intoneCCM

The Lead Magnet (10-Point Actionable Checklist) - Strategic Data Security for SaaS Startups

CTOs and Compliance Officers at health-tech startups, especially those dealing with data security, compliance, and scaling challenges.

1. Inventory All PHI (Protected Health Information)

List every database, folder, and third-party app (Slack, Email, AWS) that touches patient data.

- **EagleEye365° Advantage:** Use our **Auto-Discovery Module** to scan your entire cloud environment and identify hidden PHI silos you might have missed.

2. Execute BAAs (Business Associate Agreements)

Identify every vendor (Sub-processor) you use. Send and sign a BAA with each.

- **The Example (BAA Snippet):** "Business Associate agrees to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality and integrity of Electronic PHI."

3. Encrypt Data at Rest & In Transit

Enable AES-256 encryption on cloud buckets; ensure API calls use TLS 1.2+.

- **EagleEye365° Advantage:** Our **Encryption Monitor** provides real-time alerts if a database bucket is accidentally switched to "public" or "unencrypted" status.

4. Set Up Unique User IDs

Disable all "shared logins." Assign a unique ID to every employee to track access.

- **The Example (Audit Log):** User ID: DEV_04 | Action: Accessed DB_Patient_Records | Timestamp: 2026-03-18 10:15:02 UTC.

5. Enable Automatic Log-Offs

Configure your application to automatically log users out after 15 minutes of inactivity.

6. Perform a Technical Gap Analysis

Scan your infrastructure for open ports or unencrypted databases.

- **EagleEye365° Advantage:** Run a **One-Click Gap Analysis** to see exactly which HIPAA controls are currently "Failing" versus "Passing" in your live environment.

intoneCCM

The Lead Magnet (10-Point Actionable Checklist) - Strategic Data Security for SaaS Startups

CTOs and Compliance Officers at health-tech startups, especially those dealing with data security, compliance, and scaling challenges.

7. Draft Your Privacy Policy

Create a "Notice of Privacy Practices" (NPP) and make it easily accessible in your website footer.

8. Conduct a HIPAA Risk Assessment

This is a mandatory annual requirement to identify potential vulnerabilities.

- **The Example (Risk Assessment Outline):**
    1. **Identify Assets:** (e.g., AWS EC2 instances, S3 buckets).
    2. **Identify Threats:** (e.g., Unauthorized access, data loss).
    3. **Assess Controls:** (e.g., Are passwords rotated every 90 days?).
    4. **Determine Likelihood/Impact:** (High/Medium/Low).
- **EagleEye365° Advantage:** Automatically generate your **Risk Assessment Report** based on real-time system data, saving weeks of manual documentation.

9. Conduct "Sanctions" Training

Train all staff on HIPAA and have them sign a document acknowledging penalties for mishandling data.

- **EagleEye365° Advantage:** Store and track employee training certificates in our **Compliance Vault** for easy retrieval during an audit.

10. Establish an Emergency Access Plan

Document clear procedures for accessing PHI during a system failure or cyberattack.

Ready to Automate Your Compliance? Book a Demo

Resources: HIPAA 2026 Regulatory Guide | Unified GRC Solutions

---

© 2026 IntoneCCM & EagleEye365°. All Rights Reserved. *Confidentiality Notice: This checklist is for informational purposes and does not constitute legal advice.*