POLICY: The Health Insurance Portability and Accountability Act (HIPAA), a federal law, was passed to protect patient privacy with regard to medical information. This policy establishes the standards and procedures for the uses and disclosures of protected health information maintained by Stillwater Center to ensure compliance with federal law.

Responsibilities Defined:

Delegated Access Coordinator. The Clinical Quality Manager will serve as the Delegated Access Coordinator. The Delegated Access Coordinator shall be responsible for defining, in consultation with the appropriate Data Manager, divisional access profiles for employees of her/his division by type of protected health information the employees are authorized to access.

The Delegated Access Coordinator shall identify the types of protected health information to which each user needs access, under what conditions each user needs access, and the limit of access necessary for the user to perform her/his job requirements as specified in her/his position description and her/his need to know.

Data Managers. The Emergency, Respite, and Program Manager, Nurse Manager, and Facilities Manager serve as Data Managers for their respective department.

If any Stillwater employee chooses to maintain a personal database containing individually identifiable health information generated in the course of performing professional responsibilities, he/she will be responsible as the data manager for that database and must follow all applicable laws, regulations, policies, and procedures.

The Data Manager is responsible for ensuring that any and all applicable policies are fully executed for the protected health information for which he/she is responsible.

Individuals (clients, families, staff) whose individually identifiable health information is part of Stillwater protected health information have the right to request correction of inaccurate individually identifiable health information. Requests are made in writing to the Center’s Delegated Access Coordinator.

The Data Manager is responsible to determine that the person requesting the protected health information has the authority to receive the disclosure if the identity of such authority is not known to Stillwater. The Data Manager shall obtain any documentation, statements, or representation whether oral or written, from the person requesting the protected health information when such documentation, statements, or representation is a condition of the disclosure.

The Data Manager is responsible to ensure that information has been de-identified if the requesting party does not have the authority to receive protected health information.

The Data Manager shall not permit external data users to access protected health information unless the external user meets the standards for business associates.

The Data Manager shall comply with any state, federal, or regulatory agency that requests to be granted access to protected health information under law or regulation. In such cases, to the extent possible, the Fiscal Services department shall request a Business Associate agreement be negotiated between Stillwater and the agency before access is granted to the protected health information.

Disclosure to the Individual: Stillwater may disclose protected health information to the individual who is the subject of the information, or his/her guardian.

Use and Disclosure for Treatment, Payment, or Health Care Operations:

A. Stillwater may use and disclose protected health information for treatment, payment, and health care operations within the following restrictions:

1. Protected health information may be used or disclosed for Stillwater’s own treatment, payment, and health care operations.
2. Protected health information may be disclosed to a health care provider for treatment activities.

3. Protected health information may be disclosed to another covered entity for health care operation activities of Stillwater if:
   a. The entity to which the protected health information is to be disclosed has or had a relationship with the individual who is the subject of the protected health information being requested and has the authority to receive such information; or,
   b. The protected health information pertains to such relationship, and the disclosure is for:
      (1) The purposes listed in paragraphs V. A. 1. and 2. (above); or,
      (2) The purpose of health care fraud and abuse detection or compliance.

Disclosure to a Business Associate: Stillwater may disclose protected health information in accordance with a valid business associate agreement (attached).

Disclosures Requiring the Opportunity for the Individual to Agree or Disagree: Except when the individual expresses an objection to the use or disclosure of the protected health information, Stillwater may:

1. Disclose to a family member, relative, or close personal friend of the individual, or any other person identified by the individual, the protected health information that is directly relevant to such person’s involvement with the individual’s care.

2. Use or disclose protected health information to notify, or assist in the notification (including locating or identifying) 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.

If the individual is not present or the opportunity to agree or disagree to the use or disclosure cannot practicably be provided because of the individual’s incapacity or an emergency circumstance, Stillwater may exercise professional judgment to determine whether the disclosure is in the best interest of the individual, and if so, disclose the protected health information that is directly relevant to the person’s involvement with the individual’s health care.

Disclosures Not Requiring an Opportunity for the Individual to Agree or Disagree:

Disclosures required by law: Stillwater may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.

Disclosure when abuse, neglect, or domestic violence is believed: Stillwater may disclose protected health information about an individual whom Stillwater reasonably believes is 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:

To the extent the disclosure is required by law; or, if the individual agrees to the disclosure.

Disclosure as provided in articles of existing labor contracts (FOP, etc.)

Stillwater must immediately inform the individual of the disclosure.

Disclosure for Judicial and Administrative Proceedings: Stillwater may disclose protected health information in the course of any judicial or administrative proceeding:

In response to a court or administrative tribunal, provided Stillwater discloses only the protected health information expressly authorized by such order; or,

In response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order or administrative tribunal, provided that Stillwater has received reasonable assurance that the individual has been given notice of the use and disclosure of his/her protected health information or the party requesting such information has made a good faith effort to provide a written notice to the individual.

Disclosure for Law Enforcement Purposes: Stillwater may disclose protected health information to a law enforcement official for law enforcement purposes if:

The disclosure is required by law and the information sought is relevant and material to a legitimate law enforcement inquiry; the request is limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and de-identified information could not reasonably be used.
Disclosures Relating to Decedents: Stillwater may disclose protected health information about an individual who has died to:

1. A law enforcement official, for the purposes of alerting law enforcement of the death of the individual if Stillwater suspects the death may have resulted from criminal conduct.
2. A coroner or medical examiner, for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
3. Funeral directors, consistent with applicable law to carry out their duties with respect to the decedent.

Disclosure for Government Programs Providing Public Benefits: Stillwater may disclose protected health information to another agency administering the government program relating to the health plan (Title XIX, Medicaid) as required or expressly authorized by statute or rule.

Disclosures to Public Health Authorities: Stillwater may disclose protected health information for public health activities to a public health authority that is authorized by law to collect or receive such 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 conduct of public health surveillance, public health investigations, and public health interventions, or at the direction of a public health authority.

Disclosures for Health Oversight Activities: Stillwater may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations, proceedings or actions; inspections; licensure reviews; disciplinary actions; or other activities necessary for appropriate oversight.

Minimum Necessary Use and Disclosure and Exclusions: When using, disclosing, or requesting protected health information, the authorized data user shall make reasonable efforts to limit the use, disclosure, or request of the protected health information to the minimum amount necessary to accomplish the intended purpose.

When disclosing protected health information that is requested from Stillwater on a routine and recurring basis, the authorized data user shall only disclose the amount of protected health information reasonably necessary to achieve the purpose for which the disclosure was requested.

Responding to the Request: Prior to a disclosure being released to the requesting party, the Data Manager must ensure that the disclosure is properly approved by the appropriate department head.

Authorized Data Users: All employees with access to protected health information may have access only on a need-to-know basis.

An authorized data user who finds that he/she has retained or been inadvertently granted access beyond that appropriate to his/her current job responsibilities shall report this incident to his/her supervisor or department head.

It is the responsibility of every authorized data user to maintain confidentiality of protected health information, even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is considered public information.

All authorized data users shall be formally charged with the responsibility and obligation to:

1. Access only that data for which they have a need to know.
   a. Disseminate data to others only on a need to know basis.
   b. Safeguard the confidentiality and integrity of protected health information.
2. External authorized data users shall have this responsibility and obligation specified through a Business Associate agreement with Stillwater.
3. Authorized data users who access data for which they do not have a need to know or is outside that authorized by the Delegated Access Coordinator, may lose their access privileges.
4. Authorized data users who are employees of Stillwater who commit breaches of confidentiality under this procedure are subject to appropriate corrective action in accordance with the Montgomery County’s corrective action policies.
5. Each vendor, contractor or affiliate of Stillwater, with access to protected health information is subject to, and has the responsibilities outlined in this policy, as well as those outlined in their own organization’s policy on confidentiality of information.