enVisiAIn

Security Awareness Training Module

Protecting patient trust in AI-augmented vision care

Employee Training • Security Policies • Compliance Culture

Why security matters here

At enVisiAIn, a breach is not only a data event — it can become a patient safety event.

Patient trust
Users rely on our devices to interpret the physical world safely.

Regulatory duty
HIPAA and privacy obligations require safeguards for sensitive health data.

Business continuity
Clinics and support teams need reliable access to critical services.

Training goal: turn every employee into a control point — not a weak point.

What we protect

Sensitive data classes

- ePHI: medical history, clinician notes, care status
- Biometrics: retinal scans, sensor data, eye movement
- Vision data: live/stored camera feeds and surroundings
- Location: GPS, routes, homes, clinics, emergency events
- AI outputs: recommendations, alerts, model confidence logs

Collect less • Protect more • Share only when authorized

Policy 1: Acceptable use

Use company systems only for approved work — and handle data according to role, need, and authorization.

Do

Use approved apps, storage, devices, and communication channels.

Do

Lock screens, protect badges, report lost devices immediately.

Do not

Upload patient data, video, code, or biometrics to personal AI/chat/cloud tools.

Do not

Access patient, clinic, or source-code data outside your job need.

Security behavior standard: “minimum necessary access, maximum accountability.”

Policy in action: phishing defense

Stop the breach before it starts

- Check sender, domain, tone, urgency, and unexpected links.
- Never approve MFA prompts you did not initiate.
- Verify money, vendor, password, or patient-data requests using a second channel.
- Report suspicious emails/messages immediately — do not investigate alone.

PAUSE

VERIFY

REPORT

Policy 2: compliance and data handling

Compliance is what trust looks like on paper — and in practice.

HIPAA mindset

Protect electronic health information with administrative, physical, and technical safeguards. Treat access, audit logging, encryption, and training as part of patient care.

Privacy-by-design

Keep data on device where possible. De-identify before cloud analytics. Use consent and purpose limits for model training.

Minimum necessary

Collect what we need, retain only as long as approved, and disclose only through authorized business or clinical channels.

Never use patient data for demos, testing, personal AI tools, or screenshots unless explicitly approved.

Policy 3: remote access and devices

Hybrid work rules

- Use only approved remote access methods: VPN, ZTNA, or secure cloud identity.
- MFA is mandatory; password-only access is prohibited.
- Restricted data stays off personal devices and personal cloud storage.
- Lost devices, suspicious prompts, or abnormal logins are urgent reports.

Company-managed device + MFA + approved connection

Your role in incident response

Report early. Preserve evidence. Do not cover tracks.

1 Stop
Do not click further, forward data, or keep troubleshooting alone.

2 Preserve
Keep the device/email/window available. Do not delete messages or logs.

3 Report
Contact Security with who, what, when, where, and screenshots if safe.

4 Follow up
Cooperate with containment, password resets, access review, or device return.

Fast reporting is protection, not blame.

Quick knowledge check
What should you do?

Scenario A

A vendor asks you to export a raw patient video clip to help debug an AI model.

Correct move: refuse the request and route it through Privacy/Security approval.

Scenario B

You receive an MFA push you did not initiate while off-site.

Correct move: deny it and report it as suspicious.

Scenario C

Your company laptop with dashboard access is missing from your car.

Correct move: report immediately so access can be locked and device wiped.

Employee pledge: I will use approved systems, protect sensitive data, verify unusual requests, and report concerns quickly.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). Secure Our World. https://www.cisa.gov/secure-our-world

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.

U.S. Department of Health and Human Services. (2024). Summary of the HIPAA Security Rule. Office for Civil Rights.

Federal Trade Commission. (n.d.). Privacy and security: Business guidance. https://www.ftc.gov/business-guidance/privacy-security

Visuals generated for this training module using AI image generation.