III. Privacy Polices and Notices of Privacy Practices

PRIVACY POLICY

Creation Date: 2020-07-22 10:34:31	Effective Date: 7/22/2020	Approval Date: 7/22/2020

Review Date:_____	Revised Date:_____	Approval:_____
Review Date:_____	Revised Date:_____	Approval:_____
Review Date:_____	Revised Date:_____	Approval:_____
Review Date:_____	Revised Date:_____	Approval:_____

Reference: 45 CFR Part 164—Privacy and Security

Policy: Introduction

hereby implements this **Privacy Policy** pursuant to the **Health Insurance Portability and Accountability Act of 1996 ("HIPAA")** and the **Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH")** with respect to its activities when receiving protected health information ("PHI"). The policies described within this document also have expanded policies elsewhere in this manual.

Members of 's workforce may have access to PHI as defined by HIPAA.

- **Workforce member** means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. The term also includes the employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a business associate, is under the direct control of the business associate.
- **Protected Health Information ("PHI")** means information that is created or received from a covered entity and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information of persons living or deceased.

It is 's policy to comply with **HIPAA's** requirements for the privacy of PHI. To that end, all members of 's workforce who have access to PHI must comply with this Privacy Policy. For the purposes of this Policy, 's workforce includes individuals who would be considered part of the workforce under **HIPAA** such as employees, trainees, and other persons whose work performance is under the direct control of whether or not they are paid by The term "employee" includes all of these types of workers.

No third-party rights are intended to be created by this Policy. reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA or HITECH the Policy shall be aspirational and shall not be binding upon . To the extent this Policy is in conflict with the HIPAA Privacy Rule, the HIPAA Privacy Rule shall govern.

Covered Entity Responsibilities

1. Privacy Officer and Contact Person
   The Administrator will be the Privacy Officer for . The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy of PHI in the possession of Heywood Medical Group, including but not limited to this Privacy Policy. The Privacy Officer will also serve as the contact person for individuals who have questions, concerns, or complaints about the privacy of PHI.

   The Privacy Officer is responsible for ensuring that complies with the provisions of the **HIPAA Privacy Rule** regarding third-party business associate vendors or subcontractors, including the requirement that a **HIPAA**-compliant Business Associate Agreement is in place with business associate vendors or subcontractors of The Privacy Officer shall also be responsible for monitoring compliance with the **HIPAA Privacy Rule** and this Privacy Policy.

2. Workforce Training
   It is 's policy to train all members of its workforce who have access to PHI on 's Policy and Procedures. The Privacy Officer is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out 's functions in compliance with **HIPAA** and **HITECH**.

3. Safeguards and Firewall
   will establish appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of **HIPAA's** requirements. has implemented Security Policies that set forth the security measures in place to protect the privacy of PHI.

4. Complaints
   Sarah King-Brown will be the practice's contact person for receiving complaints.

The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request.

5. Sanctions for Violations of Privacy Policy
   Sanctions for using or disclosing PHI in violation of **HIPAA** or this **HIPAA Privacy Policy** will be imposed in accordance with 's discipline policy, up to and including termination.

6. Mitigation of Inadvertent Disclosures of PHI
   shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of **HIPAA** or the policies and procedures set forth in this Policy. As a result, if an employee or business associate vendor or subcontractor becomes aware of an unauthorized use or disclosure of PHI, either by an employee or a business associate vendor or subcontractor, the employee or business associate vendor or subcontractor must immediately contact the Privacy Officer so that appropriate steps to mitigate harm to the patient can be taken.

7. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy
   No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under **HIPAA**.

8. Documentation
   's privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

   The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. will maintain such documentation for at least six years.

9. Workforce Must Comply with 's Policy and Procedures
   All members of 's workforce (described at the beginning of this Policy and referred to herein as "employees") who have access to PHI must comply with this Policy.

10. Breach Notification Requirements
    will comply with the requirements of the **HITECH Act** and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if or one of its business associate vendors or subcontractors discovers a breach of unsecured PHI.

11. Mandatory Disclosures of PHI

PHI must be disclosed in the following situations:

- The disclosure is to the individual who is the subject of the information;
- The disclosure is required by law; or
- The disclosure is made to HHS for purposes of enforcing HIPAA.

12. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without the patient's authorization when specific requirements are satisfied. The requirements include prior approval of the Privacy Officer. Permitted are disclosures—

- about victims of abuse, neglect or domestic violence;
- for treatment purposes;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaveric organ-, eye- or tissue-donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- for functions relate to workers' compensation programs.

13. Disclosure of Sensitive Information

At no time may a patient's sensitive information, including HIV/Aids, drug and/or alcohol, genetic, mental health, sexually transmitted diseases or family planning be disclosed without the patient's consent.

14. Complying with the "Minimum-Necessary" Standard

- ***Minimum Necessary When Disclosing PHI***: , when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. All disclosures not discussed in this Policy must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.
- ***Minimum Necessary When Requesting PHI***: , when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for is requested. All requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.
- To the extent practicable, will limit its use and/or disclosure of PHI to a Limited Data

Set. If it is not practicable for to limit its use and/or disclosure of PHI to a Limited Data Set, will use the *"Minimum Necessary" PHI* to accomplish the purpose of the use or disclosure.

- **Limited Data Set** is PHI that excludes the following identifiers of the individual or of relatives, employers, or household members of the individual:
  - Names;
  - Postal address information, other than town or city, State, and zip code;
  - Telephone numbers;
  - Fax numbers;
  - Electronic mail addresses;
  - Social Security numbers;
  - Medical record numbers;
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/license numbers;
  - Vehicle identifiers and serial numbers, including license plate numbers;
  - Device identifiers and serial numbers;
  - Web Universal Resource Locators (URLs);
  - Internet Protocol (IP) address numbers;
  - Biometric identifiers, including finger and voice prints; and
  - Full face photographic images and any comparable images.

15. Disclosures of PHI to Business Associates

Employees may disclose PHI to 's business associate vendors or subcontractors and allow 's business associate vendors or subcontractors to create or receive PHI on its behalf. However, prior to doing so, must first obtain assurances from the business associate vendor or subcontractor that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a Business Associate Agreement is in place.

Business Associate is an entity that:

- Performs or assists in performing function or activity involving the use and disclosure of PHI; or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

16. Disclosures of De-Identified Information

may freely use and disclose information that has been "de-identified" in accordance with the HIPAA Privacy Rule. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

17. Accounting

An individual has the right to obtain an accounting and an Access Report of certain access and disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, (except for disclosures of electronic disclosures of Electronic Health Records----EHRs—the specifics to be determined by future rulemaking).
Exceptions to the right to an accounting apply in the following cases:

- to carry out treatment, payment, or health care operations (except in the case of EHRs, for which this exception does not apply);
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- to disclosures that occurred prior to the compliance date.

shall respond to an accounting request within 60 days. If is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.
The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings.