

**Instructions —**

Use this guide as a fast, decision-oriented template during a hospital cyber incident: open the Executive Brief, fill the header (who/what/when/RAG) and a ≤5-line snapshot, then list clinical/business impact, affected systems, actions taken, next milestones with ETAs/owners, and the 2–3 approvals leadership must make. Drop in quick charts (impact metrics, recovery milestones, resource ask) if they clarify decisions. Publish the brief within 60 minutes of detection and update it at milestones or every 2–4 hours. Keep details concise, move technical depth to the appendix, version the file with timestamp + RAG, and share only through approved channels.

**Executive Brief — Cybersecurity Incident (Hospital)**

Concise decision brief covering impact, response timeline, and resource requirements.

**Header (top of page)**

Hospital: [Hospital Name]

Incident: [Ransomware / Suspected Intrusion / Phishing-led Compromise]

Date/Time First Detected: [MM/DD HH:MM]

Current Status (RAG): [🟢/🟡/🔴]

IR Lead: [Name, Title, Contact]

Brief Owner: [Name] • Last Updated: [MM/DD HH:MM]

**1) Situation Snapshot (≤5 lines)**

* What happened, where, and high-level cause if known.
* What’s currently impacted and what’s contained.
* Regulatory/clinical safety note if any (e.g., diversion, downtime charting).

**2) Clinical & Business Impact (bullets)**

* Patient Care: [e.g., EHR read-only; manual charting in ED/ICU].
* Operations: [e.g., imaging delayed; lab results via phone only].
* Financial: [est. revenue at risk/day or overtime costs].
* Compliance/Legal: [HIPAA risk; breach assessment in progress].
* Third Parties: [key vendor/system status].

**3) Affected Systems (scope)**

• EHR: [Normal / Degraded / Offline]

• PACS/Imaging: [state]

• LIS/Lab: [state]

• AD/Identity: [state]

• Email/M365/Workspace: [state]

• Network Segments: [e.g., Clinical VLANs segmented; RDP blocked]

• Medical Devices: [exceptions/compensating controls]

**4) What We’ve Done (Containment)**

* [Timestamp] Isolated affected subnets/endpoints; blocked indicators.
* [Timestamp] Disabled compromised accounts; enforced MFA resets.
* [Timestamp] Engaged IR retainer / forensics; preserved evidence.
* [Timestamp] Switched to downtime procedures (unit list).
* [Timestamp] Notified leadership/Legal/Privacy/Comms; created exec channel.

**5) Recovery Plan & Timeline**

* T0–24h: [e.g., gold image prep, priority server triage, restore tests].
* 24–72h: [e.g., staged restores for EHR, PACS; app smoke tests].
* >72h: [e.g., backlog reconciliation; audit; lessons learned].
* Next Milestone: [Name] • ETA: [MM/DD HH:MM] • Owner: [Name]

**6) Resource Requirements (Decisions Needed)**

* People: [# IR engineers], [# desktop hands], [on-call hours].
* Vendors: [IR retainer hours], [EHR vendor task order], [M365 specialist].
* Budget (not-to-exceed): $[amount] for [timeframe].
* Authorizations Requested Today: [e.g., overtime, emergency PO, PR statement].

**7) Risks & Blockers (Top 3)**

1. R1: [Risk + impact + mitigation owner].
2. R2: [Risk + impact + mitigation owner].
3. R3: [Risk + impact + mitigation owner].

**8) Communications & Compliance**

* Internal: staff bulletin [sent/planned at HH:MM], clinical guidance link.
* External: payer/partner notification [Y/N], media holding statement [Y/N].
* Regulatory: OCR/breach evaluation window status; counsel engaged [Y/N].

**9) Executive Decisions Requested (clear, binary)**

* Approve $[amount] for [vendor/service] — Yes/No
* Authorize after-hours cutover at [time window] — Yes/No
* Public statement if downtime > [X] hours — Yes/No

**Appendix**

**A) Timeline (detailed)**

[Add timestamped bullets]

**B) Contact Roster**

IR Lead, Legal/Privacy, Comms, EHR vendor, ISP, Cyber insurer

**C) Indicators of Compromise (IOC) Summary**

[Short list or link]

**D) Post-Incident Actions (to schedule)**

Tabletop exercise, policy updates, budget requests

**Chart Tables**

*Impact Metrics*

| Metric | Value |
| --- | --- |
| Units on Downtime | 7 |
| Avg Lab Turnaround Delay (min) | 22 |
| Imaging Backlog (studies) | 134 |
| Help Desk Tickets (24h) | 286 |
| ED Throughput Change (%) | -9 |

*Recovery Milestones*

| Milestone | Planned | Actual | Owner |
| --- | --- | --- | --- |
| Forensic Triage Start | 08:00 | 08:10 | IR Team |
| Priority Server Inventory | 09:00 | 09:30 | Infra |
| EHR Read-Only Online | 14:00 |  | Apps |
| PACS Restore Test | 16:00 |  | Imaging IT |
| Email Phish Controls Tightened | 18:00 | 17:45 | SecOps |

*Resource Ask*

| Category | Units |
| --- | --- |
| Overtime Hours | 120 |
| IR Retainer (hrs) | 60 |
| EHR Vendor Support (hrs) | 40 |
| Endpoint Reimage Count | 75 |
| Temporary Laptops | 25 |