TOMPKINS COUNTY ADMINISTRATION

County Compliance Committee

Think Compliance First!

2014 Year-end County Compliance Progress Report

Year At-a-Glance.

The Tompkins County Compliance Program ("Program") is designed to demonstrate good stewardship of the people's trust and resources, focusing on regulatory compliance controls, policies, and staff training that encourage a culture of integrity and transparency. A ten-member Compliance Committee works closely with the County Administrator in the implementation of the Program, which includes the following core elements:

- Reviewing, assessing, and revising existing policies and procedures for the purpose of addressing areas of compliance risk;
- Working with departments to develop standards and processes for addressing specific functional risk areas;
- Developing internal systems and controls to promote compliance in accordance with our legal and ethical requirements;
- Identifying/monitoring potential non-compliant issues; and
- Assisting with education and outreach to staff.

During the 2014 operating year, the Committee increased its membership from eight to ten members with the addition of the Healthcare Privacy and Security Officer and the Director of Human Rights. The Committee continued its work in the area of information technology (IT) compliance, including privacy, data protection and information security policy development. This work was highlighted by the successful completion of two new administrative policies: Acceptable Use of County Information Technology Resources and Breach-Incident Response. Both policies were adopted by the Legislature on September 2, 2014. The Committee also revised the Compliance Program Document to include information and guidance related to the work of the Privacy and Security Work Group (PSWG) and a County-wide administered Limited English Proficiency (LEP) Plan. Finally, efforts continued in the areas of program outreach and training to all County staff and elected officials. The *Key Accomplishments* section of this report provides details on all of these activities.

Key Accomplishments.

Task 1: *Support Information Technology (IT) Compliance and Policy Development.*

The Compliance Committee, with assistance from the Information Technology Services (ITS) director and staff, continues to gain a clearer understanding of the trends in perceptions and potential threats that affect the collection, management, and safeguarding of personal and confidential information. One way this is being accomplished is by working closely with the ITS director in the development of policies that guide appropriate use of County technology resources and that inform best practice for data management and protection. During 2014, the Committee reviewed the first in a series of ITS policies with a focus on end-user awareness and data security. The new policy on Acceptable Use of County Information Technology Resources, adopted in early September, provides a common standard for prudent and responsible use of the County's information technology assets, such as computers, networks, and Internet access, to support productivity and to facilitate efficiencies in meeting daily operations. The Committee also conducted the initial review of the County's new policy on data breach response and mitigation. Also adopted in September, the Breach-Incident Response policy ensures that Tompkins County's response to any suspected breach of private and confidential information complies with State and Federal laws and minimizes harm to individuals served or employed by the County. These policies have been incorporated into the Administrative Policy Manual, which can be accessed at http://tompkinscountyny.gov/ctyadmin/policy/index . Further, the Healthcare Security and Privacy Officer, Deputy ITS Director, Department Heads, and the County Compliance Officer have started to educate the Tompkins County Workforce on these new policies and procedures.

In the coming year, the Compliance Committee will continue to assist with initial review of policy content and will support the ITS director as needed during the formal policy amendment process. ITS policies currently under development include Data Inventory, Classification, and Protection; User Identification, Passwords and Account Management; Remote Access and Mobile Device Management; Cellular Phones; Social Media; Information Technology System Roles and Authority; and Information Technology Risk Assessment and Management.

Task 2: *Recommend a Strategy for Staff Training on IT Policies.*

The Compliance Committee seeks to recommend a strategy for staff training to promote responsible and confident use of IT resources, and for advancing awareness of the organization’s commitment to good privacy and data protection practices. The focus in 2014 was on evaluating online training possibilities, which included the County’s own Lawson server as well as other third-party solutions. One third-party solution closely considered is an interactive, self-paced training series produced by the SANS (**S**ysAdmin, **A**udit, **N**etworking and **S**ecurity) Institute. SANS is a cooperative research and education organization and an industry leader in information and cyber security training. The SANS online courseware allows staff to choose from a menu of training modules in order to satisfy Health Information Affordability and Accountability Act (HIPAA) requirements and broader data protection training for satisfying our internal ITS compliance requirements. Additionally, these modules appear to align with current (and future) ITS policy, providing an interactive learning experience to meet both individual staff and County organizational needs for capacity building. As the review of potential training solutions continues, an interim approach to training staff on ITS policies is in progress. A brief overview of the new ITS policies has been added to existing compliance and HIPAA training curriculums. This short-term approach will remain in place until a more comprehensive training solution is established. Meanwhile, the Committee is also involved in discussions with the Personnel Commissioner about implementing a county-wide learning management platform that would serve as a central repository for all required staff training, including ITS compliance.

Task 3: *Recommend a process for conducting Security Risk Analysis required by HIPAA.*

HIPAA requires each covered County department to conduct an accurate and thorough HIPAA Security Risk Analysis (SRA) to identify how protected health information (PHI) may be at risk. To help departments meet this requirement, the PSWG researched, tested, and reviewed available SRA tools. The review included tools offered by Clearwater Compliance, the HIPAA Collaborative of Wisconsin, the Healthcare Information and Management Systems Society, and the National Institute of Standards and Technology (NIST).

The PSWG initially selected the NIST tool because it combined into one free, user-friendly application an accounting of all HIPAA Security Rule requirements with the NIST standards cited in U.S. Department of Health and Human Services Office of Civil Rights (OCR) SRA guidance. In March of 2014, the U.S. Office of the National Coordinator for Health Information Technology (ONC) and the OCR released a new, free SRA tool. The PSWG tested the tool and found that it improved upon the NIST tool, while maintaining the incorporation of Security Rule requirements and the NIST standards.

The Healthcare Security and Privacy Officer and the PSWG are currently using the new ONC/OCR tool to assist HIPAA-covered County Department Heads, at their request, with completion and review of their required SRAs. Department Heads may contact the Healthcare Security and Privacy Officer to request assistance with their SRA. The length of time needed for each SRA varies depending on the size and complexity of a Department’s technology, with the smallest and least complex departments requiring a minimum of two weeks.

SRA reviews will be completed by Department Heads annually, during the first quarter of the year, and whenever there is a significant technology change (e.g., implementation of a new electronic health record protocol). HIPAA risk mitigation plans resulting from department SRAs will serve as work plans for department HIPAA risk management processes.

SRAs and resulting risk mitigation plans from all departments will be stored electronically in one central folder to make them easily accessible for centralized risk management activities, including internal and external compliance audits. The Healthcare Security and Privacy Officer and the PSWG will periodically monitor progress on risk mitigation plans, and offer assistance to departments as needed.

Task 4: *Update the Compliance Program Document.*

The County Compliance Program Document (CPD) is the blueprint for the Program, including its purpose, related policies, and procedures for guiding program success. The CPD was developed in 2011 when the County Compliance Program was established. Since that time, there have been changes in legislation, such as the modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, as well as adjustments to our compliance program in general. Given this, the Committee found it necessary to conduct a thorough review of the CPD, focusing on the need for policy updates, new content, and overall improved document quality that takes into account consistency and readability. In addition to formatting changes and updates to ensure accuracy, key content additions to the CPD include the following:

- *Breach Incident Procedures*—In accordance with the 2013 HIPAA Omnibus Rule requiring guidelines for safeguarding personal information (PI) and personal health information (PHI), the CDP now includes a common standard for reporting a known or suspected breach (i.e., unauthorized access, use, or disclosure) of PI or PHI. The CPD provides a quick overview of the regulation, specific procedures for responding to a breach, and the new Breach Incident Investigation Form for documenting the breach and tracking its resolution.

- *Limited English Proficiency Plan*—As a recipient of federal funds, Tompkins County is required to develop and implement a system by which persons with Limited English Proficiency (LEP) can meaningfully access County programs and services. Pursuant to Title VI of the Civil Rights Act and Executive Order 13166, Tompkins County now has in place an improved county-wide approach to providing reasonable accommodations for LEP individuals. The primary provisions of the LEP Plan are to (1) identify individuals who need language assistance, (2) identify ways to accommodate LEP persons, (3) train staff regarding the Plan for accommodating LEP persons, (4) provide notice to LEP populations about the Plan, and (5) regularly monitor and update the Plan.

The fully revised CPD is available on the compliance program Website at http://www.tompkinscountyny.gov/tccp.

Task 5: *Add to the Compliance Fact Sheet Series.*
In the second year of the compliance program, the Committee introduced a “fact sheet” series as a simple, handy approach to emphasizing key points of the County Compliance Program. Each fact sheet is limited to two pages of information (one sheet of paper with double-sided print) and only focuses on a single topic or issue.

The Committee thought it important to have a fact sheet that raises awareness about the protection of Personal Information (PI) and Protected Health Information (PHI), highlighting the potential risks, and to provide guidance, including reasonable and appropriate measures to protect the integrity, confidentiality, and security of PI and PHI. The Committee selected this topic because it has become a major concern for local governments due to the volume of information we handle on any given day and the methods we use for maintaining and sharing this information in our various interoperable electronic environments.

The unlawful use or misuse of PI or PHI can impact an individual’s ability to get a job, secure a loan, obtain insurance, defend against identity theft, or benefit from public programs. Harm to our County organization due to unauthorized access or disclosure of PI and PHI could include legal liability, the payment of fines imposed by regulatory authorities, and loss of the public trust. The new fact sheet on *Safeguarding Protected Information* covers these items and also gives instruction on what to do in the case of potential loss, theft or compromise of PI, PHI, or other sensitive data, whether suspected or confirmed. The new fact sheet on *Safeguarding Protected Information* can be found on the compliance program Website at http://www.tompkinscountyny.gov/tccp.

Issues and Opportunities.
There were no significant issues identified during the 2014 operating year. Opportunities for Program enhancement are discussed in the following section that outlines the Committee’s work plan for the coming year.

What to Expect in 2015.

Compliance Education and Training. The Committee will continue to provide education opportunities regarding the importance of compliance and highlighting the components of the County's Program. Emphasis will be on risk-prevention, data protection and IT compliance, and accountability to ensure that County employees (and contract agencies) are following all applicable laws and regulations and know what to do if they witness or are asked to participate in any activity that could result in non-compliance. The Committee will also continue to provide guidance on compliance training content as plans evolve and decisions are made regarding a county-wide online learning management system.

Policy Review and Development. The Compliance Committee will continue to provide general oversight and review of the development of County-wide administrative policies that support good practice in compliance governance. The Committee recognizes that sound policies, coupled with a straightforward process for adoption and implementation, help make compliance a part of the fabric of the organization. Clear, unified administrative policies provide standards and procedures to both minimize risk and comply with regulations now and in the future.

The policy-related initiatives outlined for 2015 include the following:

- Continuing review of IT policies prior to formal policy amendment processes.
- Incorporating HIPAA updates, per the work of the Privacy and Security Work Group (PSWG), in the form of new administrative policy or potential revisions to the Compliance Program Document.
- Examining the current policy amendment process (Administrative Policy 01-04) carefully in order to make adjustments where necessary.

Risk Assessment. One element of an effective compliance program is the routine evaluation of its utility and benefit, that is, actively seeking evidence that the program is actually working. The Department of Health and Human Services Office of Inspector General (OIG)—the entity that produced the compliance model most widely used by state and local governments—recommends that one way organizations can evaluate compliance program effectiveness is through routine risk assessments. The results offer quantifiable data on workforce knowledge and perceptions that can be used to guide and monitor compliance program success. The Committee will re-visit the department risk assessment exercise launched in 2012, and will look to revise the content to meet current trends with the goal of conducting a follow-up risk assessment survey in 2016. Managing the information that is gathered will be challenging, but the learning gained will help determine how the Committee needs to work with departments to implement effective risk mitigation strategies.

This report prepared and submitted by

The Tompkins County Compliance Committee

Paula E.F. Younger
Deputy County Administrator
County Compliance Officer
Chair, County Compliance Committee

Patricia Carey
Commissioner
Department of Social Services

Frank Kruppa
Director
Public Health Department

Sue Romanczuk
Commissioner
Department of Mental Health Services

Deb Prato
Commissioner
Personnel Department

Greg Potter
Director
Information Technology Services

Rick Snyder
Director
County Finance Department

Karen Baer
Director
Office of Human Rights

Karen Gonta
Healthcare Security & Privacy Officer

Jonathan Wood
County Attorney