RESOLUTION NO. 370-22 9/27/22 COL HD HIPAA Policy rev

ADOPTING CAYUGA COUNTY "HIPAA POLICY"

BY: Chris Petrus, Chair, Government Operations Committee

WHEREAS, Cayuga County (the "County") is committed to compliance with all applicable laws and regulations including, but not limited to, the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and as supplemented by the Privacy and Security Regulations found at 45 Code of Federal Regulations ("CFR") §§160 and 164 (herein collectively "HIPAA"); and

WHEREAS, the County is a "covered entity" as that term is defined under HIPAA, but also qualifies as a "hybrid entity" under 45 CFR §164.103 and 164.105, due to having health components and non-health care components within its organization; and

WHEREAS, the Operations Officer and County Attorney have reviewed the previous work of the Compliance Committee as well as the existing HIPAA policies maintained by the Public Health Department, the Mental Health Department, and the Sheriff's Department and have identified the need for a County-wide HIPAA Policy to further enhance the security and privacy of individuals' protected health information throughout all County Departments;

WHEREAS, the Legislature upon receiving the recommendations of its staff, has also determined that the County may more effectively and efficiently administer its policies and procedures for HIPAA compliance by designating the County as a "hybrid entity," as that term is defined under HIPAA, 45 CFR §164.103 and 164.105; and

WHEREAS, the Legislature finds it is in the public interest to adopt a County-wide HIPAA policy; now, therefore, be it

RESOLVED, that the Cayuga County Legislature does hereby designate the County as a "hybrid entity," pursuant to 45 CFR §§164.103 and 164.105; and be it further

RESOLVED, that the following Cayuga County departments are hereby designated as healthcare components within the County's hybrid entity: (1) Public Health Department; (2) Community Mental Health Center; (3) Sheriff's Department, Jail Facility, and Emergency Management Office; and be it further

RESOLVED, that all other Cayuga County departments or offices not otherwise specified or designated as healthcare components are hereby designated as non-healthcare components. Healthcare components are not free to exchange PHI with non-healthcare components unless such disclosure is permitted by law. Some employees may perform both healthcare components and non-healthcare components functions as part of their job responsibilities. Any person who performs duties for both healthcare components and non-healthcare components must not use or disclose PHI in a way that would be impermissible under HIPAA; and be it further

RESOLVED, that the Cayuga County Legislature does hereby adopt the attached Cayuga County HIPAA Policy to be added to the Cayuga County Policy Manual; and be it further

RESOLVED, that the Operations Officer is hereby designated the Compliance Officer for purposes of coordinating the activities of the Privacy Officers designated within each health care component and document the administration of the within County-wide HIPAA Policy; and be it further

RESOLVED, the County's healthcare components are hereby directed to institute appropriate training, policies and procedures for compliance with HIPAA and consistent with the County-wide policy; and be it further

RESOLVED, that the policy be posted on the County Website as well as on the webpage of each of the health care components, the County Portal and distributed by the Clerk of the Legislature to all Department Heads; and be it further

RESOLVED, that this resolution will take effect immediately upon its adoption.

SEAL OF CAYUGA COUNTY NEW YORK

State of New York }
County of Cayuga }

I do hereby certify, that I have compared the forgoing copy of a Resolution duly passed and adopted by the Cayuga County Legislature at a meeting held on the 27th day of September 2022 with the original Resolution, and that the same is a true and correct copy and transcript thereof, and the whole thereof.

Given under my hand and official seal September 28th, 2022

Sheila P. Smith
CLERK, CAYUGA COUNTY LEGISLATURE

CAYUGA COUNTY POLICY

DEPARTMENT: **Legislature**

POLICY TITLE: **Cayuga County HIPAA Policy**

EFFECTIVE DATE: **September 27, 2022**

RESOLUTION NO.: **370-22**

SUPERSEDES POLICY OF: **N/A**

Objective: This is a County-wide policy to provide for the security and protection of "Protected Health Information" ("PHI") (as defined below) through clear and concise instructions on the administration of the "HIPAA Rules" within County Departments.

Policy:

In 1996, Congress enacted the Health Insurance Portability and Accountability Act [PL 104–191 (42 USC §210, *et seq*.)] ("HIPAA") to improve the efficiency and effectiveness of the health care system. HIPAA authorized the United States Department of Health and Human Services ("HHS") to adopt national standards designed to ensure the security and privacy of individuals' health information. As required by HIPAA, HHS issued the Standards for Privacy of Individually Identifiable Health Information (45 CFR §164, *et seq.*) (the "Privacy Rule") and the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"). The Privacy Rule established national standards for the use and disclosure of individually identifiable health information-called "protected health information" or "PHI", as well as standards for individuals' privacy rights to understand and control how their health information is used. The Security Rule established a national set of security standards for protecting certain health information that is held or transferred in electronic form.

HIPAA and the Privacy and Security Rules were updated in 2009 under the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and again in 2013 under the Omnibus Rule. HIPAA, the Privacy and Security Rules, the HITECH Act and the Omnibus Rule are collectively referred to as the HIPAA Rules.

Protected health information ("PHI") is defined as information, including demographic data that relates to an individual's past, present or future physical or mental health or condition, 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 identifies the individual. "EHR" refers to electronic health records whose use, management, distribution and disclosure is protected under HITECH. Unless the context suggests otherwise, the term "PHI" is deemed to include all forms of electronic health records, "EHR".

The County of Cayuga (the "County") is committed to compliance with all applicable laws and regulations including, but not limited to, the HIPAA Rules. The County further recognizes that in fulfilling its various functions and missions, it has several departments which will come into possession of, use and disclose PHI. Therefore, it is incumbent upon the County to establish a county-wide policy and procedure for handling such information in a manner that complies with HIPAA and its implementing rules and regulations.

I. DESIGNATIONS

A. Hybrid Entity. County activities include both HIPAA covered and non-covered functions. Accordingly, the County shall be designated a "Hybrid Entity" so that it may more effectively and efficiently administer these policies and procedures in compliance with the HIPAA Rules. The County shall also designate one or more Compliance Officers, HIPAA Privacy Officers and a HIPAA Security Officer all of whom shall assist with overseeing and implementing the policies and procedures outlined herein.

B. Health Care Components.

a. For purposes of this policy a reference to "health care component" refers those departments within the organization who perform the functions of a health plan, health care clearinghouse, or health care provider as defined under the HIPAA Rules.

b. The County Board of Legislators has designated by resolution the County departments that shall be its health care components. The designated health care components are:

(a) Public Health Department;
(b) Community Mental Health Center ("Mental Health Department"); and
(c) Sheriff's Department (Jail Facility);
(d) Emergency Management Office.

c. Such designations may be amended from time to time. The Department head of each designated health care component, or their designee, shall be responsible for administration of this policy. Each health care component may develop and implement procedures for implementing this policy that apply within their respective departments, provided that such procedures meet or exceed the minimum requirements set forth herein, as well as all HIPAA laws, rules and regulations, as the same may be amended from time to time.

d. Each health care component is responsible for protecting PHI to the same extent as is required of a "covered entity" as that term is defined under the HIPAA Rules. Without limiting the generality of the foregoing, a health care component may not disclose PHI to a non-health care component of the County under circumstances that would be prohibited under this policy if the non-health care component were a separate legal entity.

e. Each non-health care component which receives PHI from a health care component must protect the PHI to the same extent as a health care component and is prohibited from using, sharing or disclosing the PHI except in compliance with this policy.

f. An employee who works in a health care component and also in a non-health care component may not use, share or disclose PHI that was created, used or received in the employee's capacity as a member of the health care component's workforce in a manner that is prohibited under this policy.

C. Officers.

1. **"HIPAA Privacy Officer"** shall be the employee within each health care component designated by the Department Head who is responsible for overseeing the department's compliance with the HIPAA Rules including:

a. Implementing the Privacy Rule within such department and overseeing compliance with this policy as well as any applicable departmental policies and procedures;
b. Supervising and assisting departmental staff in overseeing and monitoring the protection of PHI;
c. Designing and implementing departmental procedures, standards, and guidelines, including minimum requirements that provide adequate protection of PHI for their respective health care component.
d. Provide copies of all departmental procedures relative to this HIPAA Policy to the Compliance Officer.
e. Work with the Compliance Officer with responding, investigating and documenting actual or suspected breaches in confidentiality or integrity of PHI within their respective health care component.

2. **"HIPAA Security Officer"** shall be the Cayuga County Chief Information Officer or his or her deputy. The HIPPA Security Officer shall be responsible for:

a. Overseeing and monitoring compliance with the Security Rule, particularly with regard to the electronic receipt and transmission of PHI.
b. Assisting each of the departmental Privacy Officers in overseeing and monitoring the security of PHI.

c. Designing and implementing procedures, standards, and guidelines, including minimum requirements that provide adequate information security for electronic PHI for all County health care components.
d. Assisting the Privacy Officer(s) and Compliance Officer in responding to actual or suspected breaches in confidentiality or integrity of PHI.

3. The **"Compliance Officer"** shall be the Operations Officer for the County and shall be responsible for working with the HIPAA Privacy Officer(s) in connection with actual or suspected breaches in confidentiality or integrity of PHI, as well as the investigation and documentation for same.

   a. The Compliance Officer shall report to and work collaboratively with the Chairperson of the Legislature (or designee) while handling any reports of and/or suspected breaches in confidentiality or integrity of PHI, and the investigation and documentation for same in accordance with this policy.

   b. The Compliance Officer shall maintain copies of all departmental procedures relative to this HIPAA Policy.

II. NOTICE OF PRIVACY PRACTICES

A. General Rules.

1. Except as stated in subparagraph II(A)(2) below, every individual whose interaction with the County or the County's services results in the creation, receipt, maintenance, or transmission of PHI shall be provided notice of the County's privacy practices written in plain language and as more fully described in this Section.

2. Pursuant to federal regulations [45 C.F.R. § 164.520(a)(3)], the rules pertaining to Notice of Privacy Practices described herein do not apply to the Cayuga County Jail, and inmates housed therein are not entitled to notice of the County's privacy practices.

B. Content of Notice. Each health care component shall develop a Notice of Privacy Practice ("Notice") containing all of the elements required by the Privacy Rule, as well as any other information required by applicable State or federal regulations, and it shall be implemented in accordance with the HIPAA Rules. The Notice shall contain at a minimum the following information:

1. A prominent display of the statement "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

2. A description of the health care component's uses and disclosures.

3. A statement that genetic information will not be disclosed absent authorization.

4. A description of patient's rights including but not limited to the right to:

   a. Request a copy of their medical record.
   b. Request that the County corrects their medical record.
   c. Request confidential communications.
   d. Request that the County limit what information it uses or shares.
   e. Obtain a list of those with whom the County has shared their PHI with.
   f. Obtain a copy of the County's Notice of Privacy Practices.
   g. Choose another individual to act on behalf of the patient.
   h. File a complaint.

5. A description of the health care component's responsibilities, including a statement that the health care component:

   a. Is required to maintain the privacy of PHI.

b. Is required to abide by the terms of its Notice, and
c. Reserves the right to change the terms of its Notice.

6. The contact information for the health care component's Privacy Officer(s) as well as the Compliance Officer.

7. The effective date of the Notice of Privacy Practices.

C. Provision of Notice.

1. *Generally.*

a. The Notice shall be made available on request to any individual.

2. *Each health care component providing direct treatment:*

a. Must provide Notice at the patient's first date of service delivery or in an emergency situation, as soon as reasonably practicable after the emergency treatment situation.
b. Absent an emergency situation, a good faith effort shall be made to obtain a written acknowledgement of receipt of the Notice. If an acknowledgement is not obtained, the good faith efforts and reason why the acknowledgment was not retained shall be documented.
c. If the health care component has a physical delivery site: it shall have the Notice available at the service delivery site and post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.
d. *Changes to Notice*. The terms of the Notice may be changed from time to time. If a material change to the Notice is made, the revised Notice shall be prominently displayed on the County's website, available at the service delivery site and posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.
e. *Electronic Notice*.
i. The Notice shall be prominently posted on the health care component's website and made available electronically through the website.
ii. An electronic version of the Notice may be provided to an individual via e-mail if the individual has agreed in writing to receive electronic notice. If it is known that an e-mail transmission failed, a paper copy of the Notice shall be provided to the individual.
iii. If the first service delivery to an individual is delivered electronically, electronic Notice shall be provided automatically and contemporaneously in response to the individual's first request for service.
iv. All individuals receiving electronic notice shall retain the right to obtain a paper copy of the Notice upon request.

C. Documentation. Compliance with this Section (Notice of Privacy Practices) shall be documented by retaining copies of the Notice issued and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment.

III. USES AND DISCLOSURES NOT REQUIRING AUTHORIZATION

A. Generally. No County employee shall use or disclose PHI unless permitted or required under the HIPAA Rules. In circumstances where use and disclosure of PHI is permitted or required, such use and disclosure may not necessitate obtaining the patient's authorization to do so. Nevertheless, reasonable efforts shall be made to obtain an individual's authorization to use and disclose PHI in every instance.

B. Required Uses and Disclosures Not Requiring Authorization.

1. *To the individual.*
a. Disclosure must be made to an individual properly requesting his or her PHI and does not require prior authorization, except for psychotherapy notes and information compiled in anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

2. *When required by the Secretary of HHS.*
   a. Disclosure must be made when required by the Secretary of HHS to investigate or determine the County's compliance with the HIPAA Rules and do not require prior authorization.

C. Permitted Uses and Disclosures Not Requiring Authorization. All permitted uses and disclosures not requiring authorization made under this subsection shall, before being used and disclosed, be reviewed and approved by the Privacy Officer.

1. *For Treatment, payment or health care operations.* PHI may be used or disclosed without patient authorization for treatment, payment or health care operations.

   a. More specifically, PHI may be used or disclosed without patient authorization:
      i. For a County health care component's own treatment, payment or health care operations.
      ii. For treatment activities of a health care provider.
      iii. To another covered entity or health care provider for the payment activities of the entity that receives the information.
      iv. To another covered entity for health care operations activities of the entity that receives the information, if:
         a) Each entity either has or had a relationship with the individual who is the subject of the PHI being requested,
         b) The PHI pertains to such relationship, and
         c) The disclosure is for the County's own treatment, payment or health care operations or for treatment activities of a health care provider; or for the purpose of health care fraud and abuse detection or compliance.

   b. Restriction on use and disclosure of PHI.
      i. An individual has the right to request, in writing, that the County's health component restrict the use and disclosure of their PHI for treatment, payment or health care operations or for involvement in the individual's care or for notification purposes.
      ii. Except as set forth below, the health care component is not required to agree to an individual's request for a restriction. But, if it does, it is bound to such restriction except in an emergency situation.
      iii. The County must agree to an individual's request to restrict disclosure of PHI about an individual to a health plan if:
         a) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and
         b) The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the County in full.
      iv. The County may terminate a restriction on the use and disclosure of PHI, if:
         a) The individual agrees to or requests the termination in writing or
         b) The individual orally agrees to the termination and oral agreement is documented.
      v. All restrictions to the use and disclosure of PHI shall be documented.

   c. Confidential Communications.
      i. An individual is permitted to request to receive communications of PHI by alternative means or at alternative locations. Such request shall be in writing directed to the Privacy Officer. All reasonable requests shall be accommodated.

2. *As required by law.*
   a. PHI may be used or disclosed without authorization or an opportunity to agree or object to the extent that such use or disclosure is required by law. However, such use and disclosure shall be limited to the relevant requirements of such law.

3. *Public health activities.*
   a. PHI may be used or disclosed without authorization or an opportunity to agree or object for the following public health activities and purposes:
      i. Public health authority – PHI may be disclosed to a public health authority that is authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability,

including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. PHI may also be disclosed at the direction of a public health authority to an official of a foreign government agency that is acting in collaboration with a public health authority.

ii. Abuse or neglect – PHI may be disclosed to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

iii. FDA – PHI may be disclosed to a person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity.

iv. Communicable diseases – PHI may be disclosed to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.

v. Employer – PHI may be disclosed to an employer, about an individual who is a member of the employer's workforce so long as:
   a) The County provided health care to the individual at the request of the employer
      1) to conduct an evaluation relating to medical surveillance of the workplace or
      2) to evaluate whether the individual has a work-related illness or injury.
   b) The PHI that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance; and
   c) The County provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:
      1) By giving a copy of the notice to the individual at the time that health care is provided; or
      2) If the health care is provided on the employer's work site, by posting the notice in a prominent location where the health care is provided.

vi. School – PHI may be disclosed to a school where the individual is a student or prospective student if:
   a) The PHI disclosed is limited to proof of immunization,
   b) The school is required to have such proof of immunization, and
   c) The health care component obtains and documents an agreement, whether oral or written, for such disclosure from either:
      1) A parent, guardian, or other person acting in loco parentis of the individual, or
      2) The individual, if the individual is an adult or emancipated minor.

b. County Department of Public Health
   i. The County Department of Public Health may use and disclose PHI, without authorization or an opportunity to agree or object, in all cases in which it is permitted to disclose such information for public health activities under subsection (iii)(1)(a) above "Public health authority."

4. *Abuse, neglect or domestic violence.*
   a. PHI may be used or disclosed without authorization or an opportunity to agree or object about an individual whom the County reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence:

      i. To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law,
      ii. If the individual agrees to the disclosure, or
      iii. To the extent the disclosure is expressly authorized by statute or regulation, and
         a) The County believes the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
         b) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the PHI represents that the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

   b. If a disclosure is made under this subsection, the individual must be promptly informed that such a report has been or will be made, except if:

i. Informing the individual would place them at risk of serious harm, or

ii. A personal representative would be informed and it is believed that the personal representative is responsible for the abuse, neglect or other injury and that informing such person would not be in the best interest of the individual.

5. *Health oversight activities.*
   a. PHI may be disclosed without authorization or an opportunity to agree or object to a health oversight agency for oversight activities authorized by law.

   b. PHI shall not be disclosed without authorization or an opportunity to agree or object where the activity is an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

      i. the receipt of health care.
      ii. a claim for public benefits related to health, or
      iii. qualifications for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

   c. To the extent that any County health care components are a health oversight agency, it may use PHI for health oversight activities as permitted by this policy.

6. *Judicial and administrative proceedings.*

   a. PHI may be disclosed without authorization or an opportunity to agree or object in the course of any judicial or administrative proceeding:

      i. In response to an order of a court or administrative tribunal, provided only the PHI expressly authorized by such order is disclosed, or

      ii. In response to a subpoena, discovery request, or other lawful process so long as the County receives satisfactory assurance. Any subpoenas, discovery requests, or other lawful process requesting disclosure of PHI shall be directed to the to the relevant health care component's Privacy Officer with a copy to the County Attorney's Office.

7. *Law enforcement purposes.*
   a. PHI may be disclosed without authorization or an opportunity to agree or object for a law enforcement purpose to a law enforcement official under certain conditions. Law enforcement purposes may include:

      i. Disclosure required by law, or
      ii. Compliance with a court order, warrant, subpoena or summons, a grand jury subpoena, administrative request.

   b. PHI may be disclosed without authorization or an opportunity to agree or object in response to law enforcement official's information requests for identifying or locating a suspect, fugitive, material witness, or missing person.

   c. PHI may be disclosed without authorization or an opportunity to agree or object in circumstances related to a crime including medical emergencies.

8. *Coroners, medical examiners, and funeral directors.*
   a. PHI may be used or disclosed without authorization or an opportunity to agree or object to a coroner, medical examiner or funeral director as necessary to carry out their duties with respect to the decedent.

9. *Cadaveric organ, eye or tissue donation purposes.*

a. PHI may be used or disclosed without authorization or an opportunity to agree or object to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

10. *Research.*
    a. If the departmental Privacy Officer approves, PHI may be used or disclosed without authorization or an opportunity to agree or object for research.

11. *Averting serious threat to health or safety*.
    a. If the departmental Privacy Officer approves, PHI may be used or disclosed without authorization or an opportunity to agree or object if, in good faith, it is believed that the use or disclosure:
        i. Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the use or disclosure is to someone that is able to prevent or lessen the threat; or
        ii. Is necessary for law enforcement to identify or apprehend an individual.

12. *Specialized government functions*.
    a. If the departmental Privacy Officer approves, PHI may be used or disclosed without authorization or an opportunity to agree or object for military and veteran's activities, national security and intelligence activities, protective services for the President and others, medical suitability determinations, correctional institutions and other law enforcement custodial situations, and programs providing public benefits.

13. *Workers' compensation*.
    a. PHI may be disclosed without authorization or an opportunity to agree or object as authorized by and to the extent necessary to comply with New York State laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries or illness without regard to fault.

D. Verifying Identity of Authorized Person. Prior to using or disclosing PHI under this subsection, the identity of the person requesting the PHI and the authority for that person to have access to the PHI shall be verified. (see IV.B.)

E. Disclosure Record/Log. A written record/log of every transmission or disclosure of PHI or EHR shall be kept. Information to be documented shall include:
1. The date when and the person or entity to whom the disclosure was made,
2. The purpose for the disclosure,
3. A description of the information disclosed, and
4. A basis providing the employee with the authority to transmit or disclose the PHI or EHR.

IV. USES AND DISCLOSURES REQUIRING AUTHORIZATION

A. Generally. Except for where otherwise noted in this subsection or as required by law, in the following circumstances PHI shall not be used or disclosed absent a valid authorization. (See IV.B.)

1. *Psychotherapy notes.*
    a. A valid authorization must be obtained for use and disclosure of psychotherapy notes except:

        i. To carry out the following treatment, payment or health care operations:

            1) Use by the originator for treatment of the individual;
            2) Use or disclosure by the County for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or
            3) Use or disclosure by the County to defend itself in a legal action or other proceeding brought by the individual; and
            4) A use or disclosure that is required or permitted under Section III(B) and (C) above with respect to oversight of the originator of the psychotherapy notes.

2. *Marketing.*

a. A valid authorization (See IV. B.) must be obtained for use and disclosure of PHI for marketing except if the communications is in the form of:
   i. A face-to-face communication made by the County to an individual; or
   ii. A promotional gift of nominal value provided by the County.

3. *Sale of PHI.*
   a. A valid authorization (See IV.B.) must be obtained for any disclosure of PHI which is a sale of PHI. Such authorization must state that the disclosure will result in remuneration to the County.

4. *Use and disclosure within the scope of authorization.*
   a. Use or disclosure of PHI, with a valid authorization (See IV.B.), shall be consistent with such authorization.

B. Core Elements and Requirements for a Valid Authorization. A valid authorization must contain at a minimum the following:

1. *Core elements.*
   a. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.
   b. The name or other specific information of the person(s), or class of persons, authorized to make the requested use or disclosure.
   c. The name or other specific identification of the person(s), or class of persons, to whom the County may make the requested use or disclosure.
   d. A description of each purpose of the requested use or disclosure.
   e. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
   f. Signature of the individual and date.
      i. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

2. *Required statements.*
   a. The individual's right to revoke the authorization in writing.
   b. The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.
   c. The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer be protected by this subpart.

3. *Plain language.* The authorization shall be written in plain language.

4. *Copy to the individual.* When an authorization is signed, a copy of the signed authorization shall be provided to the individual.

C. Defective Authorization. An authorization is invalid if the document has any of the following defects:

1. Expiration date has passed or the expiration event is known by the County to have occurred.
2. The authorization is incomplete.
3. It is known by the County that the authorization has been revoked.
4. The authorization is a compounding or prohibited authorization.
5. Any material information contained in the authorization that is known to the County to be false.

D. Compound Authorizations. An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization unless approved by the Privacy Officer.

E. Prohibition on Conditioning Authorizations. The provision of treatment, payment, or eligibility for benefits shall not be conditioned upon receiving a signed authorization.

F. Revocation of Authorizations. An individual may revoke an authorization provided under this section at any time, provided that the revocation is in writing, except to the extent that:

1. The County has acted in reliance thereon; or
2. If the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself.

G. Documentation. Each health care component shall be responsible for maintaining records of all authorizations and related documentation.

V. USES AND DISCLOSURES REQUIRING AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR OBJECT

A. Generally. In certain circumstances a health care component may use or disclose PHI so long as the individual is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit, or restrict the use or disclosure. In these circumstances, the individual may be informed orally and the health care component may obtain the individual's oral agreement or objection to a use or disclosure permitted under this section. All such oral communication(s) and agreement(s) or objection(s) shall be documented and retained by the relative health care component.

B. Use and Disclosure for Directory Purposes.

1. *Use and disclosure.*
   a. Except as otherwise provided in this subsection, in maintaining a directory of individuals, an individual's name, location within the County health care component, general description of individual's condition and the individual's religious affiliation may be used and disclosed.

2. *Opportunity to object.*
   a. An individual shall be informed of any PHI included in a directory and the persons to whom the health care component may disclose such information and the individual shall be provided with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted under Section (v) (B)(i) above.

3. *Emergency circumstances.*
   a. Where the individual cannot practicably be informed of the health care component's intended uses and disclosures, the health care component may still use and disclose some or all of the PHI permitted above if such disclosure is consistent with the individual's prior expressed preference or in the exercise of professional judgment the health care component determines such use or disclosure is in the individual's best interests.

C. Use and Disclosure for Involvement in the Individual's Care and Notification.

1. *Permitted uses and disclosures.*
   a. Pursuant to C(2), (3), (4) and (5) as applicable, PHI may be disclosed to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual that is relevant to such person's involvement with the individual's health care or payment related to the individual's health care. Pursuant to the same below sections that are applicable, PHI may be used or disclosed to notify, or assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

2. *Uses and disclosures with the individual present.*
   a. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by C(i) above, and has the capacity to make health care decisions, PHI may be used or disclosed if:

      i. The individual's agreement is obtained;
      ii. The individual is provided an opportunity to object to the disclosure, and the individual does not express an objection; or
      iii. In exercising professional judgment, it is inferred from the circumstances that the individual does not object to the disclosure.

3. *Limited uses and disclosures when the individual is not present.*

a. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, PHI directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes may be disclosed so long as in the exercise of professional judgment it is determined that the disclosure is in the best interests of the individual.

4. *Uses and disclosures for disaster relief purposes.*
   a. The health care component may use or disclose PHI to a public or private entity authorized by law to assist in disaster relief efforts, for the purpose of coordinating with such entities in notifying family members or others involved in the individual's health care. The requirements in Section V subsections (C)(ii), (iii) and (v) apply to such uses and disclosures to the extent that the County, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

5. *Uses and disclosures when the individual is deceased.*
   a. PHI may be disclosed to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, who was involved in the individual's care or payment for health care and to the extent that such PHI is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to the County.

VI. MINIMUM NECESSARY DISCLOSURE

A. Generally. With respect to all requests for, or the use and disclosure of PHI, the minimum PHI necessary shall be used or disclosed in accordance with the below. Under no circumstances shall an entire medical record be used, disclosed or requested unless it is specifically justified and documented as the amount reasonably necessary to accomplish the purpose of the use, disclosure, or request.

B. Minimum Necessary Uses of PHI. Reasonable efforts shall be made to identify the persons or class of persons, as appropriate, within the County who needs access to PHI to carry out their duties and the category or categories of PHI to which access is needed and any condition needed for such access.

C. Minimum Necessary Disclosures and Requests of PHI.

1. *Routine or recurring disclosures and requests.* For any type of disclosure and request made on a routine and recurring basis, policies and procedures shall be implemented by the County health care components limiting the PHI disclosed or requested to the amount reasonably necessary to achieve the purpose of the disclosure or request.

2. *All other disclosures and requests*. For all other disclosures and requests, the County health care components shall develop criteria designed to limit the PHI disclosed or requested to the information reasonably necessary to accomplish the purpose for which disclosure or request is sought and review requests for disclosure on an individual basis in accordance with such criteria.

VII. RIGHTS OF INDIVIDUALS

A. Request for Privacy Protection of PHI.

1. *Request for restriction of uses and disclosures*.
   a. An individual shall have the right to request that the health care component restricts uses or disclosures of:
      i. PHI about the individual to carry out treatment, payment or health care operations and
      ii. PHI related to involvement in the individual's care and notification purposes under Section V(C) above.

   b. Except in relation to disclosure of PHI to a health plan, the County is not required to agree to the requested restriction.

   c. Absent an emergency, if the requested restriction is agreed to, the health care component shall be permitted to use the restricted PHI, or may disclose the restricted PHI, to a health care provider for purposes of treatment of the individual.

i. If restricted PHI is disclosed to a health care provider for emergency treatment, it shall be requested that such health care provider not further use or disclose the restricted PHI.

d. If the requested restriction is agreed to, it shall not apply in certain circumstances including:
   i. When the health care component is required to disclose PHI to the Secretary of HHS to investigate to determine the health care component's compliance,
   ii. For the County's use and disclosure for facility directories pursuant to Section V(B) above, or
   iii. Section III above titled "USES AND DISCLOSURES NOT REQUIRING AUTHORIZATION."

e. A request to restrict disclosure of the individual's PHI to a health plan must be agreed to if:
   i. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and the PHI pertains solely to a health care item or service for which the individual, or other person other than the health plan, has paid the County in full.

f. An agreement to a restriction may be terminated by the health care component if:
   i. The individual agrees to or requests the termination in writing,
   ii. The individual orally agrees to the termination and the oral agreement is documented, or
   iii. When approved by the Privacy Officer, the health care component informs the individual that it is terminating its agreement to a restriction.

g. All agreements to a restriction of the use and disclosure of PHI shall be documented and retained in accordance with this policy by the respective health care component (see, Section XV[B]).

2. *Request for confidential communications.*
   a. Individuals shall be permitted to request, in writing, to receive communications of PHI from the health care component by alternative means or at alternative locations. Reasonable requests shall be accommodated.

   b. An explanation from the individual as to the basis for the requested confidential communications shall not be a condition for granting the request.

B. Request for Access to PHI.

1. *Access to PHI.*

   a. Right of access. An individual shall have a right of access to inspect and obtain a copy of their PHI for as long as the PHI is maintained by the health care component except for psychotherapy notes and information compiled in reasonable anticipation of, or for the use in, a civil, criminal, or administrative action or proceeding.

2. *Requests for access and timely action.*
   a. Individual's request for access. An individual shall be permitted to request, in writing, access to inspect or to obtain a copy of their PHI maintained by the health care component. Such written request shall be submitted to the applicable health care component's Privacy Officer who shall be responsible for receiving and processing requests for access by individuals.

   b. Timely action.
      i. If space is available, an opportunity for visual inspection of an individual's PHI must be permitted within ten (10) days of the individual's request and a copy of such records shall be furnished to the individual within a reasonable time thereafter.

      ii. If space for inspection is not available, a copy of the requested records shall be provided to the individual within a reasonable time but not more than thirty (30) days from the date of the request for access if the information is maintained on-site or sixty (60) days if the information is maintained off-site.

c. Fees. If an individual request a copy of their PHI or agrees to a summary or explanation of such information, a reasonable, cost-based fee may be imposed which shall not exceed the cost incurred by the health care component, provided that the fee includes only the cost of:

i. Labor for copying the PHI, whether in paper or electronic form;
ii. Supplies for creating the paper or electronic copy (not to exceed seventy-five cents per page);
iii. Postage; and
iv. Preparing an explanation or summary of the PHI if the individual agreed to the receipt of an explanation or summary.

The health care component shall not deny an individual a copy of their PHI based solely on the individual's inability to pay.

3. *Denial of access*.

a. Unreviewable grounds for denial. A request for access to PHI may be denied without providing the individual an opportunity for review in the following circumstances:
i. The request is for psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
ii. The County Jail or a County health care component acting under the direction of the Jail may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
iii. An individual's access to PHI created or obtained by the County in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the County has informed the individual that the right of access will be reinstated upon completion of the research.
iv. An individual's access may be denied if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

b. Reviewable grounds for denial. A request for access may be denied, with an opportunity to review the denial, in the following circumstances:
i. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
ii. The PHI refers to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person, or
iii. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

c. Making other information accessible. Where access is denied to a part of an individual's PHI, to the extent possible, an individual shall be provided access to any other PHI requested.

d. Denial. The health care component shall provide written denial to the individual within ten (10) days of the individual's request. The denial must be in plain language and contain:
i. The basis for the denial;
ii. If applicable, a statement of the individual's review rights including a description of how the individual may exercise such review rights; and
iii. A description of how the individual may file a complaint with the Compliance Officer pursuant to Section XI or to the Secretary of HHS. The description must include the name, or title, and telephone number of the Compliance Officer.

e. Review of a denial of access. If access is denied on reviewable grounds, the individual shall have the right to have the denial reviewed by a licensed professional who is designated by the health care component to act as a reviewing official and who did not participate in the original decision to deny. Alternatively, the individual may appeal the denial by filing with the NYS Department of Health at:

Access to Patient Information Coordinator
Office of Professional Medical Conduct
150 Broadway, Suite 355
Albany, New York 12204-2719

f. Other responsibility. If the health care component does not maintain the PHI requested but it knows where the requested information is maintained, it shall inform the individual where to direct the request for access.

C. Request for Amendment of PHI.

1. *Right to amend*. An individual shall have the right to request to amend their PHI for as long as the information is maintained by the County.
   a. Denial of Amendment. An individual's request for an amendment may be denied if it is determined that the PHI:
      i. Was not created by the health care component, unless the originator is no longer available to amend the information,
      ii. Is not part of a designated record set,
      iii. Would not be available for inspection under Section VII(B) above, or
      iv. Is accurate and complete.

2. *Requests for amendment and timely action*.
   a. Individual's Request for Amendment. An individual shall be permitted to request amendment of their PHI maintained in a designated record set. Such request shall be in writing, provide reason(s) supporting such request, and submitted to the relevant health care component's Privacy Officer who shall be responsible for receiving and processing requests for amendments by individuals.

   b. Timely action. An individual's request for an amendment shall be acted upon no later than sixty (60) days after receipt of such a request.
      i. If action cannot be taken within the 60-day timeframe, the health care component may have an additional thirty (30) days to respond so long as within the 60-day timeframe it provides the individual with a written statement of the reasons for the delay and the date to be completed and include the notation that the health care component has not previously had an extension on the same request.

3. *Accepting the Amendment*. If a request for an amendment is accepted, in whole or in part, the following requirements must be satisfied:

   a. Making the Amendment. Appropriate amendments shall be made to the PHI or record by, at a minimum, identifying the records in the record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment.
   b. Informing the Individual. Timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to notify the relevant person(s) with which the amendment needs to be shared in accordance with the subsection below.
   c. Informing Others. Reasonable efforts shall be made to inform and provide the amendment within a reasonable time to:
      i. Persons identified by the individual as having received PHI about the individual and needing the amendment, and
      ii. Persons, including business associates, that the health care component knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

5. *Denying the Amendment*. If a request for an amendment is denied, in whole or in part, the following requirements must be satisfied:

   a. Denial. A written denial shall be timely provided to the individual no later than sixty (60) days after receipt of the request. The denial shall use plain language and contain:
      i. The basis of the denial,
      ii. The individual's right to submit a written statement disagreeing with the denial and the individual may file such statement,
      iii. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the health care component provide the individual's request for amendment and the denial with any future disclosures of PHI that is the subject of the amendment, and
      iv. A description of how the individual may complain to the Privacy Officer or to the Secretary of HHS. The description must include the Privacy Officer's title and telephone number.

   b. Statement of Disagreement. An individual shall be permitted to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

   c. Rebuttal Statement. The health care component shall be permitted to prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, a copy shall be provided to the individual who submitted the statement of disagreement.

   d. Record Keeping. As appropriate, the record or PHI shall be identified in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the health care component's denial of the request, the individual's statement of disagreement, if any, and the health care component's rebuttal, if any, to the designated record set.

   e. Future Disclosures.
      i. If a statement of disagreement has been submitted by the individual, either the individual's request for an amendment, the health care component's denial of the request, the individual's statement of disagreement, if any, and the health care component's rebuttal or an accurate summary of any such information shall be included with any subsequent disclosure of PHI to which the disagreement relates.
      ii. If a statement of disagreement was not submitted, either the individual's request and the health care component's denial or an accurate summary of such information shall be included with any subsequent disclosure of PHI to which the disagreement relates.

5. *Actions on notices of amendment*. If the health care component is informed by another covered entity of an amendment to an individual's PHI, the health care component shall amend the PHI accordingly.

D. Request for an Accounting of Disclosures of PHI.

1. *Right to an accounting of disclosures of PHI*.
   a. An individual shall have a right to receive an accounting of disclosures of PHI made by the health care component except for disclosures:
      i. To carry out treatment, payment and health care operations as provided,
      ii. To individuals of PHI about them,
      iii. Incident to a use or disclosure otherwise permitted or required,
      iv. Pursuant to an authorization,
      v. For a health care component's directory or to persons involved in the individual's care or other notification purposes,
      vi. For national security or intelligence purposes,
      vii. To correctional institutions or law enforcement officials,
      viii. As part of a limited date set, or
      ix. That occurred prior to the health care component's compliance date.

2. An individual may obtain an accounting up to the six years prior to the date on which the accounting is requested if the request involves PHI. If the disclosures involved EHR, the accounting shall include only disclosures made within three (3) years prior to the date on which the accounting is requested.

3. The health care component must temporarily suspend a patient's right to receive an accounting of disclosures that are made to a health oversight agency or to a law enforcement agency if the agency so requests as follows:
   a. The agency provides the health care component with a written statement that providing an accounting of disclosures is reasonably likely to impede the agency's activities. The agency must specify the time for which suspension is required.

   b. The agency orally informs the health care component that providing an accounting of disclosures is reasonably likely to impede the agency's activities. If an oral statement is made, the health care component must document the statement and the identity of the agency making the statement. The health care component must temporarily suspend the patient's right to an accounting of the particular disclosures covered by the statement for no longer than 30 days. If the agency provides a written statement within 30 days of the oral statement, the health care component must temporarily suspend the patient's right to an accounting of the particular disclosures for the time specified in the written statement.

2. *Request for an accounting*. All requests for an accounting must be submitted in writing upon such form as may be provided by the health care component and shall be submitted to the Privacy Officer who shall be responsible for receiving and processing requests for an accounting by individuals.

3. *Content of the accounting*. Except as otherwise provided, an individual requesting an accounting shall be provided a written accounting including the following:
   a. Disclosures of PHI that occurred up to six years prior to the date of the request for an accounting, including disclosures to or by the health care component's business associates, or in the event of EHR disclosures that occurred within three (3) years of the date of the request,
   b. The date of the disclosure,
   c. The name of the entity or person who received the PHI and, if known, the address of such entity or person,
   d. A brief description of the PHI disclosed, and
   e. A brief statement of the purpose of the disclosure or, in lieu of such statement, a copy of a written request for a disclosure.
   f. If during the accounting period the health care component has made multiple disclosures to the same person or entity for the same purpose, it shall provide the above five requirements in addition to the frequency, periodicity, or number of the disclosures made during the accounting period and the date of the last such disclosure.
   g. If during the accounting period the health care component made disclosures of PHI for a particular research purpose, provision of the accounting shall be reviewed and approved by the Privacy Officer.

4. *Providing the accounting to the individual*.
   a. A request for an accounting shall be acted upon no later than sixty (60) days after receipt of such request. If the health care component is unable to provide the accounting within such time frame, it may extend the time to provide the accounting by no more than 30 days, provided that the health care component provides the individual with a written statement of the reasons for the delay and the date by which the accounting will be provided. Only one such extension shall be permitted.

   b. The first accounting provided to an individual in any twelve (12) month period shall be provided without charge. However, the health care component shall be permitted to impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that the individual is informed of such fee in advance.

5. *Documentation*. Any time a written accounting is provided to an individual such accounting shall be documented and retained in accordance with this policy (see, Section XV[B]).

VIII. BUSINESS ASSOCIATES

A. Business Associate Agreement Requirements. A contract between the health care component and a business associate must:

1. *Establish the permitted and required uses and disclosures*. The contract may not authorize the business associate to use or further disclose PHI in a manner that would violate the HIPAA Rules except that:
   a. The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate and
   b. The contract may permit the business associate to provide data aggregation services relating to the health care component's health care operations.

2. *Provide that the business associate will:*
   a. Not use or further disclose the information other than as permitted or required by the contract or as required by law,
   b. Use appropriate safeguards and comply, where applicable, with paragraph number 3 below with respect to electronic PHI, to prevent use or disclosure of the information other than as provided for by its contract,
   c. Report to the health care provider any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured PHI,
   d. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information,
   e. Make available PHI for an individual's right to access for amendment and incorporate any amendments to protected health information and for accounting of disclosures.
   f. To the extent the business associate is to carry out a contractual obligation, comply with the requirements that apply to the health care component in the performance of such obligation.
   g. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the health care component available to the U. S. Secretary of Health and Human Services for purposes of determining the health care provider's compliance with the HIPAA Rules and
   h. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the health care component that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

3. *Authorize the health care component to terminate the contract where business associate has violated a material term of the contract.*

B. Where Business Associate is also a Government Entity.

1. Where the business associate is another government entity, the County and/or it's health care component and the other government entity may enter into a memorandum of understanding ("MOU").

2. If a business associate is required by law to perform a function or activity on behalf of the health care component or to provide a service described in the definition of business associate to the health care component , the health care provider may disclose PHI to the business associate to the extent necessary to comply with the legal mandate provided that the health care component attempts in good faith to obtain satisfactory assurances, if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

3. The health care component may omit the termination authorization, if such authorization is inconsistent with the statutory obligations of the health care provider or its business associate.

4. The health care component may disclose only a limited data set to a business associate for the business associate to carry out a health care operation function if first approved by the relevant Privacy Officer.

C. Other Requirements for Business Associate Agreements/MOUs.

1. An agreement/MOU between a health care component and the business associate may permit the business associate to use PHI received by the business associate in its capacity as a business associate to the health care component, if necessary:

a. For the proper management and administration of the business associate, or
b. To carry out the legal responsibilities of the business associate.

2. An agreement/MOU between the health care component and the business associate may permit the business associate to disclose PHI received by the business associate in its capacity as a business associate for the purposes described above, if:

   a. The disclosure is required by law, or
   b. The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

      i. The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

D. Business Associate Agreements with Subcontractors.

1. The standards set forth in this section shall apply to the contract/MOU between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between the health care component and its business associate.

IX. TRAINING

A. Generally. As a hybrid entity, the County shall require each health care component to provide training regarding these policies and procedures to each of their employees, as follows:

   a. To each new member of the health care component's workforce within a reasonable period of time after the person joins the health care component's workforce;
   b. A refresher course shall be provided to each member of the health care component's workforce by no later than December 31 of each year.
   c. To each member of a health care component's workforce whenever there is a material change in these policies or procedures within a reasonable period of time after the material change becomes effective.

2. Evidence that the above training has been provided shall be documented and retained in accordance with this policy (see, Section XV[B]).

X. SAFEGUARDING PHI

A. The County shall have in place administrative, technical, and physical safeguards protecting the privacy of PHI, including EHR from any intentional or unintentional use or disclosure that is in violation of these policies and procedures and limiting incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

B. Such safeguarding measures shall include, without limitation:
1. Implementing a security management process, which includes conducting an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic health records (EHR) the County creates, receives, maintains, or transmits and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level;
2. Implementing procedures to guard against and detect malicious software, ransomware, exfiltration and any other form of infiltration by outside users;
3. Training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
4. Implementing access controls to limit access to EHR to only those persons or software programs requiring access.
5. To protect EHR, all records shall be encrypted and password protected when stored, received, transmitted and backed up.

C. Business Associates that hold County EHR must also comply with this Section X and annually provide the County or the applicable health care component with evidence of compliance including but not limited to 3rd party audits for assessments, certifications, and vulnerability assessments, to provide assurance that they are proactively protecting the health care component's data and have systems in place to identify breaches.

XI. COMPLAINTS

A. The County's complaint process is attached as Appendix A. Such process may be changed by the Compliance Officer from time to time to ensure compliance with all applicable laws and regulations including, but not limited to, the HIPAA rules.

B. All complaints received shall be documented to include investigation into those complaints and their disposition, if any.

XII. DISCIPLINARY ACTION

A County employee who violates this policy and/or the health care components' procedures may be subject to discipline in accordance with any applicable collective bargaining agreement or Section 75 of the Civil Service Law, if applicable, up to and including termination.

XIII. MITIGATION

The County shall mitigate, to the extent practicable, any harmful effect that is known to the County of a use or disclosure of PHI in violation of its policies and procedures or the requirements of this subpart by the County or its business associate.

XIV. RETALIATION AND WAIVER

A. Retaliation.

1. No employee of the County:

    a. Shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for reporting any violation of these policies and procedures, or participating in or cooperating with an investigation into an alleged violation.
    b. Any employee found to have intimidated or retaliated against another employee in violation of this paragraph shall be subject to discipline up to and including termination.

B. Waiver.

1. Individuals shall not be required to waive their rights under the HIPAA Rules as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

XV. DOCUMENTATION AND RETENTION

A. Documentation. The County shall:

1. Maintain this policy and any health care component related procedures in written or electronic form.

2. If a communication is required by this policy and/or the health care component's procedures to be in writing, maintain such writing, or an electronic copy, as documentation. ~~and~~ If an action, activity, or designation is required by this policy and/or health care component's procedures to be documented, maintain a written or electronic record of such action, activity, or designation.

3. Maintain sufficient documentation to prove that all notifications were made as required by this policy and/or the health care component procedures or that the use or disclosure did not constitute a breach.

B. Retention. The documentation required above shall be retained for a period of at least six (6) years from the last date the individual was a patient at or received services within a County health care component.

XVI. DATA BREACH NOTIFICATION

(See HIPAA Breach Notification and Investigation Policy)

Appendix A
Cayuga County HIPAA Complaint Process

A. Anyone who wishes to make a complaint regarding a breach or suspected breach of Protected Health Information (PHI) may contact the County Compliance Officer at the address provided below.

Cayuga County Compliance Officer
160 Genesee Street, 6th Floor
Auburn, NY 13021
315-255-4900

B. Upon receipt of the complaint, the Compliance Officer will notify the HIPAA Privacy Officer for the relevant health care component who will acknowledge receipt of the complaint by responding to the complainant in writing.

C. Following the acknowledgement of the written complaint, the HIPAA Privacy Officer for the applicable health care component (Mental Health, Health Department or Sheriff's Office), in collaboration with the Compliance Officer, HIPAA Security Officer, and county Attorney, shall conduct a full investigation to include, but not limited to, reviewing all relevant records together with any other pertinent information and interviewing employees and other witnesses as deemed necessary and appropriate.

D. Upon completion of the investigation, the Privacy Officer in consultation with the Compliance Officer and County Attorney, shall (i) advise the complainant that the investigation is concluded; (ii) if it is determined that a breach of PHI has occurred, take such action as is required under the HIPAA Breach Notification Policy (Policy No. ____); (iii) provide education or training as deemed appropriate to the involved employees; and (iv) recommend revisions to relevant policies as deemed necessary. In the event that the matters complained of result in employee discipline such discipline shall be implemented in accordance with applicable County employee policies and collective bargaining agreements.

E. Responses to the complainant shall be in writing by the appropriate health care component HIPAA Privacy Officer and in collaboration with the Compliance Officer and County Attorney (or documented when provided verbally), be timely, provide a summary of the investigation (without detailing specifics pertaining to investigation or disciplinary action, if any) and provide the corrective actions taken.

F. Language interpretation services and/or translation of the response to the complainant will be arranged by the Compliance Officer if there is any limited English proficiency.

G. If the complainant is not satisfied with the response and/or the resolution, they may file a complaint with the United States Department of Health and Human Services Officer for Civil Rights using the address, telephone number or website provided below.

United States Department of Health and Human Services Officer of Civil Rights

200 Independence Avenue, S. W.
Washington, D.C. 20201
1-877-696-6775
www.hhs.gov/ocr/privacy/hipaa/complaints/.

H. All complaints, coordination, investigation, action and responses shall be documented and retained for a period of at least six (6) years.