ICSI | INTERNATIONAL COMPUTER SERVICES

CASE STUDY

Closing the Blind Spot: Securing OCT Scanners, Fundus Cameras, and Connected Diagnostic Equipment in Eye Care Practices

How ICSI helps optometry and ophthalmology practices turn overlooked diagnostic devices from a hidden liability into a protected, monitored part of the network — without disrupting patient care.

53%	6+	60%	1 IN 5
OF CONNECTED MEDICAL DEVICES HAVE AN UNPATCHED CRITICAL VULNERABILITY	AVERAGE KNOWN VULNERABILITIES PER CONNECTED MEDICAL DEVICE	OF MEDICAL DEVICES IN USE ARE CONSIDERED END-OF-LIFE	HEALTHCARE ORGS HIT BY AN ATTACK INVOLVING A MEDICAL DEVICE (2026)

1 THE CHALLENGE

Diagnostic Equipment Is Now Part of the Attack Surface

An OCT scanner doesn't feel like a computer. Neither does a fundus camera, an auto-refractor, or an IOL calculator. To clinical staff, they're diagnostic tools — not IT infrastructure. But to a network, and to an attacker, they are exactly that: connected devices running an operating system, sitting on the same network as patient records, scheduling software, and everything else the practice depends on.

Built for Function, Not Security

Manufacturers engineer these devices for imaging accuracy and regulatory approval — not cybersecurity. Many run operating systems that haven't been meaningfully updated since purchase, because updates risk disrupting FDA-cleared functionality.

Long Service Life, Short Security Life

Equipment stays in clinical use for eight to ten years or more, often running an operating system the manufacturer stopped patching years earlier — clinically excellent, and simultaneously wide open from a security standpoint.

Shared, Flat Networks

Diagnostic devices, the EHR system, scheduling software, and guest Wi-Fi frequently sit on the same flat network — meaning one compromised device can open a path to patient records and administrative systems.

Vendor Remote Access

Imaging equipment is serviced and calibrated remotely by manufacturers or third-party vendors. That access is essential — but a compromised vendor account or unmonitored session can be a direct route into the practice's network.

> *"The diagnostic equipment sitting in your exam rooms right now may already have a known vulnerability that a manufacturer isn't going to patch — and treating it the same way you'd treat a laptop or a printer isn't enough to protect it."*

2 HOW ATTACKERS GET IN

The Typical Attack Path Through Medical Devices

1. **Initial Foothold**
   Attackers gain access through an easier, less-monitored entry point first — an unpatched network device, a compromised vendor remote-access session, or a phishing email that captures staff credentials.
2. **Lateral Movement**
   Once inside, attackers move sideways looking for higher-value targets — including imaging systems and the patient data they store or transmit. On a flat network, this step is often far easier than it should be.
3. **Escalation**
   From there, an attacker may exfiltrate patient imaging and record data, deploy ransomware across connected systems, or — in more advanced cases — attempt to interfere with device functionality itself.

Lateral movement is also the single most fixable part of the equation — which is why ICSI's approach for eye care clients starts there.

3 THE ICSI APPROACH

A Practical Security Framework for Eye Care Diagnostic Equipment

None of the following requires replacing imaging equipment or disrupting clinical workflows. It requires treating these devices as the network assets they actually are.

1 Segment Diagnostic Devices
Place OCT scanners, fundus cameras, and similar equipment on their own network segment (VLAN), separate from patient records, admin systems, and guest Wi-Fi — the single highest-impact step available to most practices.

2 Build an Actual Device Inventory
You can't protect what you don't know is on your network. A maintained inventory — including devices added years ago and rarely thought about — is the foundation everything else builds on.

3 Apply Updates on a Defined Schedule
Apply manufacturer patches and firmware updates on a set cadence, not ad hoc — and ask vendors directly about end-of-life timelines so replacement can be planned in advance.

4 Govern Vendor Remote Access
Require secure, monitored, time-limited access windows instead of standing always-on remote tools, with clear contractual expectations for encryption, authentication, and incident reporting.

5 Apply Compensating Controls
For legacy or end-of-life devices that can no longer be patched, segmentation, strict access controls, and behavioral monitoring become the primary line of defense.

6 Monitor for Unusual Behavior
Passive, clinical-environment-aware monitoring flags unexpected outbound connections or unusual data volumes — without an agent on the device or any interruption to its clinical function.

7 Include Devices in the HIPAA Risk Assessment
Any diagnostic device that stores or transmits patient data is squarely in scope for a HIPAA Security Rule risk assessment — not just servers and workstations.

Why This Matters Beyond Compliance

- Securing diagnostic equipment isn't only about avoiding a HIPAA penalty or breach notification letter — when imaging systems go down, patient care is directly affected.
- Compromised or offline devices mean delayed diagnoses, canceled imaging appointments, and disrupted scheduling for the practice.
- In more advanced incidents, attackers have shown willingness to interfere with device functionality itself, not just the data it produces.
- For a practice built around timely, accurate diagnostic imaging, this operational risk is often just as significant as the data privacy risk.

I ABOUT ICSI

Cybersecurity Built for the Way Healthcare Practices Actually Operate

ICSI (International Computer Services) provides IT and cybersecurity services designed around the operational realities of healthcare practices — including the connected diagnostic equipment that clinical care now depends on. Rather than applying generic enterprise IT playbooks, ICSI works within the constraints of clinical environments: uptime requirements, regulatory obligations, and equipment that can't simply be swapped out or restarted mid-shift.

Who We Work With
Optometry and ophthalmology practices, ambulatory surgery centers, and other outpatient healthcare providers managing connected diagnostic and imaging equipment.

What We Deliver
Network segmentation, device inventory and risk assessment, vendor access governance, ongoing monitoring, and HIPAA Security Rule alignment — without disrupting patient care.

Want to Know How Exposed Your Practice's Diagnostic Equipment Actually Is?

ICSI helps eye care practices nationwide assess and secure connected diagnostic equipment — building network segmentation, vendor access controls, and monitoring designed for clinical environments, without interrupting the patient care these devices support.

Contact ICSI for a complimentary medical device security assessment.

ICSI • INTERNATIONAL COMPUTER SERVICES • CYBERSECURITY FOR HEALTHCARE & EYE CARE PRACTICES

Framework and industry figures (FBI / healthcare-sector research) as of early 2026.