BREACH NOTIFICATION POLICY AND PROCEDURE

Note:

- Both Federal regulations and New York State law apply to breach notification.
- Federal regulations are applicable to the breach of protected health information.
- State law is applicable to the breach of personal or private information.

I. Breach of Protected Health Information

A. POLICY

The Rockland County Departments of Health, Hospitals and Mental Health (referred to individually as the "Department" and collectively as the "Departments") are committed to ensuring the privacy and security of Protected Health Information ("PHI") in accordance with federal privacy rules and regulations including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, 100 Stat. 2548, the HIPAA Administrative Simplification Rules (the "HIPAA Rules"), which are set forth in 45 CFR Parts 160, 162 and 164, the American Recovery and Reinvestment Act of 2009 ("ARRA"), Public Law 111-5, 123 Stat. 115, including, but not limited to, § 13402 of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), Title XIII of Division A and Title IV of Division B of ARRA, codified at 42 U.S.C. § 300jj et seq., § 17901 et seq., and its implementing regulations, which are set forth in 45 CFR Part 164, and the HIPAA/HITECH Omnibus Final Rule effective March 26, 2013, and any subsequent amendments.

As such, the Departments shall preserve the confidentiality of all aspects of individuals' medical records and comply with the above requirements. It is the responsibility of all staff to follow the established procedures for the handling and transmission of individual information.

The Departments are further committed, should a breach of unsecured PHI be identified, to notify affected individuals when the breach compromises the security or privacy of the PHI.

B. REFERENCES:

45 C.F.R. § 164.400 et seq.

C. DEFINITIONS

1. **Breach:** The acquisition, access, use or disclosure of PHI in a manner not permitted under 45 C.F.R., Part 164, Subpart E, which compromises the security or privacy of the PHI.

The following disclosures do not constitute a Breach:

(a) any unintentional acquisition, access, or use of PHI by a staff member or person acting under the authority of the County or a business associate, if such acquisition,

access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E; or
(b) any inadvertent disclosure by a person who is authorized to access PHI at the County or business associate or organized health care arrangement in which the County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E; or
(c) a disclosure of PHI where the County or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information; or
(d) the unintentional acquisition, access or use of health information that does not constitute individually identifiable health information; or
(e) PHI that has been de-identified or rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology specified in guidance from the Secretary of the U.S. Department of Health & Human Services (HHS).

In addition, an unauthorized or impermissible acquisition, access, use or disclosure of PHI, which does not fall within one (1) of the exceptions listed above, is presumed to be a breach unless the County or the business associate demonstrates there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(a) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
(b) the unauthorized person who used the PHI or to whom the disclosure was made;
(c) whether the PHI was actually acquired or viewed; and
(d) the extent to which the risk to the PHI has been mitigated.

2. **Discovery:** A Breach shall be treated as discovered by the County as of the first day on which such Breach is known to the County or by exercising reasonable diligence would have been known to the County. The County shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is staff member or agent of the County.

3. **Individually Identifiable Health Information:** Information that is a subset of health information, including demographic information collected from an individual, that is (a) created or received by a health care provider, health plan, employer or health care clearinghouse; and (b) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual; and (c) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information. Some of the identifiers which must be removed for the individually identifiable health information to be de-identified include, but are not limited to, names, birth dates, social security numbers, etc.

4. **Protected health information (PHI)**: Individually identifiable health information that is:

(a) transmitted by electronic media;
(b) maintained in electronic media; or
(c) transmitted or maintained in any other form or medium.

PHI does not include individually identifiable health information contained in:

(a) education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g;
(ii) records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
(iii) employment records held by the County in its role as employer; and
(iv) regarding a person who has been deceased for more than 50 years.

5. **Unsecured PHI**: PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of HHS.

D. PROCEDURE

When an unauthorized or impermissible acquisition, access, use or disclosure of PHI has been discovered, the Department's staff must adhere to the following procedures.

1. **Employee Who Discovered Breach -** The employee who discovers the unauthorized or impermissible acquisition, access, use or disclosure of PHI must immediately notify his/her unit supervisor of the incident and document in writing his/her Discovery of the incident, how it occurred and the date, time and manner of the Breach.

2. **Supervisor's Responsibilities -** The supervisor or his/her designee must:

(a) determine whether there was an unauthorized or impermissible acquisition, access, use or disclosure of PHI;
(b) if there was an unauthorized or impermissible disclosure of PHI, determine whether the PHI is Unsecured PHI;
(c) If the PHI is Unsecured PHI, determine whether the acquisition, access, use or disclosure falls within one (1) of the statutory exceptions to Breach;
(d) if one (1) of the statutory exceptions to Breach do apply, he/she must document that determination in writing and forward copies of the determination to the Risk Manager, the County Executive's Office and the County Attorney; no further action may be required at this point;
(e) however, if the disclosure does not fall within one (1) of the statutory exceptions to a Breach, conduct a Risk Assessment to determine whether there is a low probability that the PHI has been compromised;
(f) if, as a result of the Risk Assessment, the supervisor or his/her designee determines that there was no Breach, he/she must document that determination in writing and forward copies of it to the Risk Manager, the County Executive's Office and the County Attorney; no further action may be required at this point;

(g) if, however, as a result of the Risk Assessment, the supervisor or his/her designee determines that there was a Breach, he/she then must (i) document that determination in writing, (ii) identify the name(s) of the individual(s) involved and whether the Breach involved more or less than 500 individuals, (iii) notify the Risk Manager, who must comply with sections E and F below, and (iv) forward copies of the determination to the Risk Manager, the Commissioner, the County Executive's Office and the County Attorney.

E. BREACHES AFFECTING MORE THAN 500 INDIVIDUALS

If a Breach of PHI involves more than 500 individuals, the Risk Manager or his/her designee must adhere to the following procedure.

1. In the event he/she has not already done so, the Risk Manager must notify the Commissioner of the Department, the County Executive's Office and the County Attorney.

2. The Risk Manager or his/her designee shall, *without unreasonable delay* and in no case later than *sixty (60) calendar days* after the Breach was discovered or would have been known to the Department by the exercise of reasonable diligence, notify the following:

(a) **Secretary of HHS -** Notify the Secretary of HHS in the manner specified on the HHS website, which is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

(b) **Affected Individuals -** Draft a standard breach notification letter (the "Breach Notification Letter") to the affected individuals in plain language, and follow the additional requirements set forth below:

(i) Breach Notification Letter must include:

(1) brief description of what happened;
(2) date of Breach;
(3) Discovery date;
(4) description of the types of Unsecured PHI that were involved (e.g., full name, Social Security number, date of birth, home address, account number, disability code, diagnosis, etc.);
(5) any steps individuals should take to protect themselves from potential harm resulting from the Breach;
(6) brief description of what the Department is doing to investigate the Breach, mitigate harm and protect against further Breaches; and
(7) contact procedures for individuals to ask questions or learn additional information including a toll-free number, email address, website or postal address where individuals can obtain information.

(ii) Breach Notification Letter should not include the actual PHI that was Breached;

(iii) prior to mailing, forward draft of Breach Notification Letter to Commissioner, County Executive's Office and Law Department for review and approval;

(iv) mail Breach Notification Letter to individual at his/her last known address via first class mail or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail;

(v) if there is insufficient or out-of-date contact information for the individual, provide a substitute form of notice reasonably calculated to reach the individual (e.g., telephone email, etc.);

(vi) if the individual is deceased and the Department has the address of the next of kin or personal representative, mail Breach Notification Letter to that person via first class mail;

(vii) if there is insufficient or out-of-date contact information for the next of kin or personal representative, no further action is required;

(viii) if there is insufficient or out-of-date contact information for ten (10) or more affected individuals, post a conspicuous notice on the County website on the home page for ninety (90) days OR place a conspicuous notice in major print in the local newspaper or broadcast media where the affected individuals likely reside and, in either case, include a toll-free number that remains active for at least ninety (90) days where individuals can learn whether their Unsecured PHI may be included in the Breach; and

(ix) if the situation is deemed urgent because of possible imminent misuse of Unsecured PHI, provide information to the affected individuals by telephone or other means in addition to the notice provided above.

(c) **Local Media -** Notify prominent local media via a press release, which must include the same information contained in the Breach Notification Letter.

F. BREACHES AFFECTING LESS THAN 500 INDIVIDUALS

If a Breach of PHI involves less than 500 individuals, the Risk Manager or his/her designee must adhere to the following procedure.

1. In the event he/she has not already done so, the Risk Manager must notify the Commissioner of the Department, the County Executive's Office and the County Attorney.

2. The Risk Manager or his/her designee shall notify the following:

(a) **Affected Individuals -** Draft a standard breach notification letter (the "Breach Notification Letter"), written in plain language, and follow the additional requirements set forth below:

(i) Breach Notification Letter must include:

(1) brief description of what happened;
(2) date of Breach;
(3) Discovery date;
(4) description of the types of Unsecured PHI that were involved (e.g., full name, Social Security number, date of birth, home address, account number, disability code, diagnosis, etc.);
(5) any steps individuals should take to protect themselves from potential harm resulting from the Breach;
(6) brief description of what the Department is doing to investigate the Breach, mitigate harm and protect against further Breaches; and
(7) contact procedures for individuals to ask questions or learn additional information including a toll-free number, email address, website or postal address where individuals can obtain information.

(ii) Breach Notification Letter should not include the actual PHI that was Breached;

(iii) prior to mailing, forward draft of Breach Notification Letter to Commissioner, County Executive's Office and Law Department for review and approval;

(iv) mail Breach Notification Letter to individual at his/her last known address via first class mail or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail;

(v) if there is insufficient or out-of-date contact information for the individual, provide a substitute form of notice reasonably calculated to reach the individual (e.g., telephone email, etc.);

(vi) if the individual is deceased and the Department has the address of the next of kin or personal representative, mail Breach Notification Letter to that person via first class mail;

(vii) if there is insufficient or out-of-date contact information for the next of kin or personal representative, no further action is required;

(viii) if there is insufficient or out-of-date contact information for ten (10) or more affected individuals, post a conspicuous notice on the County website on the home page for ninety (90) days OR place a conspicuous notice in major print in

the local newspaper or broadcast media where the affected individuals likely reside and, in either case, include a toll-free number that remains active for at least ninety (90) days where individuals can learn whether their Unsecured PHI may be included in the Breach;

(ix) if the situation is deemed urgent because of possible imminent misuse of Unsecured PHI, provide information to the affected individuals by telephone or other means in addition to the notice provided above; and

(x) Breach Notification Letter must be sent *without unreasonable delay* and in no case later than *sixty (60) calendar days* after the Breach was discovered or would have been known to the Department by the exercise of reasonable diligence.

(b) **Secretary of HHS -** The Risk Manager shall maintain a log of such Breaches and provide notice to the Secretary of HHS within *sixty (60) days* after the end of each calendar year in the manner specified on the HHS website, which is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

G. NOTIFICATION OF A BREACH BY A BUSINESS ASSOCIATE

1. Business associates or contracted agencies shall report any unauthorized or impermissible acquisition, access, use or disclosure of PHI to the Department on the date of Discovery or no later than five (5) calendar days from the Discovery of the Breach.

2. The Business Associate shall identify each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed during the Breach along with the individual's contact information.

3. The County shall promptly notify individuals about a Breach of their Unsecured PHI by the Business Associate in accordance with the requirements set forth above, except where a law enforcement official determines that notification would impede a criminal investigation or cause damage to national security.

4. If the Business Associate has determined, after conducting a Risk Assessment, that the disclosure does not constitute a Breach, it must provide the Department with a copy of the Risk Assessment.

H. LAW ENFORCEMENT IMPLICATIONS

1. If a law enforcement official states to the Department that a notification, notice or posting required above would impede a criminal investigation or cause damage to national security, the Department shall delay notification of the Breach as follows:

(a) if the official's statement is in writing and specifies the time for which a delay is required, the Department shall delay notification for the specified time period; or

(b) if the official's statement is oral, the Department shall document in writing the official's name, title, employer, contact information and date, time and content of his/her statement and delay the notification no longer than thirty (30) days from the date of the official's oral statement unless the official subsequently provides a written statement during that time period.

II. Breach of Personal or Private Information

A. POLICY

The Department is committed to ensuring the privacy and security of computerized data, which may include personal and private information, in accordance with the New York General Business Law.

As such, the Department shall preserve the confidentiality of all aspects of computerized data, including personal and private information including, but not limited to, social security numbers or financial information. Breaches of such data may require notification under New York State law.

The Department further is committed to notifying affected individuals when the security, confidentiality or integrity of their personal or private information is compromised.

B. REFERENCE

New York General Business § 899-aa.

C. DEFINITIONS

1. **Breach of the Security of the System:** The unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality or integrity of Personal Information maintained by the Department.

The following disclosure does not constitute a Breach of the Security of the System:

(a) a good faith acquisition of Personal Information by an employee or business associate for purposes of County business, provided that the Private Information is not used or subject to unauthorized disclosure.

In determining whether there has been a Breach of the Security of the System, the Department may consider the following factors, among others:

(a) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
(b) indications that the information has been downloaded or copied; or

(c) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

2. **Personal Information:** Any information concerning a natural person, which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

3. **Private Information:** 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:

(a) social security number;
(b) driver's license number or non-driver identification card number; or
(c) 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.

The following is not private information:

(a) publicly available information that is lawfully made available to the general public from federal, state or local government records.

D. LEGAL REQUIREMENTS

Pursuant to the General Business Law, any person or business which conducts business in New York State and which owns or licenses computerized data which includes Private Information shall disclose any Breach of the Security of the System following its Discovery to any resident of New York State whose Private Information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

In addition, pursuant to the General Business Law, any person or business which maintains computerized data which includes Private Information that the person or business does not own shall notify the owner or licensee of the information of any Breach of the Security of the System immediately following discovery if the Private Information was, or is reasonably believed to have been, acquired by a person without valid authorization.

E. PROCEDURE

The Department's staff must adhere to the following procedures when there has been a Breach of the Security of the System.

1. **Employee Who Discovered Breach -** The employee who discovers the Breach of the Security of the System must immediately notify his/her unit supervisor of the incident and document in writing his/her Discovery of the incident, how it occurred and the date, time and manner of the Breach of the Security of the System.

2. **Supervisor's Responsibilities -** The supervisor or his/her designee must:

(a) determine whether there was a Breach of the Security of the System;
(b) if he/she determines that there was no Breach of the Security of the System, he/she must document that determination in writing and forward copies of the determination to the Risk Manager, the County Executive's Office and the County Attorney; no further action may be required at this point; and
(c) if, however, he/she determines that there was a Breach of the Security of the System, he/she must (i) document that determination in writing, (ii) identify the name(s) of the individual(s) involved and whether the Breach of the Security of the System involved more or less than 5,000 individuals, (iii) notify the Risk Manager, who must comply with section 3 below, and (iv) forward copies of the determination to the Risk Manager, the Commissioner, the County Executive's Office and the County Attorney.

3. Risk Manager's Responsibilities - If there is a Breach of the Security of the System, the Risk Manager or his/her designee must adhere to the following procedure.

1. In the event he/she has not already done so, the Risk Manager must notify the Commissioner of the Department, the County Executive's Office and the County Attorney.

2. The Risk Manager or his/her designee also shall notify the following:

(a) **Affected Individuals -** The Risk Manager must notify affected persons. The notification must include the Department's contact information and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of Personal Information and Private Information were, or are reasonably believed to have been so, acquired. Notification shall be directly provided to the affected persons by one (1) of the following methods below:

(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 Department in such form (The Department is not permitted to require a person to consent to accepting said notice in said form as a condition of any relationship or transaction with the Department.);
(iii) telephone notification provided that a log of each such notification is kept by the Department; or
(iv) substitute notice, if the Department demonstrates to the New York State Attorney General that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000 individuals or that the Department does not have sufficient contact information. Substitute notice shall consist of all of the following:
(1) e-mail notice when the Department has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on the Department's web site page; and
(3) notification to major statewide media.

(b) **New York State Agencies -** If any of the affected individuals are New York residents, the Risk Manager must notify the following additional agencies of the timing, content and distribution of the notices to the affected individuals along with the approximate number of affected individuals, in the manner specified on the new York State Office of Information Technology Services, which is available at http://www.dhses.ny.gov/ocs/breach-notification/, and without delaying notice to the affected persons:

(i) New York State Division of State Police, New York State Intelligence Center;
(ii) New York State Attorney General's Office, Consumer Frauds & Protection Bureau; and
(iii) New York State Department of State, Division of Consumer Protection.

(c) **National Consumer Reporting Agencies -** In the event that more than 5,000 New York residents are to be notified at one time, the Risk Manager also shall notify the national consumer reporting agencies of the timing, content and distribution of the notices to the affected individuals along with the approximate number of affected individuals. The Department shall make required notifications without delaying notice to the affected persons.

F. LAW ENFORCEMENT IMPLICATIONS

1. If a law enforcement agency advises the Department that it has determined that notification would impede a criminal investigation, the Department shall delay notification of the Breach of the Security of the System until the law enforcement agency determines that such notification does not compromise such investigation.

2. The Department should document in writing its communications with the law enforcement agency including, but not limited to, the official's name, title, employer, contact information and date, time and content of his/her statements.

III. Miscellaneous Provisions

A. CONSUMER ADVOCATE INFORMATION

1. Individuals affected by a Breach or a Breach of the Security of the System will be given the contact information of the Consumer Advocate who is responsible for receiving complaints.

2. The Consumer Advocate will provide further information as requested by the affected individual or his/her personal representative.

3. The complainant will not be intimidated, threatened, coerced, discriminated against or have any retaliatory action taken against them.

4. All complaints will be documented and presented monthly at a Incident Review Committee including disposition, if any.

B. TRAINING

1. The Risk Manager is responsible for the implementation of the Policy and Procedure.

2. The Risk Manager will train all supervisors on the Policy and Procedure.

3. The unit supervisors will train staff on their units and document the training.

4. Attendance sheets will be forwarded to Staff Training and Development

5. The unit supervisors will notify the Commissioner and Risk Manager of any staff members who fail to comply with the Policy and Procedure and apply and record appropriate sanctions and disciplinary action against such staff members.

C. NOTIFICATION TO VENDORS

1. The Commissioner or his/her designee will notify vendors and contracting agencies of the Policy and Procedure.

D. RECORD RETENTION

1. All reports, notifications, recordings, Breach Notification Letters, complaints, attendance sheets and/or any other documentation created in accordance with the sections above must be retained for a minimum of six (6) years.