

Greater Tompkins County Municipal Health Insurance Consortium

**Audit Committee**

Thursday, August 15, 2013 - 3 p.m.

**Ithaca Town Hall**

Agenda

1. Call to Order
2. Approve Minutes of July 18, 2013 meeting
3. Continued Discussion of Excellus Claims Process Privacy Questionnaire
4. Review of Draft Request for Proposals for Claims Process and Audit
5. Begin Explanation of Sections of Financial Report
6. Other Items
7. Adjournment

**Future Agenda Items:**

Review results of State Audit (Sept.) **\*Exit Meeting - August 22 - 9 a.m.**

Oversee development of Code of Ethics and Conflict of Interest Policy

Become familiar with Enterprise Risk Model (Don Barber requested)

**Minutes**  
**Greater Tompkins County Municipal Health Insurance Consortium**  
**Audit Committee**  
**July 18, 2013 - 3:00 p.m.**  
**Ithaca Town Hall**

Attendees: Steve Thayer, Judy Drake, Chuck Rankin, Laura Shawley (arrived at 3:33 p.m.)

Excused: Chantalise DeMarco

Guests: Judy Taber, Locey & Cahill; Rick Snyder, Tompkins County Finance Director

**Call to Order**

Mr. Thayer called the meeting to order at 3:05 p.m.

**Acceptance of Minutes**

The minutes of the May 16, 2013 meeting were approved as submitted.

**Discussion of Excellus Claims Process Privacy Questionnaire**

There was a brief discussion of the Privacy Examination Questionnaire that was a part of the New York State Audit. Mr. Thayer referenced string of emails in which Mr. Barber, Chair of the Board of Directors stated the Consortium's Treasurer receives paid claims detail information from both Excellus and ProAct regarding medical and pharmacy benefits paid on behalf of covered members and as a result the issues concerning the handling and securing of protected health information would most likely be an issue for the Audit Committee.

Ms. Taber distributed a copy of the examination questionnaire that was submitted to the State along with Regulation 169-Privacy of Consumer Financial and Health Information and Regulation 173-Standards for Safeguarding Customer Information. Attention was called to Section No. 10 within the Examination Questionnaire: "Has the organization developed its privacy policies and procedures in a written form? What management/internal control reports are available to monitor privacy compliance"?

The question was answered as follows: "No. The Greater Tompkins County Municipal Health Insurance Consortium has not developed any privacy policies and/or procedures at the present time. This is an item which is being taken back to the consortium Board of Directors as a potential action item. Said privacy policies and procedures will be developed as required based on the guidance of the New York State Department of Financial Services and the guidance of the Consortium's Legal Counsel".

The Committee agreed a privacy policy should be created, particularly because of HIPPA laws. Ms. Taber will look for policies that exist elsewhere that could be used as a template.

Mr. Thayer asked Ms. Pottorff to circulate the regulations to the Committee prior to the next meeting to prepare for continued discussion on this item.

**Review Initial Request for Proposals for Claims Process and Audit**

Mr. Thayer spoke of the need to have claims audited and data analyzed by a third party. The Committee began reviewing a draft Request for Proposals that was prepared in 2008 and

Consortium Audit Committee  
July 18, 2013

before the Consortium was formed. Ms. Taber said this is a specialized type of auditing that is focused more on the claims side rather than the financial side and there are many rules and regulations that are involved in addition to interpreting contract language. When Locey & Cahill perform this type of audit they usually evaluate the Administrator's work flow – how they do things, making sure their systems are secure, checking of who is involved in the process, and ensuring privacy.

A question was raised as to whether Tompkins County would still be the lead agency and it was assumed this would still be the case. Mr. Snyder saw no problems with continuing with this.

Ms. Taber asked what timeframe would be audited. Mr. Thayer suggested 2011 and 2012. Ms. Taber recommended including the period of transition to the new Pharmacy Benefits Manager. It was agreed to have the period 6-1-2011 thru 6-1-2013.

Ms. Shawley arrived at this time.

Ms. Taber said it may be a slight problem to get information from Medco as they are no longer the Consortium's Pharmacy Benefits Manager. Ms. Drake said it is very possible a provision about auditing was included in the original contract with Medco. Ms. Taber will look into this.

It was agreed Ms. Taber would forward a sample template of a medical claims Request for Proposals to Ms. Pottorff who will forward to Ms. Drake who will work on preparing new drafts of the medical and pharmacy Request for Proposals for the Committee to consider at the next meeting. It was noted that the RFP should include the City of Cortland and Town of Lansing.

Ms. Taber explained how the process works and said typically Excellus would provide a random sampling of claims for eight different claims payment amounts. Ms. Drake questioned whether Excellus could break those claims down by municipality. Ms. Taber said they could be asked.

### **Review of the 1<sup>st</sup> Quarter 2013 Financial Report**

Mr. Thayer asked if members had questions relative to the first quarter report that was prepared by the Bonadio Group and included in the agenda packet. Ms. Pottorff stated the Bonadio Group met with the State Department of Financial Services to review a draft report before it was submitted. Ms. Drake questioned whether these reports were still being reviewing by the Mr. Mickelson of the CDLM auditing firm. Upon being informed Mr. Mickelson did review the report Ms. Drake said she hopes that the Consortium can move away from that step eventually.

Consortium Audit Committee  
July 18, 2013

**Update on Transitions in Finance Department**

Mr. Snyder reported the Finance Office is still assisting the Bonadio Group in making the transition to Quickbooks. He said the employee within the Department that has been working closely with the Consortium will be leaving and there is a transition in place in that position as well. He said overall the transitions are going well.

Mr. Snyder requested and received signatures on banking forms by Mr. Thayer as Chief Financial Officer and Ms. Drake as Secretary.

**Request for Additional Information**

Ms. Shawley referred back to the financial filing and said she would like to get a better understanding of the numbers contained within the document. Mr. Thayer said getting an explanation of sections of the form could be included as regular agenda item.

**Adjournment**

The meeting adjourned at 4:15 p.m.

Respectfully submitted by Michelle Pottorff, Administrative Clerk



Municipalities building a  
stable insurance future.

125 East Court Street  
Ithaca, NY 14850  
607-274-5590  
INFO: [consortium@twcny.rr.com](mailto:consortium@twcny.rr.com)  
[www.tompkins-co.org/healthconsortium](http://www.tompkins-co.org/healthconsortium)

## Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

**PLEASE REVIEW CAREFULLY.**

### Use and Disclosures

**Treatment:** Your health information may be used by Greater Tompkins County Municipal Health Insurance Consortium (GTCMHIC) or disclosed to other organizations for the purpose of evaluating your health, diagnosing medical conditions, and providing treatment. For example, results of laboratory tests and procedures will be available in your medical record to all organizations who may provide treatment or who may be consulted by GTCMHIC representatives.

**Payment:** Your health information may be used to seek payment from your health plan, from other sources of coverage such as an automobile insurer, or from credit card companies that you may use to pay for services. For example, your health plan may request and receive information on dates of service, the services provided, and the medical condition being treated.

**Health care operations:** Your health information may be used as necessary to support the day-to-day activities and management of GTCMHIC. For example, information on the services you received may be used to support budgeting and financial reporting, and activities to evaluate and promote quality.

**Law enforcement:** Your health information may be disclosed to law enforcement agencies, without your permission, to support government audits and inspections, to facilitate law-enforcement investigations, and to comply with government mandated reporting.

**Public health reporting:** Your health information may be disclosed to public health agencies as required by law. For example, we are required to report certain communicable diseases to the state's public health department.

**Other uses and disclosures require your authorization:** Disclosure of your health information or its use for any purpose other than those listed above requires your specific written authorization. If you change your mind after authorizing a use or disclosure of your information you may submit a written revocation of the authorization. However, your decision to revoke the authorization will not affect or undo any use or disclosure of information that occurred before you notified us of your decision.

### Additional Uses of Information

**Information about treatments:** Your health information may be used to send you information on the treatment and management of your medical condition that you may find to be of interest. We may also send you information describing other health-related goods and service that we believe may interest you.

### Individual Rights

You have certain rights under the federal privacy standards. These include:

- The right to request-restrictions-on-the-use and-disclosure-of-your-protected-health-information.

- The right to receive confidential communication's concerning your medical condition and treatment.
- The right to inspect and copy your protected health information.
- The right to amend or submit corrections to your protected health information.
- The right to receive an accounting of how and to whom your protected health information has been disclosed.
- The right to receive a printed copy of this notice.

**GTCMHIC:** We are required by law to maintain the privacy of your protected health information and to provide you with this notice of privacy practices. We also are required to abide by the privacy policies and practices that are outlined in this notice.

**Right to Revise Privacy Practices:** As permitted by law, we reserve the right to amend or modify our privacy policies and practices. These changes in our policies and practices may be required by changes in federal and state laws and regulations. Whatever the reason for these revisions, we will provide you with a revised notice. The revised policies and practices will be applied to all protected health information that we maintain.

**Requests to Inspect Protected Health Information:** As permitted by federal regulation, we require that requests to inspect or copy protected health information be submitted in writing. You may obtain a form to request access to your records by contacting **Privacy Official — Attn: Employee Benefits Office- (your local municipality??).**

**Complaints:** If you would like to submit a comment or complaint about our privacy practices, you can do so by sending a letter outlining your concerns to: **Privacy Official, Attn: Benefits Employee Benefits Office, GTCMHIC, 125 East Court Street, Ithaca, NY 14850.**

If you believe that your privacy rights have been violated, you should call the matter to our attention by sending a letter describing the cause of your concern to the same address.

**You will not be penalized or otherwise retaliated against for filing a complaint. Contact**

**Person: You can receive further information concerning our privacy practices by contacting:**

**Plan Administrator  
Attn: Employee Benefits Office  
GTCMHIC  
125 East Court Street  
Ithaca, NY 14850  
607-274-5590**

This Notice is effective on or after \_\_\_\_\_2013.

---

Consortium Members:  
County of Tompkins ~ City of Ithaca ~ City of Cortland ~ Town of Caroline ~  
Town of Danby ~ Town of Dryden ~ Town of Enfield ~ Town of Groton ~ Town of Ithaca ~ Town of Lansing  
Town of Ulysses ~ Village of Cayuga Heights ~ Village of Dryden ~ Village of Groton ~ Village of Trumansburg

---

**NEW YORK STATE  
INSURANCE DEPARTMENT  
REGULATION NO. 173  
(11 NYCRR 421)**

**STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION**

I, GREGORY V. SERIO, Superintendent of Insurance of the State of New York, pursuant to the authority granted by Sections 201 and 301 and Article 24 of the Insurance Law, and in accordance with the provisions of 15 U.S.C. 6801, 6805(a)(6), 6805(b), 6805(c) and 6807 and 15 U.S.C. Chapter 94, do hereby promulgate a new Part 421 of Title 11 of the Official Compilation of Codes, Rules and Regulations of the State of New York (Regulation No. 173), to take effect upon publication in the State Register. Part 421 shall read as follows:

(ALL MATERIAL IS NEW)

**TABLE OF CONTENTS**

**GENERAL PROVISIONS**

- Section 421.0 Preamble.
- Section 421.1 Definitions.
- Section 421.2 Information security program.
- Section 421.3 Objectives of information security program.

**DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM**

- Section 421.4 Examples of methods of development and implementation.
- Section 421.5 Assess risk.
- Section 421.6 Manage and control risk.
- Section 421.7 Oversee service provider arrangements.
- Section 421.8 Adjust the program.

**ADDITIONAL PROVISIONS**

- Section 421.9 Determined violation.
- Section 421.10 Compliance date.

**GENERAL PROVISIONS**

**Section 421.0 Preamble.**

(a) This Part establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of

customer information, pursuant to sections 501, 505(b), and 507, codified at 15 U.S.C. 6801, 6805(b) and 6807, of the Gramm-Leach-Bliley Act.

(b) Section 501(a) provides that it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Section 501(b) requires the state insurance regulatory authorities to establish appropriate standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

(c) Section 505(b)(2) calls upon the state insurance regulatory authorities to implement the standards prescribed under Section 501(b) by rule with respect to persons engaged in providing insurance.

(d) Section 507 provides that a state regulation may afford persons greater privacy protections than those provided by subtitle A of Title V of the Gramm-Leach-Bliley Act. This Part requires that the safeguards established pursuant to this Part shall apply to nonpublic personal information, including health information, as health information is covered by the privacy protections set forth in Part 420 of this Title (Regulation 169).

### **Section 421.1 Definition.**

For purposes of this Part, the following definitions apply:

(a) "Customer" means any customer of the licensee as the term customer is defined in Section 420.3(h) of this Title (Regulation 169).

(b) "Customer information" means nonpublic personal information as defined in Section 420.3(r) of this Title, about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the licensee.

(c) "Customer information systems" means the electronic or physical methods used to access, collect, store, use, transmit, protect, or dispose of customer information.

(d) "Licensee" means a licensee as that term is defined in Section 420.3(p)(1) of this Title, except that "licensee" shall not include: a purchasing group; or an unauthorized insurer in regard to the excess line business conducted pursuant to Section 2118 of the Insurance Law and Part 27 of this Title (Regulation 41).



(e) "Service provider" means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services for the licensee.

**Section 421.2 Information security program.**

Each licensee shall implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities.

**Section 421.3 Objectives of information security program.**

A licensee's information security program shall be designed to:

- (a) Ensure the security and confidentiality of customer information;
- (b) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (c) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

**DEVELOPMENT AND IMPLEMENTATION OF INFORMATION SECURITY PROGRAM**

**Section 421.4 Examples of methods of development and implementation.**

The actions and procedures described in Sections 421.5 through 421.8 of this Part are examples of methods of implementation of the requirements of Sections 421.2 and 421.3 of this Part. Such examples are non-exclusive illustrations of actions and procedures that licensees may follow to implement Sections 421.2 and 421.3 of this Part.

**Section 421.5 Assess risk.**

The licensee:

- (a) Identifies reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;

(b) Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and

(c) Assesses the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

**Section 421.6 Manage and control risk.**

The licensee:

(a) Designs its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the licensee's activities;

(b) Trains staff, as appropriate, to implement the licensee's information security program; and

(c) Regularly tests the key controls, systems and procedures of the information security program. The frequency and nature of such tests are determined by the licensee's risk assessment.

**Section 421.7 Oversee service provider arrangements.**

The licensee:

(a) Exercises appropriate due diligence in selecting its service providers; and

(b) Requires its service providers to implement appropriate measures designed to meet the objectives of this Part, and, where indicated by the licensee's risk assessment, takes appropriate steps to confirm that its service providers have satisfied such obligations.

**Section 421.8 Adjust the program.**

The licensee monitors, evaluates, and adjusts, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

**ADDITIONAL PROVISIONS****Section 421.9 Determined violation.**

A contravention of Section 421.2, Section 421.3, or Section 421.10 of this Part shall be deemed to be an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in this state, and shall be deemed to be a trade practice constituting a determined violation, as defined in Section 2402(c) of the Insurance Law, in violation of Section 2403 of such law.

**Section 421.10 Compliance date.**

Each licensee shall establish policies and systems and implement an information security program pursuant to this Part by June 1, 2002.

I Gregory V. Serio, Superintendent of Insurance, do hereby certify that the foregoing is the First Amendment to 11 NYCRR 421 (Regulation 173) promulgated by me on February 7, 2002 pursuant to the authority granted by granted by Sections 201 and 301 and Article 24 of the Insurance Law, and in accordance with the provisions of 15 U.S.C. 6801, 6805(a)(6), 6805(b), 6805(c) and 6807 and 15 U.S.C. Chapter 94, to take effect upon publication in the State Register.

Pursuant to the provisions of the State Administrative Procedure Act, prior notice of the proposed amendment was published in the State Register on November 21, 2001. No other publication or prior notice is required by statute.

---

Gregory V. Serio  
Superintendent of Insurance

February 7, 2002