Gold Coast Health Plan℠
A Public Entity

POLICY AND PROCEDURE	
TITLE: Business Continuity and Emergency Response	
DEPARTMENT: Compliance, IT Infrastructure & Security	**POLICY #:** HI-060
EFFECTIVE DATE: 05/01/2025	**REVIEW/REVISION DATE:** 05/01/2025
COMMITTEE APPROVAL DATE: 07/03/2025	**RETIRE DATE:** Not Set
PRODUCT TYPE: Medi-Cal	**REPLACES:** Not Set

I. Purpose

A. Gold Coast Health Plan (GCHP) will ensure that Business Continuity and Emergency Preparedness and Response plans are developed and in place in the event of an emergency or other disruption to GCHP business operations.

B. This policy defines the requirement for a baseline business continuity plan and emergency recovery processes to be developed and implemented by GCHP that will describe the processes to recover IT systems, applications, data, and other critical business functions from any type of emergency or event that causes a major outage or long-term disruption to GCHP business operations.

C. The intent and goals of Business Continuity and Emergency Preparedness and Response plans are:

1. Provide an orderly and efficient transition from normal to emergency conditions.
2. Provide specific guidelines appropriate for complex and unpredictable occurrences.
3. Provide consistency in action
4. Establish a threshold at which an emergency response is triggered and determine who may declare an emergency event.
5. Determine Recovery Time Objectives (RTO) and Recovery Point Objective (RPO).

II. Policy

1. GCHP will ensure that it is able to continue its business operations and access its information without unacceptable delay in the event of an emergency or other occurrence that will affect business operations.
2. GCHP will establish a Business Continuity Program and recovery plans to address such emergencies and occurrences.
3. GCHP will establish an Emergency Preparedness and Response Plan as part of its Business Continuity Program in order to prepare, plan, and respond to emergency events that may affect GCHP business operations, Members, Network Providers, Subcontractors, or Downstream Subcontractors.
4. GCHP will establish procedures as part of the Business Continuity Program for responding to an emergency or other occurrence that damages systems that contain electronic protected health information (ePHI).

III. Definitions

Confidential Information: is information classified as "Confidential" by GCHP which is either protected by applicable law regarding access or disclosure of the information or information that is classified as confidential by GHCP based upon its sensitivity or that the information should be tightly restricted based upon the concept of need-to-know.

Emergency: means unforeseen circumstances that require immediate action or assistance to alleviate or prevent harm or damage caused by public health crises, natural and man-made hazards, or disasters.

Emergency Preparedness: means a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during emergency incident response.

Information System: means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. (45 CFR § 164.304)

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, and its implementing regulations.

HIPAA Security Rule: are the implementation regulations under the "HIPAA Administrative Simplification Regulations" regarding the security standards for the protection of electronic protected health information ("EPHI") which includes security standards based around administrative, physical, and technical safeguards. (45 CFR Part 160 Subpart A – Definitions - and Part 164 Subpart C

– Security Standards for the Protection of Electronic Protected Health Information).

Protected Health Information (PHI): is individually identifiable health information, which is health information that is:

1. Is created or received by a health care provider, health plan, employer, or health care clearing house; and
2. Relates to the past present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   - i. That identifies the individual; or
   - ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI can be transmitted by electronic media, maintained by electronic media, or transmitted or maintained in any other form or medium.

PHI does not include education records covered by the Family Educational Rights and Privacy Act (FERPA), employment records held by a covered entity in its role as an employer, or health information regarding any person who has been deceased for more than 50 years. (45 CFR § 160.103)

IV. Procedure

A. Business Continuity Program – The use of proactive planning and measures to avoid or mitigate risks associated with a disruption of GCHP's business operations, with a specific focus upon risks to its information systems and business processes.

2. Business Continuity Plan (BCP) – The following business contingency steps will be conducted to plan for an Emergency or other event occurring that will require the implementation of the BCP and assist in development of response plans.

   a. Emergency Response Plans – Plans to identify who is to be contacted, when, and how. Define procedures for certain Emergency events that trigger occurrences and what immediate actions must be taken for specific Emergency events.

   b. Succession Procedures – Procedures that describes the flow of responsibility for specific Emergency events that trigger BCP operations. Identifies various Emergency Response staff, business support vendors, Network Providers, and community contacts.

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the controlled version published online prevails.

c. Criticality of Service List – Lists all services and business functions and the criticality of their importance in maintaining operations under BCP operations.

d. Recovery Plans – Explains the order of recovery of systems and business operations affected in both short-term and long-term timeframes.

e. Data Backup and Restoration Plan – Details which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It will also describe how that data could be recovered under BCP operations.

f. Equipment Replacement Plan – Describes what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

g. Communication Plan – Describes the procedures and responsibilities for communication during BCP operations.

3. <u>Emergency Mode Operational Procedures</u> – GCHP will ensure that necessary requirements around the confidentiality of information such as protected health information ("PHI") are maintained, including necessary procedures are established when in emergency operational mode for workforce to access confidential data.

4. <u>Application and Data Criticality Assessment</u> – GCHP will assess the relative criticality of specific applications and data for developing plans for Data Backup and Recovery, Disaster Recovery, and Emergency Mode Operations.

5. <u>Facility Emergency Access Procedures</u> – GCHP will address its business continuity planning in physical security policies and procedures to ensure facility access in support of data recovery during BCP operations in the event of any an emergency.

6. <u>Business Continuity and Emergency Response Resources</u> – GCHP as part of planning and development of BCP, will define the staffing and resources necessary to conduct continued development, planning, and testing of BCP operations.

B. <u>Emergency Preparedness and Response Plans (Plan)</u> – Emergency Preparedness and Response plans will be developed to provide necessary procedures and protocols for how GCHP responds to various emergency events that would cause the implementation of BCP processes and procedures. Emergency response recovery will be enacted to ensure recovery or continuing operations of GCHP business operations from an

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the controlled version published online prevails.

emergency event that triggers such a response. The emergency response recovery plans will address critical business operation recovery activities.

1. Plan Events – The Plan must define Emergency events that can cause interruptions to business processes, along with the probability and impact of such interruptions and their consequences to GCHP business operations.

2. System Recovery Process – The Plan must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.System Recovery Sites – These system recovery sites can be configured in various states to provide the ability to recover from an emergency event, either fully or partially.

   a. Hot Site - This indicates the site is "live" and redundant to the main production site. A hot site may balance the load of the business interactions however it must be able to manage all connections in a stand-alone configuration should one site become unavailable.

   b. Warm Site - This type of site may provide some live services but is not required to provide services to GCHP members should it be unavailable. A warm site is generally a replication of services, but not available to GCHP Members until an Event has been declared. Any Warm Sites will have Recovery Time Objective (RTO) set and approved by Management in order to meet the goals of bringing the site to a live state.

   c. Cold Site - A cold site is where a collective or cloud service provider has been, or can be, acquired, however there are no servers, applications, or configurations in place. A cold site is for Companies that have the ability to provide an RTO without having infrastructure in place.

C. Emergency Response Team Staffing and Responsibilities – GCHP will identify a primary Emergency Response Team (Team) that will consist of a broad Team from across the organization. Further additional Team back-up support or specific business area representatives that may be necessary to support the Team based upon the Emergency Response event. The Team will be defined in the BCP along with the responsibilities for the team.

1. Team Responsibilities – The Emergency Response team will ensure specific designated responsibilities will be defined and understood by team members. The responsibilities will include, but not limited to, sending out Emergency communications to staff, Network Providers, Subcontractors, Downstream Subcontractors, Members, managing site

security, staff responsible for securing utilities, and other essential persons and entities.

2. Team Communication – Emergency Response procedures will ensure that team members have means of communicating with the Emergency Response team to report their status and ability to support the team during and after an Emergency.

D. Emergency Communications – Communication plans and procedures will be developed to ensure necessary communication with GCHP staff, business operation support vendors, Network Providers, Subcontractors, Downstream Subcontractors, DHCS, and other essential persons and entities during a disaster or Emergency Response event.

1. Emergency Response Communications – As a part of the Emergency Response Plans GCHP will ensure that emergency communications are provided to GCHP staff and all other impacted parties that are part of emergency communication plans and procedures.

   a. Emergency Staff Communications – GCHP will provide necessary communications to Staff on the impact of event, BCP procedures and methods in place, and recovery status during BCP operations

   b. External Emergency Communications – GCHP will ensure a system and process is in place to provide necessary communications and updates to Network Providers, business support vendors, Subcontractors, Downstream Subcontractors and other necessary external entities during as part of Emergency Response protocols.

2. Emergency Contact Information – GCHP will ensure that contact information is kept and readily available during an emergency as part of the Emergency Response communications which would include information such as contact name, title or position, physical location address, mailing address, telephone and/or cell phone, text, e-mail, and social media. Contact information must be updated as contract information changes, and changes must occur no less than every six (6) months.

E. Member Emergency Preparedness and Communication Plans – GCHP will maintain Member Emergency Plans specific to Members' needs during an Emergency, including Members in Long-Term Care facilities, Skilled Nursing Facilities, or other institutional settings; and for Members with disabilities, limitations in activities of daily living, and/or cognitive impairments. These Member Emergency Plans will be to ensure coordinating necessary communications to ensure Member access to health care services in the event of an Emergency.

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the controlled version published online prevails.

1. <u>Member Communication</u> – GCHP will ensure that various methods are available to provide communications to Members along with emergency protocols for the GCHP Member Contact Center.

    a. Member Emergency Protocols – GCHP will develop various processes, procedures, and staff training which will include some of the following:

        i. Call scripts to account for different Member needs and accounting for different emergency scenarios.

        ii. Contact Center staff training on crisis response.

        iii. Emergency protocols that address access to Covered Services, included warm hand-offs for Member needing immediate assistance to medical or emergency personnel.

    b. Emergency and Post-Emergency Communications – Member emergency communications during and post-emergency will include all of the following instructions to members if needed.

        i. Notify Members about available alternative primary pharmacy, dialysis center, chemotherapy, or other infusion therapy location, and other applicable treatment sites.

        ii. How GCHP may modify any Member care protocols or benefits to ensure continued access to Medically Necessary Services.

        iii. Provide Members with information on how to obtain medical authorizations, out-of-Network care, medication refills or emergency supply, Durable Medical Equipment (DME) or replacements, and Medical Records.

        iv. Inform members about how they can access behavioral and mental health services.

2. <u>Continuity of Covered Services</u> – As part of the Member Emergency Plans, any appropriate actions must be taken to ensure continuity of Covered Services for Members impacted by a federal, State, or county declared state of emergency. These actions for continuity of Covered Services taken by GCHP or as directed by DHCS, will ensure continued access for Members and will include but not limited to the following:

    a. Prior Authorization Modifications – Relaxing time limits for Prior Authorization, pre-certification, and referrals.

    b. Grievance and Appeal Modifications – Extending filings deadlines for grievances and requests for appeals in accordance with DHCS Contract requirements.

c. Provider Site Impacts – Coordinating, transferring, and referring Members to alternate sources of care when a Provider site is closed, unable to meet demands of a medical surge, or otherwise affected by an Emergency.

d. DME and Medical Supplies – Authorizing Members to replace DME or medical supplies out-of-network.

e. Out-of-Network Access – Allowing Members to access appropriate out-of-Network Providers if Network Providers are unavailable due to an Emergency or if the Member is outside of the Service Area.

i. Further, any Members outside of the GCHP Service Area affected by an Emergency can be provided information about contacting GCHP for questions, including assisting with questions regarding loss of Beneficiary Identification Card (BIC), GCHP Member ID Card, access to prescriptions refills, or how to access health care.

f. Member Emergency Contact Center Operations – Provide Extending filings deadlines for grievances and requests for appeals in accordance with DHCS Contract requirements.

F. Network Provider, Subcontractor, and Downstream Subcontractor Emergency Requirements

1. Education and Training – GCHP will provide education and training to Network Providers, Subcontractors, and Downstream Subcontractors on GCHP's Emergency Response plans and procedures. As part of the training GCHP will provide Emergency Preparedness fact sheet and resources on Emergency Preparedness, response, and communications protocols.

2. Communications During an Emergency – GCHP will ensure a communications system and process is in place to be able to provide and receive information from Network Providers, Subcontracts, and Downstream Subcontractors during an emergency. This communication process will provide information on what modifications need to be implemented during an emergency to ensure that members are able to access Covered Services and how GCHP can assist in implementing such efforts.

3. Network Provider Agreements – GCHP Network Provider agreements will include language for the Providers to perform the following actions. Annually submit evidence of adherence to CMS Emergency Preparedness Final Rule (81 FR 63859), notify GCHP of any occurrences of Provider's Emergency Plan, and notify GCHP within 24 hours of an emergency that causes provider site to shut down, they are unable to meet demands of a medical surge, or is otherwise affected by an emergency.

G. Timely Payment of Claims – BCP and Emergency Preparedness and Response plans, will identify procedures for maintaining the timely resolution of claims. When claims processing and payment functions are affected during an emergency or event triggering BCP operations, protocols will be included regarding the timely resolution of claims as a part of emergency response and recovery operations.

H. Business Continuity and Emergency Preparedness Testing and Training – GCHP will ensure necessary testing and training occurs for Business Continuity and Emergency Preparedness, in a manner consistent with industry best practices and aligned with the policies and procedures for GCHP staff.

1. Plan Testing & Exercises – After creating or updated BCP or Emergency Preparedness Plans, it is important to practice them to the extent possible to address any plan vulnerabilities before an actual Emergency arises. GCHP will conduct at a minimum annual testing drills of its BCP and Emergency Preparedness Plans.

   a. DHCS Reporting – After the completion of any testing or exercise, GCHP is required to submit a report within 30 days to DHCS that identifies:

      i. The testing activities.

      ii. Summary of outcomes.

      iii. Plan to address any vulnerabilities found.

2. Plan Review & Revisions – A periodic review of the BCP and Emergency Response Plans must occur to ensure it is kept current, any findings from disaster recovery plan testing are incorporated, and any changes to business processes or systems are included as necessary.

3. Plan Supplies and Equipment – Any necessary equipment and supplies identified in the BCP and Emergency Preparedness Plans will need to be documented and inventoried to ensure availability during an emergency.

4. Mock Disaster Drills – Upon request GCHP will participate in any mock disaster drills coordinated by governmental entities, to ensure coordination during an Emergency.

H. Emergency Preparedness Risk Assessment – GCHP will conduct an annual risk assessment of its Business Continuity and Emergency Preparedness activities that will identify the risks associated with the occurrence of various Emergency events that can affect business operations in GCHP's Service Area.

1. Emergency Events for Risk Assessment – During the risk assessment GCHP will identify and assess potential public health crisis and natural or man-made Emergencies, including but not limited to, epidemics, pandemics, earthquakes, fires, floods, storms, hurricanes, tornados, power outages, gas leaks, bomb threats or presence of explosives, explosions, hazardous materials incidents, relocations or evacuations, assaults, intrusions, bioterrorism, injuries, riots, and information technology security incidents that could arise in any location in which GCHP conducts business operations.

2. Risk Impact & Likelihood – GCHP will use its standard Enterprise Risk Assessment Tools to rate and score the likelihood and impact of each Emergency identified within the GCHP Service Area. The assessment will also identify and assess any impacts to the organizations essential supply chain that may disrupt business operations during or after an emergency event.

3. Emergency Risk Assessment Mitigation and Reporting – GCHP will follow its existing Risk Management policies and procedures for risk mitigation and reporting risk assessment results.

I. Cooperative Arrangements – GCHP will identify and attempt to establish cooperative arrangements with our local health care organizations to assist and provide mutual aid during an Emergency when business operations are affected.

V. Attachments

VI. References

B. HIPAA Security Rule: Administrative Safeguards § 164.308(a)(7)(i); Contingency Plan

C. HIPAA Security Rule: Administrative Safeguards § 164.308(a)(7)(ii)(A); Data Backup Plan

D. HIPAA Security Rule: Administrative Safeguards § 164.308(a)(7)(ii)(B); Disaster Recovery Plan

E. HIPAA Security Rule: Administrative Safeguards § 164.308(a)(7)(ii)(C); Emergency Mode Operation Plan

F. HIPAA Security Rule: Administrative Safeguards § 164.308(a)(7)(ii)(D); Testing and Revision Procedures

G. HIPAA Security Rule: Administrative Safeguards § 164.308(a)(7)(ii)(E); Applications and Data Criticality Analysis

NOTE: Printed copies of this document are uncontrolled. In the case of a conflict between printed and electronic versions of this document, the controlled version published online prevails.

H. HIPAA Security Rule: Physical Safeguards § 164.310(a)(2)(i); Contingency Operations

I. HI-054 Backup and Restoration Policy