TOMPKINS COUNTY ADMINISTRATION
County Compliance Committee

Think Compliance First!

2013 County Compliance Program Year-End 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. An eight-member Compliance Committee works closely with the County Administrator in the implementation of the Program, which includes the following core elements:

- Reviewing and assessing existing policies and procedures that address compliance risk issues;
- Working with departments to develop standards and processes that address specific risk areas and that promote compliance according to legal and ethical requirements;
- Developing internal systems and controls to carry out compliance standards and policies;
- Identifying/monitoring potential non-compliant issues; and
- Assisting with education and outreach to staff.

During the 2013 operating year, the Committee continued its work in the area of IT compliance by supporting the Information Technology Services Department in the review of new policies that set standards for acceptable use of County IT resources while ensuring data integrity and safety. The Committee also worked to strengthen the use of the *K-Checks*™ system for exclusion screening requirements, reaching out to specific staff who rely most on the use of this service. The Committee's largest undertaking, which will continue through 2014, was the review of the statutory amendments made under the Health Information Technology for Economic and Clinical Health Act (HITECH). Additionally, a Privacy and Security Work Group was established to assess the County's compliance with the new HITECH rules and to set in place policy and procedures where necessary. Finally, efforts continued in the areas of program outreach and training to all County staff and elected officials. The following *Key Accomplishments* section of this report provides details on all of these activities.

Key Accomplishments.

Task 1: *Assisted the ITS Director in the review of new IT security and acceptable use policies and procedures, and offered guidance on effective implementation strategies.*

A series of eight new County-wide IT policies were identified and outlined in 2013. As a matter of prioritization, the first in the series is a policy to guide Acceptable Use of information assets owned or maintained by the County. The policy provides a common standard for all staff, and guides prudent and responsible use in response to regulatory compliance and data security requirements. This policy was reviewed by the County Compliance Committee and by all County departments via the formal Impact Review process. We hope to have the policy adopted by the end of the first quarter of 2014.

In addition to general ITS policy development, assistance was provided to those departments that are required to comply with the HIPAA and HITECH federal mandates. Specifically, policy drafts were developed to accommodate Notice of Privacy Practice, Breach of Notification/Incident Response, Safeguarding Protected Health Information, and Laptop Use. Some of these same topics will be addressed in the upcoming county-wide policies. See additional information in the "Issues and Opportunities" section of this report.

Task 2: *Provided training and outreach to all county employees and provided guidance on best approaches for incorporating county compliance program content into an overall county training plan.*

Employee training is a key component of an effective compliance program. County employees and governing board members are expected to be familiar with the Program and to have a solid working knowledge of how the core elements of the Program relate to assigned job responsibilities. Although responsibility for this training rests with individual department heads, the Compliance Committee offered ten training session options to employees and governing board members. The sessions were offered October through December and were facilitated by County Compliance Committee Chair Paula Younger. There were a total of 130 training participants representing 15 County departments, including the County Legislature.

Compliance Program outreach continued via Department Head meetings, Cabinet meetings, and individual staff meetings upon request. Further, the County Compliance Program Web pages remain accessible to all staff. Web content includes an overview of the Program, helpful fact sheets to facilitate knowledge transfer, reference to the newly revised Code of Ethics, instructions for reporting concerns of fraud and abuse, and links to year-end progress reports.

One of the challenges for 2014 will be determining the best approach for incorporating County Compliance Program content into an universal plan of "required training" that will be established for all employees. The best approach will ensure consistency in compliance training content, minimize the use of limited trainer resources, reach larger audiences in less time and with more flexibility, and provide an efficient way of communicating compliance updates in a timely manner. Last November, Department Heads began the first in what will be a series of discussions about "required training." The discussion will focus on training relevant to all County staff, determining what training should be required across all workforce disciplines, and a common framework for managing and tracking training delivery. The County Compliance Committee will continue to monitor these discussions and will look for opportunities to provide guidance on compliance content once a strategy for implementing required training has been established.

Task 3: *Clarified the Exclusion Screening protocol used by county departments that issue RFPs, bids, and contracts.*

Earlier this year, the Office of the Medicaid Inspector General (OMIG) offered new guidance on employing or contracting with individuals or business entities that have been excluded from participating in state or federally funded healthcare programs. The referenced programs include any County health programs and services supported by Medicaid dollars. The new guidance provides that no health care program payment may be made for any items or services furnished (1) by an excluded person or (2) at the medical direction or on the prescription of an excluded person. OMIG has made it clear that failure to screen is a basis for imposition of monetary penalties.

At the outset, our County Compliance Program included guidance on Exclusion Screening. In addition to establishing a formal policy, the County also contracts with Kinney Management Services, Inc. (KMS) to perform our routine screening. Through KMS' web-based software, *Kchecks*™, the County is able to search against a central repository for individuals and entities that have been excluded. In accordance with OMIG guidelines and with the assistance of the *Kchecks*™ system, the County is able to determine the "excluded" status of potential employees and contractors.

Although our Exclusion Screening policy has been in place since 2011, some of the staff that issue RFPs and contracts or who participate in the coordination of these activities were not fully aware of how the screening is done or the process for requesting screening. So on April 22, these staff along with Compliance Committee members, Finance Department staff, and the County Risk Manager, participated in *Kchecks*™ training. The session was conducted by a KMS representative via Web interface. The training covered the following *Kchecks*™ functions:

- Search functions of State databases and Federal OIG, EPLS/SAM, and Treasury Databases;
- Manual search functions for screening a single business entity or individual;
- Secure upload capability for screening multiple names or contractors;
- Review of monthly email notifications of potential "excluded" matches;
- Recording actions taken on the matches found; and
- Availability of an electronic audit trail of matches and resolution history, if needed for audit purposes.

Following the training session, the group had an in-depth discussion about our County policy and the role and responsibilities of those involved in the managing and monitoring the screening process.

Task 4: *Established an internal Privacy and Security Work Group to determine policy needs and other activities related to compliance with federal and state privacy and security rules to safeguard protected health information.*

In January of 2013 the federal Department of Health and Human Services issued a final rule (Omnibus Rule) to modify the Health Insurance Portability and Accountability Act (HIPAA) regarding Privacy, Security, and Enforcement rules, and to implement the statutory amendments made under the Health Information Technology for Economic and Clinical Health Act (HITECH) that strengthen privacy and security protections of individuals' health information. This Omnibus rule brings a sense of urgency and accountability regarding the safeguarding of protected health information (PHI), creates new enforcement mechanisms, and significantly increases the penalties* that can be imposed for violations. These regulations are complex and expansive and require detailed and consistent attentiveness as to how protected health information is created, transmitted, stored, and received. Because Tompkins County government acts as both a provider and user of PHI, we are obligated to demonstrate compliance with these regulations.

To that end, a Privacy and Security Work Group (PSWG) was created in 2013. The PSWG members include the Public Health Administrator, Mental Health Deputy Commissioner/Mental Health Compliance Officer, Deputy Director of Information Technology, Department of Social Services Commissioner, and a newly appointed Healthcare Security and Privacy Officer who chairs the group. At-large members include the Deputy County Administrator and the Mental Health Commissioner. Beginning with the departments using the largest amount of PHI, the Work Group has begun to lead the following Health Information Privacy and Security activities for the County that will continue through 2014:

- Complete a PHI data flow analysis for each department;

- Review related department policies and procedures to compare against HITECH requirements and update where necessary;
- Update the County HIPAA Workforce Training program to ensure that required staff are trained;
- Update Business Associate Agreements to comply with new requirements;
- Complete and document continuing privacy and security analyses that identify vulnerabilities in safeguarding Protected Health Information, and determine priorities for implementation of procedures that remove or reduce risk.

*Note: Previously, HIPAA penalties could be assessed at $100 per violation, capped at $25,000 per year for multiple violations of an identical requirement or prohibition. HITECH sets the range at $100 up to $50,000 per violation, capped at $1.5 million per year for multiple violations of an identical requirement or prohibition.

Issues and Opportunities.

The need for protecting IT assets has swelled beyond routine maintenance and firewalls. Safeguarding hardware, systems, and electronic data is an emerging compliance issue that impacts almost every facet of our County operations. Although the widespread adoption of technology surely promotes productivity and increases efficiency, it also puts greater pressure on the need for improved knowledge management practices and tighter controls on information access and data integrity. Our work in 2013 laid the foundation for what is expected by State and Federal regulatory authorities, but it is imperative that we continue to take the necessary steps to strengthen policies and procedures in the areas of privacy and data security. For example, the ITS department has completed an upgrade of all County-wide security management software based on a single platform known as Sophos. The upgrade includes Email SPAM filtering, Email encryption, hard drive encryption, Anti-Virus/MalWare, and Internet filtering. Upon completion of this project, ITS has a clearer understanding of how the use and functionality of security software might better inform future policy and procedures.

Ensuring best practice for training staff on policy implementation is of equal importance. Raising awareness along with education helps staff understand their responsibilities, minimizes risk, and demonstrates accountability. A good illustration of this is the Cyber Security training session that was coordinated with ITS and presented to staff at the Mental Health and Public Health departments. Training programs like this help staff learn how to protect browsers from attack, how to properly lock computers, and how to make sure passwords are strong. Timely and targeted training aims to influence user behavior, narrowing a costly gap that can undermine the technology put in place to address security problems.

What to Expect in 2014.

Review IT Policies. The policies anticipated for Compliance Committee review are Breach Notification, Account Management, and Data Inventory/Classification. Review of the Data Inventory/Classification policy will also assist ITS in determining the best approaches for working with departments to establish how data is classified, and then the most prudent steps for ensuring data protection. The Compliance Committee will ensure that the final versions of these policies move as seamlessly as possible through the County's Impact Review and Legislative Review processes.

Recommend a Strategy for Staff Training on IT Policies. The Committee recognizes that issues surrounding employee use of computers and other County IT assets don't cease once the right equipment is installed. Appropriate IT training for staff is important, and it must be planned carefully to strike a balance between acceptable use and minimizing risk, while giving staff the flexibility needed to work effectively. The Compliance Committee will assist the IT Director with developing a training strategy.

Recommend a process for conducting Security Risk Analysis. New regulatory requirements, such as HIPAA/HITECH, and current IT best practice, call for processes that help protect against any reasonably anticipated threats or hazards to the security or integrity of electronic information. Regulatory authorities also require implementation of routine security assessments sufficient to reduce risk and vulnerability. The Committee, with guidance from the newly established PSWG, will review examples of Security Risk Analysis processes and will suggest steps for monitoring implementation by county departments.

Update the Compliance Program Document. Many changes have occurred since the County Compliance Program was established in 2011 and a complementary Program Document was produced to give guidance on policy and practice. The Committee will conduct a review of the Program Document, determine areas that need updating, and prepare new content.

Add to the Compliance Fact Sheet Series. The Committee, with guidance from the PSWG, will produce a fact sheet on HIPAA/HITECH basics.

This report prepared and submitted by
COUNTY COMPLIANCE COMMITTEE
March 2014

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

Patricia Carey, Commissioner
Department of Social Services

Greg Potter, Director
Information Technology Services

Anita Fitzpatrick, Commissioner
County Personnel

Sue Romanczuk, Ph.D.
Commissioner of Mental Health Services

Frank Kruppa, Director
County Health Department

Rick Snyder, Director
County Finance Department

Jonathan Wood
County Attorney
