Greater Tompkins County Municipal Health Insurance Consortium

CYBER SECURITY RISK ASSESSMENT POLICY
Adopted 3/28/2019

This policy document provides the Greater Tompkins County Municipal Health Consortium (Consortium) the necessary requirements and procedures to develop, implement, and maintain a Cyber Security Risk Assessment Policy. At a minimum, this policy defines commitments necessary to conduct annual risk and security assessments on all Consortium information systems to help understand and identify all current threats. Through this risk assessment process, the Consortium will improve their definition and response to vulnerabilities and gaps within processes that will improve the confidentiality and integrity for information systems and data of which the Consortium is considered the owner. Use of Consortium resources imposes certain responsibilities and obligations on Consortium officers, employees, and other authorized users, and is subject to additional Tompkins County policies, and applicable local, state, and federal laws.

The Consortium has contracted with the Tompkins County Information Technology Services Department (ITS) to provide Information Technology (IT) support and required compliance of sections of 23 NYCRR 500 Cybersecurity compliance. This agreement, regarding IT support, further requires compliance the Acceptable Use of County Technology Resources (07-01), which states that resources owned, leased, or maintained by Tompkins County, and data contained therein, shall be used to support legitimate business purposes. The agreement results in Consortium IT resources and data to be managed as an extension of the Tompkins County IT systems, security, procedures and infrastructure.

Acceptable Use

This section provides a common standard for the appropriate use of Consortium IT resources to support productivity, reduce risk, and to facilitate efficiencies in meeting daily operations and business needs. The section also guides prudent and responsible use in response to regulatory compliance and data security requirements.

The IT resources covered by this policy include:

- All computers, computer workstations, laptops, tablets, other end user devices, and network resources managed by Tompkins County ITS, or connected to the Tompkins County data network.
- All Internet access, services and data owned, leased, and/or provided by Tompkins County or the consortium and all systems and associated data supported by Tompkins County ITS related to the management and utilization of internet access.
- All e-mail systems and services owned by Tompkins County or the Consortium and/or managed by Tompkins County ITS, including County e-mail account users, and all records and information stored at any point in time within the County's e-mail system.
- All telephone and voice-mail systems and services owned or leased by Tompkins County and/or managed by Tompkins County ITS and all records and information stored at any point in time within the County's telephone and voice-mail systems.

The Director of ITS, in consultation with the Consortium Executive Director, has the authority to revoke an individual's account access based on a determination of inappropriate use, or a need to respond to known IT security issues related to any IT resources covered under this policy. Upon determination by the Director of ITS and the Consortium Executive Director, that the identified IT issue has been mitigated, access may be subsequently restored.

A. Computers, Computer Workstations, Laptops, Tablets, Other End-user Devices, and Network Resources

1. Computer equipment will not be removed from Consortium premises without either prior written authorization from the Executive Director or alternative established agency procedures. All computer equipment when removed from Consortium premises must be used for the purpose of conducting Consortium business.
2. All computer equipment and peripheral storage devices that contain confidential information, Personal Information (PI), or Personal Health Information (PHI), must be configured with encryption provided by ITS prior to removal from Consortium premises.
3. Other than Consortium business software, officers or employees shall not install or store software without prior written authorization from the Executive Director and Director of ITS.
4. ITS does not provide data backup services for data stored locally (C:/ or D:/ drives) on computers, computer workstations, laptops, tablets, or other end-user devices. The use of external internet storage services or directly attached storage devices as means of primary data storage is not permitted without prior written authorization from the Executive Director and the Director of ITS.
5. Data not related to Consortium business should not be stored on any Consortium or County computer equipment or other network resource. Tompkins County ITS will not be responsible for personal data or data not related to Consortium business.
6. A user ID and password shall be required for all computers, computer workstations, laptops, tablets, and other end-user devices owned or managed by the Consortium.
7. All computers, computer workstations, laptops, tablets, and other end-user devices when not in use during non-working hours must be completely shutdown. Network logoff, hibernate, and standby do not qualify as a complete shutdown.

B. Internet Access

1. All Consortium officers or employees are eligible to receive internet access unless otherwise stated in writing by the Executive Director.
2. User-level access to internet services and web sites is granted based on individual and business requirements. County ITS, in consultation with the Executive Director, has the authority to determine and implement the appropriate level of internet access for users.
3. Temporary internet access for non- Consortium employees or non-authorized users must be coordinated through ITS.
4. To ensure security standards, ITS is authorized to access, monitor, block, and capture any internet traffic or data passing through or maintained within the County IT system(s).

C. E-mail

1. All officers and employees of Consortium are eligible to receive an email account, unless otherwise stated in writing by the Executive Director.
2. When conducting Consortium-related business via e-mail, officers or employees and other authorized users must use e-mail system(s) provided by the Consortium or approved via written authorization by the Executive Director that shall require a commitment by the user to transfer to the Consortium e-mail system all e-mails that deal with Consortium business.
3. E-mail access at Tompkins County is controlled through individual accounts and passwords. It is the responsibility of the individual to protect the confidentiality of his or her account and password information. Each user is responsible for the content and encryption procedures of all e-mail, including attachments sent from an individual user's account or an account for which he/she may have additional responsibility.
4. All data or information residing or originating on County e-mail systems are the sole property of the Consortium and are not considered personal or private.
5. Archival and backup copies of e-mail messages and content exist in compliance with Tompkins County's records retention practices despite deletion by an individual e-mail user. Backup and archiving procedures are to ensure system and data reliability, provide for retrieval of historical

email account content and information, and to meet regulatory requirements and respond to potential e-discovery and FOIL requests.

6. E-mail that contains confidential information, PI, PHI, and information protected by New York state or federal law shall not be transmitted without proper encryption.
7. E-mail distribution lists maintained by ITS must be used to only support Consortium business.
8. E-mail access will be removed when the individual's association with the Consortium is terminated, unless other arrangements are authorized by the Director of ITS. Tompkins County is under no obligation to provide copies of, forward or maintain any content associated with an individual's e-mail account after the term of employment has ceased.
9. The Director of ITS has the authority to establish best practices for e-mail account management, which may result in limitation of e-mail attachment and mailbox size.

D. Telephone and Voice-mail

1. Limited personal use of Consortium and County telephones is allowed provided that use does not interfere with staff productivity, pre-empt any Consortium or County policy, business activity, or consume more than an acceptable amount of resources as defined by the Executive Director.
2. Personal long distance, toll-based telephone calls originating from any Consortium telecommunication equipment is prohibited unless approved by the Executive Director. Officers or employees are required to reimburse the Consortium for all personal long distance, toll-based telephone calls that are directly charged to the Consortium or County.
3. To ensure security requirements and best practice, Tompkins County ITS has the authority to monitor, filter, capture, and access any call data detail passing through or maintained within its telephone and voice-mail system(s).

E. Prohibited Use and Failure to Comply

Consortium officers or employees shall always refrain from using Consortium and County IT resources for prohibited use. Prohibited use is subject to disciplinary action up to and including termination of employment or contractual agreement. Prohibited uses include but are not limited to the following illustrative list:

- Conducting private or personal for-profit or unauthorized not-for-profit activities;
- Conducting any solicitation for any purpose except those officially sanctioned by the Consortium;
- Conducting any unlawful activities as defined by federal, state, or local law, regulation, or policy;
- Producing, accessing, displaying, or transmitting sexually explicit, indecent, offensive, harassing or intimidating material, such as pornography or racial epithets, that could reasonably be considered threatening, offensive, intimidating, or discriminatory;
- Producing, accessing, or participating in online gambling;
- Attempting to modify or remove computer equipment, components, software, or peripherals without written authorization from the Executive Director and the Director of ITS;
- Attempting to subvert the security of the Tompkins County network or network resources;
- Downloading, installing, or running software that reveal or create weaknesses in the security of the Tompkins County network or network resources;
- Accessing, copying, modifying, or deleting files, data, accounts, and access rights for applications or system functions without written authorization from the Executive Director and the Director of ITS;
- Disclosing confidential, PI, PHI, or otherwise non-public data and information without following appropriate regulatory and/or department specific disclosure processes;
- Breaking into systems and databases or acting to disrupt the functioning of systems or causing unnecessary computing disruption.
- Using Consortium and/or Tompkins County IT resources to engage in acts that unfairly monopolize IT resources for personal use to the exclusion of others. This includes streaming media (such as use of Hulu, Pandora, or Netflix) for personal use.

F. Special Requests for Access to or Monitoring of Another User's Consortium and/or ITS Accounts

Requests for access to or monitoring of another employee's or authorized user's IT resources that are covered by this policy and that are owned, maintained, or leased by the Consortium or Tompkins County government, such as e-mail account, voice-mail account, internet use activities, and Consortium or County software systems, must be submitted in writing to the Director of ITS. There are no time-based restrictions on such requests. The employee or authorized user assigned to the accounts may or may not be notified of such requests for access or monitoring or of the outcome of such requests.

G. Password Requirements - Microsoft Active Directory (network access, email, Office 365)

Passwords are an important component of information and network security. The use of a Network- ID and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is met. The minimal requirements for Microsoft Active Directory passwords are as follows:

- At least eight characters in length, and a maximum of 16 characters in length.
- At least one upper case letter, one lower case letter, one number, and one non-alphanumeric character (!, $, #, %).
- The same password, or a like password (Example: Da!sy1234 change to Da!sy12345), cannot be reused within the previous 12 password resets.
- The forced change of Active Directory passwords will occur every 90 days.
- A password can only be reset once within a 24-hour period without assistance from ITS.
- Passwords cannot contain a users' name (Suzy Smith) and users' account name (ssmith).

Intrusion Detection Sensor (IDS)

Tompkins County ITS is responsible for the implementation, management, and responses associated with an Intrusion Detection Sensor (IDS). This IT security and risk assessment system has been completed in conjunction the placement of a local edge device, management of the sensor, monitoring of logs gathered by the sensor, and alerting for critical events. The County has determined that an IDS is necessary to monitor all Internet traffic for every device or IT resource connected to the County network in order to improve security and for infrastructure, systems, software and data. ITS includes this service in the IT support of the Consortium related to all County network connected Consortium IT infrastructure and local data.

Security and Risk Assessments

The Consortium will conduct annual security/risk assessments to evaluate the level of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits in coordination with the Tompkins County ITS Department. The Consortium shall conduct security/risk assessments at minimum annually, or whenever there are significant changes to the critical information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. An agency-wide third-party assessment of all critical systems and associated security controls will be conducted on average every 3 years, or in conjunction with a similar County project.

Breach Incident Procedure

This section provides a Consortium protocol for responding to and documenting any possible breach of confidentiality and/or data. Through following this protocol, Consortium employees ensure a reduced risk of breaches effecting our participating members and their employees related to health insurance information.

Numerous situations indicate a potential breach of private or confidential information. Any Consortium employee or member who becomes aware of a situation that may put private or confidential information at risk must report the discovery as a potential breach and fulfill their responsibilities as outlined in this procedure. Any Consortium employee who fails to fulfill any applicable responsibility from this procedure may face disciplinary action up to and including termination, but may also be subject to severe monetary penalties and incarceration by Health Insurance Portability and Accountability Act (HIPAA) Enforcement entities (Federal Office of Civil Rights and New York State Attorney General).

A. General Responsibilities

Consortium Member

All Consortium members—including employees, board members, independent contractors, trainees, volunteers and other persons whose conduct in the performance of work is under the control of the Consortium—must fulfill the following Consortium Member responsibilities:

- Complete all required trainings related to preventing and responding to breach incidents.
- Immediately after discovery (and in no case later than end of business day) report any possible breach of Consortium private or confidential information to the Tompkins County Information Security Compliance Officer via the procedure defined by ITS.
- At minimum, include in the report the Consortium employee, Consortium member, or Business Associate name, names of people involved, and a brief description of the situation/incident.
- As much as possible, take steps to reduce harm to the affected individual(s).

Information Security Compliance Officer

- Respond to reports by the Consortium, Consortium Members, or Business Associate without unreasonable delay and in no case later than 24 hours after any report.
- Take the steps in Section VI below for Business Associate incidents, or fulfill the remaining responsibilities in this section for internal incidents.
- Work with the Consortium, or affected Consortium Member, to complete the **Tompkins County Breach Incident Investigation Form** without unreasonable delay.
- Determine likelihood and extent of breach according to the breach risk assessment included on the **Greater Tompkins County Health Insurance Consortium Breach Incident Investigation Form**.
- Guide Consortium in notifying affected individual(s) according to legal requirements.
- Work with Consortium to mitigate harm to affected individual(s), and recommend procedural changes to prevent future similar incidents.
- Review high-risk assessments with the Consortium and possibly the Tompkins County Breach Incident Team.
- Review all Consortium breach incidents quarterly with the Tompkins County Compliance Committee.
- Report breaches to the New York State Agencies as required by law.
- Log breaches and document process.

Director of ITS/Designee

- Serve as back-up when the Information Security Compliance Officer is absent for 1 or more business day(s).

Consortium Executive Director

- Oversee implementation and training for the Risk Assessment policy and procedures to ensure that all department workforce members and members who have access to PI or PHI are fully trained in their responsibilities detailed in this procedure.
- Maintain Business Associate Agreements with HIPAA-compliant PHI incident procedures, including breach procedures.
- Work with the Information Security Compliance Officer to complete the *Tompkins County Breach Incident Investigation Form* without unreasonable delay.

- With guidance from the Information Security Compliance Officer/Breach Incident Team, follow all steps detailed in this procedure to notify affected individuals of breach according to legal requirements.
- Work with the Information Security Compliance Officer to mitigate harm to individual(s).
- Make procedural changes recommended by the Information Security Compliance Officer and/or the Breach Incident Team to prevent future similar incidents.
- Participate on the Breach Incident Team for breaches affecting the Consortium.

B. For a Potential Breach of ANY Client Information
Immediately after discovery (and in no case later than end of business day) any Consortium member must report via the *Greater Tompkins County Health Insurance Consortium Breach Incident Investigation Form*.

Without unreasonable delay and in no case later than 24 hours after receiving a report, the Information Security Compliance Officer must contact the Consortium to begin the incident investigation.

Without unreasonable delay, the Consortium will assist the Information Security Compliance Officer in completing the *Greater Tompkins County Health Insurance Consortium Breach Incident Investigation Form* with guidance from the Information Technology Services Department as needed.

If PHI may have been compromised, the Information Security Compliance Officer will provide as detailed information as possible in the following required 4 PHI risk factors in the Risk Assessment section of the *Greater Tompkins County Health Insurance Consortium Breach Incident Investigation Form*, explaining the assessment as clearly as possible:
- The nature and the extent of the PHI involved, including types of identifiers and likelihood of re-identification;
- The unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made;
- Whether the PHI was actually acquired or viewed, or if only the opportunity existed for the information to be acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

The Information Security Compliance Officer will request Breach Incident Team involvement in the incident response process for high-risk incidents (e.g. breaches involving more than one client's information, criminal penalties, monetary penalties or employment sanctions).

The Information Security Compliance Officer will determine, based on breach definitions in the applicable laws and the results of the Breach Risk Assessment section of the *Greater Tompkins County Health Insurance Consortium Breach Incident Investigation Form*, the likelihood and extent of the breach.

C. If Investigation and Risk Assessment Rule Out Breach of ANY Client Information
If the investigation and risk assessment rule out breach of client PI and show a low probability that PHI was compromised, the Information Security Compliance Officer will log the incident as a Non-Breach Incident on the Information Incident Log and will keep all related documentation for at least 6 years.

The Consortium Executive Director, with assistance from the Information Security Compliance Officer and/or Breach Incident Team, will make necessary procedural changes to prevent future similar incidents.

If an affected individual is aware that his/her information may have been breached, the Consortium Executive Director will send a letter summarizing investigative steps and notifying him/her that no breach occurred.

D. If Investigation Shows That a Breach of Client Private Information (PI) Has Occurred

If the investigation does not rule out breach of **Private Information (PI)**, the Information Security Compliance Officer will notify the Consortium Executive Director, and will consult the New York State ITS Enterprise Information Security Office (NYS ITS EISO) regarding the scope of the breach and restoration measures.

The Information Security Compliance Officer (and Breach Incident Team, if involved) will work with the Consortium Executive Director to determine and take steps to reduce harm to the affected individual(s). The Consortium Executive Director will provide to the Information Security Compliance Officer written documentation of harm mitigation steps taken.

The Information Security Compliance Officer and/or Breach Incident Team will guide the Consortium Executive Director in notifying all affected individual(s) "in the most expedient time possible and without reasonable delay, allowing for any necessary law enforcement delay", as required in New York State law. Notification will be directly provided to all affected individuals by **one** of the following methods:

- written notice; or
- electronic notice (only at affected individual's request); or
- telephone notice (log must be kept); or
- substitute notice by **all** of the following (allowed only when cost of other methods would exceed $250,000 or there are more than 500,000 affected individuals):
- e-mail (if e-mail address known); and
- conspicuous website posting; and
- notification to major statewide media

Notice must include a description of the information breached and contact information of the Tompkins County Information Security Compliance Officer.

The Information Security Compliance Officer will complete the NYS Security Breach Reporting Form, with guidance from the Consortium Executive Director and/or Breach Incident Team as needed, and send it to the three entities required on the reverse side of the form (A template for individual notice provided must be attached). If more than 5000 NYS residents are affected by the breach, the Information Security Compliance Officer will also notify consumer reporting agencies. **Reporting to NYS agencies must not delay notification of individuals.**

After review of the incident, the Information Security Compliance Officer (and the Breach Incident Team, if involved) will evaluate whether harm has been mitigated as much as possible, and will recommend to the Consortium Executive Director further mitigation steps as necessary. The Consortium Executive Director will provide to the Information Security Compliance Officer written documentation of harm mitigation steps taken.

The Information Security Compliance Officer and/or Breach Incident Team will work with the Consortium Executive Director to evaluate procedures. The Consortium Executive Director will make procedural changes recommended to prevent future similar incidents, and will provide written documentation of changes to the Information Security Compliance Officer.

The Information Security Compliance Officer will log the incident in the Information Incident Log as a "PI Breach" and will keep all related documentation for at least 6 years.

E. If Investigation Shows That a Breach of Protected Health Information (PHI) Has Occurred

If review of the Tompkins County Breach Incident Investigation Form Breach Risk Assessment by the Information Security Compliance Officer (and Breach Incident Team if involved) determines that there is more than a low probability that PHI was compromised, then a PHI breach has occurred. The following steps must be taken:

Notify Affected Individuals. Without unreasonable delay and in no case later than 60 calendar days after the incident, the Information Security Compliance Officer (or Breach Incident Team if involved) will guide the Consortium Executive Director in notifying affected individual(s) by first class mail that their PHI has been compromised. The notification may be provided in one or more mailings as information is available. When there is insufficient or out-of-date contact information that precludes written notification to the individual, the substitute notice will be provided according to the following rules:

a. For fewer than 10 individuals, substitute notice will be provided by the alternative form of notice that is most likely to reach the individual, and may be an alternative form of written notice, a telephone notice, or another form of notice.
b. For 10 or more individuals, substitute notice will:
    - Be in the form of either a conspicuous 90-day posting on the Consortium web site, or conspicuous notice in the major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
    - Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether his/her unsecured protected health information may be included in the breach.
c. If the individual is deceased, notice will be sent by first class mail to the next of kin or personal representative if the address is known. Substitute notice will not be provided.
d. In an urgent situation in which misuse of the compromised information could be imminent, the Consortium Executive Director may contact individuals by telephone or other means, as appropriate, in addition to the required written notice.
e. The notification will be written in plain language and will include, to the extent possible:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
    - A description of the types of unsecured protected health information that were involved in the breach;
    - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
    - A brief description of what Consortium is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
    - Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Concurrently with notification, the Consortium Executive Director, with guidance from the Information Security Compliance Officer (or Breach Incident Team if involved), will take all possible steps to mitigate harm to the affected individual(s) and make necessary changes to department procedure to prevent future breaches. The Consortium Executive Director will provide written documentation of steps taken and changes made to the Information Security Compliance Officer.

If the breach affects fewer than 500 individuals, the Information Security Compliance Officer will report the breach to NYS agencies as required above, and will notify required New York State agencies no later than 60 days after the end of the calendar year.

If the breach affects 500 or more individuals, in addition to individually notifying the affected person, the following steps will be taken:

- If the 500 individuals are in the same State or jurisdiction, the Breach Incident Team will provide notice with all elements above to prominent media outlets serving the State or jurisdiction without unreasonable delay and in no case later than 60 days after the incident.
- The Information Security Compliance Officer will report the breach to the required New York State agencies, without unreasonable delay and in no case later than 60 days after the incident.

To reduce harm to individuals and prevent future breaches, the Information Security Compliance Officer (and Breach Incident Team if involved) may review the incident after notifications are complete,

and may recommend additional needed harm mitigation and/or procedural changes to the Consortium Executive Director. The Consortium Executive Director will provide written documentation of any steps taken or changes made to the Information Security Compliance Officer.

The Information Security Compliance Officer will log the incident as a "PHI Breach" on the Information Incident Log and will keep all related documentation for at least 6 years.

F. Business Associate Breach Incidents

Written Contracts/Agreements with Business Associates will state that PHI Incidents must be reported to Consortium immediately upon discovery.

All Consortium Members must report any known Business Associate PHI Breach to the Consortium Executive Director and the Information Security Compliance Officer as required as above.

After receiving a Business Associate breach report, the Information Security Compliance Officer, will report the breach to the Consortium Executive Director.

The Information Security Compliance Officer, with oversight from the Consortium Executive Director and possibly the Breach Incident Team, will take the following steps:

- Contact the Business Associate to review details of the breach incident that were not provided in the report but are required for HIPAA notification.
- Review the harm mitigation steps taken by the Business Associate and recommend additional steps if necessary.
- Notify the affected individual(s) as required under HIPAA and detailed above.
- Notify New York State agencies as required under HIPAA and as detailed above.
- Review the Business Associate's safeguards for HIPAA Compliance and recommend changes to prevent future similar incidents.