HIPAA COMPLIANCE POLICY

Sullivan County is considered a "hybrid entity" under the Health Insurance Portability Accountability Act of 1996 (or HIPAA) – i.e., an entity whose business activities include both covered and non-covered functions. Therefore, certain County divisions, departments, offices and agencies will regularly deal with individuals' personal health information (PHI) and others may not. Whether or not you regularly deal with such information, the County's HIPAA standards apply to you.

It is our policy that each employee shall comply with the HIPAA Privacy Rule and Security Rule, and each employee shall protect the confidentiality of protected health information (as discussed below).

DEFINITIONS

"*Affected Individual*" for the purposes of this policy only, an Affected Individual means a County employee, contractor, vendor, intern, and volunteer or any party acting on behalf of the County.

"Business Associate" means a person or entity who creates, receives, maintains or transmits protected health information for a function or activity of the County which involves the use or disclosure of individually identifiable health information. Examples of functions include claims processing or administration, data analysis, processing or administration, quality assurance, billing and benefit management. Services include legal, accounting and consulting.

"Covered Health Care Component" means each of the County departments designated as "health care components" of the County (see Health Care Components of the County section).

"Protected Health Information" or "PHI" means individually identifiable health information collected from an individual; any information, including demographic information, collected from an individual that is created or received by Sullivan County, its workforce or business associates. PHI can relate to past, present or future physical, or mental health or condition of an individual. In addition, PHI can relate to past, present or future payment for the provision of healthcare to an individual which identifies the individual or with respect to which there is reasonable basis to believe that information can be used to identify the individual. Examples of PHI include (but are not limited to):

- Name, address (including street address, city, county, zip code, and equivalent geocodes), names of employer, names of relatives, elements of dates (birth, death, admission and discharge), telephone numbers, fax numbers, electronic mail addresses, social security number, medical record number, member or account number, certificate/ license number, voice/fingerprints, photos, occupation or any other unique identifying number of characteristic or code.

"*Retaliation*" for the purposes of this policy only**,** retaliation is any adverse action taken against an individual and includes but is not limited to discharge, suspension, discipline, demotion, penalization, harassment, intimidation, threats, change of assignment, exclusion, avoidance, shunning, lack of recognition, discrimination or being passed over for promotion or assignment against any Affected Individual or recipient of service.

"Workforce" is defined as employees, elected officials, volunteers, trainees, and other persons who conduct, in the performance of work for Sullivan County, is under the direct control of Sullivan County, whether or not they are paid by the covered entity.

HIPAA PRIVACY AND SECURITY OFFICERS

The Compliance Officer is the HIPAA Privacy Officer and is designated by the Sullivan County Manager. The Compliance Office is located on the 2nd floor of the Government Center. The Compliance Officer can be reached at 845-807-0664 or Sullivanprivacyofficer@sullivanny.gov

Sullivan County's Chief Information Officer is identified as the HIPAA Security Officer by the Sullivan County Manager. The HIPAA Security Officer can be reached at 845-807-0110 or Sullivansecurityofficer@sullivanny.gov

HEALTH CARE COMPONENTS OF THE COUNTY

Each of the following are hereby designated "health care components" under HIPAA Regulations:

- Department of Social Services (Medicaid and Personal Care)
- The Department of Community Services (Behavioral Health Clinic)
- Public Health Services (LTHHC, CHHA, Early Intervention, Preschool Supported Health Services)
- Adult Care Center
- Office for the Aging (Case Management)
- Risk Management & Insurance (Self-Insured Plan)
- Bureau of EMS (EMS Fly Car Services)
- Jail (Medical Unit)

NOTICE OF PRIVACY PRACTICES

The Notice of Privacy Practices is created by the Compliance Office and shall contain all information required under federal regulations regarding the Notice of Privacy Practices.

Each Covered Health Care Component shall prominently post a copy of the current Notice of Privacy Practices in a location accessible to individuals applying for or receiving services.

Each Covered Health Care Component shall post the current version of its Notice of Privacy Practices on the website where services are described.

Any individual applying for or receiving health care services from Sullivan County shall be provided with the Covered Health Care Component's Notice of Privacy Practices at the first encounter, or as soon thereafter as is possible.

Acknowledgement of Receipt of the Notice of Privacy Practices shall be attempted and retained in accordance with the Covered Health Care Component's departmental procedures. If an Acknowledgment of Receipt cannot be obtained, the Covered Health Care Component must document the attempt to obtain the acknowledgment and the reasoning why a signed acknowledgment could not be obtained. Record retention requirements shall apply.

INVOLVING INFORMATION TECHNOLOGY SERVICES

To safeguard protected health information, all software utilized by any County Division, Department, Office, Agency, or Unit of the County must be under the jurisdiction of the Division of Information

Technology Services. Departments wishing to utilize new and updated software shall engage the Chief Information Officer before engaging with services, vendors, contractors, etc.

BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

The County shall include in any health care-related contract with a third party a statement regarding HIPAA Privacy obligations, also known as the Business Associate Agreement (BAA).

In collaboration with the County Attorney's Office, the HIPAA Privacy Officer and the HIPAA Security Officer are the responsible individuals for the County's Business Associate Agreement template. Departments are responsible for understanding which services and operations require a Business Associate Agreement.

Business Associate Agreements are also in place between specific County departments that share protected health information. For example, the Department of Public Health has a BAA in place with several departments due to the nature of information exchanged.

Failure to follow the terms of a Business Associate Agreement or contract with the County may result in sanctions including and up to termination of contract.

DEPARTMENT PRIVACY DESIGNEES

The County Manager shall appoint a Privacy Designee in each Covered Health Care Component. Department Privacy Designees are expected to facilitate and maintain the upholding of all County and Department HIPAA Compliance Privacy and Security policies and procedures. Department Privacy Designees sit on the County's Administrative Oversight Committee (AOC). The HIPAA Privacy Officer is responsible for creating and updating the County's privacy standards and communicating with each Privacy Designee who will be responsible for the coordination and implementation of the respective department's privacy standards.

Department Privacy Designees shall consult the HIPAA Privacy Officer and/or the HIPAA Security Officer when questions and or concerns arise on the application of County and Department Privacy and Security Policy or Procedure. Department Privacy Designees shall inform the HIPAA Privacy Officer and the HIPAA Security Officer immediately of any HIPAA Compliance issue that arises. The report shall include evidence describing the issue, outstanding questions and concerns, and key witness information. Department Privacy Designees are expected to keep the HIPAA Compliance Office abreast of changes, updates, new issues, etc. during the course of an active investigation. Departments and Department Privacy Designees are expected to cooperate throughout the investigation and demonstrate professionalism at all times.

COVERED HEALTH CARE COMPONENT WALKTHROUGHS

On a monthly basis, the Department Privacy Designee in each Covered Health Care Component shall complete a walkthrough of their department to ensure compliance with the County's HIPAA standards. Walkthroughs specifically apply to all environments and scenarios where Protected Health Information (PHI) is accessed, stored, processed, or transmitted. This includes, but is not limited to, physical locations where PHI is handled, electronic systems used for PHI management, and all staff interactions involving PHI. The scope of the walkthrough is designed to ensure comprehensive adherence to HIPAA standards across all relevant facets of departmental operations. The HIPAA Security Officer and HIPAA Privacy Officer will conduct quarterly unannounced visits in each Covered Health Care Component to further reinforce comprehensive HIPAA compliance.

COMPLAINT PROCESS

Complaints should be first reported to the respective department's Privacy Designee. The Department Privacy Designee shall then contact the HIPAA Privacy Officer. If the Department Privacy Designee is not available or if the individual prefers, questions, concerns and complaints can be forwarded to the HIPAA Privacy Officer or in the absence of such officer, to the County Manager.

It is the policy of Sullivan County that all complaints relating to the protection of health information be investigated and resolved in a timely fashion. The HIPAA Privacy Officer is duly authorized to review and investigate complaints and implement resolutions in collaboration with the HIPAA Security Officer if the complaint stems from a valid area of non- compliance with the HIPAA Privacy and Security Rule. Any recommendations for employee discipline will be made to the appropriate department head, the Commissioner of Human Resources, the County Attorney, and the Deputy County Manager.

The HIPAA Privacy Officer is the responsible individual for reporting founded breaches to the Office of Civil Rights (OCR). Reporting to other regulatory authorities (NYS Office of Mental Health, NYS Department of Health, etc.) may be required depending on the nature of the incident and shall be reported, as necessary, by the HIPAA Privacy Officer.

EDUCATION/TRAINING

Sullivan County provides training on HIPAA standards to members of the workforce which includes employees in the County's Covered Health Care Components and County departments designated as Business Associates of such Covered Health Care Components.

The training shall be provided to all members of the workforce within a reasonable period of time after an individual joins the workforce and annually thereafter.

The training shall be provided to each member of the workforce whose functions are affected by a material change in the policies or procedures required by the Privacy or Security Rule, within a reasonable period of time after the material change becomes effective.

Participation in training shall be documented and include the date of training, trainer's name, participants and the topics covered.

The County's HIPAA standards can be found on the SC Portal and are listed under HIPAA Compliance. All employees should review this information at least annually.

MINIMUM NECESSARY: ROLE-BASED ACCESS

Sullivan County workforce and Business Associates will access or disclose only the minimum amount of PHI necessary to provide services and benefits to clients. This will be in accordance with the Covered Health Care Component's department-specific policies.

Sullivan County workforce will make reasonable effort to limit the amount of PHI used or disclosed to the minimum necessary to effectively accomplish the activity. Departments subject to the requirements stated herein shall implement procedures for safeguarding PHI especially when a conflict of interest is noted. Sullivan County workforce will follow the Covered Health Care Component's department specific policies for the minimum necessary PHI to be used or disclosed.

Accessing PHI out of curiosity is not allowed. You must only access the PHI that is necessary for you to perform your job. The County conducts audits in PHI containing platforms for instances of unauthorized access. This is called snooping for PHI and may result in disciplinary action including and up to termination.

CONFLICTS OF INTEREST

The County considers it to be a conflict of interest for its workforce to provide healthcare to family members or where another conflict of interest exists. All Affected Individuals shall fully disclose all situations involving an actual or potential conflict of interest, whenever such situations arise in written format.

The written disclosure shall include the Affected Individual(s) full name, department(s) and title(s), the date the conflict was made known, and a description of the actual or potential conflict.

The County will take reasonable efforts to ensure that Affected Individuals are not assigned to their family members. In dire emergency situations, an Affected Individual may provide a service where a conflict of interest exists.

MEDICAL RECORD REQUESTS

All PHI obtained on behalf or created on a patient/client is confidential and is to be safeguarded in accordance with County policy and procedure.

Sullivan County will not use or disclose information unless either:

- The client has authorized the use or disclosure in accordance with the County's standards.
- The use or disclosure is permitted by Sullivan County policy or federal and/or state law or regulation.

Sullivan County's Covered Health Care Components will adopt procedures to reasonably safeguard client information.

All complaints related to the unauthorized use or disclosure of protected health information shall be promptly reported.

NON-RETAILIATION

The County is committed to a non-retaliation policy and recognizes the various State and Federal applicable laws and will protect any Whistleblower. Retaliation is any adverse action taken against an individual because they:

- Exercised any right established under the County's HIPAA Compliance standards and procedures.
- Participated in any process established by the County's HIPAA Compliance standards including the filing of a complaint or participating in the investigation of such complaint.

- Testified, assisted, or participated in an investigation, compliance review, proceeding, or hearing relating to the policies and procedures.

Any County employee or individual doing business with the County who engages in retaliation may be subject to disciplinary action including but not limited to termination or sanctions including but not limited to termination of contract.

DISCIPLINARY ACTION: SANCTIONS

Failure to adhere to the County's HIPAA Compliance standards may result in additional training, counseling or disciplinary action including but not limited to and including termination. A monetary fine could be imposed by the government on the individual that breaches patient/client confidentiality.