Breach-Incident Response

Objective: To ensure 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 Tompkins County.

Policy/Procedure Number: 11-47

Reference:
(All Applicable Federal, State and Local Laws)

- New York State Technology Law Section 208
- American Recovery and Reinvestment Act, Title XIII Health Information Technology for Economic and Clinical Health (HITECH) Act, Subtitle D Section 13402 Notification in the Case of Breach
- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH (Omnibus Rule)
- 45 CFR 164 Subpart D – Notification In The Case of Breach of Unsecured Protected Health Information (HIPAA Breach Notification Rule) and Section 164.530 (i) Administrative Requirements; Policies and Procedures
- Tompkins County Compliance Program Document (see section on Tompkins County Breach-Incident Procedure)

Effective Date: 09/02/2014

Responsible Department: County Administration /Mental Health

Modified Date (s):

Resolution No.: 2014-166

Next Scheduled Review: September 2019

Legislative Policy Statement:

The Tompkins County Legislature recognizes the importance of protecting information belonging to individuals served by the County, and is committed to ensuring that private and confidential information is diligently safeguarded by Tompkins County workforce members.

The Legislature also recognizes that a breach can still occur even when information is diligently safeguarded, and is committed to minimizing harm to affected individuals if a breach does occur.

The Legislature further recognizes that State and Federal laws specify breach notification requirements intended to minimize harm in the event of a breach, and that compliance with these laws requires various detailed steps to respond to a breach incident.

The Legislature believes that in order to ensure workforce compliance with the details of breach laws, Tompkins County must have in place a breach-response procedure that incorporates all requirements of breach laws, and must train all workforce members in their procedural responsibilities.

General Information:

New York State Technology Law Section 208 defines Breach of Private Information (PI) and specifies notification requirements for breaches of PI.

Similarly, the Health Insurance Portability and Accountability Act (HIPAA) defines Breach of Protected Health Information (PHI) and specifies notification requirements for breaches of PHI.

Various situations can indicate a possible breach of PI and PHI. In order to make sure that response to any potential breach complies with State and Federal laws, the discovery of any situation that may put PI and PHI at risk must be reported as a potential breach.

Because prompt notification of a breach can reduce harm, both State and Federal laws specify timeliness requirements for breach notification. State law requires notification "in the most expedient time possible and without unreasonable delay." Similarly, Federal law requires notification "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach." In addition, Federal law requires proof that notifications are made without unreasonable delay, making timely reporting, investigation, and notification essential.

The **Tompkins County Breach-Incident Procedure** (in the *Tompkins County Compliance Program* document) specifies time limits on certain steps to ensure compliance with timeliness requirements. The time limits specified are not intended to suggest that workforce members are allowed to wait these amounts of time before acting, but instead are deadlines for situations in which more expedient reporting is not possible.

The Tompkins County Privacy and Security Work Group, an interdepartmental policy-development team led by the Tompkins County Healthcare Security and Privacy Officer, developed the steps detailed in the Tompkins County Breach Incident Procedure as a breach-incident response framework that complies with State and Federal laws.

It is the legal responsibility of Tompkins County and every member of its workforce to immediately report all breaches of PI and PHI. Tompkins County and individual workforce members may be subject to severe monetary penalties and incarceration for violation of related laws.

I. Definitions:

Affected Individual(s)—The person(s) whose private or confidential information may have been compromised.

Affected Department Head—The Tompkins County Department Head within whose department a potential breach has occurred.

Breach—The unauthorized acquisition, access, use, or disclosure of protected health information (PHI) or private information (PI) which compromises the security or confidentiality of such information.

Breach-Incident Team—Includes the County Administrator, County Attorney, Deputy County Administrator/County Compliance Officer, Healthcare Security and Privacy Officer, Affected Department Head, and Director/Deputy Director of ITS as needed. This team oversees breach response for high-risk breaches when the Healthcare Security and Privacy Officer determines this is necessary.

Complaint—A report that an individual's privacy rights have been violated.

Health Information Technology for Economic and Clinical Health Act (HITECH)—Title XIII of the American Recovery and Reinvestment Act of 2009 (ARRA) was enacted to promote and expand the adoption of health information technology. Subtitle D Section 13402 of HITECH requires notification of affected individuals in the event of a breach.

HIPAA—An abbreviation for the Health Insurance Portability and Accountability Act (45 CFR 162 and 164). When referring to HIPAA, this policy refers specifically to **45 CFR 164 Subpart D – Notification In The Case of Breach of Unsecured Protected Health Information.**

Incident—Any event that potentially puts at risk the security, privacy or integrity of an individual's information. Examples include (but are not limited to) privacy complaints, reports of HIPAA violations, confidentiality breaches, missing mobile devices or computers, lost removable media, missing or altered client data, and malware intrusions.

Mobile Device—A portable computing device, such as a Smartphone, tablet computer, or laptop computer.

Omnibus Rule—A 2013 ruling that implemented certain HITECH Act requirements to strengthen HIPAA Privacy, Security, Enforcement, and Breach Notification rules.

Potential Breach—Any situation that may put the confidentiality of a person's private information at risk. Examples include (but are not limited to) privacy complaints, reports of HIPAA violations, confidentiality breaches, missing mobile devices or computers, lost removable media, missing or altered client data, and malware intrusions.

Private Information (PI)—Personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number;
2. Driver's license number or non-driver identification card number;
3. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Protected Health Information (PHI)—Any information that relates to the health of an individual, the provision of care to an individual, or the payment for the provision of health care to an individual that identifies the individual and is transmitted and/or maintained.

Removable Media—Any type of device that can store data and can be removed from a computer while the system is running. Examples include CD, DVD, portable hard drive, floppy disk, flash/USB drive, Smartphone, memory card, digital camera, and printer.

Violation—Activity or inactivity that breaks any law or regulation.

Workforce member—Legislators, employees, independent contractors, trainees, volunteers, and other persons whose conduct in the performance of work is under the control of the County.

II. Policy:

Safeguarding PI or PHI is a required priority of all members of the Tompkins County workforce. However, breaches may occur even when information is diligently safeguarded. Because quickly notifying individuals can lessen the harm caused by breach, Tompkins County Department Heads will ensure that all department workforce members are trained to follow the **Tompkins County Breach-Incident Procedure** and will ensure prompt reporting of all potential breaches. The detailed procedure is located in the *Tompkins County Compliance Program Document* and is briefly summarized below in Section III.

Several situations may put confidentiality of PI and PHI at risk. Examples include (but are not limited to) privacy complaints, reports of HIPAA violations, confidentiality breaches, missing mobile devices or computers, lost removable media, missing or altered client data, and malware intrusions. All of these are potential breaches of PI or PHI. Any workforce member who becomes aware of any situation that may put such information at risk will immediately follow the Tompkins County Breach-Incident Procedure to report the discovery as a potential breach.

Any Tompkins County workforce member who discovers that PI or PHI may have been compromised must fulfill all of his/her responsibilities as detailed in the **Tompkins County Breach-Incident Procedure**.

Any workforce member who does not fulfill his or her responsibility related to this policy may face disciplinary action up to and including termination, and may also face severe monetary penalties and incarceration by HIPAA Enforcement entities (Federal Office of Civil Rights and New York State Attorney General).

III. Procedure:

Because laws and best practices change in response to collective experience with breaches, the **Tompkins County Breach-Incident Procedure** is and will be a working document that will be updated to match evolving laws and best practices. It will be maintained within the *Tompkins County Compliance Program Document*. A brief summary of the Tompkins County Breach-Incident Procedure is provided below.

Breach Reporting and Investigation

1. Any workforce member will report any potential breach directly to the Healthcare Security and Privacy Officer, or via the anonymous Breach Hotline.

2. The Healthcare Security and Privacy Officer will contact the Affected Department Head to inform him/her of the potential breach, and will work with the Department Head to complete an investigation.

3. Based on the breach risk assessment completed during the investigation, the Healthcare Security and Privacy Officer will decide whether the incident is a breach.

4. If the incident is not a high-risk incident, the Healthcare Security and Privacy Officer will oversee the remainder of the incident response to ensure compliance with related State and Federal Laws.

5. For high-risk breach incidents, the Healthcare Security and Privacy Officer will engage the oversight of the Breach-Incident Team. The team will then review the incident investigation documentation, and oversee the remainder of the incident response.

6. The Healthcare Security and Privacy Officer will review breach incidents with the County Compliance Committee quarterly, will deliver a status report to the County Legislature semi-annually, and will keep all related documentation for six years.