Simple Guide: ***OCR Letter or HIPAA Incident?***

Your First 72 Hours Playbook

By: Shawn Awan, SkySec Founder & Lead Assessor

1) The Golden Rule: Preserve evidence before you "fix" things

Do this immediately (0–2 hours):

- ☐ *Start an incident log (date/time, who, what happened, actions taken)*
- ☐ *Snapshot current state: screenshots of alerts, ransom notes, error messages*
- ☐ *Preserve logs (EHR, firewall, email, endpoint, backups, MFA, VPN)*
- ☐ *Stop auto-deleting: increase log retention if possible*
- ☐ *Assign one incident lead (no free-for-all changes)*

Avoid:

- ☐ *Wiping/reimaging systems before evidence capture*
- ☐ *Telling staff, "it's fine" (OCR will ask what you knew + when)*

2) Contain fast, but safely (2–8 hours)

Primary objective: *Stop spread and stop data loss.*

- ☐ *Isolate affected devices (pull network cable / disable Wi-Fi / quarantine in EDR)*
- ☐ *Disable risky access paths (RDP, stale VPN accounts, shared admin accounts)*
- ☐ *Force credential reset for impacted accounts + any privileged users*
- ☐ *Verify MFA is enforced for email/EHR/remote access*
- ☐ *Confirm backups are offline/immutable and not encrypted*

Decision point: *If there's any chance of ransomware or ePHI exposure → treat as a reportable security incident until proven otherwise.*

3) Know what OCR actually wants (8–24 hours)

OCR investigations and breach reviews usually boil down to:

"Show us your proof."

Have these ready (even if imperfect):

- ☐ *HIPAA Security Risk Analysis (most recent + remediation plan)*
- ☐ *Policies: access control, incident response, backups, device/media controls*
- ☐ *Asset inventory (systems handling ePHI + vendors touching ePHI)*
- ☐ *Business Associate Agreements (BAAs) for EHR, billing, IT/MSP, cloud/email, shredding*
- ☐ *Training records (dates, attendance)*
- ☐ *Patch/vulnerability evidence (reports, ticket history)*
- ☐ *Encryption posture (laptops, backups, email, portable media)*

If you don't have these, don't panic—start building a clean packet now with dates and a remediation timeline.

4) Triage "Was ePHI exposed?" (24–48 hours)

Answer these with evidence:

- ☐ *Which systems were affected (EHR, imaging, billing, email)?*
- ☐ *Any unauthorized access to records or admin consoles?*
- ☐ *Any data exfiltration indicators (unusual outbound traffic, new mail rules, new OAuth apps)?*
- ☐ *Did attackers access email (common source of ePHI breach)?*
- ☐ *Can you prove encryption at rest for impacted devices?*

Tip: *"We believe" doesn't hold up. Logs, screenshots, and vendor attestations do.*

5) Communications (48–72 hours)

- *□ Draft internal staff guidance: what to say, what NOT to say, where to report issues*
- *□ Identify external notifications that may apply:*
  - *Patients (if breach criteria met)*
  - *HHS/OCR breach portal (timelines vary by size/impact)*
  - *State requirements (often stricter than HIPAA)*
  - *Cyber insurance carrier (if you have coverage)*
- *□ Prepare a one-page executive summary: what happened, impact, containment, next steps*

6) The "Defensibility" upgrades OCR loves (do these next)

These are high-leverage controls that reduce repeat risk:

- *□ MFA everywhere (email/EHR/remote access) + disable legacy auth*
- *□ Immutable backups + quarterly restore tests*
- *□ Endpoint protection/EDR on every device*
- *□ Admin separation (no daily driver admin accounts)*
- *□ Vendor access reviews + BAAs in one place*
- *□ Quarterly vulnerability scans + patch SLAs you can prove*

If you want this handled cleanly (fast + defensible)

SkySec can produce a "HIPAA Defensibility Packet" *in days—not months:*

- *Incident timeline + evidence preservation plan*
- *Risk analysis gap map + remediation roadmap*
- *OCR-ready documentation set (policies, inventories, BAAs, proof artifacts)*
- *Ransomware hardening priorities tailored to small practices*

SkySec finds gaps focused on real-world attack paths – not compliance theater.
Contact us www.skysecsecurity.com

SkySec