LIVINGSTON COUNTY
ADMINISTRATIVE PROCEDURE HIPAA-4

SUBJECT: Breach Notification for Unsecured Protected Health Information

ORGANIZATION RESPONSIBLE: Information Technology Security Manager
Office of Information Technology

DATE:

DEPARTMENTS/OFFICES AFFECTED:

Livingston County Health Department (Personal Health Division but excluding the Environmental Health Division);
Livingston County Emergency Medical Services Department;
Livingston County Sheriff's Office, Jail Division;
Livingston County Human Resources Department (Employee Health Benefits);
The Livingston County Information Technology Department;
Livingston County Dispatch Center, to the extent that it transmits PHI to and receives PHI from Livingston County Emergency Medical Services Department

OTHER FORMS: Attachment A: Risk Assessment Questions
Attachment B: Breach Notification Requirements

A. DEFINITIONS

Unsecured Protected Health Information: PHI that, if in electronic form is not encrypted, and PHI that if in paper form or recycled electronic form (i.e. discs) is not shredded or otherwise destroyed.

Breach: the unauthorized acquisition, access, use or disclosure of protected health information (PHI) in any form or medium, including electronic, paper or oral form which compromises the security or privacy of such information.

Unauthorized acquisition: acquisition, access, use or disclosure of PHI that is impermissible under the HIPAA Privacy Rule.

B. POLICY

The HIPAA covered components in Livingston County as identified by Resolution 2013-09-269 and their business associates are subject to the breach notification provision included in the Health Information Technology for Economic and Clinical Health ("HITECH") Act, part of the American Recovery and Reinvestment Act of 2009 ("ARRA"). The HIPAA covered components in Livingston County are:

1. (Livingston County Health Department (Personal Health Division but excluding the Environmental Health Division);
2. Livingston County Emergency Medical Services Department;
3. Livingston County Sheriff's Office, Jail Division to the extent that it provides medical care services to inmates and transmits to and receives PHI;
4. Livingston County Human Resources Department (Employee Health Benefits) to the extent that it operates the County self-funded health insurance;
5. Livingston County Dispatch Center, to the extent that it transmits PHI to and receives PHI from Livingston County Emergency Medical Services Department; and,
6. Livingston County Information Technology Department;

The HIPAA Covered Components will comply with the following notification procedures in the event of a breach of Unsecured Protected Health Information regardless of whether the breach is of information maintained by the County, or information provided to and maintained by a Business Associate on behalf of the County.

C. PROCEDURES

Responsible Person	Procedure
All Staff	When a workforce member (employee, contractor, student, resident or volunteer) becomes aware of a breach or potential breach of PHI as defined above, he/she will IMMEDIATELY notify the department's Privacy/Security Official. If a workforce member (employee, contractor, student, resident or volunteer) receives a complaint alleging a potential breach of PHI as defined above, he/she will IMMEDIATELY notify the department's Privacy Official and notify the County Privacy Officer.
Department/Office Privacy/Security Official	1. Upon report of an actual or potential breach of PHI, the Department/Office Privacy/Security shall undertake required notification except when, after undertaking a good faith risk assessment, the County Privacy Officer and the Department Head or Elected Official concludes and establishes that: - there a "low probability" of compromise of the PHI; or - One of the existing exceptions to the definition of the breach applies (i.e., unintentional good faith acquisition, access, or use of PHI by a workforce

member; inadvertent disclosure between two individuals who are otherwise authorized to access the PHI; or disclosure to an unauthorized person who would not reasonably have been able to retain such information).

2. If the risk assessment indicates that a reportable breach occurred, inform the County Privacy Officer and the Department Head or Elected Official where the breach occurred that an investigation of the cause and scope of the breach must occur and that timely notice must be sent to the clients or other individuals involved.

Department Head or Elected Official or designee of the covered entity where the breach occurred

1. Immediately begin an investigation into the scope and cause of the breach.

2. Working with the Department/Office's Privacy/Security Official, the County Privacy Officer, and the County Attorney, develop the breach notification letter that must be sent to each individual (or parent/guardian) whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

3. Breach notification letters must be sent without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered:

   a. The Department Head/Elected Official or designee may take a reasonable time to investigate the circumstances surrounding the breach, in order to collect and develop the information that is required to be included in the notice to the individual.

   b. The Department Head/Elected Official or designee is expected to notify individuals as soon as reasonably possible. The required information may be provided in multiple mailings as the information becomes available

c. The breach notification must be sent via first class mail and must contain the elements contained in Attachment B.

d. Notice by telephone or other means may be made, in addition to written notice, in cases deemed by the covered entity Department/Office to require urgency because of possible imminent misuse of unsecured protected health information.

e. If the covered entity Department/Office knows that some of the affected individuals are deceased and also knows the address of the next of kin or personal representative of the descendent, the notice must be provided to the next of kin or personal representative.

4. If the covered entity Department/Office does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, a substitute notice must be provided for the unreachable individuals. The substitute notice should be provided as soon as reasonably possible after the covered entity Department/Office is aware that it has insufficient or out-of-date contact information for one or more affected individuals. The substitute form of notice must be reasonably calculated to reach the individuals for whom it is being provided.

a. If there are fewer than 10 individuals for whom the covered entity Department/Office has insufficient or out-of-date contact information to provide the written notice, the covered entity Department/Office may provide substitute notice to such individuals through an alternative form of written notice (e- mail), by telephone or other means. Alternatively, posting a notice on the covered entity Department/Office's web site may be appropriate if the covered entity Department/Office lacks any current contact information for the individuals.

b. If the covered entity Department/Office has insufficient or out-of-date contact information for 10 or more individuals, then the covered entity Department/Office must provide substitute notice through either a conspicuous posting for a period of 90 days on the home page of its web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

c. Substitute notice through the website or media for 10 or more individuals requires the covered entity Department/Office to have a toll-free phone number, active for 90 days, where an individual can learn whether the individual's unsecured protected health information may be included in the breach and include the number in the notice.

d. If the breach of unsecured PHI affected more than 500 individuals, the notice must also be provided to prominent media outlets serving the County in the form of a press release.

County Privacy Officer

1. All breaches of unsecured PHI must be reported to the Secretary of Health and Human Services (HHS) in a manner specified on the HHS website.

   a. For breaches involving 500 or more individuals, the report must be made immediately (concurrent to the notification sent to the individual).

   b. For breaches involving less than 500 individuals, a log of such breaches must be maintained and submitted annually no later than 60 days after the end of each calendar year. The log and other documentation related to the breach (i.e. risk assessment and breach notification letter) must be maintained for six years.

Attachment A

Risk Assessment

Questions to be asked:

1) Did the use or disclosure violate the Privacy Rule?

2) Determine the nature and extent of the PHI involved (i.e., types of identifiers, likelihood of re-identification, and the amount of data and its sensitivity); the type of unauthorized person who used the PHI or to whom the data was disclosed; whether the PHI was actually acquired or viewed; and the extent to which risk to the PHI has been mitigated.

3) Did the PHI go to another covered entity? If yes, did the covered entity Department/Office obtain satisfactory assurances from the recipient that the PHI will not be further used or disclosed or will be destroyed?
If yes, no breach has occurred and notification is not required.

4) Was the PHI returned prior to it being accessed for an improper purpose? (i.e. laptop stolen and recovered with a forensic analysis that shows that its information was not opened, altered, transferred, or otherwise compromised.)

5) Was the disclosure:

   a. An unintentional acquisition, access, or use of PHI by a workforce member; or

   b. An inadvertent disclosure of PHI from an individual in the HIPAA covered entity authorized to access PHI to another individual in the HIPAA covered entity authorized to access PHI; or

   c. An unauthorized disclosure in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information? (i.e. returned, unopened mail delivered to wrong address; paper with PHI handed to wrong individual and immediately recovered)

6) Did the client make Livingston County or the covered entity Department/Office aware of the disclosure? If yes, notification is not required, unless there is reason to believe that additional disclosures were made at the same time. If so, notification is required.

Attachment B
Breach Notification Requirements

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

2) 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).

3) Any steps individuals should take to protect themselves from potential harm resulting from the breach (i.e. contact credit card company and/or credit bureau);

4) A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals (i.e. filing a police report if indicated), and to protect against any further breaches (i.e. steps being taken to improve security).

5) Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an e-mail address, web site, or postal address.

6) The notification must be written in plain language at an appropriate reading level, using clear language and syntax.

7) The notification should be translated for limited English proficient persons as needed.

8) The notification should be made available in alternate formats, such as Braille, large print, or audio as needed.

N:\Client\Livingston\Policies\HIPPA-4 - Breach Notification.doc