Retina Practice Cybersecurity & HIPAA Compliance Checklist (2025) — Florida

Practical one-pager for ophthalmology/retina clinics handling ePHI. Use as a quick audit aid for administrators & practice managers.

1) Core Safeguards (Do These First)

- Enforce MFA on EHR/PM, email, e-prescribing, cloud file sharing, and remote access (VPN).
- Full-disk encryption on all workstations, laptops, tablets; auto-lock after 5–10 minutes.
- Password manager + unique passwords; disable shared logins at front desk/tech stations.
- Endpoint protection/EDR on every device; restrict USB and block unauthorized apps.
- Patch OS/EHR/imaging software monthly; emergency patching for critical CVEs.
- Nightly offsite/cloud backups + one offline copy; test restores quarterly.
- Staff security awareness & phishing training each quarter (front desk, techs, scribes, billers).

2) HIPAA Security Rule — Required Controls

- Perform a written Security Risk Analysis (SRA) at least annually and after major changes.
- Implement Role-Based Access Control (minimum necessary); unique IDs; terminate access same-day offboarding.
- Maintain audit logs for EHR, imaging, e-prescribing; review access reports monthly.
- Transmission security: TLS-encrypted patient portal/email; encrypt exports/removable media.
- Facility security plan: server/network closets locked; visitor log; video where appropriate.
- Contingency plan: disaster recovery, data backup, and emergency-mode operations procedures; document downtime workflow.

3) HIPAA Security Rule — Addressable (Treat as Required Unless Justified)

- Workstation security & screen privacy; privacy filters in patient areas.
- Mobile Device Management (MDM) for iPads/laptops (remote wipe, pin, app control).
- Automatic logoff; session timeouts on EHR/imaging/viewers.
- Integrity controls: anti-tamper, hash/checks for exported images/docs.

4) HIPAA Privacy Rule & 21st Century Cures Act (Information Blocking)

- Right of Access: fulfill records requests within required timelines; publish simple process and fees.
- Do not “information block”: enable portal access to visit notes, imaging reports when feasible.
- Use Business Associate Agreements (BAAs) with cloud email, billing, IT, transcription, imaging vendors.
- Minimum Necessary standard in scheduling, front desk discussion, and phone disclosures.

5) Florida Information Protection Act (FIPA) — State Layer

- Maintain “reasonable” security measures for personal information (PI) of Florida residents.
- If a breach affects >500 Floridians, notify the Florida Attorney General and impacted individuals within 30 days.
- Preserve breach documentation for at least 5 years.

6) Clinical Devices & Imaging (Retina-Specific)

- Segment OCT/fundus/angiography devices from guest/staff Wi-Fi; isolate on a medical VLAN.
- Keep DICOM gateways and imaging workstations patched and backed up; restrict internet access where possible.
- Vendor maintenance mode: log any remote access; require vendor MFA and BAAs.
- Secure media export (USB/DVD) with encryption; control who can export images to outside CDs/portals.

7) Payments, Billing & Third Parties

- If storing/processing credit cards, follow PCI basics (use validated terminals; avoid storing card data).
- Vet billing companies/clearinghouses; sign BAAs and include breach-notification timelines and right-to-audit language.
- Create a vendor inventory with contacts, data flows, and contract renewal dates.

Educational aid — not legal advice. HIPAA breach notice: within 60 days; Florida FIPA AG notice: within 30 days if >500 residents.