HIPAA Privacy and Security		COO Approval Date	
		COO Signature	
		BOARD Approval Date	
Author	Shipman & Goodwin	**CEO Approval Date**	
Owner	Michelle Puhlick	**CEO Signature**	
Owner-Title/Dept	Operations	**Version #**	Board First Read 5.6.2020
Regulatory Compliance		**Regulation #**	

1. Purpose

1.1. Health Information Alliance, Inc. ("HIA") has adopted this HIPAA Privacy and Security Policy (the "Policy") to assist in the effective safeguarding and handling of Protected Health Information ("PHI") and to comply with HIPAA. This Policy contains HIA's procedures for ensuring that the use and disclosure of PHI is consistent with HIA's values, its obligations to customers, and applicable state and federal laws and regulations.

2. Scope

2.1. In the usual course, HIA is not a Business Associate of its customers because it does not perform services for or on behalf of its customers that involve the receipt, use, or disclosure of Protected Health Information. In other words, because HIA does not hold PHI, it does not maintain, access, use, or disclose PHI in the usual course.

2.2. This Policy applies only in the limited circumstance when HIA has access to PHI and is acting as a HIPAA Business Associate.

2.3. Despite Section 2.2 of this Policy, Section 9.4.ii of this Policy requiring HIA to provide notification to a Covered Entity of a Breach that occurred at a subcontractor of HIA may apply, even if HIA does not have access to PHI.

3. Definitions

"*Access*" means the ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

"*Breach*" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the PHI unless HIA demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Breach excludes:

1. Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under the authority of HIA if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

"Business Associate" means any entity that uses or discloses Protected Health Information for or on behalf of a Covered Entity as further defined at 45 C.F.R. 164.103.

"Business Associate Agreement" means the contract entered into between HIA and a Covered Entity to govern HIA's creation, use, disclosure, maintenance and return or destruction of Protected Health Information.

"Covered Entity" means those health plans, health care clearinghouses, and health care providers which meet the definition of "covered entity" at 45 C.F.R. 164.103.

"*Disclosure*" means the release, transfer, provision of, access to or divulging in any manner of information outside the entity holding the information.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as amended.

"HIPAA Compliance Officer" refers to the individual appointed by HIA to have final responsibility for the privacy and security of Protected Health Information.

"Law Enforcement Official" means any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

"Privacy Rule" means 45 CFR Part 160 and Subparts A and E of Part 164.

"Protected Health Information" ("PHI") means information that 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 identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"*Unsecured Protected Health Information*" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons.

"Workforce Members" means employees, volunteers, trainees and other persons whose conduct, in the performance of work for HIA, is under the direct control of HIA.

4. HIPAA Compliance Officer

4.1. HIA Board shall identify and appoint a HIPAA Compliance Officer to have final responsibility for the privacy and security of PHI. The HIPAA Compliance Officer may delegate certain tasks to other Workforce Members or to outside vendors so long as the HIPAA Compliance Officer maintains proper oversight of and remains responsible for the privacy and security of PHI.

5. Workforce Access to PHI

5.1. It is HIA's policy that Workforce Members shall not request access to PHI without first consulting and receiving permission from the HIPAA Compliance Officer. Any request for PHI shall be the minimum necessary to satisfy the purpose of the request.

6. Use and Disclosure of PHI

6.1. General Requirement

i. Workforce Members shall use and disclose PHI only as permitted or required by HIPAA. PHI may be used or disclosed only as necessary to perform job functions.

6.2. Business Associate Agreement

i. HIA shall enter into a Business Associate Agreement prior to receiving PHI when acting as a Business Associate.

6.3. Minimum Necessary

i. Workforce Members may use and disclose only the minimum PHI reasonably necessary for performance of the matter for which HIA is engaged.

6.4. Mandatory Disclosures of PHI

i. HIA may be required to disclose PHI in several situations, including:
    a. The disclosure is made to a governmental agency for purposes of enforcing HIPAA; or
    b. The disclosure is required by another applicable law.
ii. Any such disclosure must be approved by the HIPAA Compliance Officer.

6.5. Permissive Disclosures of PHI

i. When acting as a Business Associate, HIPAA permits HIA to disclose PHI in the following situations without the authorization of an individual:
    a. about victims of abuse, neglect, or domestic violence;
    b. for judicial and administrative proceedings of which HIA is a party;
    c. for law enforcement purposes;
    d. for public health activities;
    e. for health oversight activities;
    f. about decedents;
    g. for certain limited research purposes;

h. to avert a serious threat to health or safety;
i. for specialized government functions; and
j. that relate to workers' compensation programs.

ii. Such disclosures may be made only upon approval of the HIPAA Compliance Officer.

iii. Any disclosure of PHI by HIA shall be made in compliance with the applicable Business Associate Agreement.

6.6. <u>Disclosures of PHI Pursuant to a Written Authorization</u>

i. HIA may disclose PHI in response to a written and signed authorization. All uses and disclosures made pursuant to such authorization must be consistent with the terms and conditions of the authorization. Disclosures of PHI made pursuant to an authorization may be made only upon approval of the HIPAA Compliance Officer.

6.7. <u>Policy on Individual Rights</u>

i. This Policy does not authorize HIA or Workforce Members to receive or maintain any "designated record set" of PHI of any individual or on behalf of any Covered Entity.

ii. For purposes of this Policy, "designated record set" means a group of records maintained by or for a health care provider or health plan that is: (i) the medical records and billing records about individuals maintained by or for a health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals.

iii. To avoid receiving or maintaining a "designated record set," Workforce Members are trained not to receive PHI. In the rare occurrence that HIA requires access to PHI and the HIPAA Compliance Officer has approved such access, Workforce Members are trained to receive only such PHI about an individual as is necessary to accomplish the task on which they are working.

iv. Any request for amendment to, access to, or restrictions on PHI received by HIA from an individual will be forwarded promptly to the Covered Entity.

6.8. <u>Disclosures of PHI to Subcontractors</u>

i. In the event HIA finds it necessary to disclose PHI to a subcontractor, HIA may do so provided HIA and such subcontractor have entered into a written agreement that imposes on such subcontractor substantially the same restrictions, conditions, and requirements that apply to HIA with respect to such PHI.

ii. If any Workforce Member becomes aware of a pattern of activity or practice of a subcontractor that constitutes a material breach or violation of the subcontractor's obligations, the HIPAA Compliance Officer must be notified immediately. The HIPAA Compliance Officer shall take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, upon recommendation by the HIPAA Compliance Officer, HIA shall terminate the contract or arrangement, if feasible. If such termination is not feasible, HIA shall report the problem to the United States Department of Health and Human Services, if required to do so by applicable law.

7. Return or Destruction of PHI

7.1. Upon the termination of a matter in which PHI was received or maintained, the HIPAA Compliance Officer shall determine what obligations HIA has with respect to the PHI in the possession or control of HIA or a subcontractor of HIA. If feasible, HIA shall return or destroy all PHI in accordance with HIPAA and additional obligations that may arise from a Business Associate Agreement entered into by and between HIA and the Covered Entity. If return or destruction is not feasible, HIA shall extend the privacy and security protections set forth in HIA's policies and procedures, and the applicable Business Associate Agreement, to such PHI and shall limit further uses and disclosures of such PHI to those purposes which make return or destruction infeasible.

8. Maintenance and Safeguards

8.1. HIA shall not retain any PHI in electronic form or format. HIA shall establish appropriate safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA.

9. Breach Investigation and Notification

9.1. Discovery of Breach. A Breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a Breach is known to HIA, or, by exercising reasonable diligence would have been known to the organization. HIA shall be deemed to have knowledge of a Breach if such Breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a Workforce member or agent of the organization.

Following the discovery of a potential Breach, HIA shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each Covered Entity whose PHI has been, or is reasonably believed to by the organization to have been accessed, acquired, used or disclosed as a result of the Breach. HIA shall also begin the process of determining what state notifications are required, if any.

9.2. Breach Investigation. The HIPAA Compliance Officer shall act as the investigator of the breach. The investigator shall be responsible for the management of the Breach investigation, completion of a risk assessment and coordinating with others in the organization or the organization's outside advisors as appropriate. The investigator shall be the key facilitator for all Breach notification processes to the appropriate Covered Entities.

9.3. Risk Assessment.

i. An acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a Breach unless HIA demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:
   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   b. The unauthorized person who used the PHI or to the disclosure was made;
   c. Whether the PHI was actually acquired or viewed; and
   d. The extent to which the risk to the PHI has been mitigated.

ii. HIA shall document the risk assessment. Based on the outcome of the risk assessment, the organization will determine the need to move forward with Breach notification.

9.4. Timeliness of Notification.

i. Upon determination that Breach notification is required, the notice shall be made without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of the Breach by HIA. A shorter period may be required by the applicable Business Associate Agreement or state law.

ii. In the event a subcontractor reports a Breach to HIA, HIA shall report such Breach to the Covered Entity as required by law.

9.5. Delay of Notification Authorized for Law Enforcement Purposes. If a Law Enforcement Official states to HIA that a notification, notice or posting would impede a criminal investigation or cause damage to national security, it shall:

i. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice or posting of the time period specified by the official.

ii. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement as described above is submitted during that time.

9.6. Content of Notice. The notice must contain the following information to the extent available:

i. The identification of each individual whose unsecured PHI has been, or is reasonably believed by HIA to have been, accessed, acquired, used, or disclosed during the breach, or instructions for how the Covered Entity may obtain such information;

ii. Any other available information that the Covered Entity is required to include in notification to the individual under 45 CFR § 164.404(c) at the time of the notification or promptly thereafter as information becomes available; and

iii. Any other information required by the applicable Business Associate Agreement.

9.7. Method of Notification. The notification shall be in writing and to the party set forth in the applicable Business Associate Agreement.

10. Documentation

10.1. This Policy shall promptly be revised and made available to Workforce Members in the event changes are necessary to comply with changes in HIPAA or other relevant laws. Unless otherwise stated, any such change shall be effective only with respect to PHI created or received after the effective date of the revised policy.

10.2. HIA will document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to the PHI of Covered Entities. The documentation of any policies and procedures, actions, activities, and designations may

be maintained in either written or electronic form. HIA will maintain such documentation for at least six (6) years.

11. Training

11.1. HIA shall provide Workforce Members with training that instructs them not to request access to the PHI of customers unless authorized by the HIPAA Compliance Officer.

11.2. In the event HIA is acting as a Business Associate, all Workforce Members who access PHI with the permission of the HIPAA Compliance Officer shall receive training on the privacy and security of PHI, and how to identify and promptly report Breaches within the organization, prior to receiving such access to PHI and annually thereafter.

11.3. The HIPAA Compliance Officer shall ensure that all vendors and subcontractors of HIA that receive, create or have access to PHI, if any, are aware of and are required to comply with HIA's privacy and security policies and procedures, including this Policy, whether through contract language or otherwise, provided; however, vendors and subcontractors who are not Workforce Members are not required to attend privacy and security training at HIA.

12. Reporting Violations and Imposing Sanctions

12.1. Any actual or reasonably suspected violation of this Policy shall be reported to the HIPAA Compliance Officer. The HIPAA Compliance Officer will document and investigate such reports in a timely manner. The HIPAA Compliance Officer will review policy and procedure violations and recommend corrective or disciplinary measures, if any, to Human Resources or HIA management, as appropriate.

12.2. Corrective or disciplinary measures for Workforce Members may include, but not be limited to: (i) retraining; (ii) removal of access or other authorizations; (iii) verbal and written warnings; and (iv) termination.

12.3. Corrective action for independent contractors may include, but not be limited to: (i) termination of the contract or relationship with the vendor; and (ii) not renewing such contract or relationship.

13. Complaints

13.1. The HIPAA Compliance Officer is responsible for receiving and responding to complaints about HIA's privacy procedures. HIA shall not retaliate against an individual who submits a complaint.