Continuity Hub • Field Operations Quick Card

Healthcare Continuity Compliance: CMS, Joint Commission & HIPAA in Miniature

Current version — Oct 31, 2026
Update history: continuityhub.org/healthcare-continuity-compliance-cms-joint-commission-hipaa/

THE UNIFIED CORE PRINCIPLE: ONE PROGRAM, THREE REGIMES

Healthcare continuity mandates protect patient safety, life support, and health information during disruptions. CMS, TJC, and HIPAA represent three complementary views of the same operational framework: **CMS Conditions of Participation** (statutory right to participate in Medicare), **The Joint Commission EM Standards** (deemed accreditation conditions), and **HIPAA 45 CFR §164.308(a)(7)** (statutory ePHI contingency protection).

1. CMS Emergency Prep

CONDITIONS OF PART

Authorities: Social Security Act §1861(e); 42 CFR 482 (Hospitals), 483 (LTC/SNF), 460 (PACE), 486 (Dialysis). Also covers HHA, Hospice, ASC.

- **EP Committee:** Senior leadership governance, cross-functional (clinical, IT, admin, ops), external public health coordination, regular reviews.
- **EOP Scope:** Comprehensive all-hazards plan, clear incident command structure, staffing/supplies, utility failures, patient evacuation.
- **Communication:** Internal staff alert/recall, external authorities/media/patients, redundant backup systems.
- **Cyber & IT:** IT recovery for clinical care, data backups, ransomware response procedures.

2. Joint Commission EM

ACCREDITATION

Current Renumbered Standards: EM.09 through EM.17 (replaces legacy EM.01, EM.02, EM.03 numbering; same substance, updated crosswalk).

- **EM.09 / EM.10:** Program structure, qualified leadership oversight, Incident Command System, succession planning.
- **EM.11 / EM.12:** Hazard Vulnerability Analysis (all-hazards), Emergency Operations Plan, Section 1135 waiver procedures.
- **EM.12.02 / EM.13:** Redundant communications, staff recall, disaster privileging, continuity of operations (COOP).
- **Utilities:** Emergency generator capacity for critical operations, regular testing, fuel reserves + fuel vendor contracts.

3. HIPAA Security Rule

45 CFR 164.308

Mandate: §164.308(a)(7) Contingency Plan protecting electronic Protected Health Information (ePHI) during emergencies and system downtime.

- **Data Backup Plan:** Automated daily (or more frequent) backups of all ePHI; stored separately & encrypted offsite; regular restore tests.
- **Disaster Recovery Plan:** Documented procedures to restore systems within acceptable timeframes; alternative processing; recovery priority ranking.
- **Emergency Access:** Documented manual/temporary procedures for authorized staff to access ePHI; audit trail logging; termination protocol.
- **Testing & BAAs:** Annual contingency testing & remediation; BA agreements mandating equivalent contingency plans.

SURVEY ENFORCEMENT & PENALTY STAKES: CMS deficiencies trigger *Condition-Level Findings* leading to Medicare termination. TJC deficiencies result in withheld or revoked accreditation. HIPAA violations enforced by HHS OCR result in tiered Civil Monetary Penalties (with annual caps/inflation adjustments), criminal penalties for willful neglect, and mandatory corrective action plans.

THE MANDATORY 2-EXERCISES-PER-YEAR RULE (CMS & TJC EM.16)

STATUTORY REQUIREMENT

Both CMS Conditions of Participation and Joint Commission Standard EM.16.01.01 mandate that healthcare facilities conduct **two formal emergency preparedness exercises each year**:

Exercise 1: Community-Based or Facility-Based Functional:
Full-scale or functional drill engaging community emergency response, local public health, or mutual aid partners. If community exercise is unavailable, facility-based functional exercise is required.

Exercise 2: Second Mandatory Exercise:
Additional full-scale exercise, facility-based drill, or tabletop scenario testing a distinct hazard from the Hazard Vulnerability Analysis (e.g., cyber/ransomware, severe utility loss, mass surge).

- **Departmental & Targeted Drills:** Unit-level drills at more frequent intervals (quarterly/semi-annual best practice).
- **Staff Training Cadence:** Initial training during orientation/hire; mandatory refresher at least every 2 years (CMS) and annually (TJC EM.15.01.01).

Grounded strictly in published post 46 • Form CH-46-QC

Continuity Hub • Field Operations Quick Card

Cross-Regime Alignment Matrix, Utility/IT Mandates & Survey Day Protocol

Current version — Oct 31, 2026
Update history: continuityhub.org/healthcare-continuity-compliance-cms-joint-commission-hipaa/

THREE-REGIME REGULATORY CROSSWALK

Continuity Domain	CMS Emergency Preparedness	Joint Commission (TJC)	HIPAA Security Rule §164.308
Planning & Governance	Written EOP addressing all-hazards; EP committee with leadership governance.	EM.09.01.01 (Program), EM.10.01.01 (Qualified leadership), EM.11.01.01 (HVA).	Documented Contingency Plan (§164.308(a)(7)); business associate agreements.
Incident Command & Staff Roles	Incident command structure; clear staff roles & emergency responsibilities.	EM.10.01.01: Incident Command System; chain of command; succession plan.	Emergency access role permissions; termination of emergency access rights.
Utility & Power Systems	Utility failure plans (power, water, gas, comms); generator backup adequacy.	Emergency generator capacity for all critical ops; routine testing; fuel contracts.	Physical and environmental controls supporting continuous ePHI data center ops.
Communications	Internal alert/recall; external patients, media, authorities; backup comms.	EM.12.02.01: Redundant communication systems; staff notification/recall.	Secure transmission protocols for ePHI during emergency manual downtime.
IT, Backups & Cyber	Clinical IT recovery; data backups; specific ransomware response procedures.	Critical system continuity under EOP; electronic health record resilience.	Automated daily backups; offsite encryption; disaster recovery; restore testing.
Training Cadence	Initial hire & at least every 2 years for all staff; documented attendance.	EM.15.01.01: Initial orientation & annual refresher for all staff.	Security awareness and emergency contingency training for all ePHI handlers.
Testing & Exercises	2 exercises/yr (1 community/functional + 1 second exercise); documented.	EM.16.01.01: 2 exercises/yr; EM.17.01.01: After-action reports (AAR) & remediation.	Annual testing of data backup, disaster recovery, and emergency access plans.

Utility & Emergency Power Mandates — CMS / TJC

- **Generator Capacity:** Must support *all critical operations*, life safety, clinical monitoring, and essential refrigeration.
- **Testing Schedule:** Routine testing (monthly/quarterly) and maintenance inspection records readily accessible for surveyors.
- **Fuel Supply:** Sufficient on-site fuel for extended power interruptions + written contracts/agreements for emergency fuel replenishment.
- **Automatic Transfer:** Automated switching systems to transition from primary utility to emergency generator power upon grid loss.
- **Water & Medical Gas:** Emergency water reserves and failure protocols for piped clinical gases.

IT Recovery & HIPAA Contingency — HIPAA / CMS

- **Backup Frequency:** Automated daily (or more frequent) backup of all electronic protected health information (ePHI).
- **Separation & Offsite:** Backups stored separately from primary infrastructure; encrypted offsite storage facility or secure cloud.
- **Restore Verification:** Regular testing verifying that backups are uncorrupted and can be fully restored within clinical timeframes.
- **Emergency Access & Downtime:** Paper forms and manual workflows for clinical care during total IT / EHR blackout.
- **Ransomware Response:** Documented isolation, incident response, containment, and recovery steps without compromising ePHI integrity.

SURVEYOR INSPECTION DAY: TOP 6 EVIDENCE BINDERS TO PULL — SURVEY READINESS

1. Current Written EOP & HVA: Evidence of annual review, leadership signature, and community emergency management coordination (MOUs).
2. Committee Minutes: Documented regular meetings of the Emergency Preparedness Committee showing cross-functional review and updates.
3. Training Attendance Roster: Logs proving 100% of staff received initial hire and biennial (CMS) / annual (TJC) emergency training.
4. 2-Exercise Evidence & AARs: Documentation of the community-based functional drill and second exercise, with formal After-Action Reports.
5. Generator Logs & Fuel Contracts: Weekly inspection logs, monthly load tests, and active signed vendor fuel replenishment contracts.
6. HIPAA Contingency & IT Restore Logs: Annual DR test report, automated daily backup verification, and emergency access procedure reviews.