E-ISSN: 3050-9459
Journal of Ophthalmology and Advance Research

ATHENAEUM SCIENTIFIC PUBLISHERS

Review Article

Health Insurance Portability and Accountability Act Classification and Privacy Governance in Direct-Pay Refractive Surgery Organizations in the USA: A Narrative Legal and Policy Review and Proposed Framework

Stephen N Joffe[1*]

[1]University of Cincinnati Medical Center, Cincinnati, Ohio, USA

***Correspondence author:** Stephen N Joffe, MD, University of Cincinnati Medical Center, Cincinnati, Ohio, USA; Email: stephen@sjoffe.com

Citation: Joffe SN. Health Insurance Portability and Accountability Act Classification and Privacy Governance in Direct-Pay Refractive Surgery Organizations in the USA: A Narrative Legal and Policy Review and Proposed Framework. J Ophthalmol Adv Res. 2026;7(3):1-20.

https://doi.org/10.46889/JOAR.2026.7303

Received Date: 29-07-2026

Accepted Date: 06-09-2026

Published Date: 13-09-2026

Copyright: © 2026 The Authors. Published by Athenaeum Scientific Publishers.

This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

License URL:

https://creativecommons.org/licenses/by/4.0/

Abstract

Background: Direct-pay refractive surgery combines clinical care with consumer-facing marketing, financing, imaging, device connectivity and remote communications. Payment method alone does not determine whether the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies.

Objective: To clarify the legal classifications relevant to direct-pay refractive surgery and propose an ophthalmology-specific enterprise privacy-governance framework.

Methods: This narrative legal and policy review searched PubMed, Google Scholar, eCFR, Federal Register, GovInfo, HHS, FTC, NIST, federal and state judicial sources and selected state legislative repositories through 31 August 2026. Primary law and official guidance were prioritized. Sources were classified as binding law, regulation, precedent, agency guidance, proposed rule or voluntary framework. One author selected and synthesized the sources; there was no duplicate independent legal review. The proposed framework was derived by thematic synthesis and mapping of established controls to the refractive surgery data lifecycle.

Synthesis: Covered-provider status requires electronic transmission of health information in connection with an HHS-standard transaction. Business-associate status is distinct. Non-HIPAA data may remain subject to the FTC Act, the Health Breach Notification Rule, state consumer-health-data and biometric laws, contracts and tort law. Refractive surgery adds distinctive risks involving corneal maps, facial and periocular images, surgical video, laser and diagnostic-device clouds, AI screening, testimonials, remote follow-up and financing-linked marketing. A proposed framework integrates legal-role mapping, ophthalmic data inventories, proportionate baseline and maturity controls, incident response and measurable assurance.

Conclusion: The framework is conceptual and unvalidated. Prospective testing, patient and stakeholder input and jurisdiction-specific legal review are required before its effectiveness can be inferred.

Keywords: Health Insurance Portability and Accountability Act; Direct-Pay Healthcare; Refractive Surgery; Consumer Health Data; Privacy Governance; Cybersecurity; Artificial Intelligence

Abbreviations

AI: Artificial Intelligence; DRPGF: Direct-Pay Refractive Privacy Governance Framework; FTC: Federal Trade Commission; HBNR: Health Breach Notification Rule; HIPAA: Health Insurance Portability and Accountability Act of 1996; HHS: United States Department of Health and Human Services; MFA: Multifactor authentication; MSO: Management-Services Organization; NIST: National Institute of Standards and Technology; PHI: Protected Health Information

Introduction

Direct-pay refractive surgery sits at the boundary between clinical medicine and consumer commerce. Patients commonly self-refer, compare prices, schedule through digital channels, use financing and pay most or all procedure charges without a health plan claim. These commercial features can foster the mistaken conclusion that a cash-only or insurance-independent practice is outside the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA, however, classifies regulated actors by defined functions and transactions rather than by the dominant source of revenue [1-4].

The analysis also cannot stop with HIPAA. The Health Information Technology for Economic and Clinical Health Act and the 2013 Omnibus Rule extended direct obligations to business associates [5,6]. The Federal Trade Commission (FTC), state legislatures, contracts, professional duties and tort law can reach patient-linked information that is not Protected Health Information (PHI) under HIPAA. This layered environment is especially important in refractive surgery because clinical data are routinely connected to lead generation, financing, cloud-connected diagnostic devices, surgical planning, photography, remote follow-up and Artificial Intelligence (AI).

Ophthalmic data are not homogeneous. Corneal topography and tomography, wavefront and biomechanical measurements, full-face or periocular photographs, iris information, surgical video and longitudinal image sets can be clinically indispensable while also supporting identification, inference or secondary analytics. AI applications already span corneal and refractive decision support and ophthalmic literature has emphasized the privacy implications of image-rich datasets and the need for privacy-preserving approaches [7-9]. A governance model designed only around the electronic medical record therefore misses material parts of the refractive surgery data lifecycle.

This review has four aims: to define the direct-pay refractive surgery organization; state the HIPAA threshold and organizational roles precisely; distinguish legal authority from guidance and voluntary practice; and propose a practical, explicitly unvalidated governance framework tailored to multi-site ophthalmic operations. The analysis concerns United States law current through 31 August 2026. It is educational and does not provide legal advice for a specific organization.

Methodology

Design and Research Questions

This was a narrative doctrinal legal and policy review, not a systematic review or an empirical evaluation. The research questions were: (1) when can a direct-pay refractive surgery provider be a HIPAA covered entity; (2) how do business-associate, hybrid-entity and affiliated-covered-entity concepts apply to common ophthalmic structures; (3) which non-HIPAA federal and representative state rules materially affect the same data; and (4) how can established privacy and security controls be adapted to the refractive surgery data lifecycle.

Sources and Search Strategy

Searches were conducted and updated between 25 July and 31 August 2026. Biomedical literature was searched in PubMed and Google Scholar using combinations of: (HIPAA OR health privacy OR consumer health data OR cybersecurity OR biometric OR artificial intelligence) AND (ophthalmology OR refractive surgery OR LASIK OR corneal topography OR corneal tomography OR ophthalmic imaging OR remote monitoring). Legal research used eCFR, Federal Register, GovInfo, HHS Office for Civil Rights, FTC, NIST, federal and state judicial repositories and the legislative or code repositories of Washington, Nevada, Connecticut, Colorado, Illinois and Texas. Search phrases included covered entity, standard transaction, business associate, hybrid entity, affiliated covered entity, self-pay restriction, online tracking technology, health breach notification, consumer health data, biometric identifier, HIPAA Security Rule, multifactor authentication, encryption, claims attachments and private right of action. Citations within controlling authorities and official guidance were reviewed to identify additional primary sources.

Selection Criteria

Federal or state statutes, final regulations, judicial opinions, official agency guidance, proposed rules and voluntary standards were included when they directly informed classification, privacy rights, security, breach response, tracking, consumer health data, biometrics, AI or enforcement in a US refractive surgery context. Peer-reviewed English-language publications were included when they described clinically relevant ophthalmic data or technology. Foreign law, superseded materials, duplicate sources, vendor marketing claims and secondary commentary were excluded when a primary or official source was available. State laws were selected as representative examples, not as a 50-state survey. Source selection was iterative and relevance-based; a PRISMA flow was not used because the principal method was doctrinal analysis of heterogeneous legal authorities.

Authority Classification and Review Process

Each proposition was checked against the highest available authority and labeled conceptually according to Table 1. Binding statutes and final regulations were not treated as equivalent to case law, agency guidance, proposed rules or voluntary NIST frameworks. Judicial decisions were limited to their holdings and jurisdictional context. One author performed source selection, interpretation and synthesis. No second author independently reviewed the legal sources and there was no formal disagreement-resolution process. Ambiguities were handled by returning to the controlling text, comparing official guidance, narrowing the stated proposition and identifying uncertainty. The manuscript has not been independently reviewed by a qualified US healthcare attorney or privacy professional.

Source type	Legal weight	How used in this review	Example
Statute	Binding within its jurisdiction, subject to interpretation and preemption.	Controls the legal rule; quoted or paraphrased narrowly.	HIPAA; FTC Act; state statutes
Final regulation	Binding on regulated persons within delegated authority after effective/compliance dates.	Distinguished from proposals and guidance.	45 CFR Parts 160, 162, 164; 16 CFR Part 318
Judicial precedent	Binding or persuasive according to court, jurisdiction, posture and later history.	Limited to the court's holding and material facts.	AHA v Becerra; Acara; Byrne
Agency guidance	Official interpretation or enforcement position; not independently equivalent to statute or regulation.	Used for interpretation and operational examples; controlling text prevails.	HHS tracking and cloud guidance
Proposed regulation	No present binding effect unless and until finalized.	Described only as proposed regulatory direction.	2025 HIPAA Security Rule NPRM
Voluntary framework	Nonbinding unless adopted by contract, policy or another authority.	Used to organize controls, not to state legal mandates.	NIST CSF 2.0; NIST AI RMF
Author-derived framework	Conceptual; no independent legal or empirical authority.	Presented as a proposal requiring validation.	DRPGF

Abbreviations: AI, artificial intelligence; DRPGF, Direct-Pay Refractive Privacy Governance Framework; FTC, Federal Trade

Source type	Legal weight	How used in this review	Example
Commission; HBNR, Health Breach Notification Rule; HIPAA, Health Insurance Portability and Accountability Act; MFA, multifactor authentication; PHI, protected health information.			

Table 1: Hierarchy and treatment of authorities in this review.

Framework Derivation

The proposed Direct-Pay Refractive Privacy Governance Framework (DRPGF) is author-derived. Control concepts were extracted from HIPAA requirements and guidance, NIST Special Publication 800-66 Revision 2, the NIST Cybersecurity Framework 2.0 and the NIST AI Risk Management Framework; grouped by thematic synthesis; and mapped to the refractive patient and data journey from lead acquisition through screening, imaging, surgery, postoperative monitoring, testimonials, retention and deletion. Practical multi-site operational experience informed workflow examples. No Delphi process, expert consensus panel, patient consultation, formal scoring method, prospective testing or external validation was performed. The framework is therefore a conceptual proposal whose feasibility and effectiveness remain to be tested.

Operational Definition and Scope

For this review, a direct-pay refractive surgery organization is any US person or group that furnishes or supports elective corneal or lens-based refractive procedures for which the patient pays most or all of the procedure charge outside a health-plan claim. The term can include a solo practice, group practice, corporate LASIK chain, ambulatory surgery center, Management-Services Organization (MSO), professional corporation or limited-liability entity, parent company, call center or mixed insurance/direct-pay practice. Inclusion in this operational definition does not itself establish a HIPAA role. Classification must be performed separately for each legal entity and, where permitted, each designated component.

The review focuses on organizations that combine one or more clinical sites with shared marketing, scheduling, financing, analytics, technology, imaging or vendor management. It does not assume that all entities under one brand have the same legal status. Nor does it attempt a comprehensive analysis of state medical-record, telehealth, professional- licensure, advertising or corporate-practice-of-medicine law. Table 1 provides the authority hierarchy used throughout; Table 2 compares the principal federal and representative state privacy regimes.

Regime	Regulated entity / scope	Protected data	Consent and deletion	Breach / notice	Enforcement and private action
HIPAA Privacy, Security and Breach Rules	Covered entities and business associates in their regulated roles.	PHI; Security Rule applies to electronic PHI.	Authorizations and individual rights are rule-specific; no general deletion right. Self-pay restriction applies when 45 CFR 164.522 conditions are met.	Notice to individuals, HHS and sometimes media for breaches of unsecured PHI; business associate notifies covered entity.	HHS OCR; state attorneys general in defined circumstances; no general private HIPAA cause of action.
FTC Act, section 5	Persons within FTC jurisdiction; unfair or deceptive acts or practices.	Consumer information implicated by representations, sensitivity, security and context.	No omnibus consent/deletion code; duties arise from deception/unfairness analysis and specific orders.	No general section 5 breach-notice rule, but a failure or misrepresentation may be actionable.	FTC; no private action under the FTC Act itself.

Regime	Regulated entity / scope	Protected data	Consent and deletion	Breach / notice	Enforcement and private action
FTC HBNR	Vendors of PHRs, PHR-related entities and defined service providers; applies outside HIPAA breach-rule coverage for the information at issue.	Unsecured PHR-identifiable health information in a covered personal health record.	Not a general consent/deletion statute; unauthorized acquisition includes unauthorized disclosure under the 2024 amendments.	Individual and FTC notice; media notice for specified large state/jurisdiction breaches; timing and content in 16 CFR Part 318.	FTC; violations treated as violations of an FTC trade regulation rule.
Washington My Health My Data Act	Regulated entities and small businesses conducting business or targeting consumers in Washington, subject to exemptions.	Broad consumer health data, including inferred and location-related data; PHI and other specified data exemptions.	Dedicated notice; separate consent for collection/sharing subject to necessity exception; signed authorization for sale; access, withdrawal and deletion rights.	No standalone incident-notice scheme replacing generally applicable breach law.	Violation is an unfair/deceptive act under Washington Consumer Protection Act; public and qualifying private enforcement may be available.
Nevada consumer health data law	Regulated entities doing business or targeting products/services in Nevada; includes certain data collected in Nevada; exemptions apply.	Broad consumer health data, including derived/inferred, biometric, genetic and precise-geolocation information used to identify health status.	Notice; affirmative consent for collection/sharing subject to exceptions; written sale authorization; access and deletion rights.	Security and processor duties; separate Nevada breach law may apply.	Nevada Attorney General; chapter states no private right of action.
Connecticut consumer health provisions	Controllers subject to Connecticut Data Privacy Act, with thresholds and exemptions.	Consumer health data used to identify physical or mental health condition or diagnosis; statutory definitions control.	Consent for specified processing/sale; access and deletion rights; targeted geofencing restrictions.	Security and processor duties; separate breach statute may apply.	Connecticut Attorney General has exclusive enforcement authority under the Act.
Colorado Privacy Act (representative comprehensive law)	Controllers meeting statutory business/consumer thresholds, subject to exemptions.	Personal data; health condition/diagnosis and biometric data may be sensitive data.	Consent for sensitive-data processing; access, correction, deletion, portability and opt-out rights; data-	Reasonable security duty; separate Colorado breach statute may apply.	Attorney General and district attorneys; no general private right under the

Regime	Regulated entity / scope	Protected data	Consent and deletion	Breach / notice	Enforcement and private action
			protection assessments for heightened risk.		Act.
Abbreviations: AI, artificial intelligence; DRPGF, Direct-Pay Refractive Privacy Governance Framework; FTC, Federal Trade Commission; HBNR, Health Breach Notification Rule; HIPAA, Health Insurance Portability and Accountability Act; MFA, multifactor authentication; PHI, protected health information					

Table 2: Comparison of principal federal and representative state privacy regimes.

HIPAA Applicability and Organizational Roles

Covered-provider threshold: A health care provider is a HIPAA covered entity when the provider transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard [2,3]. The threshold is not satisfied merely because the provider uses an electronic record, emails a patient, stores images in the cloud or otherwise transmits health information electronically. Conversely, direct payment is not an exemption. A standard eligibility inquiry, claim, remittance, referral certification or another covered transaction conducted electronically by the provider or by a billing service on its behalf may satisfy the test [2-4]. The inquiry must examine actual transactions, including uncommon workflows after complications, limited insurance benefits, acquisitions or mixed-service lines (Fig. 1).

Covered entity and business associate are distinct roles: A covered provider qualifies because it meets the provider-and-standard-transaction definition. A business associate, by contrast, creates, receives, maintains or transmits PHI on behalf of a covered entity while performing specified functions or services [2,11,12]. An MSO, cloud host, call center, analytics company or centralized technology entity may be a business associate for particular services without becoming a covered entity merely by performing those services. Business associates have direct statutory and regulatory duties, but their role, permitted uses, downstream subcontractors and reporting obligations differ from those of covered entities [5,6,11,12]. A business-associate agreement documents a relationship; it does not convert an otherwise impermissible data use into a lawful one.

Hybrid and affiliated structures: A single legal entity that performs covered and noncovered functions may elect to be a hybrid entity and formally designate its health care components [10]. Legally separate covered entities under common ownership or control may designate an affiliated covered entity if regulatory conditions are met [10]. These are not interchangeable concepts and should not be applied across an enterprise by informal branding.

Consider a simplified structure: ParentCo owns an MSO, two professional practices and an ambulatory surgery center. Practice A electronically submits claims for medically necessary eye care and is a covered provider. Practice B performs only self-pay LASIK and conducts no standard transaction; on those facts it is not a covered provider. The surgery center submits electronic claims and is a covered entity. The MSO is not thereby a covered entity, but it may be a business associate when it hosts records, schedules patients or analyzes PHI for the covered practices. If one legal entity itself operates both covered and noncovered functions, a documented hybrid designation may be available; if the covered professional entities and center are separate but under common control, they may evaluate affiliated-covered-entity status. Corporate and state professional- practice rules may change the permissible structure, so the example is explanatory only.

Self-payment restriction: A covered provider must agree to an individual's requested restriction on disclosure to a health plan when four conditions are met: the disclosure would be for payment or health care operations and is not otherwise required by law; the restriction concerns disclosure to a health plan; the PHI pertains solely to a health care item or service for which the provider has been paid in full; and payment in full was made by the individual or another person other than the health plan [13]. The right applies to the particular paid item or service. It does not create a general HIPAA exemption, bar uses within the provider otherwise permitted by law or prevent a disclosure required by law. Registration, records-release and billing systems need a reliable flag and downstream controls to honor the restriction.

Claims attachments: HHS's 2026 final rule adopted standards for health care claims attachments and electronic signatures used with those claims attachments [14]. The official citation begins at 91 FR 14350; the rule became effective 26 May 2026 and has a 26 May 2028 compliance date. It did not finalize the proposed prior-authorization attachment standards. For a direct-pay enterprise, the rule is relevant only where a covered entity conducts the affected claims-attachment transactions; it should not be described as converting ordinary clinical uploads or prior-authorization attachments into new standardized transactions.

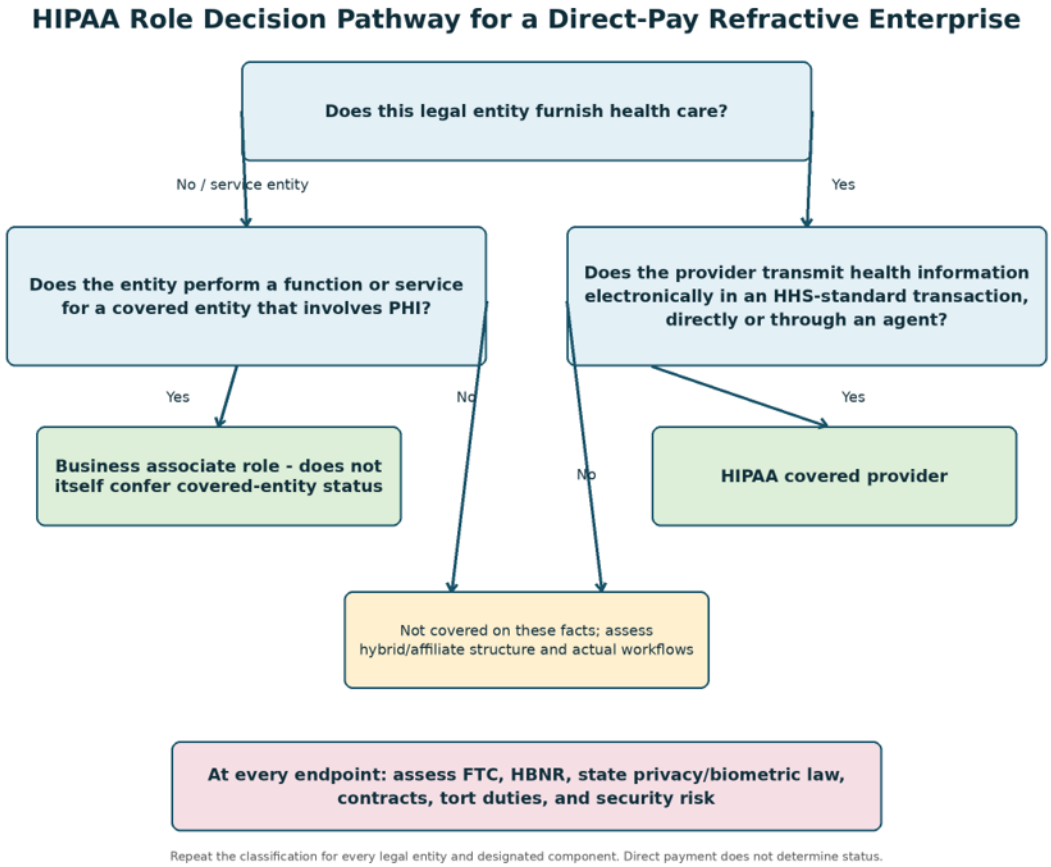

Figure 1: Role-specific HIPAA decision pathway for a direct-pay refractive surgery enterprise. Covered-provider status depends on the electronic standard-transaction test. Business-associate status is a distinct role and does not itself make an entity a covered entity. Hybrid- and affiliated-covered-entity analysis follows the legal structure. Non-HIPAA duties may apply at every endpoint.

The Refractive Surgery Data Lifecycle

The ophthalmology-specific contribution of the framework begins with a data inventory that follows the patient rather than a single system. Before a clinical relationship is established, an advertisement, symptom quiz, candidacy tool, location lookup, call recording, financing application or appointment request may link identity to procedure interest. Once evaluation begins, refraction, pachymetry, keratometry, corneal topography and tomography, epithelial thickness, aberrometry, pupillometry, dry-eye measures and ocular-surface images can be collected. The resulting dataset may be copied into an electronic record, image archive, diagnostic-device workstation, surgeon planning tool, vendor cloud or research and AI environment.

Corneal maps and high-dimensional ophthalmic images warrant more than generic chart controls. Serial maps may reveal disease, surgical candidacy and treatment history; embedded metadata may reveal device identifiers, site, operator or acquisition time. Full-face and periocular photographs can expose identity and facial geometry. Iris, voice or face templates used for authentication may also be regulated biometric data. The enterprise should document the raw image, derived measurements, template or embedding, metadata, purpose, legal status, access, retention, export paths and whether the vendor can reuse the information.

Surgical video and laser-platform data create additional pathways. Video used for quality assurance, teaching, credentialing,

litigation defense or marketing may capture the patient's face, voice, room audio, staff, device screens and identifiers. Diagnostic and laser systems may synchronize cases, nomograms, treatment files, maintenance logs or outcomes with manufacturer or third-party clouds. Procurement must distinguish remote support from independent analytics or product development and should define permitted use, locations of processing, subcontractors, security, incident notice, return or deletion and training-data rights.

Testimonials and before-and-after images sit at the clinical-marketing boundary. A general clinical consent, privacy notice or consent to treatment is not a substitute for an authorization that satisfies applicable disclosure and marketing rules. The request should be voluntary, separated from care and financing, specific as to media and duration and capable of withdrawal prospectively where required. Reposting by affiliates, influencers, advertising platforms or agencies must be included in the data-flow review.

Remote postoperative monitoring can include symptom questionnaires, uncorrected visual acuity, photographs, video, messages, medication use, device readings, location and escalation notes. These data need identity verification, secure routing, clinically defined response times, emergency instructions and retention in the authoritative record. Table 3 converts these ophthalmic data types into a minimum control map.

Data / workflow	Distinctive risk	Minimum controls
Corneal topography, tomography, pachymetry, epithelial maps, aberrometry	High-dimensional clinical data; metadata and longitudinal linkage; copying across device, EMR, vendor cloud and AI systems.	Named owner; data-flow map; role-based access; export controls; retention; vendor-use limits; validation of interfaces and AI use.
Facial and periocular photography	Direct identification, face geometry, incidental surroundings, reuse for education or marketing.	Separate clinical and marketing purposes; authorization where required; metadata review; restricted galleries; retention/deletion; biometric-law analysis.
Iris, retina, voice or face templates	Biometric identification may persist despite removal of names; state definitions and healthcare exclusions differ.	Document whether raw data or template is stored; consent/notice; security; vendor/subprocessor terms; no secondary use without review.
Surgical video and room audio	Captures patient, staff, screens, procedure details, voice and unplanned identifiers.	Purpose-specific recording policy; visible notice/authorization as applicable; access log; editing/redaction; disclosure and retention controls.
Laser and diagnostic-device cloud	Remote support, treatment files, nomograms, telemetry, cross-site aggregation, foreign processing and legacy security.	Connectivity inventory; least privilege; MFA where supported; segmentation; business-associate/data-processing terms; subprocessor and deletion schedule; downtime plan.
AI candidacy or outcome prediction	Dataset shift, bias, opaque recommendations, training reuse, device/site variation and automation bias.	Intended-use statement; local validation; human override; change control; outcome monitoring; training exclusion or authorization; incident escalation.
Remote postoperative monitoring	Identity, image/message routing, delayed escalation, emergency symptoms, personal-device and	Approved platform; identity verification; response-time standard; emergency instructions; record integration; retention and access controls.

Data / workflow	Distinctive risk	Minimum controls
	messaging exposure.	
Financing, leads, testimonials, before-and-after images	Procedure interest linked to identity, credit attributes, tracking, audience creation and public redistribution.	Data minimization; separate financing/clinical disclosures; event-level tag review; purpose-specific testimonial authorization; state-law rights workflow.
Abbreviations: AI, artificial intelligence; DRPGF, Direct-Pay Refractive Privacy Governance Framework; FTC, Federal Trade Commission; HBNR, Health Breach Notification Rule; HIPAA, Health Insurance Portability and Accountability Act; MFA, multifactor authentication; PHI, protected health information		

Table 3: Ophthalmology-specific data and minimum governance controls.

Digital Tracking, FTC Duties and State Consumer Health Data

Tracking technologies. HHS's current guidance distinguishes authenticated pages from unauthenticated public pages and explains that disclosures depend on the regulated entity, the information and the context [15]. Authenticated portals commonly expose PHI because the organization can relate the user to care. Unauthenticated appointment forms, condition-specific questionnaires and known-patient interactions may also disclose PHI when the transmitted information relates to an identifiable individual's health care. The legal analysis must occur at the page, event, parameter and recipient level.

American Hospital Association v Becerra vacated a specific portion of HHS guidance: the theory that HIPAA obligations are necessarily triggered when tracking technology connects an individual's internet protocol address with a visit to an unauthenticated public webpage addressing specific health conditions or providers, without more [16]. The court did not invalidate HIPAA for authenticated portals, appointment forms, information voluntarily submitted by a user or interactions where the individual is known to be a patient. HHS's page now states the limited effect of the order and that the agency is evaluating next steps [15]. The decision therefore does not justify blanket deployment of pixels or session replay across a refractive surgery website.

FTC Act and Health Breach Notification Rule. When HIPAA does not govern the information at issue, Section 5 of the FTC Act may still prohibit unfair or deceptive privacy or security practices [17]. The 2024 amendments to the FTC Health Breach Notification Rule (HBNR) clarified coverage of many health applications and connected technologies, revised the definition of breach to include unauthorized disclosure, clarified that a personal health record may have the technical capacity to draw information from multiple sources and modernized notice content and delivery [18,19]. The HBNR applies to vendors of personal health records, PHR-related entities and specified service providers with respect to unsecured PHR-identifiable health information that is not regulated by the HIPAA breach rule for that entity and information. It is not a general breach rule for every medical practice. FTC matters involving GoodRx and BetterHelp illustrate separate Section 5 and health-data disclosure risks, but their facts should not be automatically imputed to an ophthalmic practice [20,21].

Representative state laws. Washington's My Health My Data Act regulates broadly defined consumer health data, requires a dedicated notice, separate consent for collection and sharing subject to exceptions, authorization for sale, deletion rights, processor terms, security and geofencing restrictions; violations are tied to the state Consumer Protection Act [22]. Nevada's consumer-health-data provisions similarly address notice, affirmative consent, deletion, processor duties, sale authorization, security and geofencing, with Attorney General enforcement and no private right created by the chapter [23]. Connecticut's consumer-health amendments require consent for specified processing and sales, create access and deletion rights and restrict geofencing in defined health settings, with exclusive Attorney General enforcement under the Connecticut Data Privacy Act [24]. These statutes differ in definitions, thresholds, exemptions, territorial reach, effective dates, cure provisions and remedies. Some contain data-level HIPAA exemptions; others have broader entity or activity exemptions. Comprehensive privacy statutes such as the Colorado Privacy Act add consent for sensitive data, deletion and opt-out rights, security duties and data-protection assessments even though they are not dedicated health-data statutes [25]. Table 2 is a structured comparison, not a complete state-law survey. A multi-state enterprise should maintain a jurisdiction matrix covering patient, device, employee, marketing

and vendor data and obtain state-specific advice before assuming that HIPAA status resolves the analysis.

Cybersecurity and Operational Resilience

Current law versus recommended and proposed controls. The current HIPAA Security Rule requires regulated entities to use reasonable and appropriate administrative, physical and technical safeguards for electronic PHI [26,27]. Accurate and thorough risk analysis is a required foundation [28]. Some implementation specifications are required, while others are addressable. Addressable does not mean optional: the entity must implement a reasonable and appropriate measure, adopt an equivalent alternative or document why the specification is not reasonable and appropriate in the circumstances [26,27]. Unique user identification is a current required implementation specification. By contrast, the current rule treats encryption and decryption for stored electronic PHI and encryption in transmission as addressable specifications. The current rule does not expressly mandate Multifactor Authentication (MFA) by name. MFA and encryption are nonetheless widely recommended risk-reduction practices and may be necessary in a given risk context. HHS's 2025 proposed Security Rule would, with limited exceptions, require MFA, encryption at rest and in transit, vulnerability scanning, network segmentation and other prescriptive measures, but those proposals are not current law as of the law- current date [31]. Table 4 labels mandatory, addressable, proposed and voluntary practices separately. NIST Special Publication 800-66 Revision 2 maps the current Security Rule to cybersecurity resources [29]. The NIST Cybersecurity Framework 2.0 organizes outcomes across Govern, Identify, Protect, Detect, Respond and Recover [30]. These voluntary frameworks do not create legal duties by themselves, but they provide a structured way to operationalize risk management. HHS has also emphasized system hardening and timely management of known vulnerabilities [32].

Control	Status under current HIPAA Security Rule	Essential baseline	Maturity-level extension
Risk analysis and risk management	Risk analysis and reasonable risk management are required for regulated entities.	Document systems, electronic PHI, threats, vulnerabilities, likelihood/impact, measures, owners and review after material change.	Continuous risk quantification, automated evidence, board risk appetite, independent validation.
Identity and access	Unique user identification is required; access authorization/management duties apply.	Unique accounts, least privilege, prompt joiner/mover/leaver actions, privileged-account control, quarterly high-risk access review.	Central identity governance, phishing-resistant authentication, just-in-time privilege, behavior analytics.
Multifactor authentication	Not expressly mandated by name in the current rule; may be reasonable and appropriate. Proposed rule would require MFA with limited exceptions.	MFA for remote, administrative, email, cloud and vendor access; document unsupported legacy exceptions.	Phishing-resistant MFA across all supported workflows; device-bound authentication and conditional access.
Encryption	Addressable for stored electronic PHI and transmission under current specifications. Proposed rule would be more prescriptive.	Encrypt supported endpoints, servers, backups, portable media and external transmissions; document equivalent/exception decisions.	Central key management, customer-managed keys where justified, automated certificate and cryptographic lifecycle governance.
Vulnerability and configuration management	Derived from risk analysis/management and reasonable safeguards; specific scan frequencies in the 2025 proposal are not current law.	Supported inventory, secure baselines, risk-based patch deadlines, external scanning, legacy-device isolation and exception register.	Continuous exposure management, authenticated scanning, annual penetration tests, attack-path analysis.

Control	Status under current HIPAA Security Rule	Essential baseline	Maturity-level extension
Logging and detection	Activity review and audit-control requirements apply; implementation remains risk-based.	Log administrative, EMR, cloud, identity and device events; preserve time synchronization and incident evidence; define alert owners.	Central SIEM, 24-hour monitoring, cross-site correlation, user/entity behavior analytics.
Backup and recovery	Contingency planning, backup, disaster recovery and emergency-mode operation requirements apply.	Protected backups, documented recovery objectives, restore tests, clinical downtime procedures.	Immutable/offline copies, automated recovery validation, cyber-recovery environment, enterprise exercises.
Vendor security	Business-associate assurances and risk management apply where relevant; non-HIPAA contracts may create other duties.	Inventory, risk tier, due diligence, appropriate agreements, incident deadline, subprocessor visibility, return/deletion.	Continuous monitoring, concentration-risk analysis, audit rights testing, coordinated incident exercises.
Abbreviations: AI, artificial intelligence; DRPGF, Direct-Pay Refractive Privacy Governance Framework; FTC, Federal Trade Commission; HBNR, Health Breach Notification Rule; HIPAA, Health Insurance Portability and Accountability Act; MFA, multifactor authentication; PHI, protected health information			

Table 4: Cybersecurity control priority and legal status as of 31 August 2026.

For a small or independent practice, the essential baseline is deliberately narrower than a mature enterprise program: an accountable owner; current legal-role and data/ system/vendor inventories; risk analysis; unique accounts and least privilege; MFA for remote, administrative, email and cloud access as a recommended safeguard; encryption or documented equivalent decisions; supported configurations and patching; protected and tested backups; workforce training; vendor contracts; and a practiced incident plan. Maturity controls can add centralized identity governance, security-information and event management, 24-hour monitoring, microsegmentation, data-loss prevention, automated vendor monitoring, adversarial testing and independent certification. Binding duties are not waived for small entities, but the current rule expressly permits consideration of size, capability, infrastructure, cost and risk [27].

Incident response must branch by legal regime and clinical effect. Under the HIPAA Breach Notification Rule, an impermissible use or disclosure is presumed to be a breach unless a documented assessment demonstrates a low probability that PHI was compromised; covered entities and business associates have defined notification duties [33]. The HBNR, state laws, contracts, payment-card requirements and consumer promises may trigger different decisions and deadlines. A cloud provider that maintains encrypted electronic PHI without the key can still be a business associate [34]. Refractive surgery downtime plans should cover access to diagnostic history, treatment files, medications, postoperative triage and the safe postponement of surgery, not only restoration of the office network.

Artificial Intelligence, De-identification and Biometrics

AI risk classification. AI should be governed by function and data rather than by a single enterprise label. Table 5 separates: clinical decision-support systems; imaging algorithms; generative documentation tools; patient-facing chatbots; marketing and lead- scoring systems; and administrative automation. Each class has a different combination of privacy, accuracy, consent, bias, human-oversight, clinical-safety, recordkeeping and liability risk. The NIST AI Risk Management Framework provides a voluntary Govern-Map- Measure-Manage structure but does not establish clinical efficacy or legal compliance [35].

AI class	Refractive surgery example	Primary risks	Minimum governance
Clinical decision support	Candidacy, ectasia risk, treatment selection, outcome prediction.	Clinical harm, bias, automation bias, unclear intended use, liability, silent model change.	Clinical owner; intended-use and validation plan; subgroup/site testing; human decision; override; change and outcome monitoring.
Imaging algorithm	Segmentation or interpretation of topography, tomography, epithelial or ocular-surface images.	Device shift, poor image quality, re-identification, training provenance, performance drift.	Image/data lineage; quality thresholds; device-specific validation; access and training controls; drift and failure monitoring.
Generative documentation	Draft consultation, operative or postoperative notes.	Fabricated findings, omission, disclosure to vendor, overreliance, uncertain record provenance.	Approved environment; minimum data; clinician verification; audit trail; no autonomous signing; contract and retention controls.
Patient-facing chatbot	Candidacy education, scheduling, postoperative questions.	Misleading advice, emergency delay, identity/age issues, sensitive conversation retention, implied diagnosis.	Scope disclosure; scripted escalation; emergency warnings; tested content; identity controls; retention and human handoff.
Marketing and lead scoring	Predict procedure interest or conversion from browsing, calls, demographics or financing.	Sensitive inference, discrimination, opaque targeting, consent mismatch, tracking disclosure.	Purpose limitation; legal/state review; feature inventory; fairness tests; audience restrictions; opt-out/consent controls.
Administrative automation	Call summaries, coding support, vendor triage, staff scheduling.	Propagation of errors, workforce surveillance, unauthorized access, unreviewed downstream action.	Risk tier; least privilege; sample validation; human approval for consequential action; logs; rollback and vendor controls.
Abbreviations: AI, artificial intelligence; DRPGF, Direct-Pay Refractive Privacy Governance Framework; FTC, Federal Trade Commission; HBNR, Health Breach Notification Rule; HIPAA, Health Insurance Portability and Accountability Act; MFA, multifactor authentication; PHI, protected health information			

Table 5: AI risk classes in a refractive surgery organization.

Clinical candidacy and imaging models may analyze corneal tomography, topography, epithelial thickness, aberrometry, biomechanics, age, refraction and outcomes. Controls should address intended use, training population, validation at each device/site, performance across subgroups, change control, clinician override, failure escalation and documentation of the human decision. Generative documentation requires verification against the encounter and controls against invented findings. Patient chatbots need clear scope, emergency routing, identity and age handling, conversation retention rules and prohibition on representing automated output as a diagnosis.

Consumer-grade generative AI creates a distinct disclosure pathway. Patient information entered into a public or unapproved tool may be logged, retained, reused for service improvement or model training, reviewed by personnel, transferred to subprocessors or processed in other jurisdictions depending on the provider's current terms and settings. The workforce should not assume that deletion of a chat or removal of a name prevents those uses. Approved enterprise contracts should define data ownership, permitted purpose, retention and deletion, training exclusion, subprocessors, processing location, security, incident reporting, audit evidence and return of data. Where PHI is handled on behalf of a covered entity, business-associate analysis

remains necessary [12,34].

De-identification. HIPAA permits two methods: Expert Determination, under which a person with appropriate statistical and scientific knowledge determines and documents that the risk of identification is very small; and Safe Harbor, which requires removal of 18 categories of identifiers and no actual knowledge that the remaining information can identify an individual [36,37]. Safe Harbor includes full-face photographs and comparable images, biometric identifiers including finger and voice prints and any other unique identifying characteristic or code. Pseudonymization, cropping, masking a name or removing direct identifiers alone is not necessarily de-identification.

Residual risk is substantial in image-rich ophthalmology. Facial and periocular images, voice recordings, iris or retinal patterns, rare corneal findings, device metadata and longitudinal high-dimensional image sets can permit linkage or inference even when common identifiers are removed. The appropriate method may require expert assessment, data- minimization, feature extraction instead of raw-image release, controlled access, contractual limits, federated or other privacy-preserving methods and re-identification testing [8,9,37].

Biometric laws add a separate classification question. Illinois defines biometric identifiers to include retina or iris scans, voiceprints and scans of face geometry, but also excludes information captured from a patient in a health care setting and specified health-care information; its statute contains a private right of action [38]. Texas regulates commercial capture of biometric identifiers, including retina or iris scans, voiceprints and records of face geometry, with consent, retention/destruction, disclosure and security provisions enforced by the Attorney General [39]. The exclusions and facts matter. A clinical photograph may be outside one biometric definition while a face template generated from the same image for identity verification or marketing analytics requires separate analysis.

Proposed Direct-Pay Refractive Privacy Governance Framework

Status and originality. The DRPGF does not claim that data inventories, access control, vendor oversight, incident response, risk assessment or audit are new; these are established HIPAA and NIST concepts [26,29,30,35]. Its proposed contribution is the adaptation and integration of those controls for a direct-pay, multi-entity refractive surgery model. The framework couples two authoritative registers - legal role by entity/ component and ophthalmic data lineage by workflow - and applies one control library across clinical, marketing, financing, device-cloud, AI and remote-care environments. It also distinguishes a resource-conscious baseline from maturity controls and links each domain to measurable evidence. This integration, not invention of the underlying controls, is the framework's asserted originality (Fig. 2).

The framework has six domains. Governance assigns board or executive accountability, privacy and security leadership, risk appetite, resources and escalation. Classification maintains the entity/component HIPAA role, business-associate relationships, applicable states and source-authority status. Ophthalmic data stewardship maps data from lead to deletion and gives each system, device, dataset and vendor an owner. Lifecycle controls embed privacy and security into product design, procurement, access, imaging, surgery, marketing, AI, remote care, retention and disposal. Response coordinates legal, security, clinical, vendor, insurance and communications decisions. Assurance tests controls, tracks exceptions and corrective actions and reports defined metrics. The domains are shown in Fig. 2 and representative operational measures are defined in Table 6.

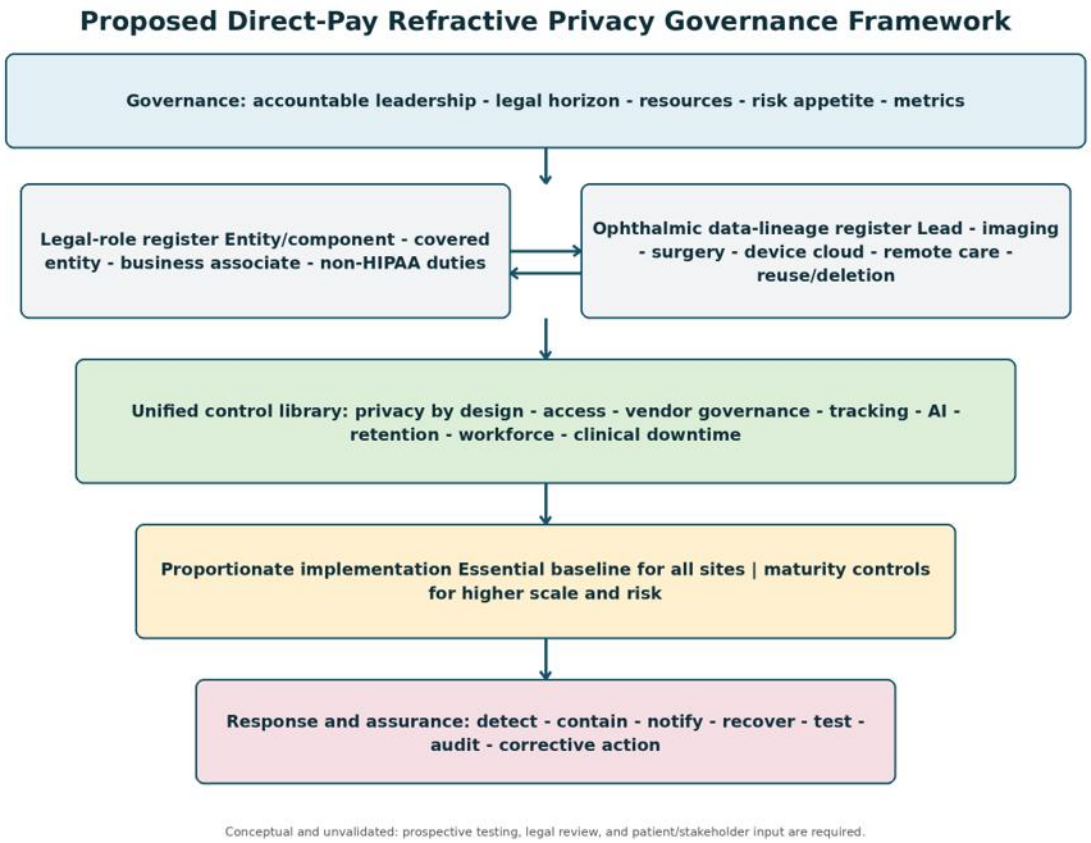

Figure 2: Proposed Direct-Pay Refractive Privacy Governance Framework. The model joins a legal-role register to an ophthalmic data-lineage register, applies baseline and maturity controls across the patient journey and closes the loop through response and assurance. The framework is conceptual and has not been externally validated.

Measure	Operational definition	Interval / owner	Illustrative target*
Applicability review completion	Number of active legal entities/components with a signed assessment reviewed within 12 months divided by total active entities/components in the register.	Quarterly / legal-compliance	100%; review within 30 days of material change
Critical vulnerability age	Median and 95th-percentile calendar days from validated identification/publication (whichever is later under policy) to remediation or approved time-limited exception for critical vulnerabilities on in-scope assets.	Monthly / security	P95 <=15 days internet-facing; <=30 days other, unless documented alternative
MFA coverage	Active in-scope user and privileged accounts protected by enforced MFA divided by all active in-scope accounts, excluding approved technical exceptions.	Monthly / identity-security	>=98% users and 100% privileged; all exceptions time-limited
Backup restoration success	Successful representative restore tests meeting recovery-point and recovery-time objectives divided by scheduled restore tests.	Quarterly / IT-clinical operations	100%; failed test corrected and repeated within 30 days
Departed-user	Elapsed time from authoritative termination notice to	Monthly / HR and	Immediate for

Measure	Operational definition	Interval / owner	Illustrative target*
disablement	disablement across defined critical systems; report median and P95.	identity	involuntary/high-risk; P95 <=4 hours otherwise
Privacy-review cycle time	Business days from receipt of a complete intake to documented approval, rejection or conditional decision; report routine and high-risk reviews separately.	Monthly / privacy	Median <=10 days routine; <=30 days high-risk
Incident containment time	Elapsed time from verified severity assignment to documented isolation or risk-stabilization; report median/P90 by severity and exclude false positives.	Per incident and quarterly / incident commander	P90 <=4 hours for severity 1; local targets for lower severity
Corrective-action closure	Corrective actions closed with evidence by approved due date divided by all actions due in period; overdue high-risk actions reported separately.	Monthly / control owners-compliance	>=95% on time; zero overdue critical actions without executive exception
*Targets are author-proposed starting points for local calibration. They are not statutory safe harbors, consensus benchmarks or validated predictors of effectiveness. Abbreviations: AI, artificial intelligence; DRPGF, Direct-Pay Refractive Privacy Governance Framework; FTC, Federal Trade Commission; HBNR, Health Breach Notification Rule; HIPAA, Health Insurance Portability and Accountability Act; MFA, multifactor authentication; PHI, protected health information			

Table 6: Proposed operational definitions and illustrative targets for governance measures.

The dual-register design prevents two common errors. First, it avoids applying the same HIPAA label to every entity under a brand. Second, it avoids treating non-PHI or a noncovered component as unregulated. A lead record can begin outside HIPAA, become PHI when incorporated into a covered practice's record, flow to an MSO acting as a business associate and remain subject to separate state or FTC duties in another system. The legal-role register and data-lineage register should be reconciled whenever a new site, vendor, campaign, financing product, device interface or AI use is launched.

Hypothetical Multi-Site Application

ClearSight Vision is a fictional 15-site organization operating in Ohio, Washington, Nevada and Connecticut. A parent company owns an MSO; separate professional entities employ ophthalmologists; one ambulatory surgery center bills health plans electronically; and the remaining LASIK sites usually accept only direct payment. Central systems include a website with advertising tags, a call center, a customer-relationship platform, patient financing, an electronic record, corneal tomography and topography devices, a laser- manufacturer cloud, an AI candidacy score, an SMS postoperative tool and a library of testimonials and before-and-after images.

The first register shows that the surgery center and one mixed practice are covered entities because they conduct standard electronic transactions. A self-pay professional entity with no such transaction is not a covered provider on that basis. The MSO is a business associate when it provides record hosting, scheduling or analytics to covered entities; it does not become a covered entity merely because of that role. Counsel evaluates whether any single legal entity should designate hybrid components and whether separate covered entities under common control should form an affiliated covered entity.

The data-lineage register then identifies four immediate problems. First, a pixel on the appointment-confirmation page transmits procedure and appointment events to an advertising platform; it is disabled pending a page/event-level review. Second, the AI vendor's standard terms permit model improvement from uploaded corneal maps; uploads are paused until an approved

contract, training exclusion, validation plan and business-associate analysis are completed. Third, the laser cloud has remote-support access but no current subprocessor or deletion schedule; the vendor is remediated and access is restricted. Fourth, testimonial permissions do not specify social-media reuse; new, separate authorizations are implemented.

Within 90 days, ClearSight assigns executive accountability, documents transactions and business-associate relationships, inventories critical systems and vendors, tests breach and clinical-downtime escalation and deploys baseline access and backup controls. Over the next six months it completes state-specific consumer-right workflows, data maps, contract remediation, risk analyses, site-level training and device-cloud standards. The following six months add independent testing, restore exercises, AI monitoring, patient-rights simulations and mature centralized detection. This example demonstrates framework use; it is not evidence that the sequence or controls will produce a measured outcome.

Illustrative Roadmap, Metrics and Implementation Burden

Roadmap status and basis. The 90-day, next-six-month and following-six-month sequence is an illustrative dependency-based roadmap, not a validated timetable or consensus standard. The intervals reflect a practical planning convention: establish accountability and contain obvious exposure first; build inventories, contracts and repeatable controls next; then test and mature the system. An organization should shorten or extend the intervals according to legal deadlines, incidents, acquisition risk, resources and the clinical consequences of failure. A known impermissible disclosure or critical exposure cannot be deferred simply because it appears in a later phase.

Operational measures need explicit definitions. Table 6 defines numerator, denominator or time origin, measurement interval, owner and an illustrative target. Targets are author-proposed starting points for local calibration, not statutory safe harbors or evidence-based benchmarks. Metrics should be segmented by site and function, accompanied by qualitative review and designed not to penalize good-faith incident reporting.

Implementation burden is material. Small practices may lack a privacy officer, security operations center, internal auditor, procurement function or negotiating leverage with device vendors. Legacy diagnostic and laser systems may be difficult to patch or segment. Data mapping, state-law analysis, contract review, deletion propagation, validation of AI, restoration testing and external counsel require money and staff time. An overly complex program can divert resources from care and produce documentation that is not followed.

Proportionality should change implementation, not erase obligations. A solo or small group can assign a responsible clinician-administrator, retain fractional privacy and security expertise, use a managed security provider, maintain simple but authoritative inventories, standardize vendor questionnaires and contract clauses and schedule focused legal review for high-risk changes. A larger chain should support centralized identity, security monitoring, vendor assurance, data governance and independent audit. In both settings, exceptions should identify the asset and data, legal and clinical impact, business justification, compensating controls, accountable approver and expiration date.

Enforcement, Liability and Regulatory Change

Privacy failures can trigger overlapping public and private consequences. HHS Office for Civil Rights investigates complaints and conducts compliance reviews and can resolve matters through voluntary compliance, corrective action, resolution agreements or civil monetary penalties [40]. The FTC, state attorneys general, consumer-protection agencies, professional boards and contracting parties may act under separate authority. Which regulator has jurisdiction depends on the entity, information, conduct, location and statutory exemptions.

Federal appellate courts have repeatedly held that HIPAA itself does not create a private right of action, including Acara v Banks, Webb v Smart Document Solutions and Payne v Taslimi [41-43]. That principle does not create nationwide immunity from private claims. State-law negligence, breach-of-confidence, privacy, contract, consumer-protection or vicarious-liability claims depend on each jurisdiction's elements and defenses. Byrne v Avery Center permitted Connecticut negligence and confidentiality theories and held that HIPAA could inform the standard of care, while Walgreen Co v Hinchy affirmed liability under Indiana state-law theories arising from an employee's misuse of prescription information [44,45]. These decisions are illustrative, not a comprehensive statement of remedies in every state.

Regulatory horizon scanning should distinguish present duties from future possibilities. As of 31 August 2026, HHS describes the existing Security Rule as the rule currently in effect; the January 2025 cybersecurity amendments remain proposed [27,31]. The 2026 claims-attachments rule is final but has a future compliance date [14]. Each legal source in the applicability register should therefore carry an authority type, effective date, compliance date, jurisdiction, owner and next-review date. All legal and regulatory sources should be rechecked immediately before publication and before operational use.

Limitations

This review has important limitations. Source selection was structured but non-systematic and performed by one author, creating selection and interpretation risk. The review may omit relevant state medical-record, biometric, consumer, breach, advertising, professional or corporate laws and does not resolve conflicts of law. It did not include independent review by a US healthcare attorney or privacy professional. Agency guidance can change, proposed rules may be revised or withdrawn and judicial decisions can narrow or invalidate agency positions.

The DRPGF has not been empirically tested, prospectively evaluated, externally validated or compared with another governance model. Its domains and roadmap were not developed by formal expert consensus. No patients, frontline staff, technology vendors, regulators or advocacy organizations participated in its design. Costs, feasibility, usability, effect on clinical outcomes, incident rates, patient trust and unintended burdens are unknown. Corporate structures, professional-entity rules, technology configurations, resources and state jurisdiction can materially alter implementation. The framework's generalizability outside United States refractive surgery is limited. These limitations require cautious interpretation and support prospective piloting with stakeholder and patient input.

Conclusion

Direct payment is a commercial characteristic, not a HIPAA classification. A refractive surgery organization should determine status by legal entity and component, based on electronic standard transactions and distinct business-associate relationships. It should then map ophthalmic data from marketing and financing through corneal imaging, surgery, device clouds, AI, remote follow-up, testimonials, retention and deletion. Binding law, case precedent, guidance, proposed rules and voluntary frameworks must be identified separately. The proposed DRPGF adapts established controls to this combined clinical-consumer data journey and offers a proportionate baseline, maturity path, hypothetical application and defined measures. It is a conceptual tool, not proof of effectiveness or legal compliance. Real-world testing, external legal review and patient and stakeholder input are necessary before the framework can be recommended as a validated model.

Conflict of Interest

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial or non-profit sectors.

Acknowledgement

The authors have no acknowledgments to declare.

Data Availability Statement

No datasets were generated or analyzed. Search terms and source-selection methods are reported in the Methods section; cited materials are publicly available from the references.

Ethical Statement

Not applicable. This article reviews publicly available legal, regulatory, judicial, policy and scholarly sources and involved no human participants or animals.

Informed Consent Statement

Not applicable.

Qualified Legal Review

The manuscript has not been independently reviewed by a qualified US healthcare attorney, privacy professional or compliance expert. The legal analysis is framed cautiously and jurisdiction-specific legal review is recommended before operational reliance.

Artificial Intelligence Disclosure

ChatGPT (OpenAI) was used to assist with language refinement, document structure, journal-format alignment and reference-consistency checking. The author reviewed the source material, verified the analysis, revised the text and accepts responsibility for the final manuscript.

Authors' Contributions

The author conceived the article, selected and interpreted the sources, developed the proposed framework, revised the manuscript and approved the final version.

References

1. Health Insurance Portability and Accountability Act of 1996, Pub L No. 104-191, 110 Stat 1936 (1996). [Last accessed on: September 06, 2026] https://www.govinfo.gov/app/details/PLAW-104publ191.
2. Definitions. 45 CFR sec 160.103 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160/subpart-A/section-160.103.
3. Administrative requirements. 45 CFR Part 162 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-162.
4. US Department of Health and Human Services. Summary of the HIPAA Privacy Rule. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.
5. Health Information Technology for Economic and Clinical Health Act, Pub L No. 111-5, div A, title XIII; div B, title IV, 123 Stat 226 (2009). [Last accessed on: September 06, 2026] https://www.govinfo.gov/app/details/PLAW-111publ5.
6. Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules. 78 Fed Reg 5566 (25 January 2013). [Last accessed on: September 06, 2026] https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the.
7. Rampat R, Deshmukh R, Chen X, Ting DSW, Ang M, Said DG. Artificial intelligence in cornea, refractive surgery and cataract: basic principles, clinical applications and future directions. Asia Pac J Ophthalmol (Phila). 2021;10(3):268-81.
8. Yang Y, Chen X, Lin H. Privacy preserving technology in ophthalmology. Curr Opin Ophthalmol. 2024;35(6):431-7.
9. Nakayama LF, de Matos JCRG, Stewart IU, Mitchell WG, Martinez-Martin N, Regatieri CVS, et al. Retinal scans and data sharing: the privacy and scientific development equilibrium. Mayo Clin Proc Digit Health. 2023;1(2):67-74.
10. Organizational requirements. 45 CFR sec 164.105 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-A/section-164.105.
11. Uses and disclosures: organizational requirements. 45 CFR sec 164.504 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.504.
12. US Department of Health and Human Services. Business associates. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.
13. Rights to request privacy protection for protected health information. 45 CFR sec 164.522 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.522.
14. Administrative Simplification; Adoption of Standards for Health Care Claims Attachments Transactions and Electronic Signatures. 91 Fed Reg 14350 (24 March 2026). [Last accessed on: September 06, 2026] https://www.federalregister.gov/documents/2026/03/24/2026-05676/administrative-simplification-adoption-of-standards-for-health-care-claims-attachments-transactions.
15. US Department of Health and Human Services. Use of online tracking technologies by HIPAA covered entities and business associates. [Last accessed on: September 06, 2026]

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
16. American Hospital Association v Becerra, No. 4:23-cv-01110, 2024 WL 3075865 (ND Tex 20 June 2024). [Last accessed on: September 06, 2026] https://law.justia.com/cases/federal/district-courts/texas/txndce/4:2023cv01110/382798/60/.
17. Federal Trade Commission Act, 15 USC secs 41-58. [Last accessed on: September 06, 2026] https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act.
18. Health Breach Notification Rule. 89 Fed Reg 47028 (30 May 2024). [Last accessed on: September 06, 2026] https://www.federalregister.gov/documents/2024/05/30/2024-10855/health-breach-notification-rule.
19. Health Breach Notification Rule. 16 CFR Part 318 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318.
20. Federal Trade Commission. GoodRx Holdings, Inc., matter no. 2023090. [Last accessed on: September 06, 2026] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc.
21. Federal Trade Commission. BetterHelp, Inc., matter no. 2023169. [Last accessed on: September 06, 2026] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter.
22. Washington My Health My Data Act. Rev Code Wash Chapter 19.373 (2026). [Last accessed on: September 06, 2026] https://app.leg.wa.gov/RCW/default.aspx?cite=19.373&full=true.
23. Nevada security and privacy of consumer health data. Nev Rev Stat secs 603A.400-603A.550 (2026). [Last accessed on: September 06, 2026] https://www.leg.state.nv.us/NRS/NRS-603A.html.
24. Connecticut Data Privacy Act and consumer health data provisions. Conn Gen Stat secs 42-515 to 42-526 (2026 Supp), as amended. [Last accessed on: September 06, 2026] https://www.cga.ct.gov/current/pub/chap_743jj.htm.
25. Colorado Privacy Act. Colo Rev Stat secs 6-1-1301 to 6-1-1314 (2026). [Last accessed on: September 06, 2026] https://coag.gov/resources/colorado-privacy-act/.
26. Security standards for the protection of electronic protected health information. 45 CFR Part 164, Subpart C (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C.
27. US Department of Health and Human Services. Summary of the HIPAA Security Rule. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
28. US Department of Health and Human Services. Guidance on risk analysis requirements under the HIPAA Security Rule. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.
29. Marron J. Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: a cybersecurity resource guide. NIST Special Publication 800-66 Revision 2. Gaithersburg (MD): National Institute of Standards and Technology; 2024.
30. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg (MD): NIST; 2024.
31. HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information. Proposed rule. 90 Fed Reg 898 (6 January 2025). [Last accessed on: September 06, 2026] https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information.
32. US Department of Health and Human Services. January 2026 OCR Cybersecurity Newsletter: system hardening and secure configurations. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-january-2026/index.html.
33. Notification in the case of breach of unsecured protected health information. 45 CFR Part 164, Subpart D (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-D.
34. US Department of Health and Human Services. Guidance on HIPAA and cloud computing. [Last accessed on: September 06, 2026]

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html.
35. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg (MD): NIST. 2023.
36. Other requirements relating to uses and disclosures of protected health information. 45 CFR sec 164.514 (2026). [Last accessed on: September 06, 2026] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.514.
37. US Department of Health and Human Services. Guidance regarding methods for de-identification of protected health information in accordance with the HIPAA Privacy Rule. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html.
38. Illinois Biometric Information Privacy Act. 740 ILCS 14 (2026). [Last accessed on: September 06, 2026] https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57&Print=True.
39. Texas Business and Commerce Code, Chapter 503: Biometric Identifiers (2026). [Last accessed on: September 06, 2026] https://statutes.capitol.texas.gov/?artSec=&chapter=BC.503&code=BC&tab=1.
40. US Department of Health and Human Services. Enforcement highlights. [Last accessed on: September 06, 2026] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html.
41. Acara v Banks, 470 F3d 569 (5th Cir 2006). [Last accessed on: September 06, 2026] https://www.ca5.uscourts.gov/opinions/pub/06/06-30356-CV0.wpd.pdf.
42. Webb v Smart Document Solutions, LLC, 499 F3d 1078 (9th Cir 2007). [Last accessed on: September 06, 2026] https://law.justia.com/cases/federal/appellate-courts/ca9/05-56885/0556885-2011-02-25.html.
43. Payne v Taslimi, 998 F3d 648 (4th Cir 2021). [Last accessed on: September 06, 2026] https://www.ca4.uscourts.gov/opinions/187030.P.pdf.
44. Byrne v Avery Center for Obstetrics & Gynecology, PC, 327 Conn 540, 175 A3d 1 (2018). [Last accessed on: September 06, 2026] https://law.justia.com/cases/connecticut/supreme-court/2018/sc19873.html.
45. Walgreen Co v Hinchy, 21 NE3d 99 (Ind Ct App 2014). [Last accessed on: September 06, 2026] https://caseclips.courts.in.gov/2014/11/20/walgreen-v-hinchy/.

About the journal

ATHENAEUM SCIENTIFIC PUBLISHERS

Journal of Ophthalmology and Advance Research is a peer-reviewed, open-access scholarly journal published by Athenaeum Scientific Publishers. The journal publishes original research articles, case reports, reviews, editorials and commentaries within its defined scope, with the aim of supporting scientific research and clinical knowledge in ophthalmology.

All manuscripts are evaluated through an independent peer-review process conducted in accordance with the journal's editorial policies and established publication ethics. Editorial decisions are made solely on the basis of academic merit.

Manuscript submission: https://athenaeumpub.com/submit-manuscript/