Incident Response Plan

ClearPath Pharmacy: GRC Portfolio

Document information	Details
Organization	ClearPath Pharmacy: Specialty Pharmacy Services
Document title	Incident Response Plan
Document ID	CP-IRP-001
Classification	Confidential: Internal Use Only
Version	1.0
Effective date	May 18, 2026
Next review date	May 18, 2027
Prepared by	Information Security & Compliance Department
Approved by	Information Security Steering Committee

Governing framework: NIST SP 800-61, Computer Security Incident Handling Guide. This plan is the operational follow-through to ClearPath's HIPAA Security Risk Assessment, NIST CSF 2.0 Gap Analysis, and Incident Response Policy (CP-POL-003).

1. Purpose and Scope

This plan defines how ClearPath Pharmacy prepares for, detects, responds to, and recovers from information security incidents, with particular attention to incidents that involve electronic protected health information (ePHI). It applies to all ClearPath systems, workforce members, contractors, and Business Associates.

2. Incident Response Team and Roles

Role	Responsibility
Incident Lead	Owns the incident end to end; declares severity; coordinates the response and the decision to close.
Technical Lead	Investigation, containment, eradication, and recovery on affected systems.
Communications Lead	Internal updates and any external or patient communications.

Role	Responsibility
Compliance / Privacy Officer	Determines whether PHI is involved and drives the HIPAA breach-notification decision.
Executive Sponsor	Risk acceptance, resourcing, and sign-off on major decisions.

3. Incident Classification and Severity Levels

Severity	Definition	Examples
SEV-1 (Critical)	Confirmed or likely PHI breach, or major outage of a core system	Ransomware on pharmacy systems; confirmed exfiltration of ePHI
SEV-2 (High)	Security event with potential PHI impact or significant disruption	Phishing with credential compromise; lost device that may hold PHI
SEV-3 (Medium)	Contained event, no confirmed PHI impact	Blocked malware on one endpoint; single failed-control finding
SEV-4 (Low)	Minor or policy event, no service or data impact	Spam, isolated policy violation

4. The Four-Phase Response Process

Phase 1: Preparation

- Maintain the IR team roster, contact tree, and on-call coverage.
- Keep tools, logging, and backups in place and tested before an incident.
- Train workforce on reporting; run tabletop exercises (see Section 8).

Phase 2: Detection and Analysis

- Identify incidents from alerts, user reports, vendor notices, or monitoring.
- Triage, validate, and classify severity using Section 3.
- Determine whether ePHI is involved, which starts the HIPAA decision branch in Section 6.

Phase 3: Containment, Eradication, and Recovery

- Short-term containment: isolate affected systems to stop spread.
- Long-term containment and eradication: remove the threat and close the entry point.

- Recovery: restore from clean backups, validate integrity, and monitor for recurrence.

Phase 4: Post-Incident Activity

- Hold a blameless review within two weeks of closure.
- Document root cause, timeline, and corrective actions; feed them back into Preparation.
- Update controls, playbooks, and the risk register.

5. Escalation and Communication Plan

Trigger	Escalate to	Channel and timing
SEV-3 or below	Incident Lead	Ticket and team channel, same business day
SEV-2	Incident Lead + Compliance Officer	Direct contact within 1 hour
SEV-1 or any suspected PHI breach	Full IR team + Executive Sponsor	Immediate phone escalation; bridge opened

6. HIPAA Breach Notification Decision Branch

If an incident involves PHI, the HIPAA Breach Notification Rule applies. The Compliance / Privacy Officer runs this branch in parallel with technical response.

1. Determine whether PHI was acquired, accessed, used, or disclosed in a manner not permitted, and run the four-factor risk assessment to decide if it is a reportable breach.
2. Notify affected individuals without unreasonable delay and no later than 60 calendar days from discovery.
3. Notify the HHS Secretary: within 60 days if 500 or more individuals are affected; otherwise in the annual log.
4. Provide media notice to prominent outlets if 500 or more individuals in a single state or jurisdiction are affected.
5. Document the determination and all notifications, whether or not notification is required.

7. Reporting and Documentation Requirements

- Open an incident record at detection; maintain a timestamped timeline through closure.
- Record severity, systems affected, PHI determination, actions taken, and notifications.
- Retain incident documentation per the HIPAA six-year retention expectation.

8. Incident Playbooks

8.1 Ransomware

Detection signs: Encrypted files, ransom notes, mass file-rename events, backup tampering alerts.

Immediate steps: Isolate affected hosts from the network; do not power off (preserve memory); engage Technical Lead; verify backup integrity.

Who to notify: Incident Lead, Executive Sponsor; Compliance Officer if PHI systems are in scope (presumed breach under OCR guidance unless low probability is demonstrated).

Recovery: Restore from clean, offline backups; rebuild compromised hosts; rotate credentials; confirm eradication before reconnect.

Post-incident notes: Root-cause the entry vector; close it; update detection and tabletop scenarios.

8.2 Phishing / Business Email Compromise

Detection signs: Reported suspicious email, unexpected MFA prompts, mailbox rules added, anomalous logins.

Immediate steps: Quarantine the message tenant-wide; reset affected credentials; revoke active sessions; check for mailbox forwarding rules.

Who to notify: Incident Lead; Compliance Officer if a mailbox contained PHI.

Recovery: Re-enable accounts after reset and MFA re-enrollment; remove malicious rules; monitor for reuse.

Post-incident notes: Targeted user awareness follow-up; tune mail filtering.

8.3 Lost or Stolen Device with PHI

Detection signs: Reported lost or stolen laptop, phone, or removable media; missing asset at inventory.

Immediate steps: Remote-wipe or lock the device; disable associated accounts; determine whether ePHI was present and whether it was encrypted.

Who to notify: Incident Lead and Compliance Officer immediately; encryption status drives the breach determination.

Recovery: Reissue hardware; confirm encryption baseline on replacement.

Post-incident notes: If unencrypted PHI was present, run the Section 6 branch; reinforce full-disk encryption policy.

8.4 Confirmed PHI Data Breach

Detection signs: Validated unauthorized access, exfiltration, or disclosure of ePHI.

Immediate steps: Contain and preserve evidence; convene the full IR team; begin the Section 6 notification branch immediately.

Who to notify: Full IR team, Executive Sponsor, and legal/counsel; notifications per Section 6 timelines.

Recovery: Restore affected systems; remediate the root cause; offer remediation to affected individuals as appropriate.

Post-incident notes: Complete OCR-aligned documentation; corrective action plan; lessons learned.

9. Plan Testing and Review Cadence

- Run at least one tabletop exercise per year using one of the playbooks above.
- Review and update this plan annually, or after any SEV-1 or SEV-2 incident.
- Validate the contact tree and backup restoration quarterly.