Greater Tompkins County Municipal Health Insurance Consortium

408 East Upland Road, Suite 2 • Ithaca, New York 14850 • (607) 274-5590
healthconsortium.net • consortium@tompkins-co.org

"Individually and collectively, we invest in realizing high quality, affordable, dependable health insurance."

AGENDA

Operations Committee
February 6, 2025 – 1:30 P.M.
GTCMHIC Conference Room or Via Online Zoom

1. Call to Order (1:30) L. Granger

2. Changes to the Agenda

3. Approval of July 9, 2024 Minutes (1:35)

4. Executive Director Report (1:40) E. Dowd

a. Executive Director Update
b. **Resolution:** Amendment to Resolution No. 034-2024 – Creation of 2025 Committee Structure and Appointments of Committee Members – Appointment of Ellen Hersey to Operations Committee
c. **Resolution:** Approval of Information Security Policies and Procedures for the GTCMHIC (January 2024, Version 1.0) and Approval of Annual Cyber Security Risk Assessment
d. **Resolution:** Approval of the GTCMHIC Participant Plan Option Parameters Policy
e. Department of Financial Services Update
    i. MCA
    ii. Audit
    iii. SPD
f. **Resolution:** Amendment to the Consortium Metal Level Options, Blue Traditional Options, and PPO Options Benefit Booklets AMENDMENT #1 January 2025

5. Benefits Manager Update (2:05) K. Rodrigues

a. 2025 Notice of Privacy Practices Update
b. Plan Consolidation Update
c. Website Update
d. 2024 Plan Utilization Management Overview
e. Wellness Survey Result Summary
f. **Resolution:** Cancellation of Consortium Hosted Flu Clinics

6. Future Discussion Topics: (2:30) L. Granger

a. Notice of Privacy Practices 2025 Version

7. Adjournment (2:35)

Next Meeting: April 3, 2025

Greater Tompkins County Municipal Health Insurance Consortium
Operations Committee Minutes – DRAFT
July 9, 2024 – 1:30 p.m.
GTCMHIC Headquarters (408 E. Upland Road, Ithaca, NY), or Remote Zoom

Present: Laura Granger*, Committee Chair; Judith (Judy) Drake, Committee Vice Chair; Ruby Pulliam; Sunday Earle*; Mark Emerson*; Rita McCarthy* (arrived 1:40p) w/ Melissa Greenthal*
Excused: Elin Dowd*, Executive Director; Janine Bond
Absent: Kerrie Fusco; Brian Weinstein; Kemi Shokunbi
Staff/Guests: Teri Apalovich, Finance Manager; Lynne Sheldon, Clerk of the Board; Kylie Rodrigues, Benefits Specialist

* = Via Zoom remote

Call to Order

Ms. Granger, Chair, called the meeting to order at 1:36 p.m.

Changes to the Agenda

There were no changes to the agenda.

Approval of June 6, 2024 Minutes

It was MOVED by Ms. Drake, seconded by Mr. Emerson, and unanimously adopted by voice vote by members present and seen members via online, to approve the minutes of June 6, 2024. MINUTES APPROVED.

Executive Director Report

Update

Ms. Rodrigues said that Ms. Dowd was excused from the meeting, but Ms. Dowd has asked her to report some items.

Ms. Rodrigues said the Consortium has not received the final report from the DFS regarding their audit (2016-2021) of the Consortium. She said the closing interview with DFS was in November 2023. She also reported that 2024 Summary Plan Documents (SPD) were submitted this week.

Ms. Rodrigues reported that DFS requested the Consortium to reprocess “evergreen” resolutions that municipalities submitted to approve the amended Municipal Cooperative Agreement (MCA) resolutions for 2024 as well as the signature 2024 MCA approval forms. She said the Consortium is in the process of getting new documents from approximately 16 municipalities. Ms. Rodrigues said once the 2024 MCA is approved, the DFS will release a New Certificate of Authority which will increase into territories of Livingston and Monroe Counties.

Ms. Rodrigues said the Finance Committee is meeting today and discussion will include the 2025 budget. She said the Consortium is seeing a drastic increase in claims. She also said three new members will be presented for approval: Towns of Corning and Sterling, and Village of Baldwinsville (Total of 62 new subscribers)

Ms. Granger asked if the Consortium had an idea of what the budget increase maybe. Ms. Apalovich said last year the increase was 8% and speculation will be 10% this year. Ms. Apalovich said the Consortium is just starting discussion at the Finance Committee that afternoon and Executive Committee soon after. She said additional budget information would be available after those meetings.

Premium Policy Update

Ms. Rodrigues said that the Premium policy was discussed by the Executive Committee last month and they suggested more detail be added to the policy. Ms. Rodrigues said that the policy reflects the timeframe as to when late notices are sent out and when late fees are applied to late payments. She said the policy was in place for several years but was on pause during the Covid pandemic. Ms. Rodrigues said the Consortium is looking to re-implement it, since the Consortium currently does have some municipalities who are sending in late payments.

Strategic Initiatives Update

Guest Policy

Ms. Rodrigues explained to the Committee that of all the Strategic Initiatives what were previously presented to the Committee, the one that was sent back for further review was the "Guest Policy". She further explained that that the "Guest Policy" was completely re-done and presented today to seek the Committee's approval.

MCA Recommendations

Ms. Rodrigues explained Consortium staff met with the Consortium's attorney to discuss several possible updates to the MCA, including, but not limited to:

- Name change of the Consortium – The Consortium continues to vet new names.
- The Chief Financial Officer (CFO) listed within the MCA is from the City of Ithaca who has recently retired – The Consortium is researching recommending other municipalities.
- Items within the MCA that may not need to be included or may be better served written as a policy.
- When and how the Executive Committee can act in lieu of the Board of Directors.

Resolutions

Approval of Amendment to Adopt the "Premium Payment Policy"

RESOLUTION NO. XXX - 2024 – APPROVAL OF AMENDMENT TO ADOPT THE PREMIUM PAYMENT POLICY

MOVED by Ms. Drake, seconded by Ms. Pulliam. The resolution was unanimously adopted by voice vote of members present, and visibly seen members via remote locations to approve the following resolution.

WHEREAS, per Resolution No. 33 of 2020, the Greater Tompkins County Municipal Health Insurance Consortium, (GTCMHIC), approved a policy to adopt a late payment fee policy that can be administered to all participants in circumstances where premium payment is not received in a timely manner, and

WHEREAS, the current policy refers to accounting staff, “Principal Accountant” to make adjustments to future invoices. The Consortium’s current financial staff member capable of adjustments has since been named as, “Finance Manager”, which shall be updated to the amended Premium Payment Policy, and

WHEREAS, the current Premium Payment Policy indicates “each participant’s monthly premium equivalent, by enrollee classification, shall be paid by the first day (1st) of each calendar month during the Plan Year”. Due to the current financial system software set to automatically generate payment reminders, the GTCMHIC has since revised the date to the seventh day (7th) of each calendar month during the Plan Year, and

WHEREAS, in addition to payment modifications, the GTCMHIC’s financial system software now sends monthly premium invoice reminders automatically 14 days before the premium invoice due date and again on the due date if no payment has been received. Another reminder will be sent 7 days after the due date with the one percent (1%) late fee included on the invoice. If a payment has not been made 90 days after the due date, the Executive Director will be notified, now therefore be it

RESOLVED, on recommendation of the Operations Committee, That the Executive Committee, on behalf of the Board of Directors, hereby adopt the GTCMHIC’s “Approval of Amendment to Adopt the Premium Payment Policy”, attached hereto as "Exhibit A", effective immediately.

* * * * * * *

<u>Adoption of “Meetings Policy and Procedures”</u>

RESOLUTION NO. XXX - 2024 – ADOPTION OF “MEETINGS POLICY AND PROCEDURES”

MOVED by Ms. Pulliam, seconded by Mr. Emerson. The resolution was unanimously adopted by voice vote of members present, and visibly seen members via remote locations to approve the following resolution.

WHEREAS, The Greater Tompkins County Municipal Health Insurance Consortium (GTCMHIC) is a unique, "hybrid" organization formed and operates under various and differing sections of NY State law. With municipal governments as its primary membership, and public monies as its primary source of revenue, certain aspects of the Consortium's operations – in particular, certain meetings – are subject to NY State Open Meeting Law (OML), while others are not, and

WHEREAS, the GTCMHIC created a "Meetings Policy and Procedures" to clarify and codify how Consortium meetings must operate in an effort to efficiently conduct the business of the Consortium, while remaining compliant with statute when required, and

WHEREAS, the "Meetings Policy and Procedures" shall reference and clarify the following:

- Purpose/Definitions
- Board(s)/Committee(s) Subject to OML
- Board(s)/Committee(s) Not Subject to OML
- Specific Meetings Rules & Procedures for Board(s)/Committee(s) Subject to OML
- Specific Meetings Rules & Procedures for Board(s)/Committee(s) Not Subject to OML
- General Meetings Rules & Procedures for All Board(s)/Committee(s)

Therefore now be it

RESOLVED, on recommendation of the Operations Committee, That the Executive Committee, on behalf of the Board of Directors, hereby adopt "Meetings Policy and Procedures" attached hereto as "Exhibit A", effective immediately.

* * * * * * *

Future Discussion Topics

2025 Operation Meeting Dates

Adjournment

The meeting was adjourned at 2:01p.m.

Respectfully submitted by Lynne Sheldon, Clerk of the Board

The next meeting will be held October 3, 2024

Greater Tompkins County Municipal Health Insurance Consortium

408 East Upland Road, Suite 2 • Ithaca, New York 14850 • (607) 274-5590
healthconsortium.net • consortium@tompkins-co.org

"Individually and collectively, we invest in realizing high quality, affordable, dependable health insurance."

RESOLUTION NO. XXX-2025 - AMENDMENT TO RESOLUTION NO. 034-2024 – CREATION OF 2025 COMMITTEE STRUCTURE AND APPOINTMENTS OF COMMITTEE MEMBERS – APPOINTMENT OF ELLEN HERSEY TO OPERATIONS COMMITTEE

WHEREAS, a vacancy of a labor representative on the Operations Committee exists, and

WHEREAS, it is deemed to be in the best interest of Committees to continue to have a member, such as Ellen Hersey, Tompkins County Public Library who will represent the labor interests on this Committee, therefore be it

RESOLVED, on recommendation of the Operations Committee, That the Executive Committee, on behalf of the Board of Directors, appoints the above committee member effective immediately with the term expiring December 31, 2026.

****

Greater Tompkins County Municipal Health Insurance Consortium

408 East Upland Road, Suite 2 • Ithaca, New York 14850 • (607)274-5590
healthconsortium.net • consortium@tompkins-co.org

"Individually and collectively, we invest in realizing high quality, affordable, dependable health insurance."

RESOLUTION NO. XXX-2025 – APPROVAL OF INFORMATION SECURITY POLICIES AND PROCEDURES FOR THE GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM (GTCMHIC) – JANUARY 2024 Version 1.0 AND APPROVAL OF ANNUAL CYBER SECURITY RISK ASSESSMENT

WHEREAS, Per previous Resolution 042 of 2023, Tompkins County IT Department recommended that FoxPointe Solutions perform GTCMHIC management-requested assessments and reporting services as GTCMHIC's Virtual Chief Information Security Officer ("VCISO"), cybersecurity consultant, and to manage GTCMHIC's Information Security program, and

WHEREAS, these Information Security Programs require policies and procedures to be put in place to conduct independent audits of their cybersecurity programs and the GTCMHIC to be compliant with all applicable laws and regulations, which require approval annually and

WHEREAS, This program also includes policies and procedures required under the current versions of NYS DFS 23NYCRR500 Cybersecurity Rule (with limited exemptions), NY State SHIELD Act (§899-bb), HIPAA/HITECH Acts Security and Breach Laws (45CFR164.306-316, 45CFR164.400- 414) and the Gramm-Leach-Bliley Act (GLBA) (GLBA Title 16, Chapter 1, Part 314 of Subchapter C, Safeguards Rule, and

WHEREAS, FoxPointe Solutions has provided and reviewed in depth the said above policies and procedures with third party Tompkins County IT Department and GTCMHIC Staff Members, and

WHEREAS, FoxPointe Solutions has recently completed the annual Cyber Security Risk Assessment on behalf of the GTCMHIC, and has prepared a thorough complete report and therefore be it,

RESOLVED, on recommendation of the Operations Committee, That the Executive Committee, on behalf of the Board of Directors, approves the Information Security Policies and Procedures for the GTCMHIC and the following Cyber Security Risk Assessment performed by FoxPointe Solutions.

****

Greater Tompkins County Municipal Health Insurance Consortium

Information Security Policies and Procedures

January 2024
Version 1.0

Policy Approval and Review History

Policy Revisions:

Date	Revision Log	Updated By
January 2024	v1.0 Initial Release	
January 2025	First Review and Update	Carl Cadregari

This Policy and Procedure shall be reviewed annually and updated consistent with the requirements established by the Board of Directors, Greater Tompkins County Municipal Health Insurance Consortium (GTCMHIC) Senior Management, Federal and State law(s) and regulations, and applicable accrediting and review organizations.

Table of Contents

Policy Administration 4
Mandatory Annual Information Security Training Policy 6
Information Technology Acceptable Use 7
Breach Notification Policy 11
Information Security and Privacy Policy 12
Access Controls Policy 13
Incident Response Policy 15
Personnel Security Policy 17
Security Assessment and Authorization Policy 19
Risk Assessment Policy 20
Media Protection Policy 21
Information Security Program Management Policy 22
Contingency Planning Policy 24
IT Systems Backup and Disaster Recovery 26
IT Systems Disposal and Data Sanitation Policy 28
GTCMHIC Personal Device Agreement 29
Definitions 30

Policy Administration

Purpose:
To establish the process for the development, updating, and approval of the policies, procedures, and guidelines.

Policy:
It is the policy of GTCMHIC to implement policies to guide the GTCMHIC to be compliant with all applicable laws and regulations and create standard practices across the GTCMHIC .

Procedure:

I. Policies

a. Creation
   i. Policies may be created in cooperation with GTCMHIC Management or governance committee.
   ii. Policies are created in response to governance, operational, or regulatory needs of GTCMHIC .

b. Approvals
   i. Governance policies and documents will be reviewed by Management, presented to legal counsel for review and advisement as necessary, and presented to the Board of Directors for final review and approval.
   ii. All other policies will be reviewed by Management, presented to the applicable governance committee for review and approval, and then presented to the Board of Directors for final review and approval.
   iii. Once approval is received; the policy is ready for implementation.

c. Implementation
   i. The policy will be posted on the GTCMHIC internal SharePoint site under the "Policies and Procedures" section and filed in the applicable folder.
   ii. When needed, an announcement will be given to appropriate GTCMHIC Staff, highlighting all new policies.

d. Revisions
   i. All policies will be reviewed by Management as needed, but no less than once every year, for adherence to all applicable laws and regulations and standard practices across the GTCMHIC.
   ii. All revisions will be documented in the revision log at the start of this document.
   iii. All revisions to governance policies and documents will be reviewed by Management, presented to legal counsel for review and advisement as necessary, and then presented to the Board of Directors for final review and approval.
   iv. All substantive revisions to all other policies will be reviewed by Management, presented to the applicable governance committee for review and approval, and then presented to the Board of Directors for final review and approval.
   v. Revisions not classified as substantive, but not relating to document formatting, require GTCMHIC Management review prior to implementation.

II. Procedures

a. Creation
   i. Procedures are created in response to the need to add detail, guidance, or standards to policies, project implementations, or guidelines.

b. Approvals
    i. All procedures will be reviewed by an applicable member of GTCMHIC Management.
    ii. Once Management approval is received, the procedure is ready for implementation.
c. Implementation
    i. The procedure will be posted on the GTCMHIC SharePoint site under the "Policies and Procedures" section and filed in the applicable folder.
d. Revisions
    i. All procedures will be periodically reviewed by the applicable GTCMHIC department, functional area, or project team, for consistency with subject area industry practices and operational practices across the GTCMHIC .
    ii. All revisions to procedures not relating to document formatting will be reviewed and approved by Management.

III. Sanctions

i. All staff will abide by the policies and procedures of GTCMHIC . Non-compliance sanctions will include those needed up to termination and legal proceedings.

Mandatory Annual Information Security Training Policy

Purpose:
To ensure that staff have been trained and retrained in a variety of mandatory subject matters.

Policy:
All staff shall be required to complete the Mandatory Training at hire and annually thereafter.

Procedure:

I. At least annually, all staff members shall satisfactorily complete education on the following topics as they apply to their position:
    a. NY DFS Cybersecurity Rule, HIPAA/HITECH Rule, NY SHIELD Act, other needed State and Federal Data privacy and security rules;
    b. Security Awareness and Identify Theft; and
    c. Others as needed.

II. Satisfactory completion of the mandatory courses will be monitored by Management, and a record of satisfactory completion will be maintained.

Information Technology Acceptable Use

Purpose:
To ensure that all directors, officers, staff, contractors, volunteers, third party service organizations, and other organizations understand the acceptable use of information technology devices and resources at GTCMHIC . Inappropriate use exposes GTCMHIC to risks including virus attacks, compromise of network systems and services, and legal issues.

Policy:
GTCMHIC is committed to protecting the integrity and availability of its data environment. The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to GTCMHIC established culture of openness, trust, and integrity; however, no expectation of privacy is granted, and Management will electronically monitor access to systems, data and applications.

Procedure:

I. Prohibited Activities.

Staff are prohibited from the following activities. The list is not all inclusive. Other prohibited activities are referenced elsewhere in this document or within other policy documents.

a. Crashing an information system: Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.

b. Attempting to break into an information resource or to bypass a security feature: This includes running password-cracking programs or sniffer programs and/or attempting to circumvent file or other resource permissions.

c. Introducing, or attempting to introduce, ransomware, computer viruses, trojan horses, peer-to-peer ("P2P"), or other malicious code into an information system.

d. Browsing: The willful, unauthorized access to or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. GTCMHIC has access to information that is protected by regulations that stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.

e. Personal or Unauthorized Software: Use of personal software is prohibited. All software installed on GTCMHIC assets of any type must be approved in writing by GTCMHIC Management.

f. Software Use: Violating or attempting to violate the terms of use or license agreement of any software product used by GTCMHIC is strictly prohibited.

g. System Use: Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures, or business interests of GTCMHIC is strictly prohibited.

II. Electronic Communication, Email, Internet Usage.

a. As a productivity enhancement tool, GTCMHIC encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by GTCMHIC owned equipment are considered the property of GTCMHIC , not the property of individual users. Consequently, this policy applies to all GTCMHIC assets and staff and covers all electronic communications including, but not

limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

b. GTCMHIC provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, applications, networks, software and services are intended for business purposes. However, incidental personal use is permissible as long as:
    i. it does not consume more than a trivial amount of staff time or resources,
    ii. it does not interfere with staff productivity,
    iii. it does not preempt any business activity, and
    iv. it does not violate any of the following:
        1. Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
        2. Illegal activities – Use of GTCMHIC information resources for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited.
        3. Commercial use – Use of GTCMHIC information resources for personal or commercial profit is strictly prohibited.
        4. Political Activities – All political activities are strictly prohibited on GTCMHIC premises. GTCMHIC encourages its staff to vote and to participate in the election process, but these activities must not be performed using GTCMHIC assets or resources.
        5. Harassment – GTCMHIC strives to maintain a workplace free of harassment and that is sensitive to the diversity of its staff. Therefore, GTCMHIC prohibits the use of computers, e-mail, voice mail, instant messaging, texting, and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but are not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening, or showing disrespect for others.
        6. Junk E-mail: All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations, is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

c. GTCMHIC and its IT vendor are responsible for servicing and protecting its equipment, networks, data, and resource availability and may be required to access and/or monitor electronic communications.

d. GTCMHIC reserves the right, at its discretion, to review any staff's files or electronic communications to the extent necessary to ensure that all electronic media and services are used in compliance with all applicable laws and regulations as well as GTCMHIC policies.

e. Staff should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.
f. All users of the GTCMHIC e-mail system shall comply with the e-mail controls set in place.
g. All use of assets and any transmission of data will be protected via the approved encryption technology.

III. Internet Access.

a. Internet access is provided for GTCMHIC users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by GTCMHIC should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc.
b. Users must understand that individual Internet usage is monitored, and if a staff member is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken, up to and including termination.
c. Many Internet sites, such as games, unapproved file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by GTCMHIC routers and firewalls. This list is constantly monitored and updated as necessary. Any staff visiting pornographic sites will be disciplined, up to and including termination.

IV. Personal Devices.

a. The use of personally owned devices to access organizational information systems containing PHI/PII/NPI is prohibited without written authorization from Management.
b. All use of assets and any transmission of data will be protected via the approved encryption technology.
c. All restricted activities referenced elsewhere in this policy also apply to activities performed on personal devices.
d. Staff may request access to GTCMHIC e-mail or selected GTCMHIC systems on their personal devices. A condition for this access is that the device must be secured with all available security mechanisms.
e. A lost or stolen personal device with any access to or the ability to access GTCMHIC data access will be subject to remote wipe technology by GTCMHIC to protect potentially breaching confidential or protected information.
f. Staff should notify GTCMHIC within one hour if a device that accesses GTCMHIC data is lost or stolen. Additionally, an excessive number of incorrect logins from a personal device may trigger remote wipe of that device.
g. All personal devices with access to GTCMHIC systems or data must be updated regularly with the most current available version of the operating system.
h. All personal devices that store/access or interact with Protected Information or Personally Identifiable Information (PII/NPI) must be encrypted.
i. All personal devices that access PHI/PII/NPI sensitive information must be protected with virus protection, and the most recent security patches and upgrades.
j. Staff accessing GTCMHIC systems remotely from personal devices must use the approved VPN and adhere to all GTCMHIC privacy and security policies and procedures to ensure data security.
k. Staff using personal devices to access GTCMHIC systems assumes all risks of loss or damage to the device. GTCMHIC may choose to assist the staff member with troubleshooting issues

with the device related to the access of the GTCMHIC system but is not responsible for problem resolution.

V. Protection of Data.

a. All users of the GTCMHIC information systems that contain PHI/PII/NPI or sensitive information shall secure the information by locking the session (such that the information on the monitor is concealed) or logging out of the system when not in direct sight of the workstation.

b. Confidentiality Agreement
    i. Users of GTCMHIC information resources shall sign an appropriate confidentiality agreement (Appendix A). The agreement shall include the following statement, or a paraphrase of it:
    ii. I understand that any unauthorized use or disclosure of information residing on the GTCMHIC information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.
    iii. Temporary workers and third-party employees shall sign a confidentiality agreement document prior to accessing GTCMHIC information resources.
    iv. Confidentiality agreements shall be reviewed annually.

c. PHI/PII/NPI must not be stored outside the GTCMHIC Data Warehouse system.

Breach Notification Policy

Purpose:
To ensure that all data incidents and possible breach violations are evaluated to determine if a breach notification must be filed with the appropriate regulatory body.

Policy:
It is the policy of GTCMHIC to maintain privacy and security measures to protect the confidentiality of information by preventing unauthorized acquisition, access, use, or disclosure of Protected Information (PHI/PII/NPI). Pursuant to any regulations promulgated thereunder, as well as pursuant to applicable New York State privacy laws and regulations, GTCMHIC will notify individuals when an impermissible acquisition, access, use, or disclosure of PHI/PII/NPI is presumed to be a breach, unless a documented risk assessment demonstrates a low probability that the PHI/PII/NPI has been compromised.

Procedure:

I. Suspected or confirmed breaches of the security or confidentiality of PHI/PHI/PII/NPI will invoke certain actions by Management to determine the degree of risk and impact of the breach upon an individual(s) and, under specific circumstances, notification of the breach to the affected individual(s).

II. Staff, committee members, directors, vendors, and partner organizations shall report any potential breach within 24 hours or without unreasonable delay to Management, who will conduct an investigation into the potential breach.

III. The investigation and steps will be thoroughly documented by Management and will follow the needed incident reporting plans.

IV. If Management concludes that no breach has occurred, as that term is defined in the laws and regulations affecting GTCMHIC, Management will recommend the appropriate corrective action based on the disclosure.

V. If Management confirms that a breach of security or confidentiality has occurred, Management will, as soon as possible but no later than required by law after the discovery of the breach, notify the individual(s) whose information was breached along with the appropriate cyber liability insurance carrier.

VI. If it is determined that a breach occurred, an analysis of the requirements for notification of the State in which the individual resides will be conducted and documented by Management.

VII. Management shall maintain documentation of the name of each individual notified, each log maintained by GTCMHIC , and any other notification as required by law.

VIII. Management shall report all identified potential breaches to the Board of Directors.

Information Security and Privacy Policy

Purpose:
This policy serves to establish the information security and privacy measures and responsibilities of GTCMHIC staff and TSPs and all vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the shared information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for the GTCMHIC .

Procedure:

I. Management is responsible for ensuring that security measures are assessed, planned, and implemented to protect privacy and confidentiality of PHI/PII/NPI and sensitive information.

II. GTCMHIC shall reasonably comply with all NY State and other required laws, regulations, and standards (e.g., PCI DSS) to protect PHI/PII/NPI for privacy and security.

III. GTCMHIC shall protect all sensitive information created internally, transmitted to, reasonably interacted with or received from all third-party service organizations.

IV. GTCMHIC (or its designated Third-party service provider (TSP)) will apply systems, applications, and computer changes, updates, and patches as soon as possible from the release of the update. Security patches will be applied within one week of release.

V. GTCMHIC shall provide education and tools to assist staff and others with access to PHI/PII/NPI, and sensitive information with compliance of NYS, and other regulatory agencies' privacy, security, and confidentiality requirements.

VI. GTCMHIC shall require an executed reciprocal Business Associate Agreement (BAA), contract, or other device (or a combination of two (2) one-way BAAs) with all TSPs and Partner Organizations as part of the contracting process and prior to the execution of any project activities or exchange of PHI/PII/NPI, or sensitive information.

VII. GTCMHIC shall require an executed BAA with all vendors as part of the contracting process and prior to the execution of any services that may provide access to PHI/PII/NPI, or sensitive information.

VIII. GTCMHIC shall require an executed nondisclosure agreement or approved confidentiality clauses in contracts or service level agreements with vendors that will not have access to PHI/PII/NPI but may have access to sensitive information.

IX. All GTCMHIC staff, vendors, teams, participating organizations, and any other persons who have access to GTCMHIC information systems or to other sensitive information shall sign a "Confidentiality Agreement" document prior to receiving access to PHI/PII/NPI or sensitive information.

Access Controls Policy

Purpose:
This policy serves to establish the access controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for the GTCMHIC .

Procedure:
Management is responsible for ensuring that information system access security measures and controls are assessed, planned, and implemented for GTCMHIC computer systems to protect the privacy and confidentiality of individual and other sensitive information. The security measures and controls must address the following:

I. Roles-based Access

a. PHI/PII/NPI shall be accessed only by approved users.
b. All new accounts shall be vetted through the system-specific roles-based access matrices to determine the appropriate user group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account and shall be reviewed annually.
c. Multi-Factor Authentication (MFA) will be used for access to the network and any external (cloud) based systems.

II. Account Management

a. Each information system shall be assessed to determine the appropriate account types required to support organizational missions/business functions:
    1. Individual
    2. System
    3. Application
    4. Guest
    5. Emergency
    6. Temporary
b. System administrators shall be assigned for each information system.
c. All new information system accounts require prior approval of GTCMHIC Management.
d. The use of all information system accounts shall be monitored.
e. System administrators shall be notified by the corresponding GTCMHIC Management for the removal of or disabling of accounts.
f. All high-risk accounts (e.g., staff terminated "for cause") will be disabled within 60 minutes of discovery of risk and Information system accounts shall be monitored for atypical use.

III. Access Enforcement.

Access enforcement mechanisms shall also be employed at the application and service level to provide increased information security if required.

IV. Information Flow Enforcement.

All information systems containing PHI/PII/NPI or sensitive information enforce approved access.

V. Separation of Duties.

Management will review all access to confirm if any additional steps need to be taken to remove or minimize any Separation of Duties issues. Auditing of access controls shall be performed by an individual other than the system owner of the information system.

VI. Least Privilege.

GTCMHIC shall employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks and duties.

VII. Unsuccessful Logon Attempts.

All information systems containing PHI/PII/NPI, or sensitive information shall be configured to lock out a user account automatically after three (3) invalid login attempts during a 15-minute time period. The lock out time period shall persist for a minimum of one (1) hour.

IX. Session Lock.

Each information system containing PHI/PII/NPI, or sensitive information shall have a defined automatic session lock based on timeframe of inactivity documented as part of the system configurations.

X. Session Termination.

Each information system containing PHI/PII/NPI, or sensitive information shall have a defined automatic session termination condition (e.g., a designated timeframe of inactivity) documented as part of the system configurations.

XI. Authentication to Systems.

All information systems containing PHI/PII/NPI, or sensitive information require identification and authentication to the system prior to performing actions within the system.

XII. Remote Access.

a. Remote access to all information systems containing PHI/PII/NPI or sensitive information shall require MFA and an approved, encrypted VPN connection and be monitored and audited for unauthorized access.
b. All computers and devices (internal or external) that require network access to an information system containing PHI/PII/NPI shall be securely configured.
c. Up-to-date system patches AND current anti-virus software is required.
d. The confidentiality and integrity of all remote access sessions accessing information systems containing PHI/PII/NPI or sensitive information shall be protected by cryptographic mechanisms.

XIII. Wireless Access.

The following wireless restrictions and access controls shall be implemented:

a. Wireless device service set identifier broadcasting shall be disabled;
b. Encryption protection is enabled;
c. Personal firewalls are utilized on all wireless clients;
d. File sharing is disabled on all wireless clients; and
e. Wireless access and activity are monitored and recorded, and the records are reviewed on a regular basis.

XIV. Mobile/Portable Devices.

a. Mobile devices that cannot connect to an information system with a physical connection (e.g., smart phones, e-readers, and tablets) shall not be permitted to be utilized to access GTCMHIC information systems containing PHI/PII/NPI that has not been approved by Management.
b. All mobile and portable devices shall be physically secured when not in use.

Incident Response Policy

Purpose:
This policy serves to establish the incident reporting controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for the GTCMHIC .

Procedure:

I. Oversight.

Management and the Security Officer are responsible for ensuring that GTCMHIC utilizes a documented incident response program and that all security incidents, outside those seen as incidental (i.e., ping sweeps, etc.), are investigated and brought to resolution.

II. Incident Response Training.

Upon hire, upon changes to incident response responsibilities, when necessary due to information systems changes, and at least annually thereafter, all staff and users of GTCMHIC information systems shall be trained on Incident Response training consistent with their role and responsibilities.

III. Incident Handling.

a. Upon Management request, the Security Officer is responsible for:
    i. Investigating and reviewing any reported incidents.
    ii. Coordinating incident handling activities with contingency planning activities.
    iii. As needed or warranted, working with appropriate Management and the Executive Director to determine the level of disciplinary action. Disciplinary actions, depending upon the severity of the incident, could result in:
        1. Education and/or verbal or written warning.
        2. Termination of privileges to access information systems and records.
        3. Termination of employment.
        4. Termination of the Partner Organization from the GTCMHIC .
    iv. Working with appropriate areas to ensure that plans are developed to address any gaps in security or confidentiality.

b. Staff and Users' Responsibility
    i. Staff and users of GTCMHIC information systems are responsible for the following:
        1. To abide by all GTCMHIC policies regarding information security and confidentiality of PHI/PII/NPI, and sensitive information, whether accessing the information at work or outside of work (e.g., home).
        2. To immediately report all information security and confidentiality incidents to their supervisor and/or the Security Officer.

c. Incident information and individual incident responses shall be correlated to achieve an organization-wide perspective on incident awareness and response.

IV. Incident Response Testing.

a. Documented tests must be performed annually.
b. The results shall be documented and retained for a minimum of six years.

V. Incident Monitoring and Reporting.

a. Information system security incidents shall be tracked and documented and retained for a minimum of six years.

b. Information system security incidents shall be reported to Management and if warranted, the Board of Directors.

VI. Incident Response Plan.

a. An incident response plan shall be documented and maintained that:
    i. Provides a roadmap for implementing GTCMHIC incident response capability;
    ii. Describes the structure and organization of the incident response capability;
    iii. Provides a high-level approach for how the incident response capability fits into the overall organization;
    iv. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    v. Defines reportable incidents;
    vi. Provides metrics for measuring the incident response capability within the organization;
    vii. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    viii. Is reviewed and approved by the Information Technology, Informatics, and Data Governance Committee
b. The incident response plan shall be distributed to GTCMHIC Management.
c. The incident response plan shall be reviewed for updates as needed or at least annually.
d. The incident response plan shall be updated to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
e. The incident response plan shall be protected from unauthorized disclosure and modification.

Personnel Security Policy

Purpose:
This policy serves to establish the personnel security controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for GTCMHIC .

Procedure:

I. Oversight.

Management is responsible for personnel security controls.

II. Position Risk Designation.

a. GTCMHIC staff positions shall be designated with a risk level that determines the screening criteria and authorization levels for information system access.
b. Risk levels shall be reviewed when position duties change or at least annually.

III. Personnel Screening.

a. All GTCMHIC staff positions shall require background checks prior to the commencement of employment that minimally includes the verification of:
    i. Social Security Number;
    ii. Address History;
    iii. Highest level of education/degree; and
    iv. Criminal background.
b. Rescreening shall be required if a change in position requirements designates a higher risk level and higher screening criteria.

IV. Personnel Termination.

a. Upon termination of individual employment:
    i. The system administrator of each information system shall disable information system access within 24 hours;
    ii. Management retrieves all security-related organizational information system related property; and
    iii. A Management representative retains access to organizational information and information systems formerly controlled by the terminated individual.
b. All access and privileges to systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence).

V. Access Agreements.

a. All users of GTCMHIC information systems are required to sign a "Confidentiality Agreement" document and abide by its contents prior to being granted access to the information systems. This agreement shall be re-signed at least annually or when the contents of the agreement are substantively edited.
b. Anyone who wishes to use a personal device to access GTCMHIC information systems is required to sign a "GTCMHIC Personal Device Agreement" document and abide by its contents, prior to being given access to GTCMHIC information systems from a personal device. This agreement shall be re-signed at least annually or when the contents of the agreement are substantively edited.

VI. Third Party Personnel Security.

a. Personnel security requirements including security roles and responsibilities for contractors and vendors shall be established and documented at the time of engagement and reviewed for updates as responsibilities and duties change or at least annually thereafter.
b. Contractors and vendors are required to agree to comply with GTCMHIC policies and procedures.
c. The documented security roles and responsibilities shall determine the access levels of the contractors and vendors for information systems and physical access.
d. Contractors and vendors shall be granted minimal system and physical access required to perform the duties they are contracted to perform.
e. Contractors and vendors are required to notify GTCMHIC Management of any personnel transfers or terminations of their personnel who possess organizational credentials and/or badges, or who have information system privileges within 1 calendar day.

Security Assessment and Authorization Policy

Purpose:
This policy serves to establish the security assessment and authorization controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for GTCMHIC .

Procedure:

I. Oversight.

Management is responsible for developing and maintaining a secure information systems environment.

II. Security Assessment Plan.

a. A security assessment plan base core NIST SP800-53r5 controls mapped to the laws and regulations affecting GTCMHIC shall be developed and maintained that describes the scope of the assessment including:
   i. Security controls to be assessed
   ii. Assessment procedures to be used to determine security control effectiveness
   iii. Assessment environment, assessment team, and assessment roles and responsibilities

b. The security controls shall be assessed in the information systems and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

c. A security assessment report shall be produced at least annually that documents the results of the assessment;

d. The results of the security control assessment shall be presented in writing to Management.

III. System Interconnections.

a. All connections from an information system containing PHI/PII/NPI or sensitive information to other information systems shall be authorized by Management.

IV. Security Authorizations.

All systems containing PHI/PII/NPI shall be authorized by Management prior to commencing operations based on the implementation of agreed-upon security controls.

V. Continuous Monitoring.

All information systems containing PHI/PII/NPI shall have a specific continuous monitoring program developed, implemented, and reported to Management as required to meet the standards applicable to the organization.

VI. Internal System Connections.

a. Management shall authorize connections of defined internal information system components or classes of components to the information system (e.g., system connections with mobile devices, notebook/desktop computers, printers, copiers, facsimile machines, scanners, sensors, and servers).

Risk Assessment Policy

Purpose:
This policy serves to establish the risk assessment controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for GTCMHIC.

Procedure:

I. Oversight.

Management is responsible for developing and maintaining secure information systems.

II. Security Categorization.

a. Information and the information systems containing PHI/PII/NPI, or sensitive information shall be categorized in accordance with regulations, applicable laws, and standards.

III. Risk Assessment.

a. An assessment of risk, based on key NIST SP800-53r5 controls mapped to the laws and regulations affecting GTCMHIC, will include the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information that it processes, stores, or transmits shall be conducted for each information system containing PHI/PII/NPI, or sensitive information;
b. Risk assessment results shall be documented and supplied to Management;
c. Risk assessment results shall be reviewed as needed but not less than annually;
d. Risk assessment results of information systems containing PHI/PII/NPI, or sensitive information shall be disseminated to Management; and
e. TSP and vendor risk assessments will be conducted at onboarding of any new vendor and at least annually thereafter.

IV. Penetration Testing and Vulnerability Scanning.

a. External penetration testing will be completed at least annually, or comparable measures and testing will be completed per the laws and regulations affecting GTCMHIC;
b. Scans for vulnerabilities in the information system containing PHI/PII/NPI or sensitive information and hosted applications shall be performed regularly;
c. Vulnerabilities will be remediated without undue delay whenever possible;
d. Privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities shall be utilized to facilitate more thorough scanning.

Media Protection Policy

Purpose:
This policy serves to establish the media protection controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the shared information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for GTCMHIC .

Procedure:

I. Oversight.
Management is responsible for ensuring protection of all digital and non-digital media in support of all regulatory requirements.

II. Media Access.
Only individuals authorized by Management shall have access to digital and non-digital media containing sensitive data.

III. Media Marking.
a. Information systems media containing PHI/PII/NPI or sensitive information shall be marked indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

IV. Media Storage.
a. Information systems media shall be protected until the media are destroyed (or sanitized) per the applicable laws and regulations.

V. Media Transport.
a. All digital media containing PHI/PII/NPI or sensitive information shall be protected via approved encryption technology.

VI. Cryptographic Protection.
Information systems and emails containing PHI/PII/NPI or sensitive information shall implement cryptographic mechanisms to protect the confidentiality and integrity of information stored or transmitted.

VIII. Media Use.
a. The use of unapproved personally owned media to access organizational information systems containing PHI/PII/NPI is prohibited.
b. All portable storage devices shall be encrypted.
c. All portable storage devices shall be assigned to an identified owner.

IX. Media Related Records.
a. Inventory and disposition records for information system media shall be maintained to ensure control and accountability of sensitive information.
b. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

Information Security Program Management Policy

Purpose:
This policy serves to establish the information security program management for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for GTCMHIC .

Procedure:

I. Oversight.

Management is responsible for developing and maintaining a security program under the direction of the Information Technology, Informatics, and Data Governance Committee.

II. Information Security Program Plan.

a. An organization-wide information security program plan shall be developed and disseminated that:
   i. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
   ii. Includes the identification and assignment of roles, responsibilities, Management commitment, coordination among organizational entities, and compliance;
   iii. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
   iv. Is approved by Management.

b. The organization-wide information security program plan shall be reviewed at least annually.

c. The plan shall be updated to address organizational changes and problems identified during plan implementation or security control assessments.

d. The information security program plan shall be protected from unauthorized disclosure and modification.

III. Chief Information Security Officer.

An information security officer (ISO) shall be appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

IV. Information Security Resources.

a. All information services budget requests shall include the resources needed to implement the information security program. All exceptions to this requirement shall be documented.

b. A business case shall be created to request the resources required.

V. Information System Inventory.

An inventory of GTCMHIC information systems shall be developed and maintained.

VI. Information Security Measures of Performance.

Information security measures of performance shall be developed, monitored, and reported to the Information Technology, Informatics, and Data Governance Committee.

VII. Enterprise Architecture.

An enterprise architecture shall be developed with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

IX. Critical Infrastructure Plan.

Information security issues shall be addressed in the development, documentation, and updating of a critical infrastructure and key resources protection plan. Protection strategies are based on the prioritization of critical assets and resources.

X. Risk Management Strategy.

a. A comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems shall be developed.
b. An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.
c. The risk management strategy shall be implemented consistently across the organization.
d. The risk management strategy shall be reviewed and updated as required to address organizational changes.

XI. Security Authorization Process.

a. The security state of organizational information systems and the environments in which those systems operate through security authorization processes shall be managed (i.e., documented, tracked, and reported).
b. Individuals shall be designated to fulfill specific roles and responsibilities within the organizational risk management process.
c. The security authorization processes shall be fully integrated into an organization-wide risk management program.

XIV. Testing, Training, and Monitoring.

a. A process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems shall be developed and maintained, and executed in a timely manner.
b. Testing, training, and monitoring plans shall be reviewed for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

XVI. Threat Awareness Program. A threat awareness program shall be implemented that includes a cross-organization information-sharing capability of threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, and threat intelligence (i.e., indications and warnings about threats that are likely to occur).

Contingency Planning Policy

Purpose:
This policy serves to establish the contingency planning controls for GTCMHIC staff and vendors.

Policy:
It is the policy of GTCMHIC to implement security measures and controls to protect the information systems environment and the privacy and confidentiality of protected information, to include financial, business, or other sensitive information for GTCMHIC .

Procedure:

I. Oversight.

Management is responsible for developing and maintaining contingency planning utilizing the applicable guidance from TSPs and those included in the applicable regulations and laws.

II. Contingency Plan.

a. GTCMHIC has a contingency plan for information systems containing PHI/PII/NPI or sensitive information that:
    i. Identifies essential GTCMHIC missions and business functions and associated contingency requirements;
    ii. Provides recovery objectives, restoration priorities, and metrics;
    iii. Addresses contingency roles, responsibilities, assigned individuals with contact information;
    iv. Addresses maintaining essential GTCMHIC missions and business functions despite an information system disruption, compromise, or failure;
    v. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
    vi. Is reviewed and approved by Management.
b. Copies of the contingency plan shall be retained by Management and other stakeholders identified within the contingency plan.
c. Contingency planning activities shall be coordinated with incident handling activities.
d. Reviews of the contingency plans for information systems containing PHI/PII/NPI or sensitive information occur at least annually.
e. Changes to the contingency plan changes shall be communicated.
f. The contingency plan shall be protected from unauthorized disclosure and modification.
g. Capacity planning shall be conducted so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
h. Information systems containing PHI/PII/NPI or sensitive information shall be identified and Management will define an approved Maximum Tolerable Downtime (MTD) for the business functions and make plans for the resumption of essential missions and business functions within that timeframe.
i. Critical information system assets (technical or operational) supporting essential missions and business functions shall be identified.

III. Contingency Training.

Contingency training shall be provided to personnel consistent with assigned roles and responsibilities annually.

IV. Contingency Plan Testing.

a. Contingency plans for information systems containing PHI/PII/NPI or sensitive information shall be tested annually using NIST defined tests and exercises and reported to Management.

V. Alternate Storage Site.

a. When required, an alternate storage site shall be established, including necessary agreements to permit the storage and retrieval of information system backup information.
b. The alternate storage site must provide information security safeguards equivalent to that of the primary site.
c. The alternate storage site shall be separated from the primary storage site to reduce susceptibility to the same threats (e.g., natural disasters, structural failures, hostile cyberattacks).

VI. Alternate Processing Site.

a. When required, an alternate processing site shall be established, including necessary agreements to permit the transfer and resumption of information system operations for essential missions/business identified Recovery Time Objectives (RTO) and business function MTDs when the primary processing capabilities are unavailable.

VII. Information System Recovery and Reconstitution.

a. GTCMHIC shall provide for the recovery and reconstitution of information systems to a known state after a disruption, compromise, or failure of the system. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner.

IT Systems Backup and Disaster Recovery

Purpose:
The purpose of this process is to establish the standards for data backup, disaster recovery, and data retention of GTCMHIC information.

Definitions:

Incremental Backup:
Any backup in which only the data objects that have been modified since the time of some previous backups are copied.

Synthetic Full Backup:
A synthetic backup is identical to a regular full system backup in terms of data, but it is created when data is collected from a previous, older full backup and assembled with subsequent incremental backups.

Warm Site:
These sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. Warm sites may have backups on hand, but they may not be complete and may be between several days and a week old. The recovery will be delayed while backup tapes are delivered to the warm site or network connectivity is established and data is recovered from a remote backup site.

Procedure and Guidance:
A critical component of any data backup and recovery procedure is to properly identify all environments and the associated data – that requires backup procedures.

The following procedures encompass system resources and supporting assets that are owned, operated, maintained and controlled by GTCMHIC .

Backup:

File and System Backups:
GTCMHIC utilizes industry standard software to automate the backup processes. Server snapshots as well as user profiles on GTCMHIC -owned laptops and desktops are backed-up via automated configurations.

Onsite Backup:
GTCMHIC uses industry standard software to schedule and manage automated backups for Information Systems on the GTCMHIC network. Backups run daily Monday through Friday during off hours to reduce the impact on the production network. GTCMHIC runs a full back up on all virtual servers.

Backups will be changed daily (Monday-Friday) and are on a four-week rotating schedule before being overwritten. Backups will be labeled Mon – Fri with a corresponding week number.

Offsite Backup:
GTCMHIC is contracted with Tompkins County for secure offsite storage of backups.

Warm Site Backup:
GTCMHIC is contracted with Tompkins County for a warm site backup. Warm site testing will coincide with annual offsite Disaster Recovery testing.

System Restore:
In the event of systems failure, GTCMHIC will contact Tompkins County to initiate the applicable system restore process.

Disaster Recovery Testing:
GTCMHIC will conduct an annual disaster recovery test that may be part of the incident response test or another table-top test.

IT Systems Disposal and Data Sanitation Policy

Purpose:
The purpose of this policy is to establish standards for the disposal of retired IT assets and the secure destruction/sanitation of GTCMHIC data storage media.

Retiring Assets:
When GTCMHIC IT determines that an IT asset has reached its end of life and is no longer covered under warranty, the device will be moved out of the production environment. GTCMHIC IT will update the IT i nventory spreadsheet to signify the changes.

Decommissioning Assets:
Hard drives, media, and/or portable data storage must be removed from the IT asset prior to the disposal of the asset. The removed media is documented within the IT Systems Disposal log sheet before being sent for Data Wipe/Sanitation.

GTCMHIC assets must be deidentified prior to leaving the building for disposal. GTCMHIC tags, labels, or stickers are to be removed.

Data Wipe/Sanitation:
GTCMHIC is required to securely wipe/sanitize data storage devices including hard drives and portable media. Data Wipe/sanitation processes are required to meet or exceed the requirements defined by New York State and other standards. If this process is completed by a TSP, they are required to provide documented proof of media sanitation back to GTCMHIC once complete.

Data Storage Media Destruction:
Data Storage Media is required to be destroyed by New York State and other standards once the media has been sanitized. A certificate of destruction is required once the process is completed.

Disposal:
GTCMHIC is required to safely dispose of GTCMHIC decommissioned assets. Once GTCMHIC IT assets have been deidentified and data storage media has been removed or data sanitized, and the asset destroyed, the asset can be removed from the assets of GTCMHIC.

GTCMHIC Personal Device Agreement

GTCMHIC may grant staff access to their e-mail accounts, calendars, and selected IT systems from a personal device. This agreement outlines conditions of staff access to GTCMHIC IT systems. My signature below indicates my acknowledgment of these conditions:

a. The cost of acquiring and maintaining the personal device as well as all operational/connectivity charges are my responsibility. GTCMHIC will not pay for or reimburse the employee for any of such costs or expenses. In addition, GTCMHIC shall not be responsible for any increased or additional connectivity charges incurred by the employee as a result of accessing GTCMHIC IT systems with a personal device.
b. Email messages shall be available on the personal device for as long as required by the business.
c. The device must be minimally secured with a passcode and optimally, all available security mechanisms.
d. A lost or stolen personal device with GTCMHIC data access may be subject to remote wipe technology by GTCMHIC or its IT vendor to protect potentially breaching confidential or protected information. Additionally, an excessive number of incorrect logins from a personal device may trigger remote wipe of that device.
e. All personal devices with access to GTCMHIC systems or data must be updated regularly with the most current available version of the operating system.
f. All personal devices that store PHI/PII/NPI or PII must be encrypted to New York State's encryption standards.
g. Staff accessing GTCMHIC systems remotely from personal devices must adhere to all GTCMHIC privacy and security policies and procedures to ensure data security.
h. Staff using personal devices to access GTCMHIC systems assumes all risks of loss or damage to the device. GTCMHIC may choose to assist the staff member with troubleshooting issues with the device related to the access of the GTCMHIC system but is not responsible for problem resolution.
i. At the conclusion of my employment, I shall be promptly removed from access to all GTCMHIC IT systems

Printed Name: _____ Date: _____

Signature: _____

*Staff includes but is not limited to: Directly employed and leased staffs, contractors, agents, consultants, volunteers, and others who act on GTCMHIC 's behalf.

Definitions

Staff includes directly employed and leased employees, contractors, agents, consultants, volunteers, and others who act on GTCMHIC 's behalf.

These policies pertain to all staff, vendors, teams, participating organizations, and any other persons who have access to GTCMHIC information systems or to other sensitive information.

Personally Identifiable Information (PHI/PII/NPI) is information that can be reasonably assumed to identify the individual person including, but not limited to all individual or combined attributes associated with the laws, regulations and standards affecting GTCMHIC including but not limited to:

- Names of individual, relatives, and employer;
- Address or address codes, email address, IP address, and Universal Resource Locator (URL);
- Birth date, telephone and fax numbers;
- Social Security, Health Plan Beneficiary, Certificate, License, and Vehicle numbers;
- GTCMHIC Unique Record or account numbers;
- Finger or Voice prints and Photographic or Diagnostic images.
- Zip Code;
- All elements of Dates (except year) for dates directly related to an individual;
- Telephone Numbers;
- Fax Numbers;
- E-mail addresses;
- Social Security Numbers;
- Medical Data and Record Numbers;
- Insurance Numbers;
- Individually Identifiable Health Information (IIHI)
- Credit Card Numbers;
- Certificate / License Numbers (example Passport Numbers, Vehicle Identifiers, License Plate Numbers;
- Device Identifiers and Serial Numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code.

Sensitive information is information that relates to GTCMHIC organizational proprietary information or participating organizations' competitive information, including but not limited to:

- Financial payments to participating organizations;
- Contract details with participating organizations;

- Any participating organization's proprietary information that could result in anti-competitive discussions or behaviors (including but not limited to salary data, prices or pricing structure, strategic plans);
- GTCMHIC compliance complaints and/or investigations; and
- Confidential employee information.

Breach is the unauthorized acquisition, access, use, or disclosure of unsecured PHI/PII/NPI that compromises the security or privacy of such information. A breach is not considered to have occurred if the information has been de-identified. There are some basic exceptions to the definition of "breach."

1. The unintentional acquisition, access, or use of PHI/PII/NPI by a workforce member or person acting under the authority of GTCMHIC or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The information cannot be further used or disclosed in a manner not permitted by any Privacy Rule.
2. The inadvertent disclosure of PHI/PII/NPI by a person authorized to access PHI/PII/NPI at GTCMHIC or a business associate to another person authorized to access protected information at GTCMHIC or a business associate, or arrangement in which GTCMHIC participates. The information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
3. GTCMHIC or one of its business associates has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

Risk Assessment is the annual (or as needed due to material changes in circumstances), documented evaluation based on NIST, GLBA, HIPAA, NY DFS, and New York State standards that considers at least the following factors:

1. The nature and extent of the PHI/PII/NPI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI/PII/NPI or to whom the disclosure was made;
3. Whether the PHI/PII/NPI was actually acquired or viewed; and
4. The extent to which the risk to the PHI/PII/NPI has been mitigated (was the information immediately sequestered or destroyed?).

Digital Media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.

Non-Digital Media: Includes, for example, paper and microfilm.

Security Plans: Need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans.

Local Maintenance and Diagnostic Activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection.

Nonlocal Maintenance and Diagnostic Activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.

Account is any combination of a User ID (username) and a password that grants an individual access to a computer, an application, the network, or any other information or technology resource.

IT Administrator is any individual that has access to create, modify, or disable accounts

Organizational Users are GTCMHIC employees.

Non-Organizational Users are users from organizations other than GTCMHIC . Other organizations include Vendors, Consultants, and Reporting Partners. Non-organizational users requesting access to GTCMHIC devices, including devices that contain are required to complete an IT External IT System User Pledge. Non-organizational users with access to systems containing PHI/PII/NPI are required to provide a proof their identity which can include but is not limited to attesting to a completed I9 background check prior to employment with their organization or showing a valid state issued Photo ID. State issued photo ID's validated by a GTCMHIC Staff member prior to creation of new accounts.

Retired IT Asset can include data, monitors, laptops, desktops, servers, and portable data storage media. Once IT equipment has reached end of support, the PC will be decommissioned and prepped for disposal.

Decommissioned IT Asset are retired assets with Physical Data Storage media removed. Physical identifiers, such as GTCMHIC tags, labels, or stickers, are required to be removed from decommissioned assets prior to disposal.

Data Storage Media is a data storage device is any physical or electronic asset or computing hardware that is used for storing, porting, and extracting data files and objects. It can hold and store information both temporarily and permanently, and can be internal or external to a computer, server, or any similar computing device.

Greater Tompkins County Municipal Health Insurance Consortium

408 East Upland Road, Suite 2 • Ithaca, New York 14850 • (607) 274-5590
healthconsortium.net • consortium@tompkins-co.org

"Individually and collectively, we invest in realizing high quality, affordable, dependable health insurance."

RESOLUTION NO. XXX-2025 Approval of the the Greater Tompkins County Municipal Health Insurance Consortium's Participant Plan Option Parameters Policy

WHEREAS, the Greater Tompkins County Health Insurance Consortium, "Consortium", Municipal Cooperative Agreement, Section A, Participants, stipulates that participation in the Medical Plan(s) by some, but not all, collective bargaining units or employee groups of a Participant shall not be permitted without a Board approved waiver. Participants with a waiver allowing active employees not enrolled in Consortium benefit plan options, must, within 3 (three) years of the date of enrolling in the Consortium, fully enroll all of their active employees in Consortium plan options. Failure to comply with this provision may be grounds for termination from participation in the Consortium, and

WHEREAS, per Resolution No. 013-2016, the Consortium approved Guidelines for Members Changing Plans, but provided broad guidance on municipal member, "Participant", plan option parameters, and

WHEREAS, that since the implementation of the guidelines there have been an increase in the number of Participants and the development of Metal Level Plan options to the Consortium's menu of plan offerings, and

WHEREAS, the Consortium continues to work on plan consolidation to limit enrollment in the older style Indemnity (Classic Blue) and PPO plans and encourage all Participants to offer Metal Level Plans, to achieve administrative efficiencies. The Consortium has been successful in removing plan options that have no one enrolled or less than five subscribers per Resolution No. 051-2023, therefore be it

RESOLVED, on recommendation of the Operations Committee, That the Executive Committee, on behalf of the Board of Directors, hereby adopts the updated attached Participant Plan Option Parameters Policy,

RESOLVED, further, that the Policy will be made available on the Consortium website and sent via email to all Directors and Benefit Clerks to be implemented as of January 1, 2026.

****

Participant Plan Option Parameters Policy

Originally Adopted by Board of Directors 05-26-2016
Updated and Adopted by Board of Directors 09-25-2025 PENDING

Future Effective Date: January 1, 2026

Purpose:
The purpose of this policy is to establish the guidelines and parameters for selecting health insurance plans offered to Participants (Municipality Members) in the Greater Tompkins County Municipal Health Insurance Consortium (Consortium). This policy ensures the Consortium continues to provide competitive, cost-effective health insurance coverage while maintaining fairness and clarity in plan offerings.

Policy:
Section 1: Covered Lives
The Consortium offers coverage to the following individuals under its health insurance plans:

1. Active Employees
2. Non-Medicare-Aged Retirees
3. Medicare-Aged Retirees

Through an employee's enrollment, they become a subscriber, and the subscriber's dependents can be covered under the same health insurance plan. Subscriber dependents include:

- Spouse
- Domestic Partner
- Child (Natural, Adopted, Stepchild, Domestic Partner's child)

This coverage ensures that eligible dependents of subscribers are included in the same health insurance plan, provided they meet the definition of a dependent as outlined.

Section 2: Qualifying Events for Plan Changes
The following are qualifying events that allow changes in benefit plans at the time of the event:

- Marriage
- Divorce
- Legal Separation
- Birth
- Death
- Change in Legal Custody Status
- Dependent Aging Off (26 years of age)
- Loss of Eligibility for Medicare or Medicaid
- Loss of Coverage (from other health insurance plan i.e., spouse or parent coverage)
- Start or Loss of Employment
- Newly Negotiated Union Contract
    - (Requires a sixty-day notice for mass member movement outside of Open Enrollment.)

Participant Plan Option Parameters Policy

Originally Adopted by Board of Directors 05-26-2016
Updated and Adopted by Board of Directors 09-25-2025 PENDING

All other plan changes would occur during Annual Open Enrollment held November 1-November 30th of each calendar year, with an effective date of January 1st of the next calendar year.

Section 3: Municipal Member Plan Changes

- **a.** Any plan changes must be submitted to the Consortium using the "New Plan Addition Form" which can be provided upon request.[1]
- **b.** A 90-day notice must be given to the Consortium on any plan changes and all documentation is due no later than October 15th to ensure a January 1st start date.
- **c.** **Participants must maintain enrollment in the new plan for a period of at least three years**. This three-year commitment helps to balance the premium revenue against claims expenses, supporting the financial integrity and sustainability of the Consortium's health insurance offerings.[2]

Section 4: Participation in the Medical Plan(s):

a. Participation in the Medical Plan(s) by some, but not all, unions or employee groups of a Participant shall not be permitted unless the Board of Directors approves a waiver.[3]
b. A waiver may be granted if it is determined that the Consortium's plans are non-competitive with current union-contracted health insurance coverage. See Section 6: Waivers.

Section 5: Plan Selection Parameters for All Participants:

Grandfathering of past Indemnity and PPO plan options:
All Participants who currently offer Classic Blue 50/150, Classic Blue 100/200, PPO 10/35, PPO 10/100, and PPO 15/35, in combination with the 2T1, 2T2, 2T3, 3T3, 3T5a, 3T6, 3T7, 3T9, and 3T10 prescription plans will be asked to work on consolidating all active employees to the following plan offerings ~~within the next five years by allowing no new hires to enroll after 2031:~~

- Classic Blue 50/150 3T6 RX
- Classic Blue 50/150 3T9 RX
- PPO 10/35 3T7 RX
- PPO 10/35 3T6 RX

Board of Directors waivers can be granted for those unable to transition due to union contracts. Any plans that have zero enrollment will be eliminated from Consortium menu of plan offerings.[4]

---

[1] Motion No. 002-2023- Motion to Approve the Proposal of the "New Plan Addition Form" for Use by Municipalities to the GTCMHIC
[2] Resolution No. 013-2016- Approval of Guidelines for Members Changing Plans
[3] Municipal Cooperative Agreement: Section A Sub-Paragraph 5.
[4] Resolution No. 051-2023- Amendment to Resolution No. 032-2022 that Amended Resolution No. 011-2020 "Authorization by the Board of Directors to Remove Benefit Plans from the Consortium's Menu of Benefit Plan Offerings" By Restricting Plan Enrollment.

Grandfathering of Retirees' Coverage:
All retirees enrolled in Classic Blue plans and PPO plans will be grandfathered to remain on coverage. If a retiree transitions off any of the Classic Blue plans or PPO plans listed above, they cannot re-enroll. For example, if a retiree leaves Classic Blue coverage and switches to the Medicare Supplement Plan MS4, they cannot opt back into Classic Blue during the next open enrollment period.

Health Insurance Offering for Active Employees and Non-Medicare-Aged Retirees:
All Participants are permitted to select one or more of the Consortium's "metal level" benefit options as the Participant's health insurance offering to its entire population of employees and non-Medicare-aged retirees.

1. If offering more than one plan it must be due to the Participant's union contracts. Multiple plan options can lead to adverse selection, resulting in an imbalance between premium revenue and claims expenses.
2. If offering multiple plans, the Participant must be reducing plan selection down to two plan options for active employees and non-Medicare- aged retirees within five years of implementing multiple plan options. This allows for the transition from grandfathered plans to metal level plans and facilitates the renegotiation of union contracts.
3. The goal should be to only offer one health plan for all active and non-Medicare-aged retirees per Participant regardless of size.

The available plans for selection are:

- Platinum Co-Pay Plan
- Gold High Deductible Health Plan
- Silver High Deductible Health Plan
- Bronze High Deductible Health Plan

Health Insurance Offering for Medicare-Aged Retirees:
Participants may elect to include all their Medicare-aged retirees in the same plan chosen for active employees and non-Medicare-aged retirees, seek outside non-Consortium coverage such as a Medicare Advantage Plan Option, or they may choose one of the Consortium's Medicare Supplement Plans.[5] The available Medicare Supplement Plans are:

- Medicare Supplement Plan MS3
- Medicare Supplement Plan MS4

Section 6: Waivers:
A Participant may request a waiver for non-participation in the Consortium's medical plans if they can demonstrate that the Consortium's plans are not competitive compared to existing union-contracted health insurance coverage.

[5] Resolution No. 009-2024- Amendment to Resolution No. 013-2022- Clarification Regarding Participant Medicare-age Retirees in Relation to Municipal Cooperative Agreement (MCA) Requirement

Waiver Request Process:

- Waivers must be requested prior to September 1st to be submitted for review and approval by the Consortium's Board of Directors.
- A standard waiver will be granted for a period of three years or for the length of the union contract.

Conditions for Waiver:

- Participants granted a waiver allowing active employees to remain unenrolled in Consortium benefit plans must, within three years from the date of the waiver:
    1. Fully enroll all their active employees in the Consortium plan options or prove at the end of the three-year waiver period that the Consortium plans remain non-competitive with the current plan offerings and request an extension of the waiver.[6]
    2. Consortium predetermines acceptable level of adverse selection.

The waiver process is designed to ensure that the Consortium maintains its competitive edge in offering health insurance coverage, while also providing Participants with the flexibility to adjust based on their current union contracts and competitive options.

Responsibility:

It is the responsibility of all Participants to comply with the plan selection parameters outlined in this policy. This policy will replace all prior approved guidelines and precedents approved by the Board of Directors.[7] The Executive Committee, on behalf of the Board of Directors, will review and approve waivers as necessary.

Review and Amendments:

This policy will be reviewed periodically by the Board of Directors to ensure it remains relevant and effective. Any changes to the policy will require Board approval.

[6] Municipal Cooperative Agreement Section A. Participants Section.
[7] Resolution No. 013-2016- Approval of Guidelines for Members Changing Plans

Greater Tompkins County Municipal Health Insurance Consortium

408 East Upland Road, Suite 2 • Ithaca, New York 14850 • (607) 274-5590
healthconsortium.net • consortium@tompkins-co.org

"Individually and collectively, we invest in realizing high quality, affordable, dependable health insurance."

Resolution XXXX- 2025: Amendment to the Consortium Metal Level Options, Blue Traditional Options, and PPO Options Benefit Booklets AMENDMENT #1 January 2025

WHEREAS, the Greater Tompkins County Municipal Health Insurance Consortium ("Consortium") is committed to providing comprehensive and up-to-date health insurance coverage to its members, and

WHEREAS, changes to New York State law are applicable to the Consortium's benefit offerings as of January 1, 2025, requiring amendments to the Metal Level Options, Blue Traditional Options, and PPO Options Benefit Booklets ("Booklets"), note the update does not affect the Classic Blue Secure Medicare Supplement Benefit Booklets, and

WHEREAS, the Consortium wishes to amend the Booklets to reflect these required changes in order to maintain compliance with New York state law and ensure the ongoing availability of essential services for its members, particularly in relation to maternity, newborn care, and mental health care services, and

WHEREAS, the following amendments, to Maternity and Newborn Care as it pertains to Outpatient and Professional Services section, and edits to the Mental Health Care and Substance Use Services: Outpatient Services section, see subsequent pages, are being proposed to the Booklets, which will take effect on January 1, 2025,

THEREFORE, BE IT RESOLVED that the Operations Committee recommends the approval of Amendment #1 to the Consortium's Metal Level Options, Blue Traditional Options, and PPO Options Benefit Booklets, as outlined above, to the Executive Committee for final approval.

FURTHER RESOLVED that upon approval by the Executive Committee, the amendments will be implemented and reflected in the Consortium's Metal Level Options, Blue Traditional Options, and PPO Options Benefit Booklets as of January 1, 2025.

AMENDMENT #1
TO THE
GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM
BLUE TRADITIONAL OPTIONS 1 & 2
BENEFIT BOOKLET

Greater Tompkins County Municipal Health Insurance Consortium ("GTCMHIC") desires to amend the Blue Traditional Options 1 & 2 Benefit Booklet ("Booklet") to reflect certain changes under New York state law that are applicable in 2025. As such, effective as of January 1, 2025, the Booklet is amended in the following respects:

Section IX.
Outpatient and Professional Services

1. **Outpatient and Professional Services Section.** The following paragraph is added to Maternity and Newborn Care:

   The Plan also Covers the outpatient use of pasteurized donor human milk, which may include fortifiers as Medically Necessary, for which a Health Care Professional has issued an order for an infant who is medically or physically unable to receive maternal breast milk, participate in breast feeding, or whose mother is medically or physically unable to produce maternal breast milk at all or in sufficient quantities or participate in breast feeding despite optimal lactation support. Such infant must have a documented birth weight of less than one thousand five hundred grams, or a congenital or acquired condition that places the infant at a high risk for development of necrotizing enterocolitis.

Section XII.
Mental Health Care and Substance Use Services

2 **Mental Health Care and Substance Use Services.** The Mental Health Care – Outpatient Services item is replaced with the following:

   B. **Outpatient Services.** The Plan Covers outpatient mental health care services, including but not limited to partial hospitalization program services and intensive outpatient program services, relating to the diagnosis and treatment of mental health conditions. Coverage for outpatient services for mental health care includes Facilities that have been issued an operating certificate pursuant to New York Mental Hygiene Law Article 31 or are operated by the New York State Office of Mental Health, and crisis stabilization centers licensed pursuant to New York Mental Hygiene Law section 36.01 and, in other states, to similarly licensed or certified Facilities; and services provided by a licensed psychiatrist or psychologist; a licensed clinical social worker; a licensed nurse practitioner; a licensed mental health counselor; a licensed

marriage and family therapist; a licensed psychoanalyst; or a professional corporation or a university faculty practice corporation thereof. In the absence of a similarly licensed or certified Facility, the Facility must be accredited by the Joint Commission on Accreditation of Health Care Organizations or a national accreditation organization recognized by the Plan. The Plan Covers comprehensive neuropsychological examinations for dyslexia when performed by a Health Care Professional. Outpatient services also include nutritional counseling to treat a mental health condition.

Outpatient mental health care services also include outpatient care provided at a preschool, elementary, or secondary school by a school-based mental health clinic licensed pursuant to Mental Hygiene Law Article 31, regardless of whether the school-based mental health clinic is a Participating Provider. The Plan will pay a Non-Participating Provider the amount it has negotiated with the Non-Participating Provider for the outpatient mental health care services. In the absence of a negotiated rate, the Plan will pay an amount no less than the rate that would be paid under the Medicaid program. However, the negotiated amount or the amount paid under the Medicaid program will not exceed the Non-Participating Provider's charge. The school-based mental health clinic shall not seek reimbursement from You for outpatient services provided at a school-based mental health clinic except for Your in-network Cost-Sharing.

This amendment is hereby adopted by GTCMHIC as of the effective date set forth above.

GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM

_____
Signature

Rordan Hart
Printed Name

_____
GTCMHIC Chairperson

_____
Dated

AMENDMENT #1
TO THE
GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM
METAL LEVEL OPTIONS PLATINUM, GOLD, SILVER & BRONZE
BENEFIT BOOKLET

Greater Tompkins County Municipal Health Insurance Consortium ("GTCMHIC") desires to amend the Metal Level Options Platinum, Gold, Silver & Bronze Benefit Booklet ("Booklet") to reflect certain changes under New York state law that are applicable in 2025. As such, effective as of January 1, 2025, the Booklet is amended in the following respects:

Section IX.
Outpatient and Professional Services

1. **Outpatient and Professional Services Section.** The following paragraph is added to Maternity and Newborn Care:

The Plan also Covers the outpatient use of pasteurized donor human milk, which may include fortifiers as Medically Necessary, for which a Health Care Professional has issued an order for an infant who is medically or physically unable to receive maternal breast milk, participate in breast feeding, or whose mother is medically or physically unable to produce maternal breast milk at all or in sufficient quantities or participate in breast feeding despite optimal lactation support. Such infant must have a documented birth weight of less than one thousand five hundred grams, or a congenital or acquired condition that places the infant at a high risk for development of necrotizing enterocolitis.

Section XII.
Mental Health Care and Substance Use Services

2 **Mental Health Care and Substance Use Services.** The Mental Health Care – Outpatient Services item is replaced with the following:

B. **Outpatient Services.** The Plan Covers outpatient mental health care services, including but not limited to partial hospitalization program services and intensive outpatient program services, relating to the diagnosis and treatment of mental health conditions. Coverage for outpatient services for mental health care includes Facilities that have been issued an operating certificate pursuant to New York Mental Hygiene Law Article 31 or are operated by the New York State Office of Mental Health, and crisis stabilization centers licensed pursuant to New York Mental Hygiene Law section 36.01 and, in other states, to similarly licensed or certified Facilities; and services provided by a licensed psychiatrist or psychologist; a licensed clinical social worker; a licensed nurse practitioner; a licensed mental health counselor; a licensed

marriage and family therapist; a licensed psychoanalyst; or a professional corporation or a university faculty practice corporation thereof. In the absence of a similarly licensed or certified Facility, the Facility must be accredited by the Joint Commission on Accreditation of Health Care Organizations or a national accreditation organization recognized by the Plan. The Plan Covers comprehensive neuropsychological examinations for dyslexia when performed by a Health Care Professional. Outpatient services also include nutritional counseling to treat a mental health condition.

Outpatient mental health care services also include outpatient care provided at a preschool, elementary, or secondary school by a school-based mental health clinic licensed pursuant to Mental Hygiene Law Article 31, regardless of whether the school-based mental health clinic is a Participating Provider. The Plan will pay a Non-Participating Provider the amount it has negotiated with the Non-Participating Provider for the outpatient mental health care services. In the absence of a negotiated rate, the Plan will pay an amount no less than the rate that would be paid under the Medicaid program. However, the negotiated amount or the amount paid under the Medicaid program will not exceed the Non-Participating Provider's charge. The school-based mental health clinic shall not seek reimbursement from You for outpatient services provided at a school-based mental health clinic except for Your in-network Cost-Sharing.

This amendment is hereby adopted by GTCMHIC as of the effective date set forth above.

GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM

_____
Signature

Rordan Hart
Printed Name

_____
GTCMHIC Chairperson

_____
Dated

AMENDMENT #1
TO THE
GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM
PPO OPTIONS 1, 2 & 3
BENEFIT BOOKLET

Greater Tompkins County Municipal Health Insurance Consortium ("GTCMHIC") desires to amend the PPO Options 1, 2 & 3 Benefit Booklet ("Booklet") to reflect certain changes under New York state law that are applicable in 2025. As such, effective as of January 1, 2025, the Booklet is amended in the following respects:

Section IX.
Outpatient and Professional Services

1. **Outpatient and Professional Services Section.** The following paragraph is added to Maternity and Newborn Care:

   The Plan also Covers the outpatient use of pasteurized donor human milk, which may include fortifiers as Medically Necessary, for which a Health Care Professional has issued an order for an infant who is medically or physically unable to receive maternal breast milk, participate in breast feeding, or whose mother is medically or physically unable to produce maternal breast milk at all or in sufficient quantities or participate in breast feeding despite optimal lactation support. Such infant must have a documented birth weight of less than one thousand five hundred grams, or a congenital or acquired condition that places the infant at a high risk for development of necrotizing enterocolitis.

Section XII.
Mental Health Care and Substance Use Services

2 **Mental Health Care and Substance Use Services.** The Mental Health Care – Outpatient Services item is replaced with the following:

   B. **Outpatient Services.** The Plan Covers outpatient mental health care services, including but not limited to partial hospitalization program services and intensive outpatient program services, relating to the diagnosis and treatment of mental health conditions. Coverage for outpatient services for mental health care includes Facilities that have been issued an operating certificate pursuant to New York Mental Hygiene Law Article 31 or are operated by the New York State Office of Mental Health, and crisis stabilization centers licensed pursuant to New York Mental Hygiene Law section 36.01 and, in other states, to similarly licensed or certified Facilities; and services provided by a licensed psychiatrist or psychologist; a licensed clinical social worker; a licensed nurse practitioner; a licensed mental health counselor; a licensed

marriage and family therapist; a licensed psychoanalyst; or a professional corporation or a university faculty practice corporation thereof. In the absence of a similarly licensed or certified Facility, the Facility must be accredited by the Joint Commission on Accreditation of Health Care Organizations or a national accreditation organization recognized by the Plan. The Plan Covers comprehensive neuropsychological examinations for dyslexia when performed by a Health Care Professional. Outpatient services also include nutritional counseling to treat a mental health condition.

Outpatient mental health care services also include outpatient care provided at a preschool, elementary, or secondary school by a school-based mental health clinic licensed pursuant to Mental Hygiene Law Article 31, regardless of whether the school-based mental health clinic is a Participating Provider. The Plan will pay a Non-Participating Provider the amount it has negotiated with the Non-Participating Provider for the outpatient mental health care services. In the absence of a negotiated rate, the Plan will pay an amount no less than the rate that would be paid under the Medicaid program. However, the negotiated amount or the amount paid under the Medicaid program will not exceed the Non-Participating Provider's charge. The school-based mental health clinic shall not seek reimbursement from You for outpatient services provided at a school-based mental health clinic except for Your in-network Cost-Sharing.

This amendment is hereby adopted by GTCMHIC as of the effective date set forth above.

GREATER TOMPKINS COUNTY MUNICIPAL HEALTH INSURANCE CONSORTIUM

_____
Signature

Rordan Hart
Printed Name

_____
GTCMHIC Chairperson

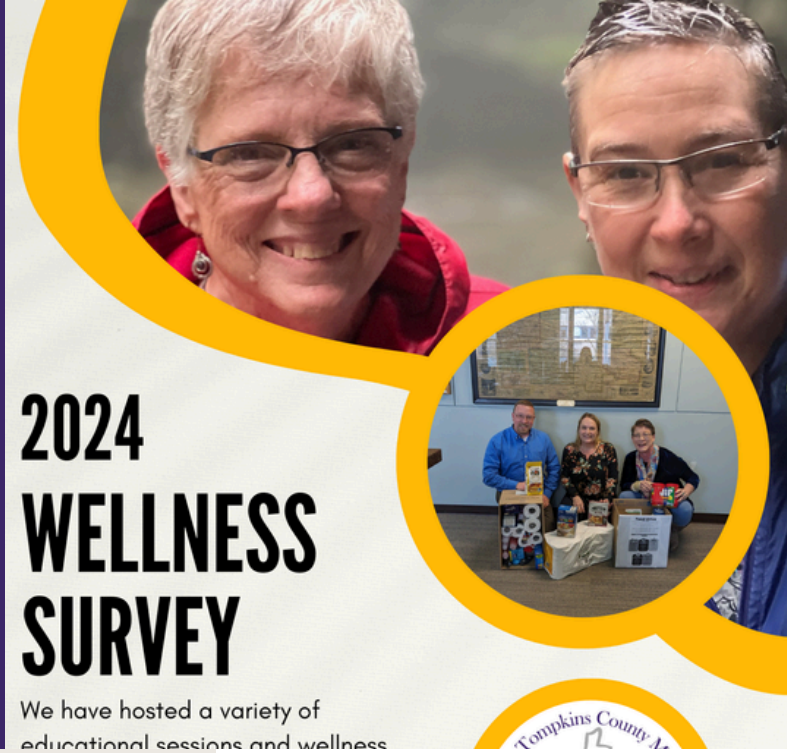
_____
Dated

2024 Wellness Program Survey Results

109 SURVEY PARTICIPANTS

IN 2024 WE HAD 583 MEMBERS PARTICIPATE IN CHALLENGES AND CLASSES.

THE MOST POPULAR CHALLENGES IN 2024 WERE "HEALTHY SPACES" AND "MAINTAIN DON'T GAIN"



Communication

- Numerous respondents assumed the wellness program was administered by their employer and not the Consortium.
- Suggestions for better communication included:
  - Flyers, emails, more advertising
  - Make sign ups easier
  - Flyers as attachments are easy to overlook
- We would encourage municipal members to clarify the difference between the Consortium Wellness Program and their yearly wellness incentive program.

Future Topics

Suggested future wellness topics include:

- Nutrition
- Mental Health
- Preventive Services
- Physical Activities- ie. hiking, yoga, strength training,
- Digital Detox
- Sleep
- Peri-Menopause
- Stress Reduction

"I have never had this type of blood work done before, great for me to know how I stand, physically." - Related to Blue4U clinics

'I WOULD LIKE TO PARTICIPATE MORE OFTEN BUT MANY TIMES MY WORK SCHEDULE DOESN'T COOPERATE." - RELATED TO HOW TO IMPROVE THE WELLNESS PROGRAM

"I enjoy the challenges, I always pick up a new tip."

We had mixed reviews on the online seminars, sometimes the time and date don't work for members. (We will start recording and sharing with those that register but miss the class).

We received a large amount of positive feedback on Blue4U coaching!

Challenge Prizes

Suggestions include:

- Google Watch
- Gym Membership
- Apple Air Pods
- Nutrition Coach for 1 Year
- FitBit
- Self-Care Experiences
- Gardening Supplies
- At-Home Gym Gear
- Restaurant Gift Cards
- Grocery Store Gift Cards

REGISTER FOR OUR WELLNESS EMAIL: HTTPS://WWW.HEALTHCONSORTIUM.NET/NEWSLETTER

Greater Tompkins County Municipal Health Insurance Consortium

408 East Upland Road, Suite 2 • Ithaca, New York 14850 • (607) 274-5590
healthconsortium.net • consortium@tompkins-co.org

"Individually and collectively, we invest in realizing high quality, affordable, dependable health insurance."

RESOLUTION: XXX-2025 – CANCELLATION OF CONSORTIUM HOSTED FLU CLINICS

WHEREAS, Previous Resolution Number 015 of 2017 continued the authorization for Greater Tompkins County Municipal Health Insurance Consortium ("Consortium") to sponsor and fund flu clinics and continue pharmacy benefit coverage for flu vaccinations for all eligible employees and retirees, spouses and dependents over the age of 19, and

WHEREAS, when administered outside of a flu clinic a member is able to receive a vaccine with no co-pay or member cost, excluding the facility fee, through a medical provider as the cost is billed as a medical claim through Excellus, and

WHEREAS, in 2015 the Committee was presented with an option to recommend that a pharmacy benefit be added to allow members to receive a vaccine at a pharmacy with no co-pay or cost to the member, which continues to be the current pharmacy benefit, and

WHEREAS, over the last five years, attendance at the Consortium hosted flu clinics has significantly decreased, and

WHEREAS, the availability of flu vaccination services through in-network pharmacies, which fully cover the cost of the vaccine under the Affordable Care Act (ACA) guidelines, provides a more accessible and convenient option for members, and

WHEREAS, as an Article 47 Consortium, we are committed to ensuring efficient use of resources and aligning with the most effective healthcare delivery models available to our members, and

WHEREAS, the Consortium can continue to provide resources and connections for municipal members who want to host independent flu clinics for their employees and retirees, and

NOW, THEREFORE, BE IT RESOLVED, that the decision to host future flu clinics be canceled, as the service is already fully covered at in-network pharmacies, offering a broader and more accessible means of vaccination to our members,

BE IT FURTHER RESOLVED, that we will continue to encourage our members to utilize in-network pharmacy flu vaccination services, in order to promote public health while ensuring the efficient allocation of resources, be it further

RESOLVED, on recommendation of the Operations Committee, that the Executive Committee, on the behalf of the Board of Directors, approves the cancelation of the Consortium hosting future flu clinics.

****