Title	Number
Breach Notification Policy	**11 (Section 79)**
Creation Date:	**September 22, 2015 Res. 298-15**
Modified Date:	**July 24, 2018, Res. 285-18**

Purpose

In compliance with the demands by Federal regulatory authorities, Cayuga County is committed to safeguarding Personal Health Information (PHI) and all other forms of Personal Information (PI). To this end, the County has adopted the "Cayuga County Breach Notification Policy," which provides a common standard for all staff regarding the processes and procedures for reporting a known or suspected information breach.

Scope

In 2013, the U.S. Department of Health and Human Services moved to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The HIPAA Privacy and Security Rules have focused on health care providers, health plans and other entities that process health insurance claims. In 2013, the HIPAA Omnibus Rule was created to expand many of the requirements to business associates of these entities that receive protected health information, such as municipalities, contractors and subcontractors. This includes Cayuga County. The rule also increases penalties for noncompliance and strengthens the Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS. On May 25th, 2018 the General Data Protection (GDPR) took effect to protect all EU citizens from privacy and data breaches with its own set of reporting requirements. In addition, on May 25th, 2018 the New York State Board of Elections implemented their requirements for Cybersecurity Incident Reporting. The Cayuga County Breach Notification Policy encompasses Personnel Information (PI) and Personal Health Information (PHI) both of which are types of information that can be used on their own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Policy

Any member of the Cayuga County workforce who becomes aware of a situation that may put client information at risk must report the discovery as a potential breach and fulfill their responsibilities as outlined in this procedure. Any workforce member who fails to fulfill any applicable responsibility from this procedure will not only face disciplinary action up to and including termination, but may also be subjected to severe monetary penalties and incarceration by Health Insurance Portability and Accountability Act (HIPAA) Enforcement entities (Federal Office of Civil Rights and New York State Attorney General).

General Responsibilities

Workforce Member

All Cayuga County workforce members must fulfill the following Workforce Member responsibilities:

Complete all required reading and training related to preventing and responding to breach incidents (Appendix A).

Immediately after discovery (and in no case later than end of business day) report any possible breach of Cayuga County client information to the Compliance Officer or designee (Appendix A).

At minimum, include in the report the Cayuga County department or Business Associate name, names of people involved, and a brief description of the situation/incident.

As much as possible, take steps to reduce harm to the affected individual(s).

Compliance Officer or their Designee

Respond to reports by contacting the affected Department Head or Business Associate without unreasonable delay and in no case later than 24 hours after any report of a possible breach is received.

Take the steps included in the **Business Associate Breach Incidents** section of this policy or fulfill the remaining responsibilities in this section for internal incidents.

Work with affected Department Head to complete the current **Cayuga County Breach Incident Investigation Form** (Appendix A) without unreasonable delay.

With input from the Breach Incident Team, determine the likelihood and the extent of a breach according to the breach risk assessment included on the Cayuga County Breach Incident Investigation Form.

Guide Department Head in notifying affected individual(s) according to legal requirements.

Work with Department Head to mitigate harm to affected individual(s), and recommend procedural changes to prevent future similar incidents.

Review high-risk assessments with Breach Incident Team.

Review all breach incidents quarterly with the Cayuga County Compliance Committee.

Report breaches to the Secretary of Health and Human Services and/or State Agencies and any other entities as required (Appendix A).

Log breaches and document process.

Chief Information Officer

Update Appendices as required. Appendices will be modified as required reading, training and breach reporting protocols are revised.

Department Head

Oversee implementation and training for this policy within the department, ensuring that all department workforce members who have access to PI or PHI are fully trained in their responsibilities detailed in this procedure.

Maintain Business Associate Agreements with HIPAA-compliant PHI incident procedures, including breach procedures.

Work with the Compliance Officer or designee to complete the Cayuga County Breach Incident Investigation Form without unreasonable delay.

With guidance from the Breach Incident Team, follow all steps detailed in this procedure to notify affected individuals of breach according to legal requirements.

Work with the Compliance Officer or designee to mitigate harm to individual(s).

Make procedural changes recommended by the Compliance Officer or designee and/or the Breach Incident Team to prevent future similar incidents.

Participate as necessary on the Breach Incident Team for breaches affecting the department.

Breach Incident Team

As requested by the Compliance Officer or designee, oversee breach incident response for high-risk breach incidents through the following:

Review breach risk assessments.

Provide guidance for notifying affected individuals of breach.

Review and recommend harm mitigation steps.

Recommend procedural changes to prevent future similar incidents.

Notify media of breaches as required by law and as detailed in this procedure.

For a Potential Breach of ANY Client Information

Immediately after discovery (and in no case later than end of business day) any Cayuga County workforce member must report any potential breach of Cayuga County client information to the Compliance Officer or designee. To allow investigation, a breach report must include at least the following: The Cayuga County department or Business Associate organization where the incident occurred, the names of people involved, and a brief description of the situation/incident, including when it happened.

In the event that a workforce member other than the Compliance Officer or designee receives a breach report, the workforce member must forward the report to the Compliance Officer or designee without unreasonable delay (in no case later than the end of business day).

When the Compliance Officer or designee and the County Administrator is unavailable for more than 1 business day, the Legislative Chair or designee will act as back-up.

Without unreasonable delay and in no case later than 24 hours after receiving a report, the Compliance Officer or designee must contact the affected Department Head to begin the incident investigation.

Without unreasonable delay, the affected Department Head will assist the Compliance Officer or designee in completing the Cayuga County Breach Incident Investigation Form (Appendix A) with assistance from the Information Technology Services Department as needed.

If PHI may have been compromised, the Compliance Officer or designee will provide as detailed information as possible in the following required 4 PHI risk factors in the Risk Assessment section of the Cayuga County Breach Incident Investigation Form, explaining the assessment as clearly as possible.

The nature and the extent of the PHI involved, including types of identifiers and likelihood of re-identification

The unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made

Whether the PHI was actually acquired or viewed, or if only the opportunity existed for the information to be acquired or viewed

The extent to which the risk to the PHI has been mitigated.

If the incident does not involve PHI, the Compliance Officer or designee will complete all other items in the Risk Assessment section of the Cayuga County Breach Incident Investigation Form, and will mark the 4 PHI items "N/A".

The Compliance Officer or designee will request Breach Incident Team involvement in the incident response process for high-risk incidents (e.g. breaches involving more than one client's information, criminal penalties, monetary penalties or employment sanctions).

The Compliance Officer or designee will determine, based on breach definitions in the applicable laws and the results of the Risk Assessment section of the Cayuga County Breach Incident Investigation Form, the likelihood and extent of the breach. The Officer will detail the decision reasoning on the Cayuga County Breach Incident Investigation Form.

If Investigation and Risk Assessment Rule Out Breach of ANY Client Information

If the investigation and risk assessment rule out breach of client PI and show a low probability that PHI was compromised, the Compliance Officer or designee will log the incident as a Non-Breach Incident on the Information Incident Log and will keep all related documentation for 6 years.

The Department Head, with assistance from the Compliance Officer or designee and/or Breach Incident Team, will make necessary procedural changes to prevent future similar incidents.

If an affected individual is aware that his/her information may have been breached, the Department Head will send a letter summarizing investigative steps and notifying him/her that no breach occurred.

If Investigation Shows That a Breach of Client Private Information (PI) Has Occurred

If the investigation does not rule out breach of Private Information (PI), the Compliance Officer or designee will notify the Chief Information Officer as needed, and will consult the New York State ITS Enterprise Information Security Office (NYS ITS EISO) regarding the scope of the breach and restoration measures (Appendix A).The Compliance Officer or designee (and Breach Incident Team, if involved) will work with the Department Head to determine and take steps to reduce harm to the affected individual(s). The Department Head will provide to the Compliance Officer or designee written documentation of harm mitigation steps taken. Examples of mitigation could include satisfactory assurances that the affected information would not further utilized or disclosed (confidentiality agreement) or that the information will be destroyed.

The Compliance Officer or designee and/or Breach Incident Team will guide the Department Head in notifying all affected individual(s) "in the most expedient time possible and without reasonable delay,

allowing for any necessary law enforcement delay", as required in New York State law. Notification will be directly provided to all affected individuals by one of the following methods:

Written notice

Electronic notice (only at affected individual's request)

Telephone notice (log must be kept)

Substitute notice by ***all*** of the following (allowed only when cost of other methods would exceed $250,000 or there are more than 500,000 affected individuals)

E-mail (if e-mail address is known); and

Conspicuous website posting; and

Notification to major statewide media.

Notice must include a description of the information breached and contact information of the Cayuga County Compliance Officer or designee.

The Compliance Officer or designee will complete the NYS Security Breach Reporting Form (Appendix A), with guidance from the Chief Information Officer/Designee and/or Breach Incident Team as needed, and send it to the three entities required on the reverse side of the form (A template for individual notice provided must be attached). If more than 5000 NYS residents are affected by the breach, the Compliance Officer or designee will also notify consumer reporting agencies. **Reporting to NYS agencies must not delay notification of individuals.**

After review of the incident, the Compliance Officer or designee (and the Breach Incident Team, if involved) will evaluate whether harm has been mitigated as much as possible, and will recommend to the Department Head further mitigation steps as necessary. The Department Head will provide to the Compliance Officer or designee written documentation of harm mitigation steps taken.

The Compliance Officer or designee and/or Breach Incident Team will work with the Department Head to evaluate procedures. The Department Head will make procedural changes recommended to prevent future similar incidents, and will provide written documentation of changes to the Compliance Officer or designee.

The Compliance Officer or designee will log the incident in the Information Incident Log as a "PI Breach" and will keep all related documentation for 6 years.

If Investigation Shows That a Breach of Protected Health Information (PHI) Has Occurred

If review of the Cayuga County Breach Incident Investigation Form Breach Risk Assessment by the Compliance Officer or designee (and Breach Incident Team if involved) determines that there is more than a low probability that PHI was compromised, then a PHI breach has occurred. The following steps must be taken

Notify Affected Individuals. Without unreasonable delay and in no case later than 60 calendar days after the incident, the Compliance Officer or designee (or Breach Incident Team if involved) will guide the Department Head in notifying affected individual(s) by first class mail that their PHI has been compromised. The notification may be provided in one or more mailings as information is available. When

there is insufficient or out-of-date contact information that precludes written notification to the individual, the substitute notice will be provided according to the following rules:

For fewer than 10 individuals:

> Substitute notice will be provided by the alternative form of notice that is most likely to reach the individual, and may be an alternative form of written notice, a telephone notice, or another form of notice.

For 10 or more individuals, substitute notice will:

> Be in the form of either a conspicuous 90-day posting on the Cayuga County web site, or conspicuous notice in the major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
>
> Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether his/her unsecured protected health information may be included in the breach.

If the individual is deceased, notice will be sent by first class mail to the next of kin or personal representative if the address is known. Substitute notice will not be provided.

In an urgent situation in which misuse of the compromised information could be imminent, the Department Head may contact individuals by telephone or other means, as appropriate, in addition to the required written notice.

The notification will be written in plain language and will include, to the extent possible:

> A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
>
> A description of the types of unsecured protected health information that were involved in the breach;
>
> Any steps individuals should take to protect themselves from potential harm resulting from the breach;
>
> A brief description of what the Cayuga County is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
>
> Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

Concurrently with notification, the Department Head, with guidance from the Compliance Officer or designee (or Breach Incident Team if involved), will take all possible steps to mitigate harm to the affected individual(s) and make necessary changes to department procedure to prevent future breaches. The Department Head will provide written documentation of steps taken and changes made to the Compliance Officer or designee.

If the breach affects fewer than 500 individuals, the Compliance Officer or designee will report the breach to NYS agencies as required and will notify the Secretary of Health and Human Services no later than 60 days after the end of the calendar year, in the manner specified on the Health and Human Services Web site.

If the breach affects 500 or more individuals, in addition to individually notifying the affected person, the following steps will be taken:

If the 500 individuals are in the same State or jurisdiction, the Breach Incident Team will provide notice with the following 5 items to prominent media outlets serving the State or jurisdiction without unreasonable delay and in no case later than 60 days after the incident.

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

A description of the types of unsecured protected health information that were involved in the breach;

Any steps individuals should take to protect themselves from potential harm resulting from the breach;

A brief description of what the Cayuga County is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Website, or postal address.

The Compliance Officer or designee will report the breach to the Secretary of Health and Human Services, without unreasonable delay and in no case later than 60 days after the incident, in the manner specified on the Health and Human Services web site (Appendix A).

The Compliance Officer or designee will complete the NYS Security Breach Reporting Form (Appendix A), with guidance from the Chief information Officer/Designee and/or Breach Incident Team as needed, and send it to the three entities required on the reverse side of the form (A template for individual notice provided must be attached). If more than 5000 NYS residents are affected by the breach, the Compliance Officer or designee will also notify consumer reporting agencies. Reporting to NYS agencies must not delay notification of individuals. To reduce harm to individuals and prevent future breaches, the Compliance Officer or designee (and Breach Incident Team if involved) may review the incident after notifications are complete, and may recommend additional needed harm mitigation and/or procedural changes to the Department Head. The Department Head will provide written documentation of any steps taken or changes made to the Compliance Officer or designee.

The Compliance Officer or designee will log the incident as a "PHI Breach" on the Information Incident Log and will keep all related documentation for 6 years.

Business Associate Breach Incidents

Written Contracts/Agreements with Business Associates will state that PHI Incidents must be reported to Cayuga County immediately upon discovery.

All Cayuga County Workforce Members must report any known Business Associate PHI Breach to the Compliance Officer or designee as required in this policy in the section titled **General Responsibilities** listed under **Workforce Member**.

After receiving a Business Associate breach report, the Compliance Officer or designee, will report the breach to the Breach Incident Team.

The Compliance Officer or designee, with oversight from the Breach Incident Team, will take the following steps:

Contact the Business Associate to review details of the breach incident that were not provided in the report but are required for HIPAA notification.

Review the harm mitigation steps taken by the Business Associate and recommend additional steps if necessary.

Notify the affected individual(s) as required under HIPAA as detailed in this policy in the section titled **If Investigation Shows That a Breach of Protected Health Information (PHI) Has Occurred**.

Notify the Secretary of Health and Human Services as required under HIPAA and as detailed in this policy in the section titled **If Investigation Shows That a Breach of Protected Health Information (PHI) Has Occurred**.

Review the Business Associate's safeguards for HIPAA Compliance and recommend changes to prevent future similar incidents.

Definitions

Affected Individual; The person(s) whose information, in the case of an information breach, may have been compromised.

Affected Department Head; The County Department Head within whose department a breach incident has occurred.

Breach of Private Information (PI); Unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach, provided that the private information is not used of subject to unauthorized disclosure. In determining whether information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, such state entity may consider the following factors, among others:

> 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
>
> Indications that the information has been downloaded or copied; or
>
> Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Breach of Protected Health Information (PHI); Any PHI access, use or disclosure impermissible under the Privacy Rule is presumed to be a breach unless a risk assessment of at least the following factors show a low probability that the information was compromised:

> The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification
>
> The unauthorized person who used the protected health information or to whom the disclosure was made
>
> Whether the protected health information was actually acquired or viewed
>
> The extent to which the risk to the protected health information has been mitigated.

Breach Incident Team; County Administrator, County Attorney, Affected Department Head(s) Chief Information Officer and IT staff as needed. Oversee breach response for high-risk breaches as requested by the Healthcare Security and Privacy Officer.

Business Associate; A person or organization that has access to the Protected Health Information of Cayuga County clients through the provision of a service to Cayuga County.

Business Associate Agreement; The written agreement required between a covered entity under HIPAA and its Business Associate detailing how the Business Associate will comply with HIPAA.

Client; Any individual served by Cayuga County and/or serving for Cayuga County.

Compliance Committee; A group of people designated and chaired by the Compliance Officer to oversee and help administer this Compliance Program.

Compliance Officer; A person within the County organization who is assigned the responsibility of maintaining and overseeing an effective County Compliance Program.

Consumer reporting agency; any person or entity which, for monetary fees, dues or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

County or County entity; the County of Cayuga, New York, its agencies, boards, bureaus, divisions, committees, commissions, councils, departments, public authorities, public benefit corporations, offices or other governmental entities performing a governmental or proprietary function for the County of Cayuga.

Discovery; Under HIPAA, a breach is considered discovered on the first day on which such breach is known or, by exercising reasonable diligence would have been known.

General Data Protection Regulation (GDPR); GDPR takes effect May 25, 2018. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Governmental Agencies; Agencies involved in healthcare investigations include, but are not limited to, the U.S. Department of Health and Human Services' Office of Inspector General, U.S. Department of Justice, Federal Bureau of Investigation, Centers for Medicaid and Medicare Services, New York State Department of Health, Office of the Medicaid Inspector General, New York State Medicaid Fraud Control Units, and New York State Office for People with Developmental Disabilities.

HIPAA; A federal law titled "Health Insurance Portability and Accountability Act". Regulations issued under HIPAA protect the privacy of health information and identifying information for all Americans. HIPAA went into effect on April 14, 2003.

Incident, Breach; Any potential violation of confidentiality law; any privacy complain or any potential breach. In the context of an information breach.

New York State Board of Elections Cyber Incident; County Boards of Elections (CBOE) must report all cyber incidents affecting or potentially affecting elections systems to the New York State Division of Homeland Security and Emergency Services (DHSES), and the New York State Board of Elections (NYSBOE).

Non-compliance; Failure or refusal to act in accordance with this Compliance Program, or other standards or procedures, or with federal, state or local laws or regulations.

Omnibus; A 2013 ruling that strengthened HIPAA Privacy and Security protections.

Private Information (PI); Private 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:

Social security number;

Driver's license number or non-driver identification card number;

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.

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 or maintained.

Regulatory Violation; Any action that constitutes fraud, abuse, or a violation of a federal, state or local law or regulation.

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

Violation; Activity or inactivity that breaks any health information confidentiality law, in the context of an information breach.