TOMPKINS COUNTY ADMINISTRATION

County Compliance Committee

Think Compliance First!

2015 Year-end County Compliance Progress Report

Year At-a-Glance.

A lot was accomplished in 2015 to enhance County compliance. ITS revised and implemented new policies that will reduce paperwork and greater protect the privacy of clients of the Mental Health Services and Public Health departments. A new electronic process for breach documentation was developed and implemented to replace an outdated paper process. A new Information Security Compliance officer helped identify software that will improve risk assessments countywide. The County also developed plans to convert to software systems that will offer greater security of important data. The coming year, 2016, the County will focus on full implementation of these improvements and develop new strategies and programs to improve compliance. This will include taking steps to improve Title VI documentation and processes to more appropriately meet regulatory standards, and, with leadership from the Personnel department, ensure compliance with various labor laws.

Key Accomplishments.

Educating for Compliance—The Committee continued to serve as a resource for compliance matters, particularly those related to risk-prevention, IT compliance, and data protection. The County Compliance Officer worked with all departments to help them meet the County's annual compliance training goal, and also delivered six education sessions to 75 County staff.

Policy Review and Development—The County's Administrative Policy 01-04 provides overall guidance to policy amendment and adoption procedures along with criteria for keeping administrative policies current and relevant. This year, 2015, was the year slated for Policy 01-04 review. There was no need to change the policy, but some minor editing was done to the text to reduce redundancy and increase ease of understanding. Additionally, the procedure section was updated to reflect a new online capability for tracking policy amendments, providing a more streamlined, paperless approach to the process.

The ITS department, with assistance from the County Compliance Committee, continued development of policies for securing and protecting the County's IT infrastructure and data. One example is the ongoing development of a reasonable social media policy that provides direction regarding account management and how to mitigate associated risks from the use of technologies hosted external to the County IT environment. This policy will also help departments maintain continuity when staff assigned to coordinate social media activities are either unreachable or leave their employment with the County.

In reviewing changes to the Health Insurance Portability and Accountability Act (HIPAA) landscape, the Public Health and Mental Health Services departments worked to adapt their policies appropriately. As an example, changes in HIPAA law now allow healthcare providers to treat patients holistically, thus minimizing conflicting treatments that could endanger a patient's health. Consequently, changes were made to internal department policies, thereby reducing client paperwork while still protecting the client's rights to privacy.

Helping Departments Diminish Risk—For its 2015 work plan, the Committee had originally considered re-visiting the department risk assessment exercise launched in 2012 and revising the content with the goal of conducting a follow-up risk assessment survey in 2016. The intent was to use the feedback from the assessment to then determine how best to help departments identify and implement effective risk mitigation strategies. However, careful review of our objective revealed a significant flaw: even if risks are identified, the County does not have an established infrastructure to support mitigation efficiently, particularly for one of the most sensitive areas of our operations—IT data management and security. The Committee quickly turned its attention to IT risk assessment because technology plays such a key role in every facet of County operations. With assistance from

the ITS director, the Committee was introduced to a software package (Varonis) that will allow for significant improvement in the analysis of data access, use, and utilization behaviors that present risk. The software provides a platform for gathering and analyzing file data use, helping departments see where sensitive content is over-exposed and lock it down before it ends up in the wrong hands. The software can also inform best practices for improvement. The Committee recommended to the County Administrator to purchase the software with a plan for implementation in 2016. (See the *Issues and Opportunities* section for more information.)

New Information Security Compliance Officer—Midyear 2015 brought to the Committee a new Information Security Compliance Officer. Serving as a member of the County ITS staff, this position is responsible for coordinating ITS security policies and federally mandated Health Insurance Portability and Accountability Act (HIPAA) policies, largely for the Mental Health Department, Public Health Department, DSS Medicaid Unit and other County departments that manage or share protected health information routinely. This position has been heavily involved in 3 projects designed for risk assessment and reduction that function as pilot projects for future implementation for all Tompkins County departments.

Breach Reporting—2015 also brought upgrades to the breach incident reporting process. ITS staff converted reporting documentation from a paper process to an electronic process. A link for reporting a security breach has been added to the County Compliance Program webpage.

Issues and Opportunities.

Educating for Compliance: Organizational Approach

There has been ongoing effort to put in place a cohesive plan for compliance training countywide since the County Compliance Program was initiated in 2011. At present, department heads are responsible for ensuring their staff receive training by using a variety of online resources available or requesting assistance from the County Compliance Officer. Although this approach appeared adequate when the compliance program was first established, as compliance requirements have expanded and become more wide-ranging in scope over time, a more comprehensive and consistent method for planning and delivering staff training is needed.

Adopting a new method means tackling some familiar and persistent challenges, including, for example:

- The scheduling, tracking, and recordkeeping associated with any large-scale training strategy;
- How to meet both general compliance awareness training needs and specific training requirements mandated by various regulatory authorities, ensuring that all training content is both current and timely;
- How to better coordinate current internal training initiatives, such as Right-To-Know, so that the entire County organization can meet various legal requirements in a way that is consistent and more efficient;
- How to develop training that addresses specific internal capacity-building needs, which may also impact our ability to demonstrate compliance in certain areas of our operations.

The first step of an organizational approach to educating for compliance is an analysis of the compliance objectives unique to each department, as well as the compliance objectives common to the organization as a whole. This helps to create a core value strategy to determine training content and identify training gaps. This aligns with the Committee's vision of a centralized data-store of training objectives with the ability to track completion of these objectives as each employee receives the training he or she needs to meet various compliance requirements.

The Personnel department has taken the lead in establishing a work team to assess training needs countywide and then implement a process for training delivery. This most likely will include steps to identify and deploy a technology for online learning management, and to update training objectives and requirements. The County Compliance Committee looks forward to collaborating with the newly established training work team to make sure that educating for compliance is a key component of the overall training strategy, and to provide input on the most salient compliance topics.

Improving Data Management to Minimize Risk

The implementation of Varonis into our IT infrastructure has substantial benefits. Varonis can analyze the data stored across all county operations and across disparate platforms to help departments manage data ownership, data access rights, data retention, and responsibilities of file system data. The software can also retain information about data accidentally deleted; assisting in the recovery of that data, and it can notify management about possible

attacks or breaches in real time. This helps ITS staff analyze behaviors that fall outside normal usage patterns and recognize when someone's account has been compromised. Cost of the software and its implementation is significant, but the return on investment will be demonstrated quickly once idle data is removed, offsetting the costs of having to purchase more storage space, and transforming the way we maintain and share data from a potential liability to a better managed asset.

What to Expect in 2016.

The Tompkins County Compliance Committee will be working on several projects for 2016. The most significant is the review of a cohesive **Title VI Plan** for the County. The Plan will ensure compliance with the Americans with Disabilities Act (ADA), Limited English Proficiency (LEP) requirements, and federal and state policies intended to ensure government contracting opportunities for minority and women-owned businesses (M/WBEs). The Committee will also review the County's **exclusion screening** process to ensure screening is completed according to administrative policy, and state and federal requirements. Included in this review will be examination of screening services offered by other vendors to determine if our current vendor agreement is competitive. The committee will also **support the efforts of the ITS and Personnel departments** as they continue to develop new policies or improve upon existing policy to meet regulatory requirements. This includes policies associated with implementation of the Varonis software (ITS) and formalizing current in-house practices related to ADA (Personnel).

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

Amy Guererri
Commissioner
Personnel Department

Frank Kruppa
Director
Public Health Department

Greg Potter
Director
Information Technology Services

Rick Snyder
Director
County Finance Department

Roger Cotrofeld
Information Security Compliance Officer

Jonathan Wood
County Attorney

With assistance from Loren Cottrell, ITS and Kit Kephart, DSS
