HEALTH DEPARTMENT

Approved by:
Current Department Review: Date: 7/2019
Last Review: Date: 8/2018
Medical Director: Date: 8/2019
Professional Advisory Committee: Date: 9/2019
Board of Supervisors: Date: 9/2019

CONFIDENTIALITY AND DISCLOSURE POLICY AND PROCEDURE

POLICY:
Essex County Health Department (ECHD) will safeguard the confidentiality of Protected Health Information (PHI) as defined on page 13 of the Essex County Health Insurance Portability and Accountability Act (HIPAA) Policy (Attachment 1) and 1US DHHS/OCR Regulation Text 45 CFR Parts 160, 162 and 164, amended 3/26/13 (Attachment 2).

DEFINITIONS
Refer to Attachment 1 for definitions not listed below.

ePHI - PHI that is produced, saved, transferred or received in an **electronic** form. Refer to the ECHD Electronic Device Security and Confidentiality Policy and Procedure for more guidance on ePHI.

Compromise of Security or Privacy: information released that poses a significant risk of financial, reputational or other harm to the client. Uses or disclosures of PHI that do not include the direct identifiers in a limited data set, date of birth or zip code do not compromise the security or privacy of the PHI.

Unsecured Protected Health Information: PHI/ePHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under 2section 13402(h)(2) of Public Law 111-5 on the HHS Web site.

Breach: the acquisition, access, use or disclosure of PHI/ePHI, which compromises security/privacy. A breach excludes:

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of ECHD or one of its contracted entities, if such acquisition, access or use was made in good faith and does not result in further use or disclosure in a manner not permitted under the privacy standards.
- Any inadvertent disclosure by a person who is authorized to access ECHD or business entity PHI/ePHI to another person authorized to access ECHD or business entity PHI/ePHI or organized health care arrangement in which ECHD participates and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.
- A disclosure of PHI where the ECHD or contracted entities has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

PROCEDURE

1 https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf
2 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

Workforce Training. All employees and contractors will review this policy and procedure and sign the Confidentiality Statement upon initial employment and annually per the ECHD Mandatory Employment Requirements Policy and Procedure and Essex County HIPAA Policy.

Physical Safeguards. ECHD staff/contractors maintain the original client record per the ECHD Medical Record Identification, Security, Storage, Retention and Destruction Policy and Procedure and the ECHD Electronic Device Security and Confidentiality Policy and Procedure.

ECHD staff/contractors do not remove the client paper clinical record from the public health department office unless needed for a client visit. If staff/contractors are unable to return the paper clinical record at the end of the day, they will consult with their supervisor to make a plan for maintaining the record securely until it is returned to the agency.

Privacy and Confidentiality of PHI and ePHI. ECHD staff will provide a Notice of Privacy Practices to all clients according to the ECHD Client Rights and Responsibilities Policy and Procedure and the Essex County HIPAA Policy.

Individual Right of Access. Employees and contractors ~~involved with the provision, coordination, and/or management of healthcare services~~ may only access PHI and ePHI they need to do their jobs.
An individual has the right to access PHI and ePHI and obtain a copy according to the Essex County HIPAA Policy. The individual requesting access will complete Authorization for Release of Health Information Pursuant to HIPAA (Attachment 3).The Director of Preventive Services (DPRevS), Director of Patient Services (DPS), Director of Public Health or designee make the determination of acceptance or denial of the request and consult the County Attorney as indicated. Attachment 1 must document the following:

1. The client name;
2. Dated signature by the client or by someone authorized to act in the client behalf;
3. The entity authorized to release the client information;
4. The type of information that authorized to be released;
5. To whom the information may be released;
6. The purpose for which the information is being released;
7. The expiration date for the release that will not exceed two years from the date the release was signed;
8. The release may be revoked at any time.

Release or transmission of client information via fax must contain the confidentiality notice. Staff and contractors will note all disclosures noted in the client record except for billing/insurance access. Any unauthorized disclosure of client information may lead to disciplinary action including suspension or dismissal from employment.

Ethics. Best practice is for the staff/contractor not to be assigned to care for a client/family to whom he/she is related in any of the following manners:

a. Immediate family: mother, father, husband or wife, children, brothers or sisters, grandchildren, or grandparents (this also includes step-relatives);
b. Aunts, uncles, cousins, nieces, or nephews;
c. Relatives by marriage: mother-in-law, father-in-law, sister-in-law, brother-in-law, etc.

Staff/contractors will notify their Supervisor or designee when a family member is receiving services, to prevent potential conflict of interest per the 3 Essex County Ethics and Disclosure Law. The Supervisor or designee will make a decision regarding whether it is a conflict of interest for the staff member to provide service for the client/family.

3 http://www.co.essex.ny.us/downloads/Local%20Law%20No.%206%20-%20Ethics.pdf

Confidentiality/Disclosure in the Event of a Breach Discovery.

A. The Director of Public Health (DPH), Director of Preventive Services (DPRevS), Director of Patient Services (DPS) or designee shall lead the following activities:

1. Notify each individual whose unsecured PHI/ePHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed because of such breach.
2. Document the breach occurrence as the first day the breach is known or, could have been known to ECHD with previous use of reasonable diligence.
3. Provide notification without unreasonable delay and in no case later that 60 calendar days after discovery of a breach. (see Law Enforcement Delay on "E" below for exceptions)
4. Include the following notification elements, to the extent possible:
    - Brief description of what happened, including the date of the breach and relevant identifiable information of the individual (s) involved.
    - Description of the types of unsecured PHI/ePHI that were involved in the breach.
    - Provide instructions for steps the individual should take to protect themselves from potential harm resulting from the breach
    - Provide a brief description of what ECHD is doing to investigate the breach, to mitigate harm to the individual and to protect against any further breaches
    - Provide contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, and/or postal address.
5. Provide written notifications in plain language by the following means:
    - First-class mail to the individual at the last known address or, if the individual agrees to electronic notice, by electronic mail.
    - One or more mailings may as more information becomes available.
6. First-class mail to the address of the next of kin or personal representative of the individual if the individual is known to be deceased. Substitute forms of notice need not be provided in this case.
7. Provide additional notice by telephone and/or other means if it is deemed to require urgency due to possible imminent misuse of unsecured PHI/ePHI.
8. Provide a substitute form of notice if there is insufficient or out-of-date contact information that prevents written notification.
    - In the case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, an alternative form of written notice, telephone or other means may provide substitute notice.
    - In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the ECHD website or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. This shall include a toll-free phone number that remains active for at least 90 days where an individual can learn whether their unsecured PHI may be included in the breach.
9. Notification to the Media. This requirement is for a breach of unsecured PHI involving more than 500 individuals.
10. Notification to the Secretary of Health and Human Services (HHS). The DPH, DPRevS, DPS or designee in consultation with the county attorney will:
    - Notify the Secretary of Health and Human Services for breaches of unsecured PHI involving 500 or more individuals, at the same time as the individual notification,
    - Maintain a log or other documentation of breaches involving less than 500 individuals.

- Provide the notification required for breaches occurring during the preceding calendar year in the manner specified on the HHS Web site, within 60 days after the end of each calendar year.
- Submit this notification electronically per 4 section 13402(h)(2) of Public Law 111-5 on the HHS Web site.

11. Notification by a Business Associate to the Agency. The Business Associate will:
    - Document the breach occurrence as the first day the breach is known or, could have been known to the business associate with previous use of reasonable diligence.
    - Provide notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.
    - Provide, to the extent possible, the identification of each individual whose unsecured PHI has been or is reasonably believed by the business associate to have been accessed, acquired, used or disclosed during the breach and any additional information required, if known.
12. Burdon of Proof. In the event of a use or disclosure in violation of the privacy standards, the DPH, DPrevS, DPS, county attorney or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach, and maintain documentation to meet this burden of proof.
13. Notification to the NYS Department of Health of any potential cybersecurity incident at the agency per Attachment 4.

Law Enforcement Delay. If a law enforcement official states to ECHD staff or business associate that a notification, notice, or posting required would impede a criminal investigation or cause damage to national security, the DPH, DPrevS, DPS shall consult with the County Attorney and delay release of information as noted below:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice or posting for the period specified by the official.
- If statement is given verbally, document the statement and include the identity of the official making the statement. The notification, notice or posting is delayed temporarily and no longer than 30 days from the date of the verbal statement, unless a written statement is submitted during that time.

Attachments

1. Essex County Health Insurance Portability and Accountability Act (HIPAA) Policy
2. US DHHS/OCR Regulation Text 45 CFR Parts 160, 162 and 164, amended 3/26/13
3. Authorization for Release of Health Information Pursuant to HIPAA
4. NYSDOH Cybersecurity Incident Reporting Notification

4 https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf