Tompkins County Compliance Program

Fact Sheet Series - Issue No. 4 (Revised 2019)

Think Compliance First!

COUNTY COMPLIANCE FACT SHEET

Safeguarding Protected Information

What happens when you witness or commit an act that compromises another individual's personal information? What would you do if you accidentally left private client information, including DOBs and SSNs, on the TCAT bus trip home? Who would you turn to if you saw documents with confidential information left out on a desk in plain view where non-authorized staff could read it? Is there a risk of retaliation if you report a known or suspected breach of private information?

The protection of Private Information (PI) has become a major concern for local governments given 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. There is an assortment of regulations, such as New York State Technology Law and modifications to HIPAA privacy rules, which require us to have appropriate safeguards in place to minimize the risk of PI data breaches.

Unfortunately, these kinds of breaches can create significant liabilities for the County and cause harm to the individuals we serve. The unlawful use or misuse of PI 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 organization could include legal liability, loss of public trust, or the payment of fines imposed by regulatory authorities. As employees of Tompkins County government we have an obligation to do all we can to safeguard protected information.

How is Protected Information Defined?

Private Information or "PI" refers to data that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information, such as medical or health-related information.

Examples of Private Information (PI) include:

- Credit card number
- Driver's license number
- Date of birth
- Passport number
- Social Security number

Examples of Personal Health Information (PHI) include:

- Health background information
- Medical records
- Lab test results and X-rays
- Medical diagnoses

Not all PI is sensitive – for example, your name, official title, official address, phone number and email address are not sensitive. However, because any of these can be added to other distinguishable information, the determination of PI often calls for a case-by-case assessment of the specific risk if this information was released into the wrong hands.

What Can You Do Now to Demonstrate Compliance?

Even if you do not know about HIPAA and/or other compliance laws, you are still subject to be charged and/or fined for noncompliance. Here are examples of reasonable and appropriate administrative, technical, and physical measures you can take to protect the integrity, confidentiality, and security of PI:

1. Discover where sensitive data resides and understand how it is used and by whom. If doing business with parties outside of County government, use Business Associate Agreements or confidentiality agreements as required.
2. Define and classify private and sensitive data in your department, along with requirements for its protection, from data creation to management to transfer to termination.
3. Look to improve or enhance protocols that are already in place, such as access to filing cabinets, restricted office access and alarm systems, secured passwords and user IDs, or use of data encryption software.
4. Implement and apply privacy protection and compliance policies across the Department.
5. Measure and monitor the use of information and those who access it, and implement an audit process to prove that the data is being protected appropriately.
6. Ensure staff are trained and be proactive in discussing PI and PHI in department meetings and other similar forums.
7. Immediately report any loss or unauthorized disclosure of PI and PHI.

How to Report Potential Loss, Theft, or Compromise of PI?

Tompkins County is committed to safeguarding protected information. Any potential loss, theft or compromise of PI, PHI, or other sensitive data, whether suspected or confirmed must be reported immediately using the **Tompkins County Breach Incident Procedure**, which can be found in Appendix A of the County Compliance Document at http://www.tompkinscountyny.gov/tccp. If you are not familiar with the Procedure, immediately notify your supervisor, your Department Head, the County Information Security Compliance Officer, or our County Compliance Officer.

You also may report the incident anonymously to the **Tompkins County Confidential Compliance Hotline at 877-348-1396**. The Tompkins County Compliance Program protects all employees who report a confidentiality breach from retaliation. If you report a known or suspected breach in good faith, your identity will be safeguarded to the fullest extent possible and you will be protected against retribution.

Need a Few More Helpful Tips?

The safeguarding of PI and PHI is a shared risk with shared responsibility that requires a coordinated effort across the entire County organization.

- Only collect information you need. Don't collect personal information about an individual just because you think that information may come in handy later.
- Keep personal information secure; do not leave PI or PHI unattended on a desk, printer, copier or fax machine.
- Prevent "shoulder surfing" and lock your screen when you step away from the computer.
- If you do need to send PI or PHI via email, always use the encryption feature.
- Don't keep information you no longer need or that you are no longer required to retain.
- Don't leave privacy to chance. Think carefully before disclosing personal information.

Resources

- Tompkins County Administrative Policy 11-47, Breach Incident Response
- Government Accountability Office (GAO) Report 08-343, Protecting Personally Identifiable Information, January 2008, http://www.gao.gov/new.items/d08343.pdf
- HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/