

Health Security Readiness Pack

Broad organizational readiness checklist

USE AND PRIVACY BOUNDARY

Educational planning tool only. Not medical, legal, regulatory, emergency-management, or cybersecurity compliance advice.

Do not write protected health information, patient names, credentials, secrets, or live incident details on this worksheet.

Review with qualified personnel. Follow official guidance, organizational policy, and applicable law.

VERSION	SOURCE	LAST REVIEWED
2026-08-21	HealthSecurity.tech	2026-08-21

Purpose: Use this broad checklist to identify essential services, patient-safety dependencies, defensive controls, continuity gaps, and accountable next actions.

1. Scope and assumptions

ORGANIZATION / UNIT

DATE

REVIEWER ROLE

SYSTEMS IN SCOPE

- ☐ Define the organizational and geographic boundary of this review.
- ☐ Record assumptions about staffing, facilities, utilities, suppliers, and technology.
- ☐ Mark unknowns rather than guessing.

2. Critical services

- ☐ List essential services in order of time sensitivity.
- ☐ Record maximum acceptable interruption as an operational planning assumption.
- ☐ Identify the person or role authorized to reduce, redirect, or restore service.

MOST TIME-SENSITIVE SERVICE

PRIMARY OWNER

3. Patient-safety dependencies

- [] Map the people, systems, devices, data, facilities, communications, and supplies each service needs.
- [] Identify dependencies shared by several critical services.
- [] Record approved alternatives and their capacity limits.

Note: Qualified clinical and operational personnel must define patient-safety limits and alternatives.

4. Cybersecurity basics

- ☐ Maintain current owners for critical assets and services.
- ☐ Use strong authentication and limit unnecessary privilege.
- ☐ Keep supported systems updated through an approved process.
- ☐ Protect backups from ordinary administrative access.
- ☐ Monitor important security and operational events.
- ☐ Keep incident and downtime contacts accessible offline.

5. Medical-device inventory

- ☐ Record category, manufacturer, model, software or firmware, owner, and support status.
- ☐ Document connectivity and clinical workflow dependency.
- ☐ Record authorized downtime alternatives or safe-mode references.
- ☐ Restrict sensitive device identifiers and network detail.

INVENTORY OWNER

LAST VALIDATED

6. Communication channels

- ☐ Define independent channels for leadership, staff, vendors, and public updates.
- ☐ Keep approved templates and contact lists offline.
- ☐ Timestamp messages and distinguish confirmed facts from assumptions.
- ☐ Establish an accessible staff help and reporting route.

7. Public-health source monitoring

- ☐ Maintain a short list of authoritative sources by domain.
- ☐ Record what each source can and cannot establish.
- ☐ Define who checks sources, how often, and what triggers escalation.
- ☐ Separate evidence confidence from operational consequence.

8. Supply and vendor dependencies

- ☐ Identify vendors that support several critical services.
- ☐ Document support, escalation, incident-notification, and recovery contacts.
- ☐ Understand key subcontractors and infrastructure dependencies.
- ☐ Record viable alternatives and time-to-switch assumptions.

HIGHEST-CONSEQUENCE VENDOR DEPENDENCY

9. Downtime continuity

- ☐ Keep approved paper materials, contact lists, and procedures accessible without the network.
- ☐ Define downtime activation and deactivation authority.
- ☐ Identify staffing, space, supply, and communication limits.
- ☐ Practice documentation custody and later reconciliation.
- ☐ Exercise at least one cross-functional scenario.

10. Recovery and after-action notes

- ☐ Restore by service priority and validate each stage.
- ☐ Communicate limitations before routine use resumes.
- ☐ Reconcile records, decisions, and work completed during downtime.
- ☐ Assign improvements to owners with dates and retest them.

NEXT REVIEW DATE

EXERCISE / REVIEW OWNER

Top five health-security risks

Current controls

Gaps and next actions

USE AND PRIVACY BOUNDARY

Educational planning tool only. Not medical, legal, regulatory, emergency-management, or cybersecurity compliance advice.

Do not write protected health information, patient names, credentials, secrets, or live incident details on this worksheet.

Review with qualified personnel. Follow official guidance, organizational policy, and applicable law.