

EMERGENCY PREPAREDNESS & BUSINESS CONTINUITY POLICY

Operations Department

Enterprise policy incorporating five operational Business Continuity Plans

DOCUMENT CONTROL	DETAIL
Organization	Curana Health
Department	Business Operations
Policy Owner	Operations Leadership
Policy Number	OPS-BCP-001
Effective Date	Upon final approval
Review Frequency	At least annually and after activation, exercise, or material change
Approval Authority	Operations Leadership and Compliance
Version	1.0

POLICY BASIS

This policy consolidates Call Center, Provider Solutions, Provider Data & Configuration, Enrollment & Billing, and Medicare Claims Processing continuity requirements.

1. Purpose

This policy establishes the Operations Department framework for preparing for, responding to, operating through, and recovering from disruptive events. It is intended to maintain critical member, provider, enrollment, billing, provider-data, configuration, call-center, and Medicare claims functions; protect data integrity and confidentiality; preserve traceability; support applicable compliance obligations; and restore standard operations safely.

2. Scope

This policy applies to Operations leadership, employees, contractors, vendors, and supporting teams involved in the following five operating areas:

- Call Center, including Member Services, Provider Services, Quality Assurance, Workforce Management, and leadership/support teams.
- Provider Solutions intake and documentation activities tied to member and provider requests.
- Provider Data Management and Configuration, including provider roster, demographic, contracting, network participation, fee schedule, contract, and benefit configuration work.
- Enrollment and Billing, including enrollment transactions, voluntary disenrollment, demographic updates, eligibility inquiries, premium management, billing inquiries, and adjustments.
- Medicare Claims Processing, including claim intake, adjudication, pricing, adjustments, reprocessing, payment, remittance, imaging, EDI/clearinghouse connectivity, and reporting.

Note: Cognizant is vendor for Curana Health operating under the BPaaS model. Cognizant BCP will also be utilized in any continuity of business plans.

3. Policy Statement

Operations will maintain documented continuity capabilities for critical work, activate program-specific controls when normal systems, staffing, facilities, connectivity, or vendors are unavailable, use approved manual tracking and alternate workflows, communicate confirmed information, protect PHI, and reconcile all continuity-period work after restoration.

4. Definitions

TERM	DEFINITION
BCP	Business Continuity Plan used to sustain and restore critical operations during and after disruption.
BIA	Business Impact Analysis.
DR	Disaster Recovery.
RPO	Recovery Point Objective.
RTO	Recovery Time Objective.
Continuity Event	An event requiring alternate staffing, systems, facility, vendor, or manual workflow controls.
System of Record	Qnxt, EAM, TCS, DMS – all Cognizant software utilized by Curana Operations

5. Risk Events Covered

CATEGORY	EXAMPLES IDENTIFIED IN THE FIVE PLANS
Technology / Connectivity	Telephony, QNXT, EAM, ServiceNow/SNOW, DMS, TCS, internet, network, document imaging, EDI, payment/remittance, reporting, and related vendor-hosted system failures.
Cybersecurity	Ransomware, data breach, cyber incident, or access-control disruption.
Workforce	Illness, weather, public health emergency, offshore emergency/weather considerations, resulting in

CATEGORY	EXAMPLES IDENTIFIED IN THE FIVE PLANS
	reduced staffing capacity.
Facility / Environment	Fire, flood, power outage, HVAC failure, natural disaster, civil unrest, evacuation, or loss of office access.(Offshore Cognizant Resources)
Vendor / External	Cognizant or other vendor outage; interpreter, telephony, IT, document handling, system-processing, data-center, cloud, or clearinghouse disruption.

6. Governance and Responsibilities

ROLE	RESPONSIBILITY
Operations Leadership	Own the policy; coordinate cross-functional activation, prioritization, leadership communication, escalation, and return to normal operations.
Department Leaders	Activate the applicable BCP; assign work; maintain continuity tracking; coordinate staff; monitor backlog and risk; confirm recovery.
Workforce Management / Team Leads	Adjust staffing, call routing, queue coverage, schedules, and frontline support for Call Center continuity.
Operations Staff / Analysts	Log, track, process, document, and reconcile requests using approved continuity procedures.
IT / Security	Confirm access impact; support connectivity, security response, restoration, and system validation.
Vendor / Cognizant	Support system recovery, disaster-recovery execution, transactions or processing assigned by the plan, and root-cause analysis where applicable.
Compliance	Assess CMS, HIPAA, prompt-pay, member-impact, regulatory-risk, and external-reporting obligations.
Dependent Teams	Coordinate impacts and work handoffs with Provider Services, Call Center, Credentialing, Contracting, Plan Management, UM Management, and other affected functions.

7. Activation and Severity

7.1 Activation Conditions

- A critical service, system, vendor, facility, or communication channel is unavailable.
- Member, provider, enrollment, billing, network, configuration, claims, payment, or regulatory processing is at risk.
- Staffing capacity is materially reduced.
- Safety, PHI, data integrity, or cybersecurity risk exists.
- The applicable department-specific trigger in Appendix A through E is met.

CONTROL	Department-specific activation thresholds differ. The applicable appendix controls for that function; immediate safety, PHI, cybersecurity, or compliance risk must be escalated without waiting for a time threshold.
----------------	--

7.2 Severity Levels

LEVEL	CONDITION	MINIMUM RESPONSE
Level 1	Limited disruption; work remains controlled.	Use local workaround, redistribute workload, notify department leadership, and monitor.

LEVEL	CONDITION	MINIMUM RESPONSE
Level 2	Multiple queues/functions affected or required work at risk.	Activate department BCP, formal manual tracking, incident channel, scheduled updates, IT/vendor escalation, and backlog controls. Leadership notification made.
Level 3	Severe, prolonged, enterprise, cyber, or multi-department disruption.	Activate Operations incident command, executive and Compliance escalation, cross-department prioritization, vendor DR coordination, and formal recovery plan. Communication Plan activated for Members, Providers, Plan leadership.

For Level 2 & 3, implement daily scrum (or more frequently if needed)

8. Enterprise Continuity Requirements

8.1 Critical Work and Prioritization

- Continue critical work identified in the applicable department appendix.
- Pause or defer noncritical projects, QA, audits, reporting, analytics, or routine requests when necessary, consistent with each appendices priorities.
- Prioritize regulatory deadlines, member-impacting work, provider network integrity, claims aging/timeliness, call access, enrollment/disenrollment, payment/remittance, and critical escalations.
- Assign every manually tracked item an owner, priority, status, and follow-up requirement.

8.2 Manual Intake and Traceability

- Use a centralized, access-controlled BCP tracker, Microsoft List, approved spreadsheet, or approved manual form.
- Time-stamp and clearly identify continuity-related records.
- Do not complete, defer, or transfer work without logging it.
- Do not delete tracker rows; update status as work progresses.
- Store continuity records in approved shared locations and preserve physical or electronic evidence as required.

8.3 Minimum Tracker Fields

FIELD	MINIMUM CONTENT
Date / Time	Date received and relevant activity timestamps.
Department / Function	Call Center, Provider Solutions, PDM, Configuration, Enrollment, Billing, Claims, or other.
Request / Work Type	Nature of request, transaction, escalation, check issue, provider change, configuration, enrollment, billing, or claim activity.
Member / Provider / Claim Identifier	Minimum necessary identifier, when available.
Source	Portal, email, mail, call, vendor, internal team, EDI, or paper.
Brief Description	Concise description of issue, request, or work.
Priority	Critical, high, standard, or department-specific priority.
Assigned Owner	Responsible analyst, agent, manager, or vendor.
Status	New, in progress, pending restoration, completed, or other approved status.
Effective / Due Date	Regulatory, contractual, implementation, payment, or requested date.
Notes / Follow-Up	Dependencies, barriers, next action, and follow-up date.
Completed / Reconciled	Completion date and system-of-record reconciliation status.

8.4 Data Protection

- Maintain HIPAA and applicable CMS data-protection requirements.
- Use encrypted remote access and approved systems and storage.
- Do not process or pay claims outside approved systems without leadership approval.
- Maintain manual logs and audit trails and reconcile work completed during the disruption.

9. Communication Requirements

- Create an incident communication channel when needed.
- Notify affected Operations teams, IT/Security, vendors, dependencies, and Compliance based on impact. Create appropriate information to Plans, Providers and Members.
- Communicate activation, temporary workflow changes, documentation expectations, staffing constraints, backlog risk, and restoration status.
- Use only confirmed information and avoid speculative restoration timelines.
- Document material communications and decisions.

CADENCE

Call Center uses 30- to 60-minute leadership updates during active incidents; PDM/Configuration and Enrollment/Billing use 2- to 4-hour updates; Provider Solutions uses daily updates; Claims uses regular vendor status calls after notification within one business hour when its BCP is activated.

10. Recovery and Return to Normal Operations

1. Validate system access, telephony, connectivity, and required interfaces.
2. Confirm data integrity before resuming processing.
3. Review all continuity trackers, intake logs, queues, physical items, and vendor records.
4. Prioritize backlog using department-specific requirements.
5. Enter or reconcile all items in systems of record and validate accuracy and completeness.
6. Confirm completion with affected stakeholders and dependent teams.
7. Archive continuity records according to retention requirements.
8. Leadership confirms deactivation and return to standard operations.

10.1 Post-Incident Review

- Document outage duration and operational impact.
- Measure backlog or affected volume.
- Identify control gaps, risks, root causes, and improvement opportunities.
- Create and track corrective actions.
- Update the policy, appendices, trackers, contacts, and procedures as needed.

11. Training, Testing, and Maintenance

- Review the policy and departmental appendices at least annually.
- Conduct continuity exercises appropriate to department risks, including DR, pandemic, remote work, system outage, telephony, and vendor scenarios.
- For Call Center, conduct semi-annual tabletop exercises and quarterly remote-work readiness checks.
- Validate relevant vendor disaster-recovery test results for Claims Processing.
- Include continuity expectations in new-hire or role training where specified.
- Retain exercise results, attendance, findings, corrective actions, and closure evidence.

12. Monitoring

DOMAIN	EXAMPLE MEASURES
Service Access	Call availability, abandonment/service impacts, request intake, interpreter availability, alternate routing.
Work Inventory	Items received, backlog volume, aging, priority distribution, status, and completion.
Enrollment / Billing	Time-sensitive enrollment/disenrollment items, eligibility gaps, billing delays, adjustments, recovery completion.

DOMAIN	EXAMPLE MEASURES
Provider Data / Configuration	Provider terminations, regulatory updates, onboarding, network changes, configuration effective dates, directory risk.
Claims	Claim intake, adjudication, payment/remittance, aging inventory, CMS timeliness risk, reconciliation.
Systems / Vendors	Outage duration, access restoration, failover/DR status, data integrity, SLA response, vendor updates.
Compliance / Experience	Member/provider impact, complaints, PHI/security events, missed deadlines, corrective actions.

13. Records and Evidence

Operations will retain policy approvals, incident records, continuity trackers, manual forms, communications, vendor updates, exercise evidence, post-incident reviews, and corrective-action documentation in accordance with applicable organizational retention standards and any more stringent legal, regulatory, contractual, or litigation-hold requirement.

14. Exceptions and Escalation

Material deviations from this policy or a departmental BCP must document the reason, impact, temporary control, approving authority, and remediation. Suspected member harm, PHI exposure, cybersecurity incident, missed regulatory deadline, payment risk, eligibility gap, or material provider/network impact must be escalated through established channels.

15. Approval

APPROVAL ROLE	NAME / TITLE	DATE
Policy Owner	Patty Rushman, Vice President of Operations	10/01/2026

Appendix A. Call Center Business Continuity Plan

SOURCE	Business Continuity Plan - Call Center 202603
--------	---

A1. Critical Functions and Maximum Allowable Downtime

FUNCTION	MAXIMUM ALLOWABLE DOWNTIME	NOTES
Inbound call handling	0-30 minutes	Core service; must remain operational.
Interpreter services	1 hour	Secondary vendor required.
QA monitoring	24-48 hours	Noncritical during emergency.
Reporting and analytics	48-72 hours	May be delayed.

A2. Activation and Continuity Controls

- Activate when call handling is interrupted more than 10 minutes, staff cannot access systems, safety risk exists, or vendor/technology outage affects service.
- Use redundant call routing, cloud-based remote login, backup IVR, VPN, manual intake forms, daily backups, encrypted remote access, and cyber incident response.
- Cross-train agents on at least two queues and leads for frontline calls; use tiered staffing.
- Maintain primary and secondary interpreter vendors and callback process.
- Relocate to an alternate site if an on-site outage exceeds 4 hours; activate remote operations within 60 minutes.
- Restore telephony first, then CRM/eligibility, interpreter services, and reporting/QA tools.

A3. Communication and Testing

- Use email, SMS, and Teams mass notification and prewritten outage, remote-activation, and recovery templates.
- Provide leadership updates every 30-60 minutes during active incidents.
- Complete annual review, semi-annual tabletop exercises, quarterly remote-work readiness checks, and new-hire BCP overview.

Appendix B. Provider Solutions Business Continuity Plan

SOURCE	Provider Solutions Business Continuity Plan
--------	---

B1. Critical Work

- Review and assess initial claim escalations.
- Intake, acknowledge, document, and review Microsoft Lists issues as systems permit.
- Receive, log, and track member and provider portal requests.
- Log and retain evidence for returned checks and refund checks.
- Capture and track void-check issues for later system entry.

B2. Manual Controls and Recovery

- Use a centralized Excel or Microsoft List tracker with date, request type, member/provider identifier, source, owner, priority, status, notes, and completion date.
- Time-stamp and label all records as BCP-related; no work is completed without being logged.
- Redistribute work based on connectivity, alternate-tool access, and cross-trained staffing; conduct daily continuity check-ins.
- Provide daily leadership updates on volume, backlog risk, staffing, and confirmed restoration status.
- After restoration, validate logs, enter backlog into systems of record, validate accuracy, archive trackers, and close the event.

Appendix C. Provider Data & Configuration Business Continuity Plan

SOURCE	Business Continuity Plan PDM and Configuration Owners identified in source: Director Jenny Moreno and Manager Mike Taylor
---------------	---

C1. Critical Functions

TEAM	CRITICAL FUNCTIONS
Provider Data	Provider roster, demographic, contracting-data, network-participation, and termination updates.
Configuration	Fee schedule, contract, and benefit configuration.

C2. Activation, Tracking, and Priorities

- Activate when QNXT outage exceeds 30 minutes, Cognizant confirms disruption, and internal IT confirms no access; Department Leaders or Operations Leadership initiate activation.
- Log provider requests in a BCP Provider Intake Tracker and configuration work in a Configuration BCP Log using Microsoft Lists.
- Priority 1: provider terminations, compliance/regulatory updates, and contract effective-date changes.
- Priority 2: credentialed provider onboarding, address changes, and specialty updates.
- Priority 3: contract and benefit configuration updates.
- Provide incident updates every 2-4 hours and notify Credentialing, Contracting, Plan Management, and UM Management.
- After restoration, validate access/data integrity, review logs, prioritize, enter updates, and confirm completion.

Appendix D. Enrollment & Billing Business Continuity Plan

SOURCE	BCP Enrollment Billing Source owner: Manager Stephanie Beringer
--------	---

D1. Critical Functions

- Enrollment adds, changes, terminations, and voluntary disenrollment.
- Demographic updates and eligibility-related inquiries.
- Billing processing, premium management, billing inquiries, and adjustments.

D2. Activation, Workaround, and Priorities

- Activate when outage exceeds 30 minutes, Cognizant confirms disruption, internal IT confirms loss of access, and Enrollment & Billing leadership initiates the plan.
- Log all requests in a centralized tracker; use email if ServiceNow is unavailable; manually track submissions and statuses.
- Validate and queue enrollment requests when EAM is unavailable. The source plan states that Cognizant will process enrollment transactions directly in MARx as needed when EAM is unavailable.
- Log billing issues and communicate delays when QNXT is unavailable; assign every request an owner and update status daily.
- Priority 1: regulatory or time-sensitive enrollments and disenrollments. Priority 2: member-impacting changes and billing issues. Priority 3: routine inquiries.
- Provide updates every 2-4 hours. After restoration, validate access/data integrity, reconcile the tracker, prioritize backlog, complete work, and confirm completion.

Appendix E. Medicare Claims Processing Business Continuity Plan

SOURCE	Business Continuity Plan Claims Processing Vendor-hosted environment with disaster recovery and pandemic recovery
--------	---

E1. Recovery Objectives

FUNCTION	PRIORITY	RTO	RPO
Claim intake: EDI and paper	High	24 hours	4 hours
Claims adjudication	High	48 hours	24 hours
Payment and remittance	High	72 hours	24 hours
Adjustments and reprocessing	Medium	5 business days	48 hours

E2. Activation and Continuity Controls

- Activate when vendor systems are unavailable more than 48 hours, vendor DR failover starts, pandemic conditions materially reduce staffing, or CMS timeliness thresholds are at risk.
- Require geographically separate primary and secondary vendor environments, routine backups/recovery testing, documented RTO/RPO commitments, and vendor notification of DR activation.
- Suspend noncritical claims work, manually track claim receipt, prioritize claims nearing CMS limits, and validate data integrity before normal processing.
- Enable remote work where possible; cross-train with the vendor; reassign staff by volume/timeliness risk; use approved overtime or surge staffing if required.
- Focus on clean claims and high-risk aging inventory; defer nonessential projects/audits; conduct daily workload and backlog review; reroute claims mailbox as required.
- Notify Operations, Compliance, and IT leadership within one business hour, establish regular vendor status calls, communicate impact to Provider Services and Call Center, and document actions.
- Do not process or pay outside approved systems without leadership approval; retain audit logs and reconcile continuity-period claims.

Appendix F. Operations Incident Checklist

- ☐ Date/time identified and source of alert
- ☐ Affected department(s), systems, vendors, and locations
- ☐ Severity level and applicable appendix activation trigger
- ☐ Activation decision and approving leader
- ☐ Safety, member, provider, financial, privacy/security, and compliance impact
- ☐ Critical work and priority decisions
- ☐ Staffing, remote-work, queue, and alternate-site actions
- ☐ Manual tracker location and assigned owners
- ☐ Internal, vendor, dependency, and Compliance notifications
- ☐ Status update cadence and confirmed restoration information
- ☐ System/access/data-integrity validation
- ☐ Backlog inventory and prioritization
- ☐ System-of-record reconciliation and accuracy review
- ☐ Stakeholder completion confirmation
- ☐ Outage duration, affected volume, gaps, root cause, and corrective actions
- ☐ Event closure and record archiving

Appendix G. Source Plans

- Business Continuity Plan- Call Center 202603.pdf
- Provider Solutions Business Continuity Plan.pdf
- Business Continuity Plan PDM and Configuration.pdf
- BCP_Enrollment_Billing.pdf
- Business Continuity Plan Claims Processing.pdf

Change Log

VERSION	DATE	CHANGE	OWNER
1.0	Upon approval	Initial Operations policy consolidating five departmental continuity plans.	Operations Leadership

EMERGENCY PREPAREDNESS & BUSINESS CONTINUITY POLICY

Clinical Programs

Enterprise framework with program-specific Business Continuity Plans for Utilization Management and Care Management / Model of Care

DOCUMENT CONTROL	DETAIL
Organization	Curana Health
Document Owner	Maureen Murray, VP Clinical Programs
Department	Clinical Programs
Policy Number	CP-BCP-001
Effective Date	Upon final approval
Review Frequency	At least annually and after activation, exercise, or material change
Approval Authority	VP Clinical Programs
Version	1.0
Classification	Confidential and Proprietary

POLICY INTENT	One enterprise policy governs emergency preparedness and business continuity across Clinical Programs. Appendices A and B contain the operational BCP requirements for UM and CM/MOC, respectively.
----------------------	--

1. Purpose

This policy establishes the enterprise Clinical Programs framework for preparedness, response, continuity, recovery, and restoration during disruptive events. It is designed to protect member safety, maintain access to medically necessary care, continue time-sensitive clinical and regulatory functions, safeguard protected health information (PHI), and support orderly return to normal operations.

This policy incorporates program-specific Business Continuity Plans (BCPs) for Utilization Management (UM) and Care Management / Model of Care (CM/MOC). The enterprise requirements in the body of this policy apply to both programs; the appendices define each program's critical functions, priorities, recovery objectives, downtime controls, and evidence requirements.

2. Scope

This policy applies to employed and contracted Clinical Programs personnel, medical leadership, supporting departments, delegated entities, downstream entities, and vendors whose services directly or indirectly affect member care, clinical determinations, care coordination, Model of Care execution, or required clinical reporting.

3. Policy Statement

Curana Health Clinical Programs will maintain documented, tested, and recoverable operations that prioritize people, member safety, continuity of care, regulatory timeframes, and data protection. During a disruption, Clinical Programs will activate a coordinated incident structure, continue critical functions through approved alternate workflows, document decisions and deferred work, and reconcile all activity after restoration.

2.1 Covered Functions

PROGRAM	FUNCTIONS IN SCOPE
Utilization Management	Prior authorization; concurrent and retrospective review; organization determinations; medical director review; provider/member notifications; clinical documentation; delegated UM oversight; regulatory and accreditation reporting.
Care Management / MOC	Care management and complex case management; behavioral health and SDoH coordination; transitions of care; HRA; risk stratification; ICP; ICT; member outreach; MOC training; performance monitoring; delegated oversight.
Shared Clinical Support	Quality Improvement; Appeals & Grievances support; Pharmacy; Member Services; Provider Services; Compliance; IT/Security; reporting and analytics; vendor management.

4. Definitions and Acronyms

TERM	DEFINITION
BCP	Business Continuity Plan used to sustain and restore critical operations during and after an interruption.
CM	Care Management.
EPI	Emergency Performance Interruption or other event materially affecting required services.
EPBCP	Emergency Preparedness and Business Continuity Plan.
HRA	Health Risk Assessment.
ICP	Individualized Care Plan.
ICT	Interdisciplinary Care Team.

MOC	SNP Model of Care.
RPO	Recovery Point Objective, or the acceptable amount of data loss measured in time.
RTO	Recovery Time Objective, or the target time to restore a function.
UM	Utilization Management.

5. Governance and Accountability

ROLE	ENTERPRISE RESPONSIBILITY
VP Clinical Programs / Incident Commander	Owns the policy; authorizes activation and deactivation; establishes priorities; coordinates executive escalation; approves temporary operating standards within authority.
Chief Medical Officer / Medical Leadership	Provides clinical oversight; supports urgent clinical and medical-necessity decisions; approves temporary clinical operating standards.
UM Leadership	Maintains the UM BCP; prioritizes determinations; assigns coverage; monitors turnaround times and notifications; manages UM backlog recovery.
CM/MOC Leadership	Maintains the CM/MOC BCP; prioritizes high-risk members, transitions, HRA/ICP/ICT activities, member outreach, and MOC evidence; manages CM backlog recovery.
Quality / MOC Lead	Monitors MOC requirements, performance measures, evidence, corrective actions, and governance reporting.
IT / Security	Coordinates technical incident response, access, restoration, cybersecurity controls, and data-integrity validation.
Compliance / Privacy	Assesses regulatory, contractual, accreditation, privacy, breach, and external reporting obligations.
Communications / Member Services	Coordinates consistent internal and external communications and alternate contact pathways.
Vendor / Delegate Owner	Escalates service disruption, obtains continuity evidence, tracks remediation, and validates recovery commitments.

AUTHORITY	The Incident Commander may delegate operational authority but retains accountability for coordinated Clinical Programs response and closure.
------------------	---

6. Events Covered and Activation

CATEGORY	EXAMPLES
Technology	Clinical platform, UM platform, EHR, data interface, network, telephony, fax, LMS, or reporting outage; cybersecurity or ransomware event.
Workforce	Pandemic, public health emergency, mass absenteeism, labor disruption, or key staff unavailability.
Facility / Environmental	Fire, flood, severe weather, utility failure, evacuation, or inaccessible workplace.

External / Government	Federal or state emergency or disaster declaration, public health emergency, or CMS emergency performance interruption.
Vendor / Delegate	Interruption of delegated UM, care management, communications, training, analytics, or other critical vendor services.

6.1 Activation Criteria

- Member safety or continuity of care is at risk.
- A critical system, data feed, facility, or communication channel is unavailable.
- UM decision or notification timeframes may be missed.
- HRA, ICP, ICT, transition, outreach, training, or MOC reporting requirements may be missed.
- Workforce capacity is materially reduced or key coverage is unavailable.
- A cybersecurity event, declared emergency, evacuation, or vendor failure affects operations.
- Leadership determines coordinated incident command is necessary.

IMMEDIATE ESCALATION	Operational thresholds do not delay immediate escalation when member safety, PHI, data integrity, or regulatory compliance is at risk.
-----------------------------	---

6.2 Incident Severity Levels

LEVEL	CONDITION	RESPONSE
Level 1	Limited disruption; critical work remains controlled.	Redistribute work, use cross-coverage, pause noncritical activities, and use approved overtime or alternate workflows.
Level 2	Moderate capacity or system reduction; deadlines or service levels at risk.	Activate program BCP; centralize prioritization; increase leadership/IT/Compliance cadence; implement formal downtime tracking.
Level 3	Severe, sustained, enterprise, cyber, or multi-program interruption.	Activate enterprise incident command; consider vendor/temporary support; executive staffing review; formal external notification assessment.

7. Enterprise Prioritization Standards

TIER	REQUIRED PRIORITY	TARGET
Tier 1	Member safety interventions; urgent clinical escalation; expedited/urgent authorizations; concurrent review; acute-event and transition tracking; medication or critical social-service access.	Immediate / continuous
Tier 2	Standard authorizations and organization determinations; post-discharge follow-up; medication reconciliation; HRA; ICP; ICT; provider and member communications.	Within applicable regulatory, contractual, MOC, and clinical timeframes
Tier 3	Routine analytics, audits, trend reporting, nonurgent training administration, and noncritical projects.	Resume according to program BCP and approved recovery plan

PRECEDENCE	Regulatory, contractual, accreditation, state, plan-specific, or member-clinical requirements take precedence when more stringent than internal targets.
-------------------	---

8. Core Continuity Requirements

8.1 Member Safety and Continuity of Care

- Prioritize clinically unstable, recently discharged, high-utilization, medication-dependent, behaviorally at-risk, and socially vulnerable members.
- Maintain access to emergency and urgently needed services; emergency screening and stabilization may not be delayed by routine authorization processes.
- Continue acute-event notification, discharge planning, post-discharge follow-up, medication reconciliation, red-flag education, and care-plan updates using available information.
- Document deferred activity and reason when disruption prevents timely completion, then prioritize reconciliation by clinical and compliance risk.

8.2 Staffing and Succession

- Maintain designated primary and backup coverage for critical leadership and operational roles.
- Maintain current contact lists, competence/cross-training records, and workload reassignment procedures.
- Use staff only within licensure, certification, competency, and authorized scope.
- Provide applicable MOC, privacy, downtime, and role-specific instructions before emergency reassignment.

PRIMARY ROLE	MINIMUM CONTINUITY COVERAGE
VP Clinical Programs	Director of UM, Director of Care Management, or designated clinical leader
Director of UM	UM Manager or designated UM leader
UM Medical Director	Alternate qualified Medical Director
Director of Care Management	Care Management Manager or designated clinical leader
Care Management Supervisor	Senior Care Manager or designated supervisor
Care Manager / Care Ally	Cross-trained care manager or assigned coverage pool
MOC / Quality Lead	Quality or MOC specialist
Training Lead	Designated clinical training or Compliance backup

8.3 Technology, Privacy, and Downtime

- Use secure VPN, multifactor authentication, approved cloud access, approved telephony, and encrypted communication tools.
- Use approved downtime forms and controlled logs with unique tracking identifiers.
- Apply role-based access and minimum-necessary PHI standards.
- Store downtime records only in approved secure locations.
- Do not send PHI through personal email, consumer messaging applications, or unapproved storage.
- After restoration, enter and reconcile downtime activity in the system of record, validate completeness, resolve duplicates, and close the downtime log.

8.4 Delegated and Downstream Entities

- Contracts or oversight tools must include continuity, notification, data protection, recovery, and evidence expectations for critical delegated functions.
- Continuity readiness will be evaluated through applicable pre-delegation review, annual oversight, audit, attestation, testing evidence, monitoring, or corrective action.
- Delegates must promptly report material disruption, member impact, missed requirements, interim controls, recovery status, and corrective actions.
- Program owners must maintain contingency options when a delegate cannot perform the required function.

9. Incident Communication and Documentation

9.1 Internal Communication

Initial and recurring communications will identify the incident, affected functions, member and compliance risk, interim controls, decision owner, open dependencies, and next update cadence. Notification groups may include Clinical Programs leadership, Medical Leadership, Compliance, Privacy, IT/Security, Quality, Member Services, Provider Services, vendor owners, and executive leadership.

9.2 External Communication

When applicable, authorized communications will provide service impacts and alternate contact or submission methods to members, caregivers, providers, facilities, delegates, health plan partners, vendors, and regulatory authorities. External communications must be coordinated with Compliance and authorized leadership.

9.3 Incident Record

- Date/time identified; incident description; affected systems/functions; severity level.
- Activation decision and approving leader; incident roster and coverage assignments.
- Member, provider, regulatory, contractual, privacy, and delegate impact assessment.
- Critical populations/cases and priority decisions.
- Communications issued and alternate channels used.
- Downtime logs, manual tracking, exceptions, and approvals.
- Restoration validation, data-integrity confirmation, backlog reconciliation, and closure.
- After-action findings, corrective action owners, due dates, status, and evidence of completion.

10. Recovery, Reconciliation, and Resumption

1. Validate system availability, security, interfaces, telephony, and data integrity.
2. Reconcile downtime records with systems of record and remove duplicate entries.
3. Identify overdue UM determinations, notifications, HRAs, ICPs, ICT activities, transitions, outreach, referrals, training, and reporting.
4. Prioritize backlog by member risk, regulatory/contractual timeframe, clinical urgency, and age of work.
5. Confirm completion, document exceptions, quantify residual risk, and report unresolved issues.
6. Obtain Incident Commander authorization to close the incident and resume standard operations.

10.1 After-Action Review

Following an exercise or actual activation, Clinical Programs will document the event, effectiveness of controls, member and compliance impact, lessons learned, corrective actions, accountable owners, due dates, and closure evidence. Material findings will be reported through applicable UM, CM/MOC, Quality, Compliance, delegation, and executive governance channels.

11. Testing, Training, and Maintenance

- Review this policy and both program BCPs at least annually and after material organizational, regulatory, system, vendor, workflow, or MOC changes.
- Conduct at least one annual tabletop exercise or document qualifying use during an actual disruption.
- Include scenarios such as UM or CM platform outage, cyber event, severe weather, staffing shortage, telephony failure, data-interface failure, and delegate failure.
- Train applicable staff on activation, downtime, escalation, privacy, member prioritization, communication, and recovery duties.
- Retain exercise plans, attendance, results, corrective actions, and evidence of closure.

12. Monitoring and Compliance Metrics

DOMAIN	EXAMPLE MEASURES
Member Safety	Urgent escalations; unresolved critical needs; successful high-risk outreach; delayed access to care.
UM	Expedited and standard timeliness; concurrent review timeliness; notification timeliness; downtime backlog; medical director escalations.

CM / MOC	HRA and ICP timeliness; ICT activity; transition follow-up; medication reconciliation; unreachable/refusal counts; backlog.
Operations	System downtime; staffing availability; workload volume; age of backlog; reconciliation completion; recovery time.
Privacy / Security	Unauthorized channels identified; data-integrity issues; privacy incidents; secure disposal or transfer of downtime records.
Delegate Oversight	Disruptions reported; continuity evidence; missed requirements; corrective actions; recovery validation.
Experience / Equity	Complaints; language/accessibility barriers; social-needs disruption; equitable outreach and alternate communications.

13. Records Retention and Evidence

Policy approvals, completion records, incident logs, downtime records, decision records, communications, exercise evidence, after-action reviews, and corrective action documentation will be retained in accordance with applicable organizational record-retention requirements and any more stringent regulatory, contractual, accreditation, litigation-hold, or plan-specific requirement.

14. Exceptions and Noncompliance

Any material deviation from this policy or a program BCP must be documented with the reason, member and compliance impact, temporary control, approving authority, and remediation plan. Suspected privacy, security, regulatory, or member-safety concerns must be escalated immediately through established reporting channels.

15. Approval and Annual Review

APPROVAL ROLE	APPROVER	DATE
Business Owner / Program Approval	Maureen Murray, Vice President of Clinical Programs	10/01/2026

Appendix A. Business Continuity Plan - Utilization Management

OWNERSHIP	Program Owner: Director, Utilization Management Executive Owner / Incident Commander: VP Clinical Programs
------------------	---

A1. UM Scope and Objectives

- Maintain access to medically necessary services and continue time-sensitive UM determinations.
- Meet applicable CMS, state, contractual, and accreditation requirements.
- Protect PHI and maintain provider, member, delegate, vendor, and regulator communications.
- Restore normal UM operations safely and reconcile all downtime activity.

A2. Critical UM Functions and Recovery Priority

PRIORITY	FUNCTION	RECOVERY OBJECTIVE
Tier 1	Urgent or expedited prior authorizations	Immediate
Tier 1	Concurrent review	Immediate
Tier 1	Hospital notifications, discharge planning, and transition coordination	Immediate
Tier 1	Medical Director escalations	Immediate
Tier 2	Standard prior authorizations	Within 24 hours or more stringent applicable timeframe
Tier 2	Organization determinations and required notices	Within applicable regulatory timeframes
Tier 2	Provider and member communications	Within 24 hours or more stringent applicable timeframe
Tier 3	Reporting and analytics	Within 72 hours
Tier 3	Quality audits and trend reporting	Within 5 business days

A3. UM Recovery Objectives

FUNCTION	RTO	RPO
Expedited authorizations	4 hours	1 hour
Concurrent review	4 hours	1 hour
Standard authorization processing	24 hours	4 hours
Appeals support	24 hours	4 hours
Reporting and analytics	72 hours	24 hours

CONTROL

These are internal operating objectives. Applicable decisions and notification requirements remain controlling when more stringent.

A4. UM Continuity Strategies

Staffing

- Crosstrain staff across intake, authorization, concurrent review, retrospective review, appeals support, and provider communication as appropriate.
- Maintain competency and cross-coverage records.
- Use Level 1 redistribution/overtime, Level 2 cross-trained redeployment, and Level 3 temporary staff, clinical vendor support, and executive staffing review.
- Maintain succession coverage for VP Clinical Programs, Director of UM, UM Manager, Medical Director, and UM Supervisor roles.

Technology and Downtime

- Use approved downtime authorization forms and assign a unique identifier to each request.
- Record receipt time, urgency, requested service, clinical information, reviewer, criteria source, decision, notification, and unresolved follow-up.
- Apply approved clinical criteria using authorized offline resources; escalate cases requiring physician review to an available qualified Medical Director.
- Use approved alternate provider submission and notification channels.
- Enter and reconcile all transactions after restoration and validate required notices and timestamps.

Vendor and Delegate Continuity

- Maintain current contacts, escalation paths, and alternate channels.
- Review applicable delegate continuity and recovery evidence through oversight processes.
- Require vendors and delegates performing UM functions to maintain tested continuity capabilities and notify Curana Health of material disruption.

A5. UM-Specific Activation Triggers

- A UM disruption exceeds the locally defined operational tolerance or required turnaround times are at risk.
- Urgent/expedited, concurrent, organization determination, or notification functions cannot be performed through normal channels.
- Material workforce loss prevents safe workload coverage.
- A cybersecurity or data-integrity issue affects UM operations.
- A vendor, delegate, or communication channel failure affects authorization intake, review, decision, or notice delivery.

A6. UM Recovery and Monitoring

- Validate systems, criteria access, decision queues, interfaces, timestamps, and notice generation.
- Reconcile downtime cases, prioritize urgent and oldest regulatory work, and confirm completion or exception status.
- Monitor expedited and standard timeliness, concurrent review timeliness, authorization turnaround, complaints, staffing availability, backlog age/volume, system recovery, and compliance exceptions.
- Complete and retain UM after-action findings and corrective actions through UM and Compliance governance.

Appendix B. Business Continuity Plan - Care Management and Model of Care

OWNERSHIP	Program Owner: Director, Care Management / MOC Program Lead Executive Owner / Incident Commander: VP Clinical Programs
------------------	---

B1. CM/MOC Scope and Objectives

- Maintain continuity of care management, care coordination, behavioral health and social-needs support, and transitions of care.
- Protect high-risk and vulnerable members and preserve HRA, risk stratification, ICP, ICT, outreach, training, and performance-monitoring functions.
- Maintain members, caregiver, provider, facility, and delegated-entity communications.
- Restore normal operations and reconcile deferred activity promptly.

B2. Critical CM/MOC Functions and Recovery Priority

PRIORITY	FUNCTION	TARGET RECOVERY
Tier 1	Member safety intervention and urgent clinical escalation	Immediate
Tier 1	High-risk member triage and outreach	Immediate
Tier 1	Hospital, emergency department, and transition-of-care tracking	Immediate
Tier 1	Medication access and critical social-service escalation	Immediate
Tier 2	Post-discharge follow-up and medication reconciliation	Within required MOC and quality timeframes
Tier 2	HRA administration and risk stratification	Within applicable MOC timeframes
Tier 2	ICP development, updates, and distribution	Within applicable MOC timeframes
Tier 2	ICT communication and coordination	Within applicable MOC timeframes
Tier 3	MOC training administration and completion evidence	Resume within 30 days
Tier 3	MOC reporting, monitoring, audit, and quality review	Resume within 30 days

B3. Population and Service Continuity

High-Risk and Vulnerable Members

- Prioritize active clinical instability, recent acute utilization, complex medication needs, behavioral health risk, caregiver instability, or urgent social needs.
- Use assigned backup staff and approved alternate contact methods.
- Escalate immediate threats through approved clinical and emergency pathways.

Transitions of Care

- Continue monitoring available admission, emergency department, discharge, and transfer.
- Complete post-discharge outreach, medication reconciliation, red-flag education, ICP updates, and follow-up coordination within applicable requirements.

- Document deferred activity and prioritized reconciliation after restoration.

HRA, ICP, and ICT

- Prioritize new, annual, change-in-condition, and high-risk HRAs; retain completion, refusal, and unable-to-contact evidence.
- Continue risk stratification using available HRA, utilization, clinical, functional, cognitive, psychosocial, and behavioral health information.
- Maintain and update ICPs using secure alternate workflows; preserve member preferences, barriers, referrals, and unresolved needs.
- Maintain ICT coordination through virtual, telephonic, or controlled asynchronous review and document participation, input, and decisions.

Behavioral Health and Social Needs

- Maintain crisis escalation and emergency referral pathways.
- Prioritize food, housing, transportation, medication, caregiver, durable medical equipment, language, and accessibility disruptions.
- Coordinate with providers, facilities, caregivers, pharmacies, and community resources using approved alternate channels.

B4. CM/MOC Downtime Procedure

7. Open the approved CM/MOC downtime log and assign a unique tracking identifier.
8. Record member contact, assessment, risk, HRA/ICP/ICT impact, transition activity, escalation, referral, barrier, outcome, owner, follow-up, and due date.
9. Store records securely and limit PHI to the minimum necessary.
10. After restoration, transfer information to the system of record, reconcile duplicates and missing elements, review overdue work by risk, and document closure.

B5. MOC Training Continuity

- Continue or reschedule required training through approved LMS, web-based, virtual instructor-led, recorded, or controlled manual alternatives.
- Retain content, attendance/completion reports, attestations, reminders, escalations, and contractor evidence.
- Reconcile deferred completions and report unresolved noncompliance through established governance.
- Ensure emergency reassigned staff receive applicable MOC and role-specific instruction before performing assigned work.

B6. CM/MOC Recovery and Monitoring

- Validate care management platform access, data feeds, interfaces, reporting, and data integrity.
- Identify overdue HRAs, ICPs, ICT activity, transition follow-up, outreach, referrals, training, and reporting.
- Prioritize member-facing backlog by clinical risk, required timeframe, social vulnerability, and age of work.
- Monitor urgent escalations, high-risk outreach, HRA/ICP/ICT completion, transition follow-up, medication reconciliation, complaints, accessibility barriers, staffing, backlog, and delegate compliance.
- Complete and retain CM/MOC after-action findings and corrective actions through applicable governance.

Appendix C. Incident Documentation Checklist

- ☐ Date and time identified
- ☐ Incident description and affected systems/functions
- ☐ Severity level and activation decision
- ☐ Approving leader and incident roster
- ☐ Member, provider, privacy, regulatory, accreditation, and contractual impact
- ☐ Critical population, cases, and caseload priorities
- ☐ Staffing changes and coverage assignments
- ☐ Communications issued and alternate contact methods
- ☐ Downtime records and manual tracking
- ☐ UM decision/notice impacts
- ☐ HRA, ICP, ICT, transition, outreach, training, and reporting impacts
- ☐ Vendor/delegate impact and escalation
- ☐ System restoration and data-integrity validation
- ☐ Backlog reconciliation and exception reporting
- ☐ After-action findings, owners, due dates, and closure evidence

Appendix D. Minimum Downtime Log Fields

FIELD	REQUIRED CONTENT
Tracking ID	Unique downtime identifier
Program / Function	UM, CM, MOC, HRA, ICP, ICT, transition, authorization, concurrent review, notice, outreach, referral, training, reporting, or other
Member / Case	Minimum necessary member or case identifier
Date / Time	Receipt, activity, contact, decision, notice, escalation, or restoration timestamp
Priority	Urgent, expedited, high, routine, deferred, or program-specific tier
Request / Activity	Service request, assessment, contact, decision, action, or barrier
Clinical / Regulatory Due Date	Applicable decision, notification, outreach, MOC, contractual, or follow-up deadline
Action / Outcome	Work completed, decision, notification, contact result, referral, or unresolved issue
Owner	Assigned staff, leader, vendor, or team
Follow-Up	Next action and due date
PHI Location	Approved secure storage location
Reconciled	System entry date, reviewer, duplicate check, and closure status

Appendix E. Reference Basis

- Emergency Preparedness and Business Continuity Plan - Care Management and Model of Care Program
- Emergency Preparedness and Business Continuity Plan - Utilization Management Program

- BCP_UM_2025
- Applicable Model of Care continuity and emergency preparedness narratives
- Specific Factor Review
- UM program and continuity-of-care policies
- Applicable CMS, state, contractual, privacy/security, accreditation, and organizational requirements

Note: Program leaders and Compliance will validate citations, policy cross-references, retention schedules, external reporting obligations, and plan-specific requirements before controlled publication.

Change Log

VERSION	DATE	CHANGE	OWNER
1.0	Upon approval	Initial enterprise Clinical Programs policy consolidating governance and incorporating UM and CM/MOC Business Continuity Plans.	VP Clinical Programs