ULSTER COUNTY
SECURITY OR PRIVACY BREACH INCIDENT PROCEDURE

I. Applicable Laws, Rules and Regulations:

- Electronic Code Federal Regulations Title 45, Subtitile A, Subchapter C §164.400-414 and 308(a)(6) defines Breach of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) and specifies notification requirements for breaches of PHI and ePHI.

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

II. Purpose:

The purpose of this procedure is to formalize the identification of, response to, and reporting of, Private Information (PI), Protected Health Information (PHI), and Electronic Protected Health Information (EPHI) data security or privacy breach or disclosure incidents. This includes identification and response to suspected or known security incidents, the mitigation of the harmful effects of known or suspected incidents to the extent possible, and the documentation and reporting of incidents and their outcomes.

III. Application:

This policy shall apply to all departments, boards, agencies and commissions of the County of Ulster ("the County".)

IV. Definition:

"Personally Identifiable Information" shall mean information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

"Private information" (PI) shall mean personally identifiable 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; or
(3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Protected Health Information" (PHI) shall mean information, including demographic data, that:

- Relates to the individual's past, present, or future physical or mental health or condition; to the provision of health care to an individual; or to past, present, or future payment for the provision of health care to the individual; and

- Identifies the individual or is information for which there is a reasonable basis to believe it can be used to identify the individual.

Protected health information can be in any form -- electronic, paper, or oral. It can include financial and demographic information collected from individuals and includes many common identifiers (e.g., name, address, birth date, Social Security Number).

"Electronic Protected Health Information" (ePHI) shall mean all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form.

"Breach" shall mean the unauthorized acquisition of or dissemination of computerized data which compromises the security, confidentiality or integrity of personal information maintained by the County or on behalf of the County by any third party.

1. Good faith acquisition of personal information by a County officer or employee or agent thereof is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
2. A compromise of private information shall mean the unauthorized acquisition of unencrypted computerized data with private information as identified as PHI, ePHI, and PI under the applicable laws and regulations
3. if encrypted data is compromised along with the corresponding encryption key, the data shall be considered unencrypted and thus fall under the notification requirements.

V. Procedure Description:

The County will respond to all impermissible uses or disclosures of protected health information and it will be presumed that a breach has occurred unless the County or its business associate, as applicable, demonstrates through the appropriate risk assessment process, that there is a low probability that the protected health information has been compromised. All disclosure, impermissible uses and breach incidents of electronic and hardcopy protected health information shall be reported and responded to promptly.

1. **Workforce Member Responsibilities** Workforce members shall immediately notify their manager or supervisor, of any suspected or confirmed breach or disclosure incident. The manager or supervisor shall report the incident to the Compliance Officer, Privacy Officer, and Security Officer as listed in the County phone directory. If anonymity is desired the workforce member may call the Ulster County Compliance Hotline as listed in the County phone directory.
   The Compliance Officer, Privacy Officer, and Security Officer will, in concert together, evaluate the situation to determine the appropriate response to the report disclosure or breach incident, and initiate the response process as required by the type of incident.

2. **Risk Assessment** The Compliance Officer, Privacy Officer, and Security Officer will WITHOUT UNREASONABLE DELAY perform and document a risk assessment based on the disclosure/breach identified and determine if the incident requires further investigation and if it is a breach of PHI, ePHI, and PI. Working with the affected departments, they shall determine if corrective actions should be implemented. The process to be followed is:

   a. Instead of assessing the risk of harm to the individual, the County and business associates must assess the probability that the protected health information has

been compromised based on a risk assessment that considers at least the following factors:

- **i.** The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (remember to include in the review a "sensitivity rating" - For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud – and if this is the case, then other laws may come into play);
- **ii.** The unauthorized person who used the protected health information or to whom the disclosure was made;
- **iii.** Whether the protected health information was actually acquired or viewed; and
- **iv.** The extent to which the risk to the protected health information has been mitigated.

3. **Notification to Affected Individuals** The County is required to notify all individuals when there has been or is reasonably believed to have been a unintended disclosure or compromise of the individual's private information (PI, PHI, ePHI)

   a. METHOD for PHI or EPHI:

   The County, following a breach or suspected breach of unsecured PHI, or EPHI in accordance with federal law shall:

   - **i.** Provide written notification by first-class mail to the individual at the last known address of the individual or,
   - **ii.** if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. A log shall be kept of each notification. The notification may be provided in one or more mailings as more information becomes available.
   - **iii.** If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.
   - **iv.** Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.
     1. In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.
     2. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the County's web site, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an

individual can learn whether the individual's secured protected health information may be included in the breach.

v. Provide notice of a breach to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This notice is in addition, not a substitute to, the required written notice.

vi. In any case deemed by the County to require urgency because of possible imminent misuse of unsecured protected health information, the County may provide information to individuals by telephone or other means, as appropriate, in addition to written notice.

b. **METHOD for PI:** The County, following a breach or suspected breach of unsecured PI in accordance with New York State law shall be provide notification to the affected persons by one of the following methods:

i. written notice;

ii. electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

iii. telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

iv. Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

1. e-mail notice when such state entity has an e-mail address for the subject persons;
2. conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and
3. notification to major statewide media.

c. **TIMING:** The County shall provide the notification required without unreasonable delay and for PHI and EPHI in no case later than 60 calendar days after discovery of a breach.

Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.

d. **CONTENT:** The content of the notification required shall include to the extent possible:

i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
iii. Any steps the individual should take to protect themselves from potential harm resulting from the breach;
iv. A brief description of what the County is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches;
v. Contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address; and
vi. The notification shall be written in plain language.
vii. A sample letter is appended to this procedure.

4. **Notification to External Agencies** the County shall, following the discovery (post risk assessment) of a breach of unsecured protected health information:
   a. Notify the Secretary of U.S. Department of Health and Human Services in the manner specified on the HHS web site located at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
   b. Complete the New York State Security Breach Reporting Form that is appended to this procedure and submit it to each of the following agencies by fax or email:
      i. New York State Attorney General's Office
      ii. New York State Division of State Police
      iii. New York State Department of State Division of Consumer Protection

5. **Response and Resolution Logging**
   a. Other than the above requirements for reporting to external agencies, all Impermissible Use, Breach, or Disclosure related incidents and their outcomes will be logged by the Compliance Officer, Privacy Officer, and Security Officer and all findings, outcomes, and communications documented.
   b. Each calendar year, the log will be reviewed and disclosures will be reported to the appropriate regulatory agency as required.
   c. The Compliance Officer, Privacy Officer, and Security Officer are responsible for maintaining all documentation on PHI, ePHI, and PI breaches for a minimum of seven years or as needed to meet any claims, legal challenges, or other compliance activities.