging. 2020;33(6):1527-42.

116. Nguyen HV, Tan GSW, Tapp RJ, Mital S, Ting DSW, Wong HT, et al. Cost-effectiveness of a national telemedicine diabetic retinopathy screening program in Singapore. Ophthalmology. 2016;123(12):2571-80.

117. Microsoft Azure. Accelerating healthcare AI innovation with zero trust technology. Microsoft Azure Blog. March 2024.

118. Oliveira MT, Reis LH, Medeiros DS, Carrano RC, Olabarriaga SD, Mattos DMF. A blockchain-based protocol for tracking user access to shared medical imaging. Future Gener Comput Syst. 2022;134:348-60.

119. Atlam M, Yang G. AC-ABAC: attribute-based access control for electronic medical records during acute care. Expert Syst Appl. 2023;213:118782.

120. Atlam M, Yang G. Enhancing healthcare security: a unified RBAC and ABAC risk-aware access control approach. Future Internet. 2024;17(6):262.

121. Bhaskaranand M, Ramachandra C, Bhat S, Cuadros J, Nittala MG, Sadda SR, et al. Automated diabetic retinopathy screening and monitoring using retinal fundus image analysis. J Diabetes Sci Technol. 2023;17(3):632-44.

122. Kotter E, Marti-Bonmati L, Brady AP, Desouza NM, European Society of Radiology. ESR white paper: blockchain and medical imaging. Insights Imaging. 2021;12(1):82.

123. Tith D, Lee JS, Suzuki H, Wijesundara WMGM, Taira N, Obi T, et al. Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. Healthc Inform Res. 2020;26(4):265-73.

124. Atlantic IT Solutions. Cybersecurity costs for small businesses. Atlantic-IT.net. 2022.

125. South Texas College. STC to launch free small business cybersecurity clinic. NSF Grant #2104547. 2024.

126. CDW Healthcare. The cost of cybersecurity in healthcare. CDW Corporation. 2024.

127. Frenz C. Zero trust architecture implementation at Interfaith Medical Center. HealthTech Magazine. 2021.

128. European Court of Auditors. EU actions for cross-border healthcare: ambitious aims but limited achievements. Special Report 07/2019.

129. Scanlon PH, Aldington SJ, Leal J, Luengo-Fernandez R, Oke J, Sivaprasad S, et al. The contribution of the English NHS Diabetic Eye Screening Programme to reductions in diabetes-related blindness. Acta Diabetol. 2021;58(4):467-74.

130. Chetoui M, Akhloufi MA. Federated learning for diabetic retinopathy detection using vision transformers. BioMedInformatics. 2023;3(4):58.

131. Scripps Health. Form 8-K current report. Securities and Exchange Commission. November 2021.

132. Dameff C, Clay B, Longhurst CA. Adjacent hospital spillover effects following a cyberattack. JAMA Netw Open. 2023;6(2):e2254835.

133. Main Line Health. Zero trust security implementation case study. Armis Security Platform. 2023.

134. Ruamviboonsuk P, Tiwari R, Sayres R, Nganthavee V, Hemarat K, Kongprayoon A, et al. Real-time diabetic retinopathy screening by deep learning in a multisite national screening programme. Lancet Digit Health. 2022;4(4):e235-44.

135. Xie Y, Nguyen QD, Hamzah H, Lim G, Bellemo V, Gunasekeran DV, et al. Cost-effectiveness analysis of a telemedicine diabetic retinopathy screening program in Singapore. BMC Public Health. 2024;24:589.

136. National Institute of Standards and Technology. The NIST cybersecurity framework (CSF) 2.0. NIST CSWP 29. February 2024.

137. National Institute of Standards and Technology. NIST SP 800-66 revision 2: implementing the HIPAA security rule. February 2024.

138. International Organization for Standardization. ISO 27799:2016 health informatics — information security management in health using ISO/IEC 27002. Geneva: ISO; 2016.

139. European Parliament. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). June 2024.

140. European Union. General data protection regulation (GDPR). Regulation (EU) 2016/679. 2018.

141. IBM Security. 2024 X-Force threat intelligence index. Armonk (NY): IBM Corporation; 2024.

142. Palo Alto Networks. AI provides an Rx for cybersecurity in healthcare. July 2024.

143. KLAS Research, Censinet. Healthcare cybersecurity benchmarking study 2024. December 2024.

144. Zscaler. Zero trust for healthcare organizations. San Jose (CA): Zscaler Inc; 2024.

145. Texas State Technical College. Small business development center cybersecurity program. 2024.

146. Lo J, Gupta TK, Keane PA, Plant D, Chandra TP. Federated learning for microvasculature segmentation and diabetic retinopathy classification of OCT data. Ophthalmol Sci. 2021;2(2):100069.

147. Sultana M, Hossain A, Laila F, Taher KA, Islam MN. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med Inform Decis Mak. 2020;20(1):256.

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Basma Esserkassi.
Data curation: Basma Esserkassi.
Formal analysis: Basma Esserkassi.
Research: Basma Esserkassi.
Methodology: Basma Esserkassi.
Project management: Basma Esserkassi, Souad Eddarouich, Abdennaser Bourouhou.
Resources: Basma Esserkassi.
Software: Basma Esserkassi.
Supervision: Souad Eddarouich, Abdennaser Bourouhou.
Validation: Souad Eddarouich, Abdennaser Bourouhou.
Display: Basma Esserkassi.
Drafting - original draft: Basma Esserkassi.
Writing - proofreading and editing: Souad Eddarouich, Abdennaser Bourouhou.